BLACK BOX NETWORK SERVICES

LPB4008A
LPB4024A

8- and 24-Port Gigabit L2 Managed PoE Switches

Meets 802.3/u/x/z Gigabit Ethernet specifications.

Includes (6) or (20) 10/100 TP ports and (2) or (4) Gigabit dual-media TP/SFP ports.

Manage the switch using:
- RS-232 serial port
- Ethernet port via CLI
- Ethernet port via Web-based SNMP

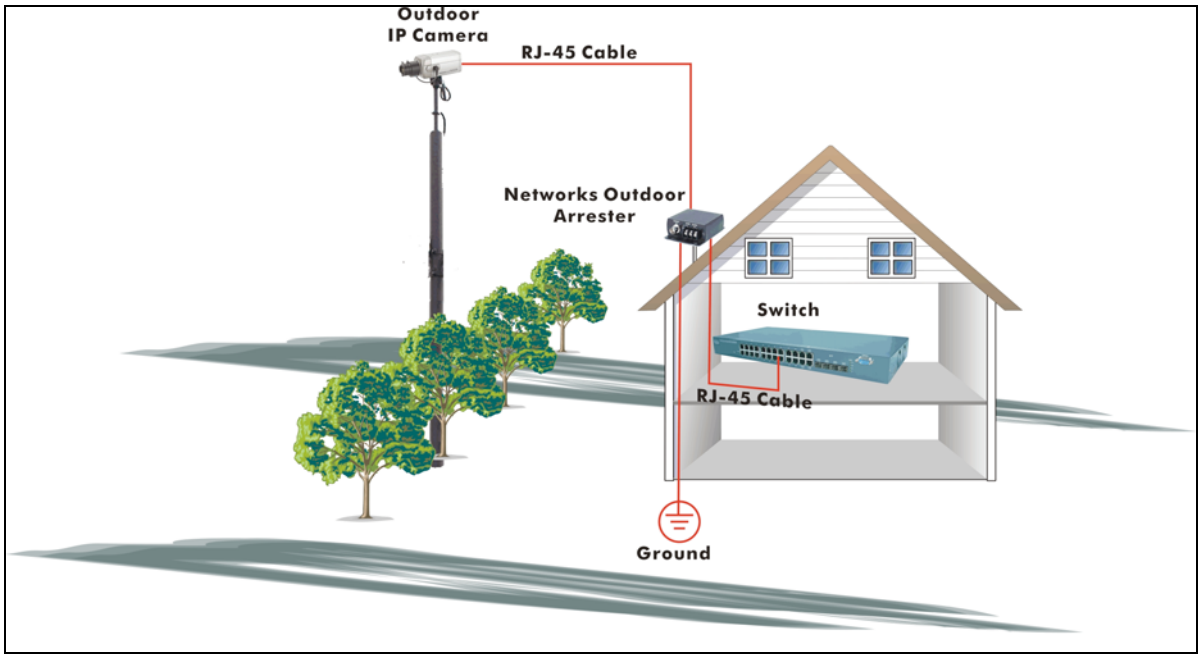
Customer Support Information

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500) •
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746 •
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018 •
Web site: www.blackbox.com • E-mail: info@blackbox.com

CAUTION: Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- If you need to connect an outdoor device with cable, then you need to add an lightning arrestor on the cable between the outdoor device and this device.



Add a lightning arrestor between an outdoor device and this switch.

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Normas Oficiales Mexicanas (NOM) Electrical Safety Statement

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    A: El cable de poder o el contacto ha sido dañado; u
    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    C: El aparato ha sido expuesto a la lluvia; o
    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    E: El aparato ha sido tirado o su cubierta ha sido dañada.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN61000-3 and the Generic European Immunity Standard EN55024.

EMC:

EN55022 (2003)/CISPR-2 (2002): class A
IEC61000-4-2 (2001): 4KV CD, 8KV AD
IEC61000-4-3 (2002): 3V/m
IEC61000-4-4 (2001):1KV (power line), 0.5KV (signal line)

Table of Contents

Table of Contents (Continued)

Table of Contents (Continued)

1. Specifications

1.1 Hardware Specifications

Standard Compliance: IEEE 802.3/802.3ab/802.3z/802.3/802.3x

Network Interface:

Configuration	Mode	Connector	Port (LPB4008A)	Port (LPB4024A)
10/100/1000Mbps Gigabit TP	NWay	TP (RJ-45)	1–6	1–20
1000BASE-SX Gigabit Fiber	1000 FDX	*SFP	7–8 (Option)	21–24 (Option)
1000BASE-LX Gigabit Fiber	1000 FDX	*SFP	7–8 (Option)	21–24 (Option)
1000BASE-LX Single Fiber WDM (BiDi)	1000 FDX	*SFP	7–8 (Option)	21–24 (Option)

*Port 7, 8 on the LPB4008A and Ports 21-24 on the LPB4024A are TP/SFP fiber dual media ports with auto-detect function

*Optional SFP module supports LC or BiDi LC transceiver.

Transmission Mode: 10/100 Mbps supports full or half duplex;
1000 Mbps supports full duplex only

Transmission Speed: 10/100/1000 Mbps for TP;
1000 Mbps for Fiber

Full Forwarding/Filtering Packet Rate: PPS (packets per second)

Forwarding Rate	Speed
1,488,000 PPS	1000 Mbps
148,800 PPS	100 Mbps
14,880 PPS	10 Mbps

MAC Address and Self-learning: 8K MAC address, 4K VLAN table entries.

Buffer Memory: Embedded 1392 KB frame buffer

Flow Control: IEEE 802.3x compliant for full duplex; Backpressure flow control for half duplex

Cable and Maximum Length:

TP	CAT5 UTP cable, up to 328 feet (100 m)
1000BASE-SX	Up to 220/275/500/550 m, which depends on Multi-Mode Fiber type
1000BASE-LX	Single-Mode Fiber, up to 10/30/50 km
1000BASE-LX WDM (BiDi)	Single-Mode Single Fiber, up to 20 km

Connectors: LPB4008A: (6) RJ-45 twisted–pair copper, (2) dual-media TP/SFP (twisted-pair/SFP);
LPB4024A: (20) RJ-45 twisted-pair copper, (4) dual-media TP/SFP (twisted-pair/SFP)

Indicators: LPB4008A: (20) LEDs: Global: (1) Power, (1) CPU, Ports 1–8: (8) Link/Speed, (8) PoE, Ports 7–8: (2) SFP (Link/Speed)
LPB4024A: (54) LEDs: Global: (1) Power, (1) CPU, Ports 1–24: (24) Link/Speed, (24) PoE, Ports 21–24: (4) SFP (Link/Speed)

Power Requirements:
LPB4008A: AC Line: Voltage: 100–240 V; Frequency: 50–60 Hz; Consumption: 65 W
LPB4024A: AC Line: Voltage: 100–240 V; Frequency: 50–60 Hz; Consumption: 185 W

Ambient Temperature: 32 to 104° F (0° to 40°C)

Humidity: 5% to 90%

Size: LPB4008A: 1.7"H x 11"W x 6.5"D (4.4 × 28 × 16.6 cm);
LPB4024A: 1.7"H x 17.4" W x 9.8"D (4.4 x 44.2 x 24.8 cm)

Weight: LPB4008A: 4.2 lb. (1.9 kg);
LPB4024A: 8.4 lb. (3.8 kg)

1.2 Management Software Specifications

System Configuration: Supports auto-negotiation on 10/100/1000 BASE-TX ports; Web browser or console interface can set transmission speed (10-/100-/1000-Mbps) and operation mode (full-/half-duplex) on each port; enable/disable any port; set VLAN group, set trunk connection.

Management Agent: SNMP support; MIB II, Bridge MIB, RMON MIB, Spanning Tree Algorithm, IEEE 802.1D, VLAN Function, Port-Based/802.1Q-Tagged, allows up to 256 active VLANs in one switch, Trunk Function; Allows Ports trunk connections; allows IGMP, IP Multicast Filtering by passively snooping on the IGMP Query

Bandwidth Control: Supports by-port Egress/Ingress rate control

Quality of Service (QoS): Referred as Class of Service (CoS) by the IEEE 802.1P standard, Classification of packet priority can be based on either a VLAN tag on packet or a user-defined per port QoS.
Two queues per port
IP TOS Classification
TCP/UDP Port Classification
IP DiffServe Classification

Port Security: Limited number of MAC addresses learned per port static MAC addresses stay in the filtering table

Internetworking Protocol:
Bridging: 802.1D Spanning Tree;
IP Multicast: IGMP Snooping;
IP Multicast Packet Filtering;
Maximum of 256 active VLANs and IP multicast sessions

Network Management: One RS-232 port as a local control console;
Telnet remote control console;
SNMP agent: MIB-2 (RFC 1213);
Bridge MIB (RFC 1493);
RMON MIB (RFC 1757) statistics;
Ethernet-like MIB (RFC 1643);
Web browser support based on HTTP Server and CGI parser TFTP software-upgrade capability

2. Overview

2.1 Introduction

The 8-Port and 24-Port Gigabit L2 Managed Power-over-Ethernet Switches (LPB4008Aand LPB4024A) are standard switches that meet all IEEE 802.3/u/x/z Gigabit Ethernet specifications. The LPB4008A switch includes six 10-/100-/1000-Mbps TP ports and two Gigabit TP/SFP ports. The LBP4024A switch includes twenty 10-/100-/1000-Mbps TP ports and four Gigabit TP/SFP ports. You can manage the switches through the RS-232 serial port via a direct connection, or through the Ethernet port using a CLI or Web-based management unit that's associated with an SNMP agent. Using the SNMP agent, the network administrator can log on to the switch to monitor, configure, and control each port's activity. Via its intelligent software, the switch also features ACL, IP-MAC Binding, DHCP Snooping, QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, and IGMP Snooping. Use it for both metro-LAN and office applications.

These PSE switches also comply with the IEEE 802.3af standard. An advanced auto-sensing algorithm enables power devices (PD) discovery, classification, current limit, and other necessary functions. It also protects against short circuits and auto-detects power-out to the PD.

This switch's Port 7 and Port 8 (LPB4008A) or Ports 21–24 (LPB4024A) include two types of media—TP and SFP Fiber (LC, BiDi LC…). These ports support 10-/100-/1000-Mbps TP or 1000-Mbps SFP Fiber with auto-detect function. Use a 1000-Mbps SFP Fiber transceiver to expand a high-speed connection.

• 1000-Mbps LC, Multimode, 50 m, SFP Fiber transceiver (LGB200C-MLC)

• 1000-Mbps LC, Single-Mode, 10 km, SFP Fiber transceiver (LGB200C-SLC10)

• 1000-Mbps LC, Single-Mode, 30 km, SFP Fiber transceiver (LGB200C-SLC30)

• 1000-Mbps BiDi LC, Single-Mode, 20 km, 1550 nm SFP Fiber WDM transceiver (LGB204C)

• 1000-Mbps BiDi LC, Single-Mode, 20 km, 1310 nm SFP Fiber WDM transceiver (LGB205C)

The 10-/100-/1000-Mbps TP standard Ethernet ports meet all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications. The 1000Mbps SFP Fiber transceiver has a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000BASE-SX/LX standards.

The 1000-Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports a bi-directional full-duplex signal over a single fiber simultaneously.

"Active PHY Power Management" and "Perfect Reach Power Management" help reduce power consumption.

The switch also supports the IEEE Standard 802.1ab Link Layer Discovery Protocol to provide a debugging tool and enhance the networking management availability. It can auto-discover a device and its topology.

2.2 Features

• QoS: Supports Quality of Service using the IEEE 802.1P standard. There are two priority queue and packet transmission schedules.

• Spanning Tree: Supports IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

• VLAN: Supports Port-based VLAN and IEEE802.1Q Tag VLAN;
Also supports 256 active VLANs and VLAN ID 1–4094.

• Port Trunking: Supports static port trunking and port trunking with IEEE 802.3ad LACP.

• Bandwidth Control: Supports ingress and egress per port bandwidth control.

• Port Security: Allows or denies forwarding and port security according to MAC address.

• SNMP/RMON
- SNMP agent and RMON MIB. The switch's SNMP agent is client software that operates using SNMP protocol to receive commands from the SNMP manager (server site) and echo the corresponding data (the MIB object). The SNMP agent actively issues TRAP information when it occurs.
- Remote Network Monitoring (RMON) is a branch of the SNMP MIB
- The switch supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, Ethernet-like MIB (RFC 1643), and Ethernet MIB (RFC 1643).

• IGMP Snooping: Supports IGMP version 2 (RFC 2236): Use IGMP snooping to establish multicast groups that will forward multicast packets to member ports, and won't waste bandwidth while IP multicast packets are running over the network.

• IGMP Proxy: multicast processing. The switch supports IGMP version 1 and IGMP version 2, to efficiently use network bandwidth, and provide fast response time for channel changing. IGMP version 1 (IGMPv1) is described in RFC1112, and IGMP version 2 (IGMPv2) is described in RFC 2236. Hosts interact with the system through the exchange of IGMP messages. Similarly, when you configure IGMP proxy, the system exhanges IGMP messages with the router upstream. However, when acting as the proxy, the system performs the host portion of the IGMP task on the upstream interface as follows:

- When queried, it sends group membership reports to the group.

- When one of its hosts joins a multicast address group to which none of its other hosts belong, it sends unsolicited group membership reports to that group.
- When the last host in a particular multicast group leaves the group, it sends an unsolicited leave group membership report to the all-routers group (244.0.0.2).

- PoE: 8 PoE ports allow power to be supplied to end devices, such as Wireless Access Points or VoIP Phones, directly through the existing LAN cables, eliminating costs for additional AC wiring and reducing installation costs.

- Power Saving
- "Active PHY Power Management" detects when the client is idle. "Perfect Reach Power Management" detects the cable length automatically, then provides the different (lower) power level needed. This saves switch power and reduces power consumption.

- LLDP (IEEE 802.1AB Link Layer Discovery Protocol)
- The switch supports LLDP automated device discovery protocol for easy mapping of network management applications.

2.3 What's Included

Your package should include the following items. If anything is missing or damaged, please contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

- (1) 8-Port (LPB4008A) or 24-Port (LPB4024A) Gigabit L2 Managed Power-Over-Ethernet Switch
- (1) set of 19" rackmounting brackets (LPB4024A only)
- (1) AC Power Cord
- (1) RS-232 Cable
- This user manual on CD-ROM

2.4 Front and Back Panel

There are six or twenty TP Gigabit Ethernet ports plus two or four SFP fiber ports for optional removable modules on the front panel of the switch. The LED display area on the left side of the panel contains a Power LED that indicates the switch's power status. 16 port status LEDs show port status on the LPB4008A, and 48 port status LEDs show port status on the LPB4024A. One RS-232 DB9 interface can be used for configuration or management.

Front Panel

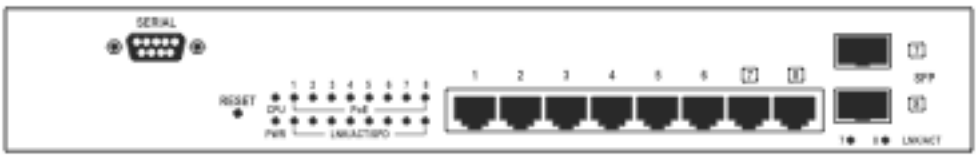


Figure 2-1. Front panel: LPB4008A.

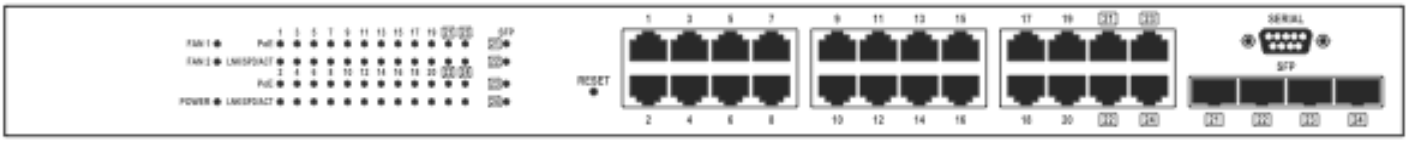


Figure 2-2. Front panel: LPB4024A.

Rear Panel

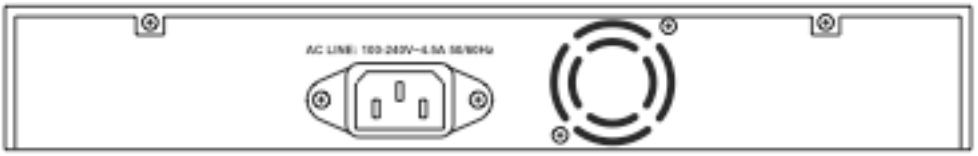


Figure 2-3. Rear panel: LPB4008A.

Figure 2-4. Rear panel: LPB4024A.

2.5 LED Indicators

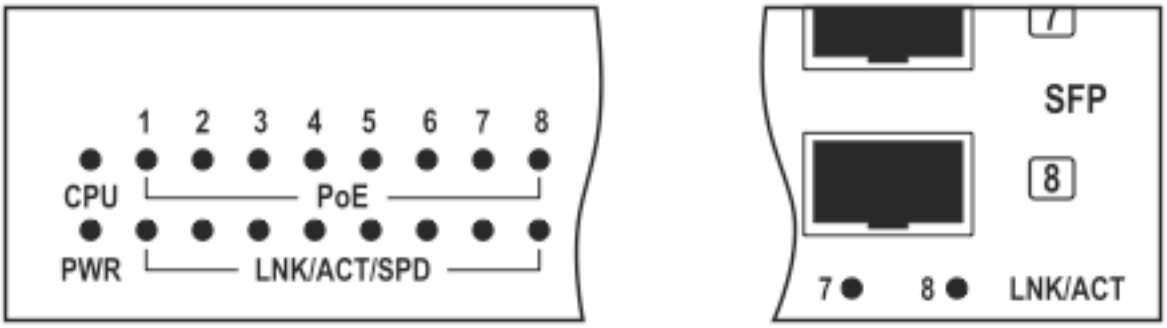


Figure 2-5. LED indicators on the LPB4008A's front panel.

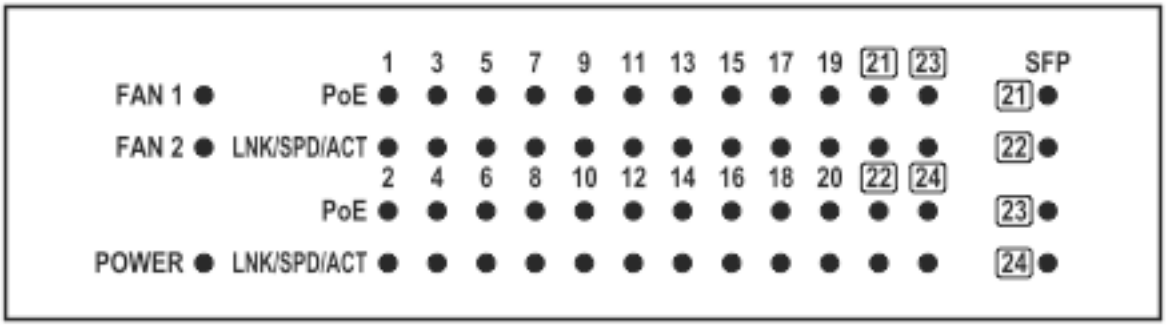


Figure 2-6. LED indicators on the LPB4024A's front panel.

Table 2-1. LED Indicators

Number	LED	Color	Function
System LED			
1	POWER	Green	Lights when power is on.
2	CPU	Green	Lights when CPU is on. Blinks when system is in self-test mode.
6	RESET		Reset button restores the management system.
10/100/1000 Ethernet TP Port 1 to 6 LED (LPB4008A) or Port 1 to 20 LED (LPB4024A)			
3	LINK/ACT/SPEED	Green	Lights when connection with remote device is good. Blinks when traffic is present. Off when cable connection is not good.
		Green/ Amber	Lights green when 1000-Mbps speed is active. Lights amber when 100-Mbps speed is active Off when 10Mbps speed is active
4	PoE	Green	Lights when PoE Power is active
1000SX/LX Gigabit Fiber Port 7, 8 LED (LPB4008A) or Port 21–24 (LPB4024A)			
5	SFP(LINK/ACT)	Green	Lights when connection to the remote device is good. Blinks when any traffic is present. Off when module connection is not good.

2.6 Optional SFP Fiber Transceiver Modules

Ports 7 and 8 on the LPB4008A include two types of media: twisted-pair (TP) and optional small form factor pluggable (SFP) fiber (LC, BiDi LC, etc.) modules. The twisted-pair ports are the switch's two rightmost RJ-45 twisted-pair connectors. For the fiber option, 1000-Mbps fiber transceiver modules slide into the switch's two fiber module slots (located to the right of the twisted-pair connectors on the switch's front panel). The fiber transceiver modules are used for high-speed connection expansion. The two fiber ports can automatically detect 10/100/1000-Mbps TP or 1000-Mbps SFP fiber.

Five 1000-Mbps transceiver modules are available. These modules are described below and shown in Figures 2-7 and 2-8.

- Small Form Factor Pluggable (SFP) Optical Transceiver, Multimode, 850-nm, 550 m (LGB200C-MLC)
- Small Form Factor Pluggable (SFP) Optical Transceiver, Single-Mode, 1310-nm, 10 km (LGB200C-SLC10)
- Small Form Factor Pluggable (SFP) Optical Transceiver, Single-Mode, 1550-nm, 30 km (LGB200C-SLC30)
- Small Form Factor Pluggable (SFP) Optical Transceiver, Single-Strand, Single-Mode Fiber WDM1550TX/1310 RX, 20 km (LGB204C)
- Small Form Factor Pluggable (SFP) Optical Transceiver, Single-Strand, Single-Mode Fiber WDM1310TX/1550 RX, 20 km (LGB205C)

Figure 2-7. LGB200C-MLC, LGB200C-SLC10, or LGB200C-SLC30 module.

Figure 2-8. LGB204C or LGB205C module.

NOTE: The LGB204C and LGB205C fiber transceivers must be used together.

3. Installation

3.1 Hardware and Cable Installation

CAUTION: Wear a grounding device to avoid damage from electrostatic discharge. Be sure that the power switch is OFF before you connect the power cord to the power source.

3.1.1 Installing an Optional SFP Transceiver Module

NOTE: If you do not plan to install SFP fiber transceivers in the switch's ports 7–8, skip this section.

Slide the fiber transceiver module into one of the two open module slots in the switch as shown in Figure 3-1.

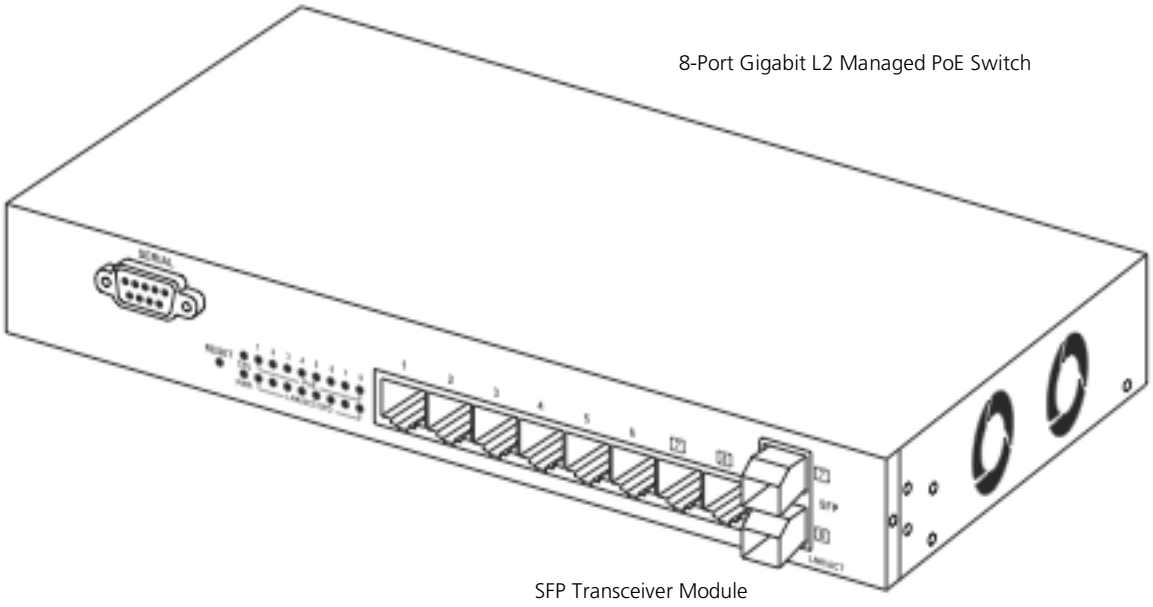


Figure 3-1. Installing the optional SFP fiber transceiver module.

Connecting the SFP Module to the Chassis

The optional SFP modules are hot-swappable, so you can plug or unplug them before or after powering on the switch.

1. Verify that the SFP module is the right model and conforms to the chassis.
2. Slide the module into the slot. Make sure that the module is properly seated against the slot socket/connector.
3. Connect the fiber optic network cable to the connector(s) on the module.

If you want to install a second module in the LPB4008A switch or second, third, and fourth module in the LPB4024A switch, repeat steps 1–3.

3.1.2 TP Port and Cable Installation

1. The switch's TP port supports MDI/MDI-X auto-crossover, so you can use both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and cross-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2).
2. Use CAT5 RJ-45 TP cable to connect to one of the switch's TP port and a network-aware device such as a workstation or a server.
3. Repeat the above steps, as needed, for each RJ-45 port you want to connect to a Gigabit 10/100/1000 TP device.
4. The switch is now ready to operate.

3.1.3 Power On

The switch supports a 100-240-VAC, 50-60-Hz power supply. The power supply will automatically convert the local AC power source to DC power. You can connect a device or module to the switch when it's powered on or off. When the power is on, all port LED indicators will light up immediately and then go off. (The power LED remains on.) To reset the switch, simply power it off, then on again.

3.1.4 Firmware Loading

After resetting, the bootloader will load the firmware into the memory. (It will take about 30 seconds.) Then all LEDs on the switch will flash once and automatically perform a self-test. The switch is now in the ready state.

3.2 Installing the Switch in a 19-Inch Wiring Rack or Cabinet

CAUTION: Allow enough space for the cooling fan at both sides of the switch to provide ventilation. Wear a grounding device for electrostatic discharge.

1. Using two screws (included), attach the rackmount ears to the switch's left and right sides. See Figure 3-2.

2. Line up the mounting holes on the switch assembly (the switch with rackmount ears installed) with the mounting holes on a 19" wiring closet rack. Install two screws (included) to hold the switch in place in the rack.

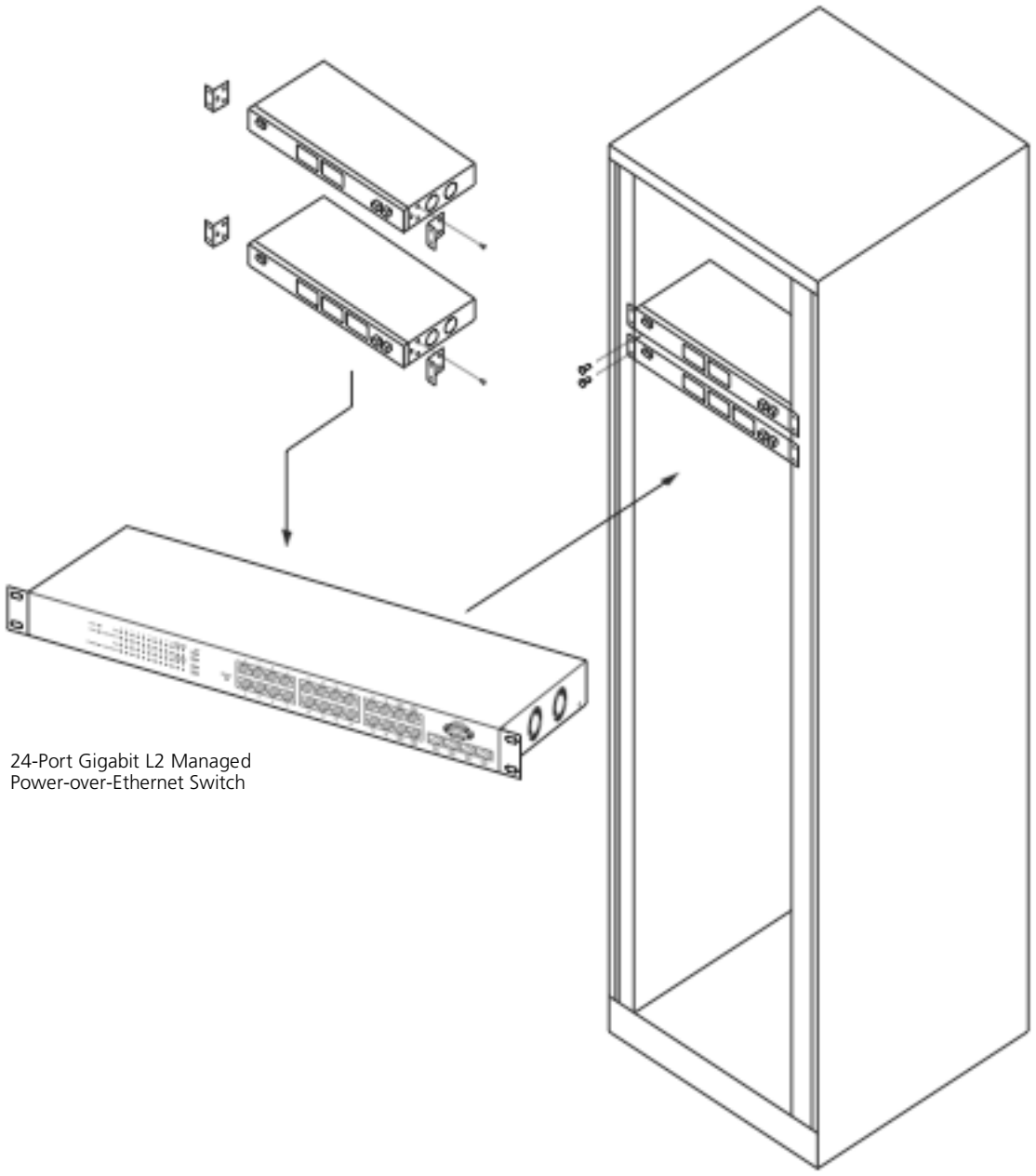


Figure 3-2. Installing the switch chassis in a 19" rack.

3.3 Cabling Requirements

For successful installation and optimum network performance, use CAT5 or CAT5e cable.

3.3.1 Twisted-Pair Ports

For a Fast Ethernet TP network connection, use CAT5 or CAT5e cable that's up to 100 meters long.

For a Gigabit Ethernet TP network connection, use CAT5 or CAT5e cable that's up to 100 meters long. We recommend using CAT5e cable for Gigabit connections.

3.3.2 Fiber Transceiver Ports

There are two categories of fiber: multimode (MM) and single-mode (SM). Multimode fiber is categorized into several classes by the distance it supports. The classes are SX, LX, LHX, XD, and ZX. The fiber modules that work with the switch have LC and BIDI LC connectors.

• 62.5/125-µm multimode Gigabit fiber with multimode LC SFP module (LGB200C-MLC).

• 9/125-µm single-mode Gigabit fiber with single-mode LC SFP module (LGB200C-SLC10 orLGB200C-SLC30).

• 9/125-µm single-strand single-mode Gigabit fiber with BiDi LC1310-nm SFP module (LGB204C).

• 9/125-µm single-strand single-mode Gigabit fiber with BiDi LC1550-nm SFP module (LGB205C).

The following table lists the types of fiber that the switch supports and those not listed here are available upon request.

<table>
<tr><td rowspan="4">IEEE 802.3z
Gigabit Ethernet
1000BASE-SX 850nm</td><td colspan="4">Multimode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multi-mode 62.5/125 m</td><td colspan="2">Multimode 50/125 m</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160MHz-Km</td><td>220m</td><td>400MHz-Km</td><td>500m</td></tr>
<tr><td>1000BASE-LX/LHX/XD/ZX</td><td>200MHz-Km</td><td>275m</td><td>500MHz-Km</td><td>550m</td></tr>
<tr><td rowspan="3">1000BASE-LX/LHX/XD/ZX</td><td colspan="4">Single-mode fiber 9/125 m</td></tr>
<tr><td colspan="4">Single-mode transceiver 1310nm 10Km</td></tr>
<tr><td colspan="4">Single-mode transceiver 1550nm 30, 50Km</td></tr>
<tr><td rowspan="4">1000BASE-LX
Single Fiber
(BIDI LC)</td><td colspan="2" rowspan="2">Single-mode
*20Km</td><td colspan="2">TX (Transmit) 1310nm</td></tr>
<tr><td colspan="2">RX (Receive) 1550nm</td></tr>
<tr><td colspan="2" rowspan="2">Single-mode
*20Km</td><td colspan="2">TX (Transmit) 1550nm</td></tr>
<tr><td colspan="2">RX (Receive) 1310nm</td></tr>
</table>

3.3.3 Switch Cascading in Topology

Theoretically, the switch partitions the collision domain for each port in switch cascading so that you may uplink an unlimited number of switches. In practice, the network extension (cascading levels and overall diameter) must comply with the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, which limit the timing requirement from physical signals defined by the Media Access Control (MAC) and PHY802.3 series specification, and timing from some OSI layer 2 protocols such as 802.1d, 802.1q, and LACP.

The fiber, TP cables, and devices' bit-time (round-trip) delay are described in Table 3-1.

Table 3-1. Cable's bit-time (round-trip) delay.

<table>
<tr><th colspan="2">1000BASE-X TP, Fiber</th><th colspan="4">100BASE-TX TP</th><th colspan="2">100BASE-FX Fiber</th></tr>
<tr><td colspan="2">Round trip Delay: 4096</td><td colspan="6">Round trip Delay: 512</td></tr>
<tr><td>Cat. 5 TP Wire:</td><td>11.12/m</td><td colspan="2">Cat. 5 TP Wire:</td><td>1.12/m</td><td>Fiber Cable:</td><td colspan="2">1.0/m</td></tr>
<tr><td>Fiber Cable:</td><td>10.10/m</td><td colspan="6">TP to fiber Converter: 56</td></tr>
<tr><td colspan="2">Bit Time unit: 1ns (1sec./1000 Mega bit)</td><td colspan="6">Bit Time unit: 0.01 s (1sec./100 Mega bit)</td></tr>
</table>

The sum of all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not apply. You may use the TP-Fiber module to extend the TP node distance over fiber optic cable and provide the long haul connection.

3.3.4 Typical Network Topology in Deployment

A hierarchical network with minimum levels of switches may reduce the timing delay between server and client station. This approach will minimize the number of switches in any one path, will lower the possibility of network loop, and will improve network efficiency. If more than two switches are connected in the same network, select one switch as a Level 1 switch and connect all other switches to it at Level 2. We recommend connecting the Server/Host to the Level 1 switch, if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Figure 3-3).

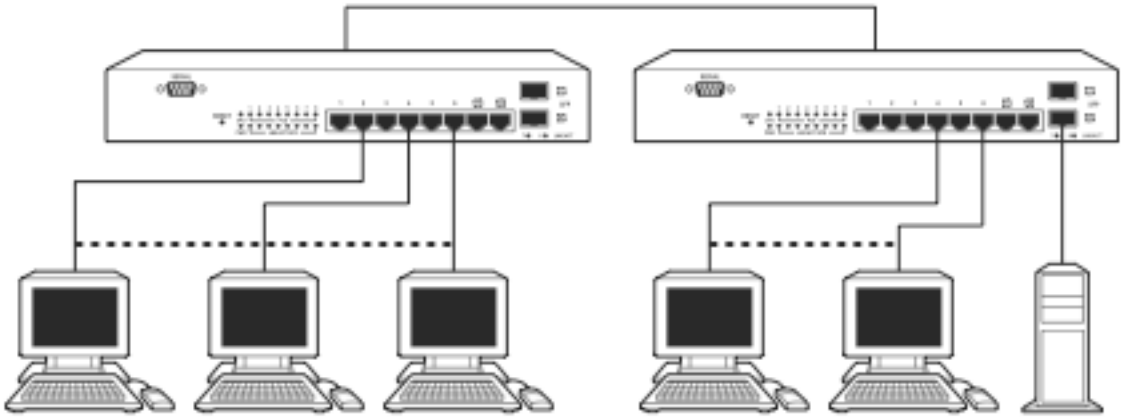


Figure 3-3. No VLAN Configuration Diagram.

If VLAN is enabled and configured, each node in the network that can communicate with each other directly is bounded in the same VLAN area.
Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. The following diagram shows how port-based VLANs and tag-based VLANs work.

Case2a: Port-based VLAN (See Figure 3-4).

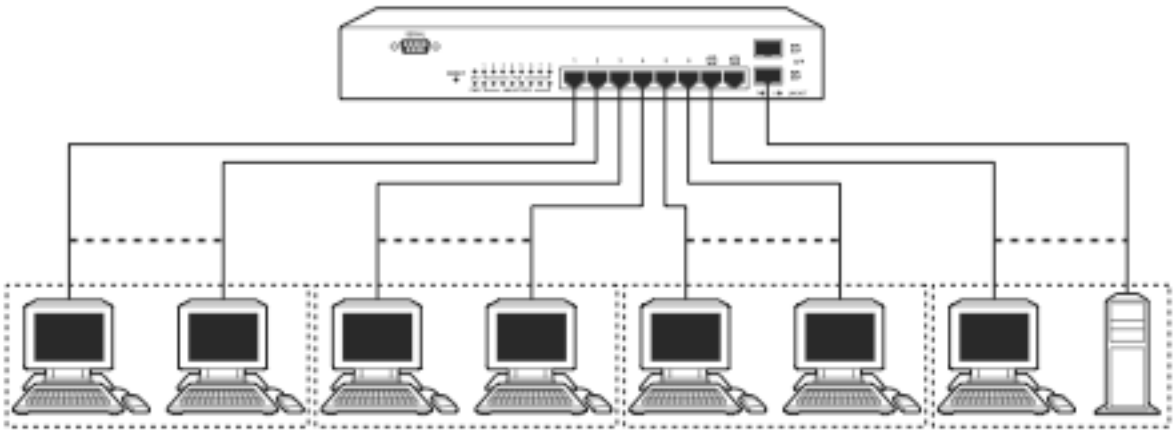


Figure 3-4 One switch connected to four VLANs in a port-based VLAN

1. The same VLAN members can not be connected to different switches.
2. All VLAN members can not access each others' VLAN members.
3. The switch manager has to assign different names for each VLAN group at one switch.

Case 2b: Port-based VLAN (See Figure 3-5).

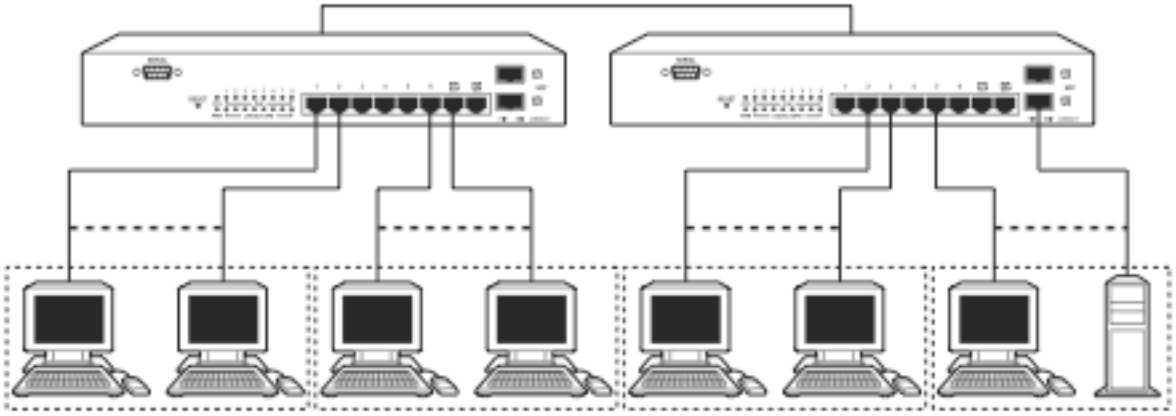


Figure 3-5. Port-based VLAN diagram.

1. VLAN1 members can not access VLAN2, VLAN3, and VLAN4 members.
2. VLAN2 members can not access VLAN1 and VLAN3 members, but they can access VLAN4 members.
3. VLAN3 members can not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members cam not access VLAN1 and VLAN3 members, but they can access VLAN2 members

Case3: The same VLAN members can be at different switches with the same VID (See Figure 3-6).

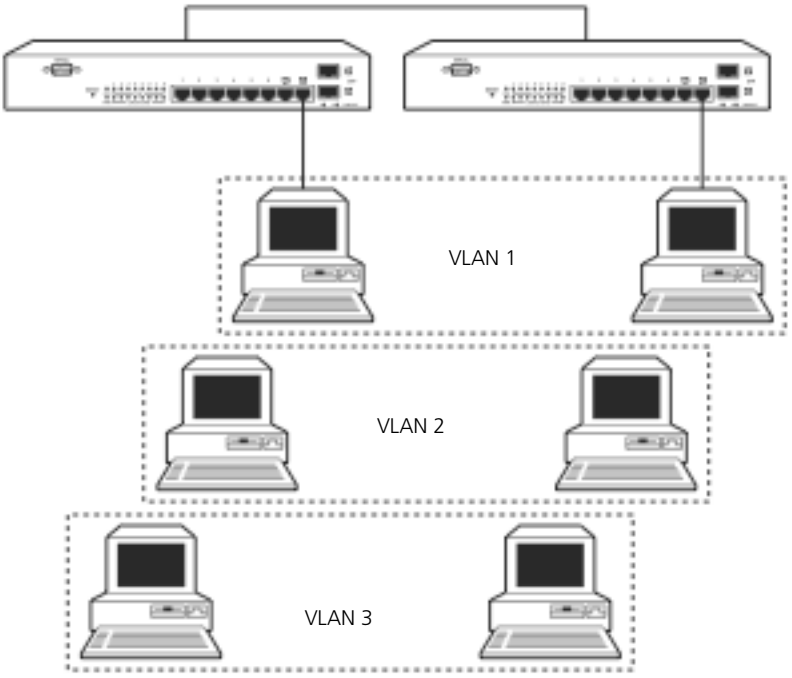
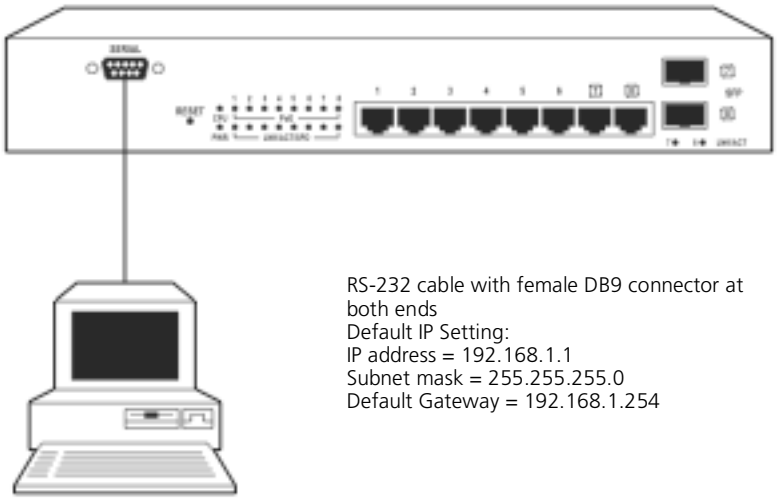


Figure 3-6. Attribute-based VLAN diagram.

3.4 Configuring the Management Agent

3.4.1 Connect To Console Port

To configure the switch via the RS-232 console port, connect the switch's serial port directly to a DTE device, for example, a PC, through an RS-232 cable with a DB9 connector. Next, run a terminal emulator with the default setting of the switch's serial port. The RS-232 interface in the switch only supports 115200 bps baud rate with 8 data bits, 1 stop bit, no parity check, and no flow control.



RS-232 cable with female DB9 connector at both ends
Default IP Setting:
IP address = 192.168.1.1
Subnet mask = 255.255.255.0
Default Gateway = 192.168.1.254

Figure 3-7. Connect the switch's RS-232 DB9 port to a serial console.

To configure the switch, follow these steps:

1. Use an RS-232 DB9 cable with a female DB9 connector that has pins 2, 3, and 7.

2. Attach the DB9 female cable connector to the male serial RS-232 DB9 connector on the switch.

3. Attach the other end of the serial RS-232 DB9 cable to the PC's serial port, running a terminal emulator supporting a VT100/ANSI terminal with the switch's serial port default settings. For example, Windows98/2000/XP HyperTerminal utility.

NOTE: The switch's serial port default settings are:

Baud rate: 115200
Stop bits: 1
Data bits: 8
Parity: N
Flow control: none

4. After you connect the cables, press the **<Enter>** key. The login prompt will be shown on the screen. The default username and password are:

Username = admin
Password = admin

3.4.2 Set IP Address, Subnet Mask, and Default Gateway IP Address

Refer to Figure 3-7, CLI Management, for details about default IP address settings. First, either configure your PC IP address or change the switch's IP address, then change the default IP address for the gateway and subnet mask.

For example, your network address is 10.1.1.0, and subnet mask is 255.255.255.0. You can change the switch's default IP address 192.168.1.1 to 10.1.1.1 and set the subnet mask to be 255.255.255.0. Then, choose your default gateway, for example, 10.1.1.254.

Default Value	LPB4008A	Your Network Setting
IP Address	192.168.1.1	10.1.1.1
Subnet	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.254	10.1.1.254

After you complete the settings for the switch, it will reboot and the configuration will take effect. You can then manage the switch via the network (either from a web browser or a Network Management System [NMS]).

NOTE: There are no default DNS settings. DNS addresses are assigned by the network administrator.

Managed Switch LPB4008A

Login: admin
Password: *****

LPB4008A

Figure 3-8. The Login Screen for CLI.

3.4.3 Managing LPB4008A through Ethernet Port

There are three ways to configure and monitor the switch through the switch's Ethernet port. They are CLI, Web browser, and SNMP manager. The user interface for the last one is NMS dependent and is not explained in this manual. CLI and Web browser management interface are described on the next page.

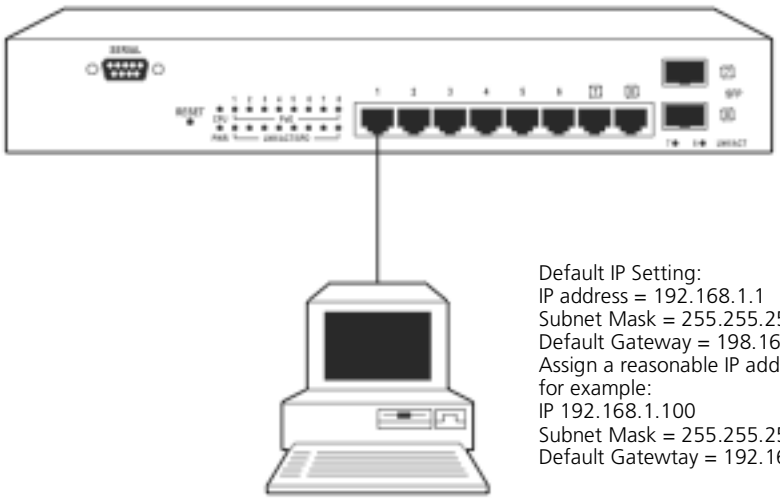


Figure 3-9. Connecting the Ethernet LAN PC to the switch for network management through an Ethernet port.

Before you communicate with the switch, finish the configuration of the IP address or make sure you know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured switch and a PC with a qualified UTP CAT5 cable with RJ-45 connector.

NOTE: If the PC connects directly to the switch, you have to setup the same subnet mask between them. The subnet mask may be different for the PC at the remote site.

2. Run CLI or web browser and follow the menu. Refer to Chapters 4 and 5.

Figure 3-10. Login Screen for Web.

3.5 IP Address Assignment

For IP address configuration, there are three parameters you need to fill in. They are IP address, Subnet Mask, Default Gateway and DNS.

3.5.1 IP address

The address of the network device is used for internetworking communication. Its address structure is shown in Figure 3-11. It is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32-bit address. Each IP address consists of two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network that the address of host refers to. The host identifier must be unique in the same LAN. The IP address we used is version 4, known as IPv4.

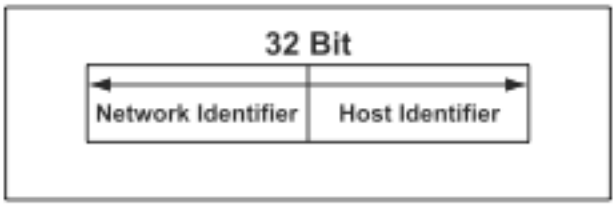


Figure 3-11. IP address structure.

Classifying addresses divides the IP address into three classes: class A, class B, and class C. The rest of the IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/Xl for example, 192.168.1.0/24. Each class has its address range described below.

Class A:
Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.

Class B:
The IP address ranges between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed by a 16-bit host address. There are 16,384 (214)/16 networks that can be defined with a maximum of 65534 (216-2) hosts per network.

Class C:
The IP address ranges between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed by an 8-bit host address. A total of 2,097,152 (221)/24 networks can be defined with a maximum of 254(28-2) hosts per network.

Class D and E:
Class D is a class with the first 4 MSBs (Most Significant Bits) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with the first 4 MSBs set to 1-1-1-1 and is used for IP broadcast.
According to IANA (Internet Assigned Numbers Authority), three specific IP address blocks (called a private IP address) are reserved for extending an internal network. They are listed below.

Class A 10.0.0.0---10.255.255.255

Class B 172.16.0.0---172.31.255.255

Class C 192.168.0.0---192.168.255.255

Refer to RFC 1597 and RFC 1466 for more information. These documents are available at www.faqs.org.

3.5.2 Subnet Mask

Subnet mask is the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address into the network prefix and the host address. It's designed to use an IP address more efficiently to manage an IP network.

For a class B network, 128.1.2.3, the default subnet mask may be 255.255.0.0. The first two bytes are all 1s. This means more than 60 thousands of nodes in flat IP addresses will be on the same network. It's too large to manage practically. If we divide it into smaller networks by extending the network prefix from 16 bits to, say 24 bits, the network uses its third byte to subnet this class B network. The subnet mask is 255.255.255.0; each bit of the first three bytes is 1. The first two bytes are used to identify the class B network, the third byte is used to identify the subnet within this class B network, and the last byte is the host number.

Not all IP addresses are available in the subnetted network. Two special addresses are reserved. They are the addresses with all zeros and all ones for the host number.

As shown in the table below, the subnet mask with a 25-bit long, 255.255.255.128 address contains 126 members in the subnetted network. The network prefix length equals the bit number with 1s in that subnet mask. Use this table to count the number of IP addresses matched.

Table 3-2. Subnet mask values.

Prefix Length	Number of IPs Matched	Number of Addressable IPs
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. A maximum of 254 effective nodes exist in this sub-netted network. It is considered a physical network in an autonomous network, so it owns a network IP address, for example, 168.1.2.0.

With the subnet mask, a bigger network can be divided into smaller networks. If you want to have more than two independent networks in a worknet, you can partition the network. In this case, subnet mask must be applied.

For different network applications, the subnet mask might be 255.255.255.240. This small network accommodates a maximum of 15 nodes.

3.5.3 Default Gateway

For the routed packet, if the destination is not in the routing table, all the traffic is sent to the device with the designated IP address, known as the default router. The gateway setting is used for Trap Events Host only in the switch.

Before assigning an IP address to the switch, check to see what IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

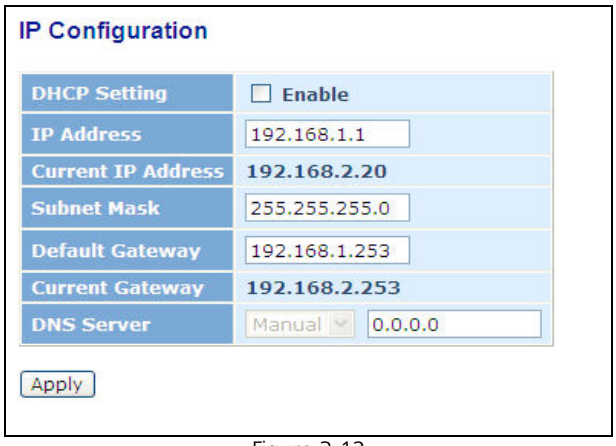


Figure 3-12

First, type in the IP Address: as shown in Fig. 2-12, enter default IP address "192.168.1.1," for instance. An IP address such as 192.168.1.x must be set on your PC.

Second, type in the Subnet Mask: as shown in Fig. 2-12, enter "255.255.255.0." Any subnet mask such as 255.255.255.x is allowed in this case.

3.5.4 DNS

The Domain Name Server translates human-readable machine names to IP addresses. Every machine on the Internet has a unique IP address. A server has a static IP address. To connect to a server, the client needs to know the IP of the server. However, users generally use the name to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to resolve the IP address of the named server.

3.6 Typical Application

LPB4008A implements 8 Gigabit Ethernet TP ports with Auto MDI-X and two slots for the removable module supporting fiber connections, including LC and BiDi-LC SFP modules. LPB4024A has 20 Gigaibit Ethernet TP ports with Auto-MDIX and four slots for fiber modules. The switch is suitable for the following applications.

- Edge Site/Remote site application is used in PoE environment (See Figure 3-13).
- Peer-to-peer application is used in two remote offices (See Figure 3-14).
- Office network (See Figure 3-15).

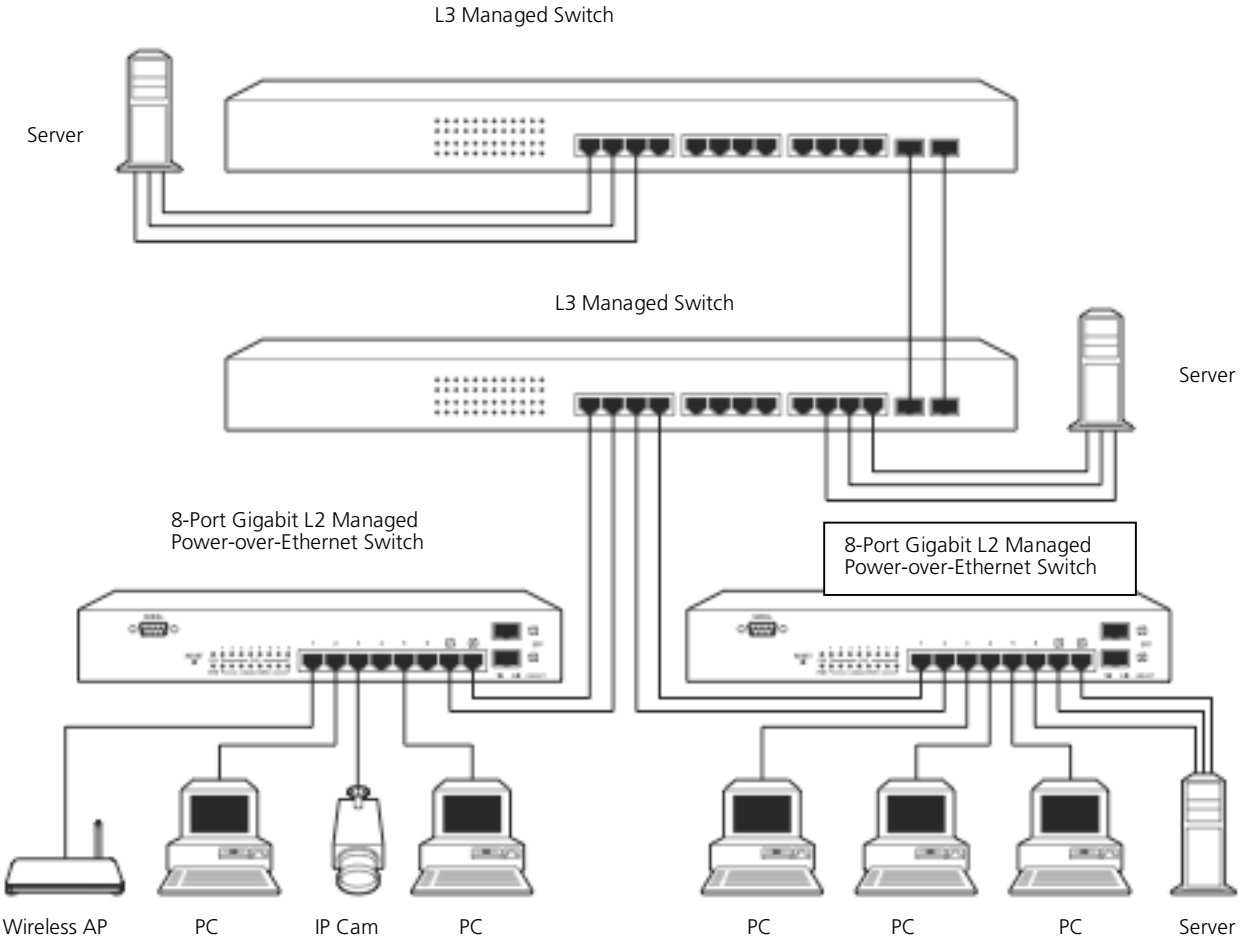


Figure 3-13. Network Connection between Remote Site and Central Site.

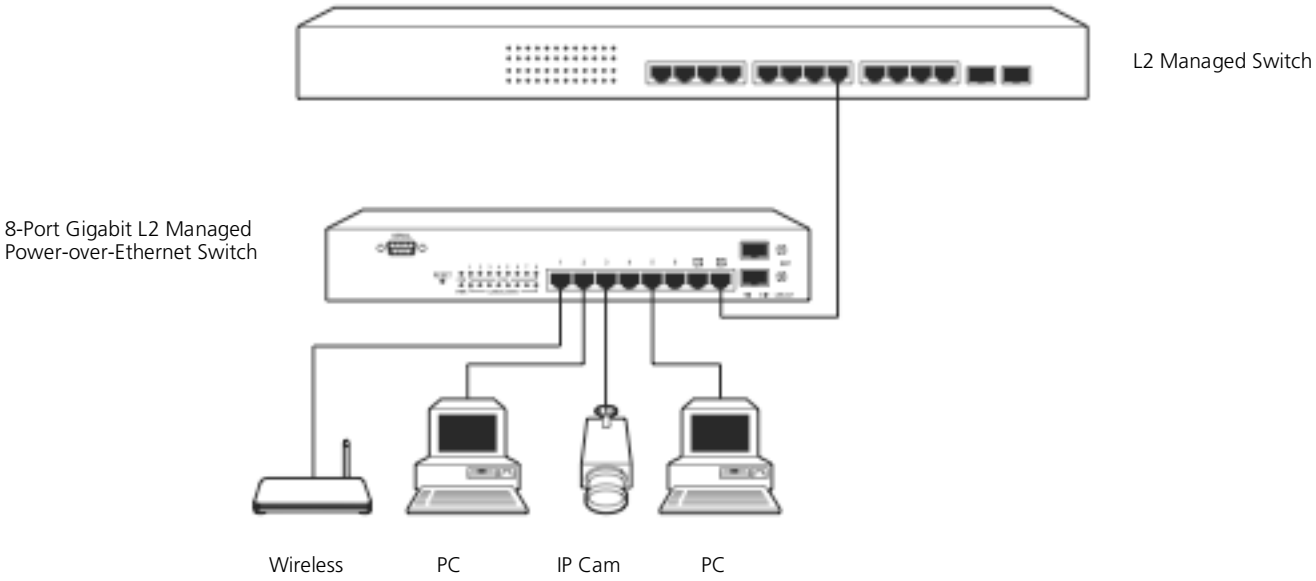


Figure 3-14. Peer-to-peer Network Connection.

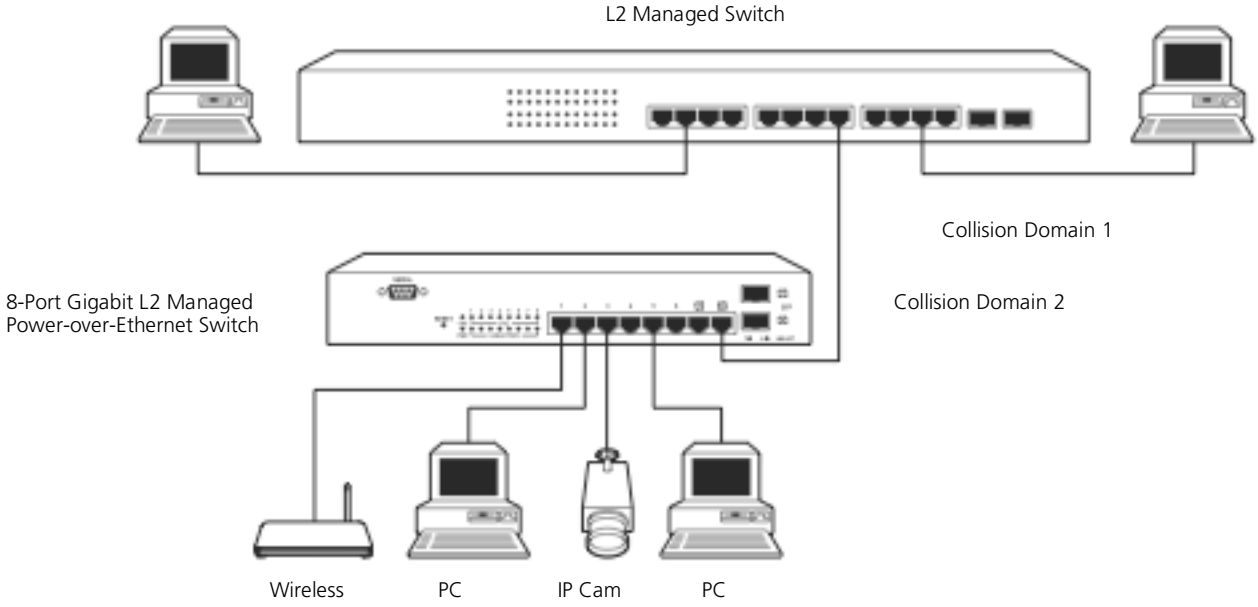


Figure 3-15. Office Network Connection.

4. Operation of Web-based Management

This chapter instructs you how to configure and manage the LPB4008A or LPB4024A through the web user interface it supports. Through any one port, you can access and monitor the switch status, including MIBs status, port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The managed switch's default values are listed in the table below:

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
Username: admin
Password: admin

After you finish configuring the managed switch in the CLI via the switch's serial interface, you can browse through the switch. For instance, type http://192.168.1.1 in the address row in a browser, and the screen shown in Figure 3-1 will appear and ask you to input your username and password to login and access authentication. The default username and password are both "admin." The first time you use the serial interface, enter the default username and password, then click the **<Login>** button. You are now logged in.

If your forgot the manager's password, click on the "Forgot Password" option in Web user interface (see Figure 4-1) or input "Ctrl+Z" in the CLI's login screen (See Figures 4-1–4-2). The system will display the user's serial number. Write down this serial number and contact Black Box Technical Support at 724-746-5500 for a temporary password. Use this new password as ID and Password to login to the system temporarily with manager authority. The user can only login to the system one time using the temporary password, so modify your password immediately after you login to the system successfully.

In this login menu, you have to input the complete username and password respectively; the switch will not give you a shortcut to username automatically. This looks inconvenient, but is safer.

The switch supports a simple user management function allowing only one administrator to configure the system at one time. If there are two or more users using administrator's identity, the switch will allow the only one who logs in first to configure the system. The rest of the users, even with administrator's identity, can only monitor the system. Users who have no administrator's identity can only monitor the system. A maximum of three users can login simultaneously to the switch.

To optimize the display effect, we recommend that you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above with 1024 x 768 resolution. The switch supports a neutral web browser interface.

In Figure 4-2, for example, the left section is the entire function tree with web user.

Figure 4-1. Login Screen.

4.1 Web Management Overview

After you login, the system information screen (Figure 4-2) appears. This page is the default and describes basic system information, including **"Model Name," "System Description," "Location," "Contact," "Device Name," "System Up Time," "Current Time," "BIOS Version," "Firmware Version," "Hardware-Mechanical Version," "Serial Number," "Host IP Address," "Host Mac Address," "Device Port," "RAM Size," "Flash Size," and "CPU Load."**. The screen tells you the software version used, MAC address, serial number, how many ports are good and so on. This is helpful for troubleshooting if the switch malfunctions.

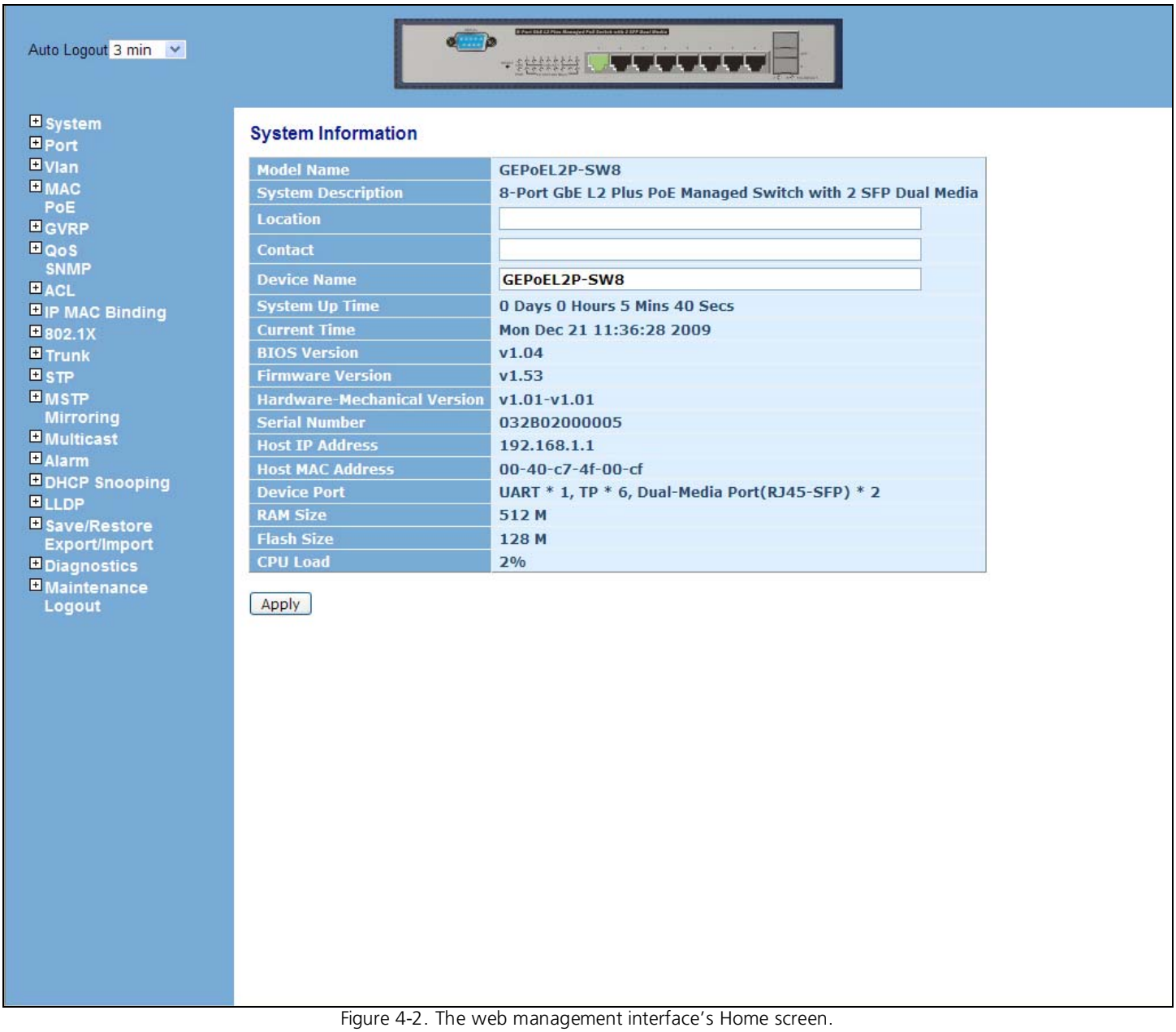


Figure 4-2. The web management interface's Home screen.

4.1.1 Screen Layout Information

The top of the screen shows the front panel of the switch. The linked ports display green; ports not linked will be dark. For the optional modules, the slot will show only a cover plate if no module is installed and will show a module if a module is present. The module image depends on the one you inserted. If disconnected, the port will be dark, if linked, green. (See Figure 4-3.)

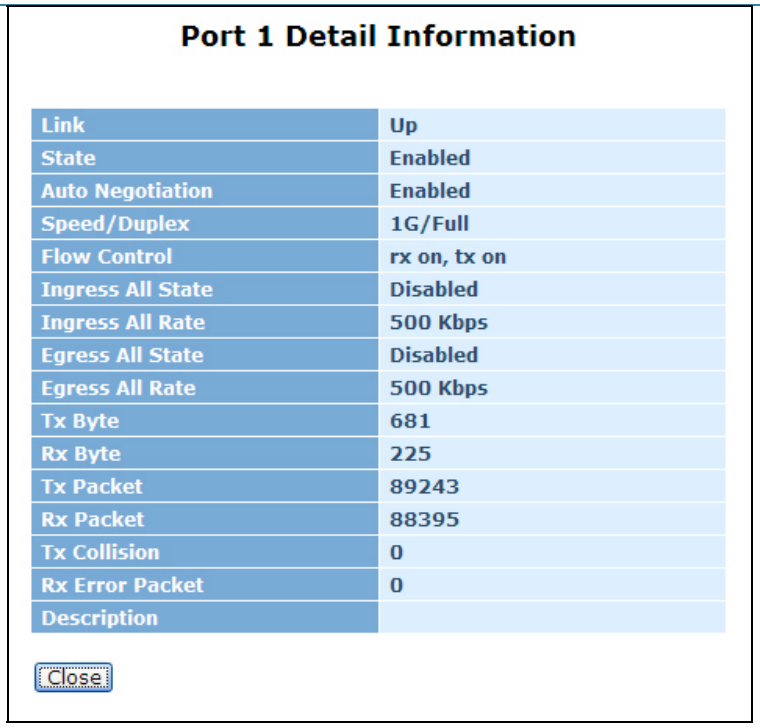
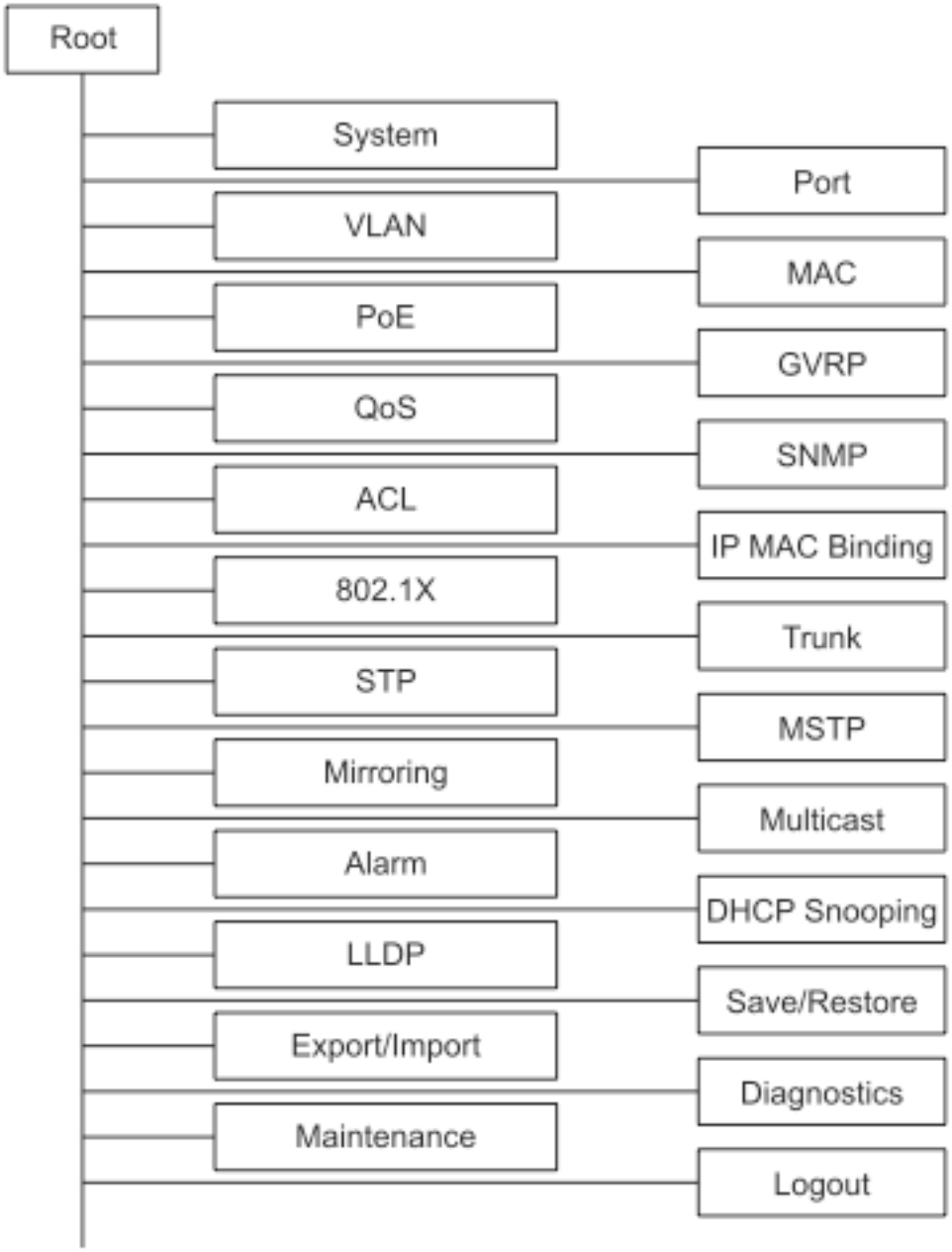


Figure 4-3. Port detail information.

Figure 4-3 shows the selected port's status, traffic status, and bandwidth rating for egress and ingress respectively. On the left-top corner is a pull-down list for Auto Logout. The auto-logout function prevents illegal users from accessing your switch as you are exiting the software. If you do not choose any selection in the Auto Logout list, the Auto Logout function turns on and the system will log out automatically after three minutes of no activity on the device. If you choose OFF, the screen will stay the same. The default value is ON.

On the left side, the page lists the main menu tree for the web. The menu is arranged hierarchically. When you open the function folder, a sub-menu will be shown. The functions of each folder are described in their corresponding sections. When you click on a function, the function is performed. The following list is the full function tree for a web user interface.

4.1.2 Structure of the Menu



4.2 System

4.2.1 System Information

Function name: System Information

Function description: Show the basic system information.

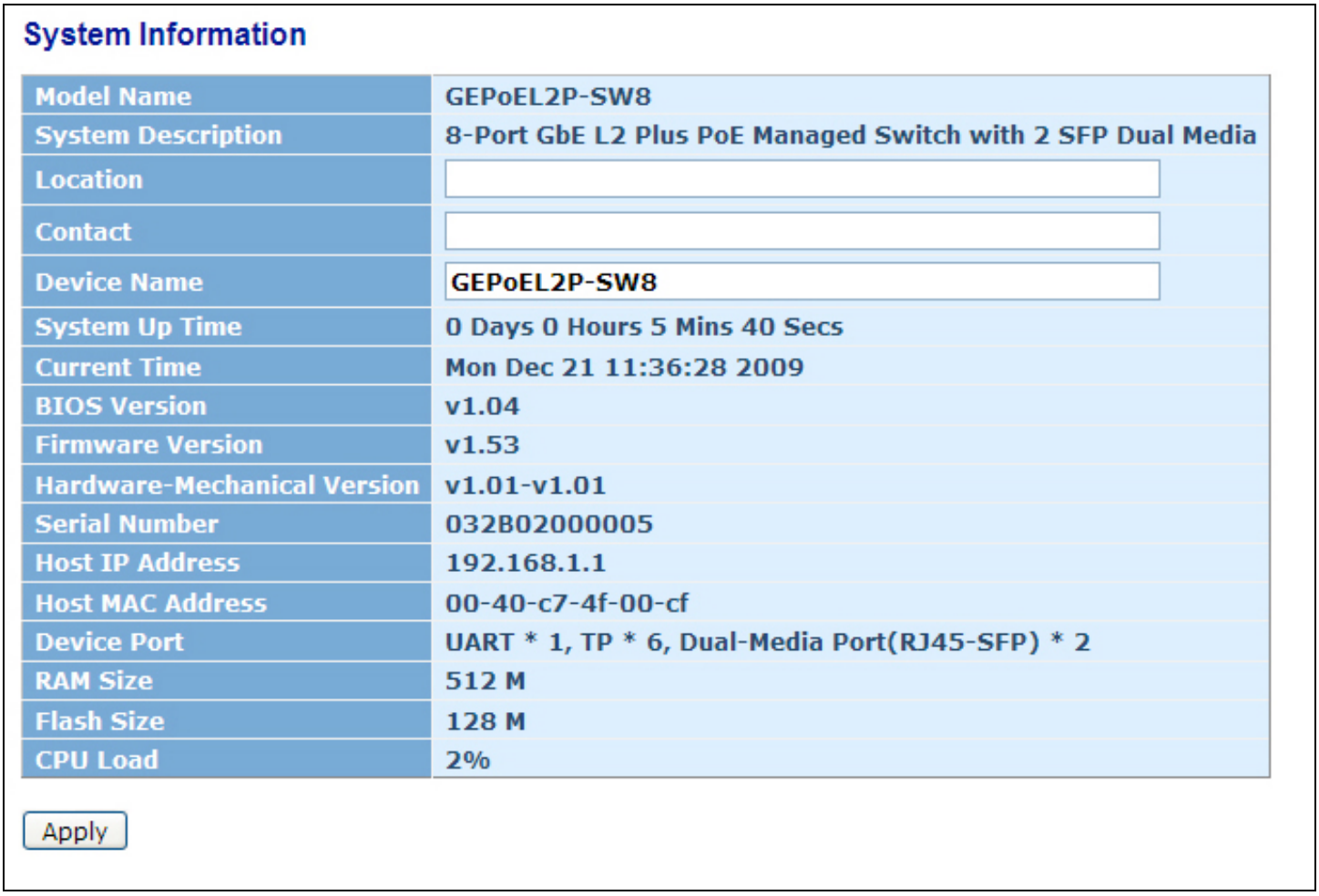


Figure 4-4. System Information.

Parameter description:

Model name: The model name of this device.

System description: Identifies the device. Here, the device is "8-Port GbE L2 Plus Managed Switch with 2 SFP Dual Media."

Location: Where the switch is located. User-defined.

Contact: To easily manage and maintain this device, write down the contact person and phone here for getting help. You can configure this parameter through the device's user interface or SNMP.

Device name: The name of the switch. User-defined. Default is LPB4008A or LPB4024A.

System up time: The time accumulated since this switch was powered on, formatted as day, hour, minute, second.

Current time: Shows the system time of the switch, formatted in day of week, month, day, hours:minutes:seconds, year. For instance, Mon Nov 30 00:00:00 1999.

BIOS version: The switch's BIOS version.

Firmware version: The switch's firmware version.

Hardware-Mechanical version: The switch's hardware and mechanical versions. The figure before the hyphen is the electronic hardware version; the one after the hyphen is the mechanical version.

Serial number: The serial number assigned by Black Box.

Host IP address:The switch's IP address.

Host MAC address: The switch's management agent's Ethernet MAC.

Device Port: Shows all of the switch's port types and numbers.

RAM size: The size of the DRAM in this switch.

Flash size: The size of the flash memory in this switch.

CPU Loading: The loading of the CPU on this switch.

4.2.2 Account Configuration

Only the administrator can create, modify, or delete the username and password. The administrator can modify other users passwords. Users logged in as Guest can only modity their own password. You must authorize the administrator/guest identites before configuring the username and password. Only one administrator is allowed to exist and can't be deleted. Up to 4 guest accounts can be created.

The default setting for user account is:

Username: admin
Password: admin

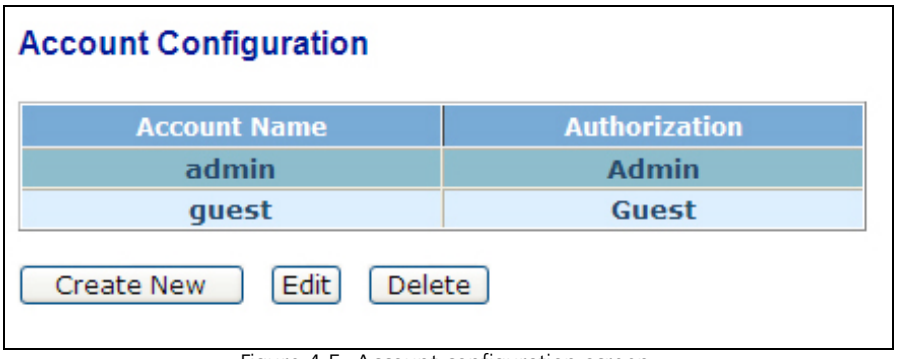


Figure 4-5. Account configuration screen.

Add Account:

Click the "Create New" button. Select the account type, "Guest" or "Operator," from the scroll-down menu. Only the Operator can change the settings. Then specify the user name and password you want.

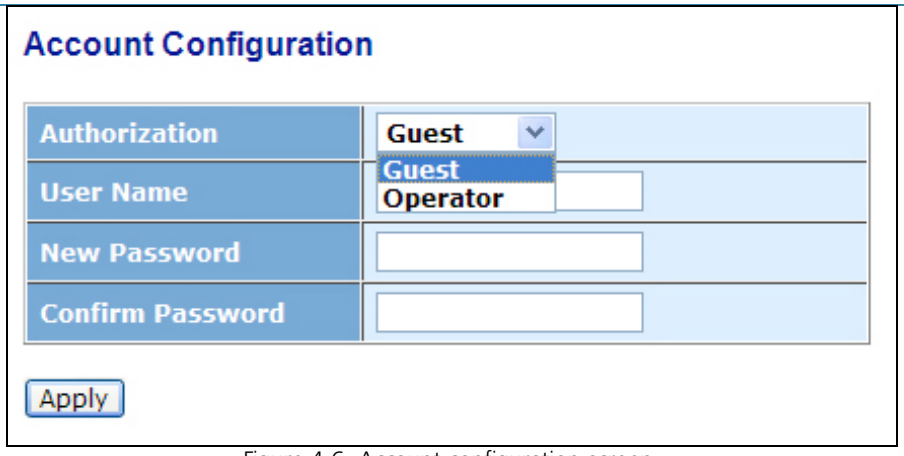


Figure 4-6. Account configuration screen.

Edit Account:

Select the account you want to edit, then click on the "Edit" button. Specify the user name and password you want.

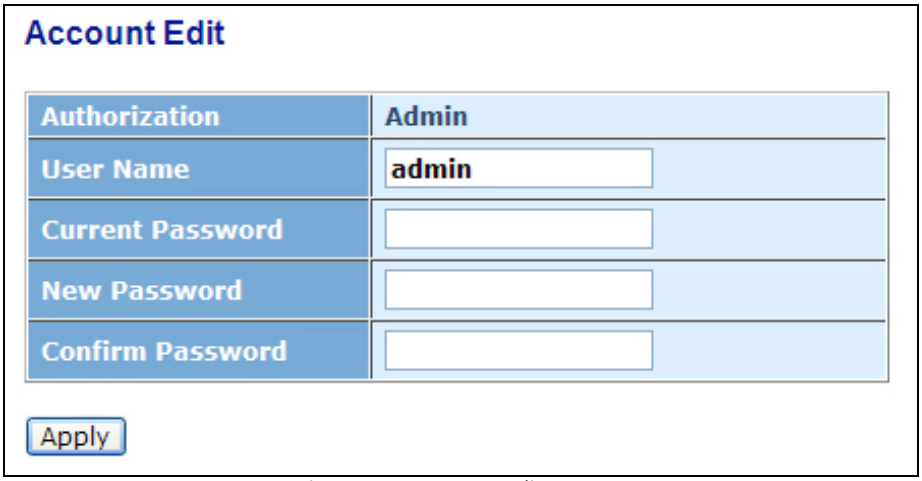


Figure 4-7. Account edit screen.

Delete Account:
Select the account you want to delete, then click on the "Delete" button.

4.2.3 Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple: just input "Year," "Month," "Day," "Hour," "Minute," and "Second" within the valid value range indicated for each item. If you input an invalid value, for example, 61 minutes, the switch will record the figure as 59.

NTP is a well-known protocol used to synchronize switch system time over a network. NTP, an Internet draft standard formalized in RFC 1305, uses version 3 protocol. The switch provides four built-in NTP server IP addresses that reside in the Internet and a user-defined NTP server IP address. The time zone is Greenwich-centered (GMT+/- xx hours).

Function name: Time
Function description:
Set the system time manually or set it by syncing from time servers. Daylight savings time is also supported.

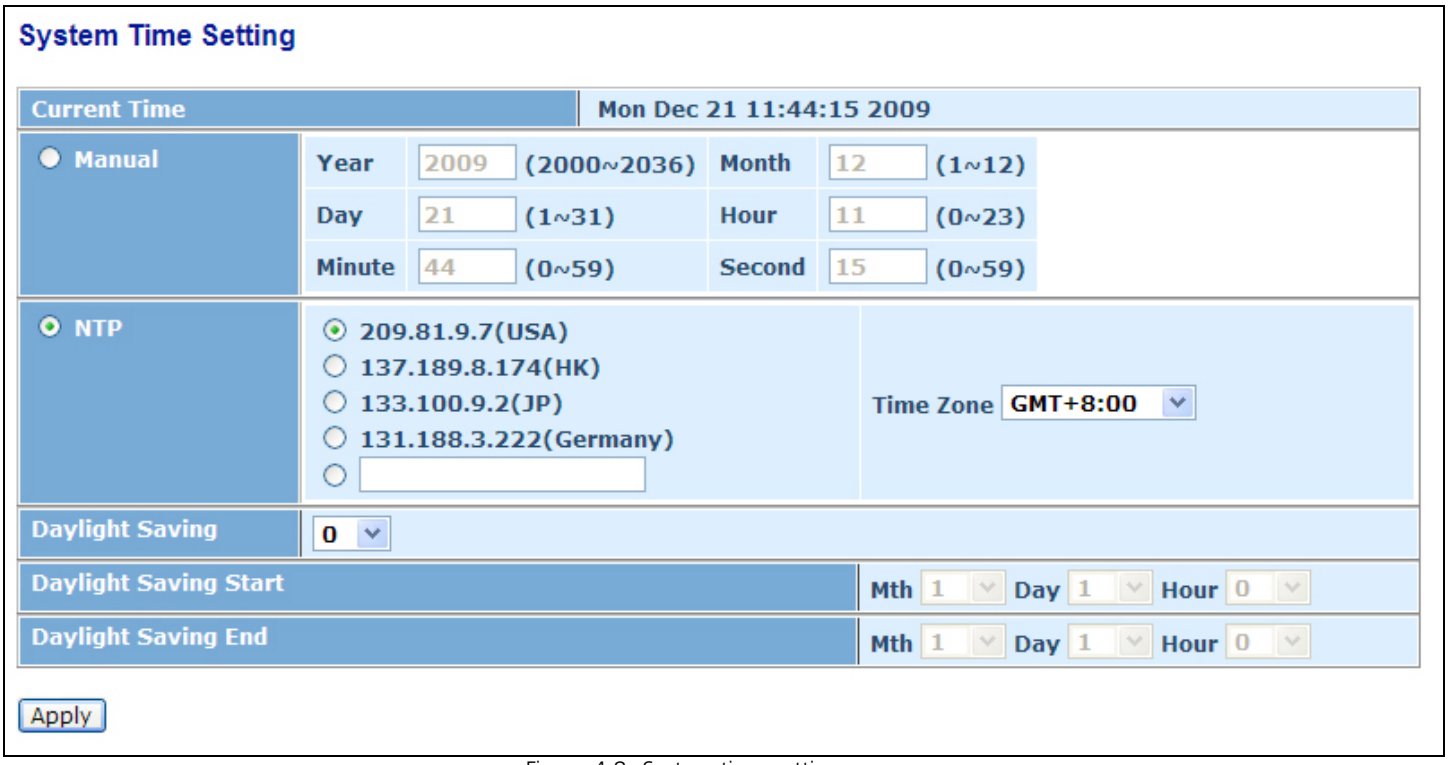


Figure 4-8. System time setting screen.

Parameter description:

Current Time: Shows the system's current time.

Manual: Click on the Manual button, type in the year, month, day, hour, minute, and second, then press the <Apply> button to adjust the time manually. Valid figures for Year, Month, Day, Hour, Minute, and Second are >=2000, 1-12, 1-31, 0-23, 0-59, and 0-59, respectively. If you input an invalid figure and press the <Apply> button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

Default: Year = 2000, Month = 1, Day = 1, Hour = 0, Minute = 0, Second = 0

NTP: Network Time Protocol (NTP) is used to sync the network time based on Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server or manually specify a user-defined NTP server and Time Zone, the switch will sync the time after you press the <Apply> button. Although it synchronizes the time automatically, NTP does not update the time periodically without user input.

The default Time Zone setting is GMT. To select a different time zone, select the time zone first and then perform time sync via NTP. The switch will combine this time zone offset and updated NTP time to calculate the local time. The switch supports configurable time zones from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Daylight Saving: Daylight savings time adjusts the time lag or advance in hours, according to the starting date and the ending date. For example, if you set the daylight savings time to be 1 hour, the system time will increase one hour after one minute. And when the time passes over the ending time, the system time will be decrease one hour after one minute.

The switch supports valid configurable daylight savings time from –5 to +5 one hour steps. It does not have to adjust current time to enact daylight savings time, and you don't have to set the starting/ending date. If you set daylight savings time to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight savings function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the Daylight Savings function and described in detail.

Daylight Savings Start: Set when to start daylight savings time.

Mth: Range is 1–12. Default: 1

Day: Range is 1–31. Default: 1

Hour: Range is 0–23. Default: 0

Day Light Saving End: Set when to stop daylight saving time.

Mth: Range is 1–12. Default: 1

Day: Range is 1–31. Default: 1

Hour: Range is 0–23. Default: 0

4.2.4 IP Configuration

IP configuration is one of the most important switch configurations. Without the proper setting, the network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via a DHCP server. When the IP address is changed, you must reboot the switch so the setting will take effect. Use the new IP to browse for web management and CLI management.

Function name: IP Configuration

Function description: Set IP address, subnet mask, default gateway, and DNS for the switch.

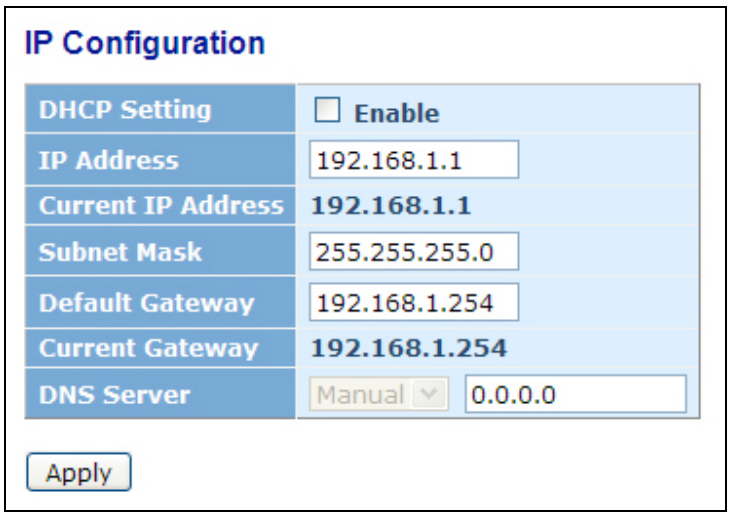


Figure 4-9. IP configuration screen.

Parameter description:

DHCP Setting: DHCP is the abbreviation for Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function. The switch supports a DHCP client that's used to get an IP address automatically if you set this function to "Enable." When enabled, the switch will issue the request to the DHCP server residing in the network to get an IP address. If the DHCP server is down or does not exist, the switch will issue the request and show the IP address requested, until the DHCP server is on. Before getting an IP address from DHCP server, the device will not continue booting. If you set this field to "Disable," you'll have to input IP address manually

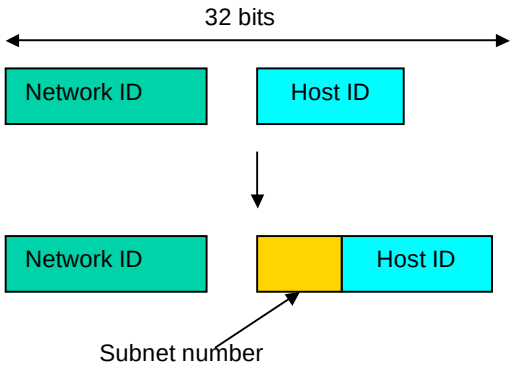
Default: Disable

IP address: Users can configure the IP settings and fill in new values when the DHCP function is set to "Disable." Click on the <Apply> button to update.

When DHCP is disabled, Default: 192.168.1.1.

If DHCP is enabled, this field is filled by DHCP server and will not allow users to set it manually.

Subnet mask: Any IP device in a network must own its IP address, which is composed of a Network address and a Host address; otherwise it can't communicate with other devices. Subnet mask enables more network addresses. Network classes A, B, and C are too large to fit for almost all networks, so, subnet mask is introduced to solve this problem. Subnet mask uses some bits from a host address and creates an IP address consisting of Network address, Subnet mask number, and host address. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number (2^[bit number of subnet number]).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices attached to the same network
Default: 255.255.255.0

Default gateway: Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for another pre-defined path, it must be forwarded to a default router on a default path. This means that any packet with an undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

DNS: Domain Name Server translates between IP address and name address.

The switch supports the DNS client function to re-route the mnemonic name address to the DNS server to get its associated IP address for accessing the Internet. Users can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with meaningful words in it. The default is no assignment of DNS address.

Default: 0.0.0.0

4.2.5 Loop Detection

The loop detection is used to detect the presence of traffic. When the switch receives a packet's (looping detection frame) MAC address that is the same as the one from the port, show Loop is detected. The port will be locked when it receives the looping detection frames. If you want to resume using the locked port, find the looping path, remove it, then select the locked port and click on "Resume" to enable it.

Function name: Loop Detection

Function description: Displays whether the switch is set up for Loop detection and whether a port has been locked due to loop detection. Also provides the ability to resume normal operation after leaving a loopback path.

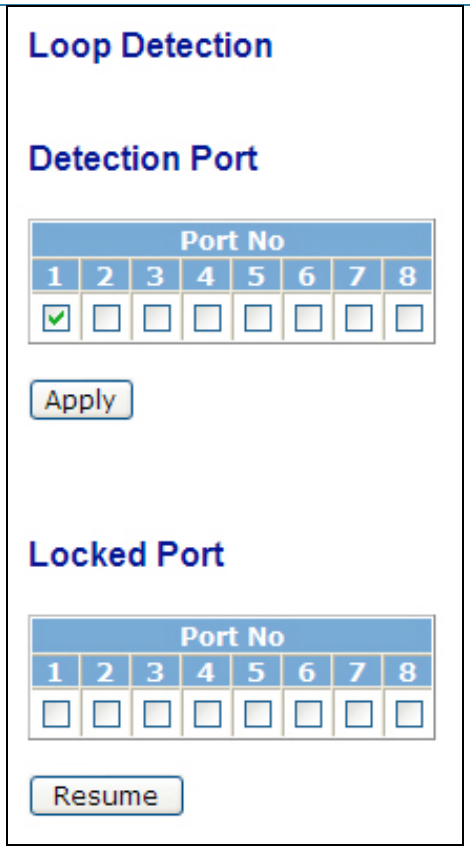


Figure 4-10. Loop detection screen.

Parameter description:

Port No: Display the port number. Valid numbers are 1–8 for LPB4008A or 1–24 for LPB4024A.

Detection Port— Enable: Choose the port number and enable the port's Loop detection. If loops are detected, the port is locked. If Loops are not detected, the port remains unlocked.

Locked Port— Resume: Choose Resume to open and unlock the port. If you do not choose Resume, the port remains locked.

4.2.6 Management Policy

Through the management security configuration, the manager can setup the switch and limit user access to this switch.
The following rules are offered for the manager to manage the switch:

Rule 1: When no lists exist, then it will accept all connections.

Accept

Rule 2: When only "accept lists" exist, then it will deny all connections, excluding the connection within the acceptable range.

Accept **Deny** **Accept** **Deny** **Accept**

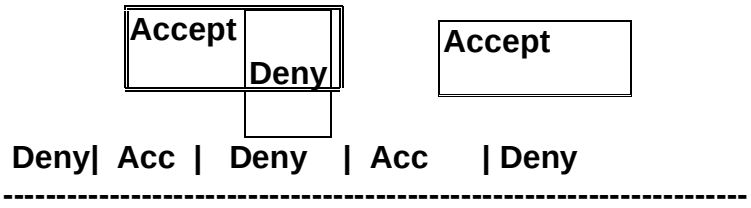
Rule 3: When only "deny lists" exist, then it will accept all connections, excluding the connection within the denying range.

Deny **Accept** **Deny** **Accept** **Deny**

Rule 4: When both "accept and deny" lists exist, then it will deny all connections, excluding the connection within the acceptable range.

Accept **Deny** **Deny** **Deny** **Accept**

Rule 5: When both "accept and deny" lists exist, then it will deny all connections, excluding the connection within the acceptable range and NOT within the denying range at the same time.



Function name: Management Security Configuration

Function description: The switch offers Management Security Configuration. With this function, the manager can easily control the mode in which the user connects to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). You can place some restrictions on the user connect mode. For example, you can decide which VLAN VID will be accepted or denied by the switch. You can also set the switch to accept or deny the users' IP range, identify user ports that will connect to the switch, or control and connect to the switch via Http, Telnet or SNMP.

Figure 4-11. Management policy list screen.

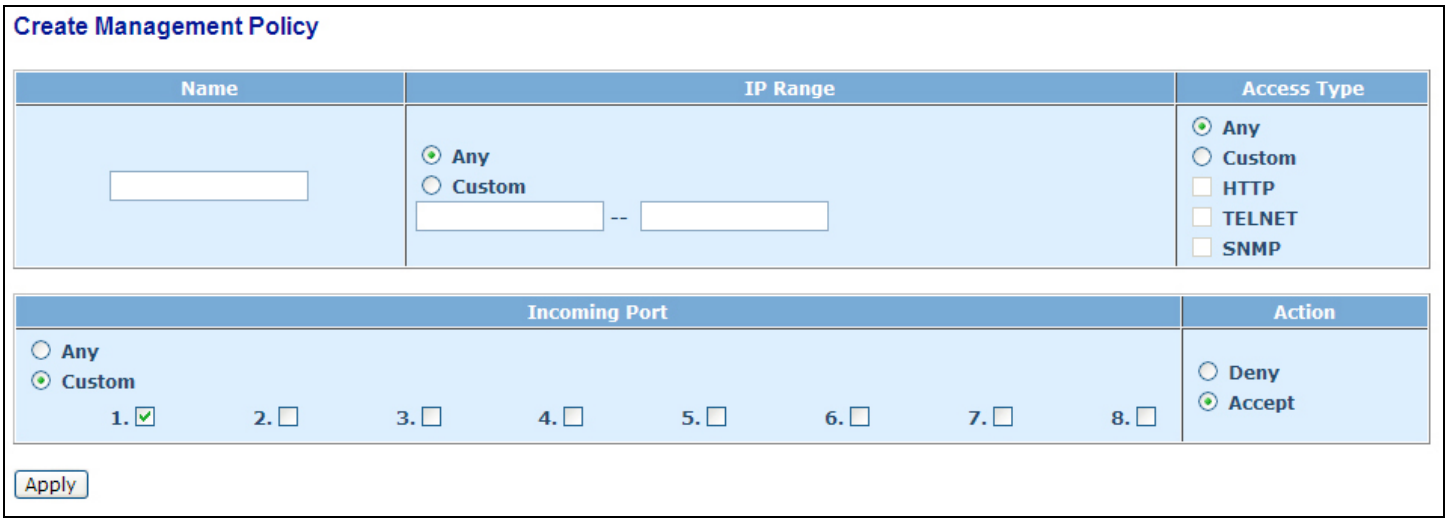


Figure 4-12. Create management policy screen.

Parameter description:

Add: Press the <Add> button to create a new Management Security Configuration after you set up the parameters mentioned above. You can also modify the existing entry by pressing this button.

Delete: Remove the existing Management Security Configuration entry from the management security table.

Name: A name can contain any letter (A–Z, a–z) and digit (0–9) with a maximum of 8 characters.

VID: The switch supports two kinds of options for managed valid VLAN VID, including “Any” and “Custom.” The default is “Any.” When you choose “Custom,” you can fill in the VID number. The valid VID range is 1–4094.

IP Range: The switch supports two kinds of options for managed valid IP Range, including “Any” and “Custom.” The default is “Any.” If you choose “Custom,” you can assign an effective IP range. The valid range is 0.0.0.0–255.255.255.255.

Incoming Port: The switch supports two kinds of options for managing a valid Port Range, including “Any” and “Custom.” The default is “Any”. You can select the ports that you want to restrict in the management security configuration.

Access Type: The switch supports two kinds of options for managed valid Access Type, including “Any” and “Custom”. Default is “Any.” If you choose “Custom,” you can access and manage the switch in three ways: via Http, Telnet, and SNMP.

Action: The switch supports two kinds of options for managed valid Action Type, including “Deny” and “Accept.” The default is “Deny”. When you choose “Deny,” you will be restricted from managing the switch based on the “Access Type” you choose. If you select “Accept,” you will have the authority to manage the switch.

4.2.7 System Log

The System Log provides information about system logs, including information about when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.

Function name: System Log

Function description: The Trap Log Data displays the log items including all SNMP Private Trap events, SNMP Public traps, and user logs that occurred in the system. In the report table, No., Time, and Events are three fields contained in each trap record.

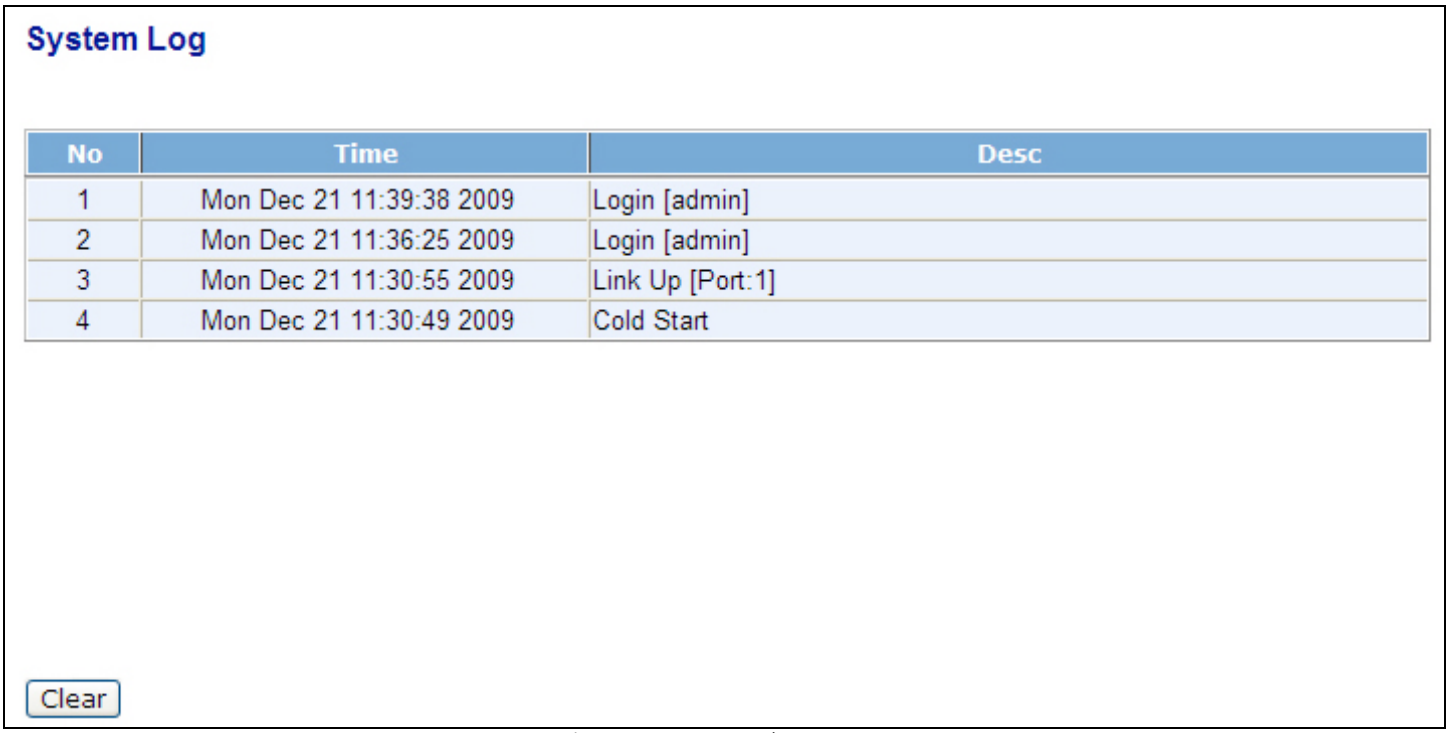


Figure 4-13. System log screen.

Parameter description:

No: Display the order number for the trap that occurred.

Time: Display the time that the trap happened.

Desc: Displays a description event recorded in the System Log.

Clear: Clear log data.

4.2.8 Virtual Stack

Function name: Virtual Stack

Function description: Virtual Stack Management (VSM) is the group management function. It allows you to automatically group switches that are in the same LAN. One switch will be the master device, and the others in this group will become the slave devices.

VSM offers a simple centralized management function. You don't need to remember the address of all devices, since the manager can manage the network using the address of the Master device. Instead of SNMP or Telnet UI, VSM is only available in Web UI (not SNMP or Telnet UI). When one switch becomes the Master, two rows of buttons for group devices will appear on the top of its Web UI. When you press these buttons, users can connect the Web UI of the devices of the group in the same window without logging in these devices.

The top left button is only for the Master device. The background color of the button you press changes to represent that the device is under your management.

NOTE: Logging into the switch via the console will remove the grouping temporarily. Each device in the group will be shown as a station address (the last number of IP Address) + device name on the button (for example, 196_LPB4008A). Otherwise, it will show " ---- " if no corresponding device exists.

Once the devices join the group successfully, then they are can be managed via Master device, and user will not be able to manage them via telnet/console/web individually.

Up to 16 devices can be grouped for VSM; however, only one Master is allowed to exist in each group. For Master redundancy, users may configure more than two devices as Master, but the Master device with the smaller MAC value will be the Master one. All 16 devices can become Master devices and back up each other.

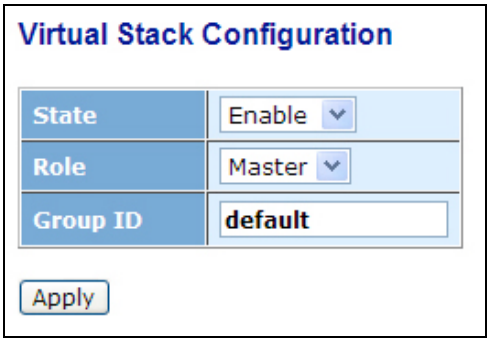


Figure 4-14. Virtual stack configuration screen.

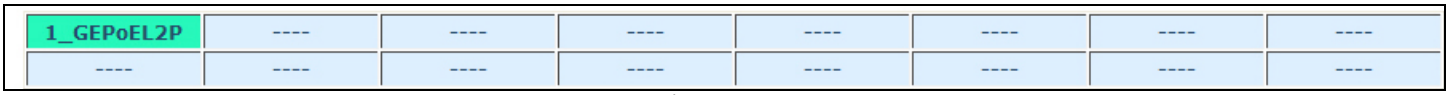


Figure 4-15.

Parameter description:

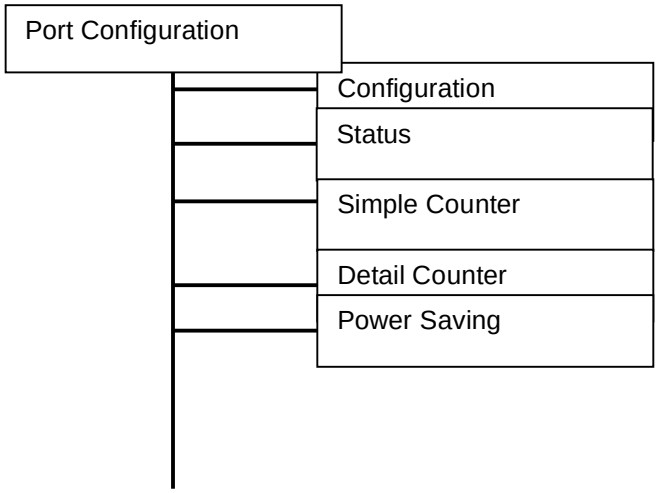
State: Activates or de-activates VSM. The default is Enable.

Role: The switch's role in the virtual stack. There are two types of roles (master and slave). The default is Master.

Group ID: The group identifier (GID) identifies the VSM. Valid letters are A–Z, a–z, 0–9, " - " and "_" characters. The maximum length is 15 characters.

4.3 Port

Four functions, including Port Status, Port Configuration, Simple Counter, and Detail Counter are used to monitor and manage ports. Each is described in detail in the following sections.



4.3.1 Port Configuration

Port Configuration changes the setting of each port. You can set/reset the several functions. They are described in detail below.

Function name: Port Configuration

Function description: Sets each port's operation mode. The switch supports three parameters for each port: state, mode, and flow control.

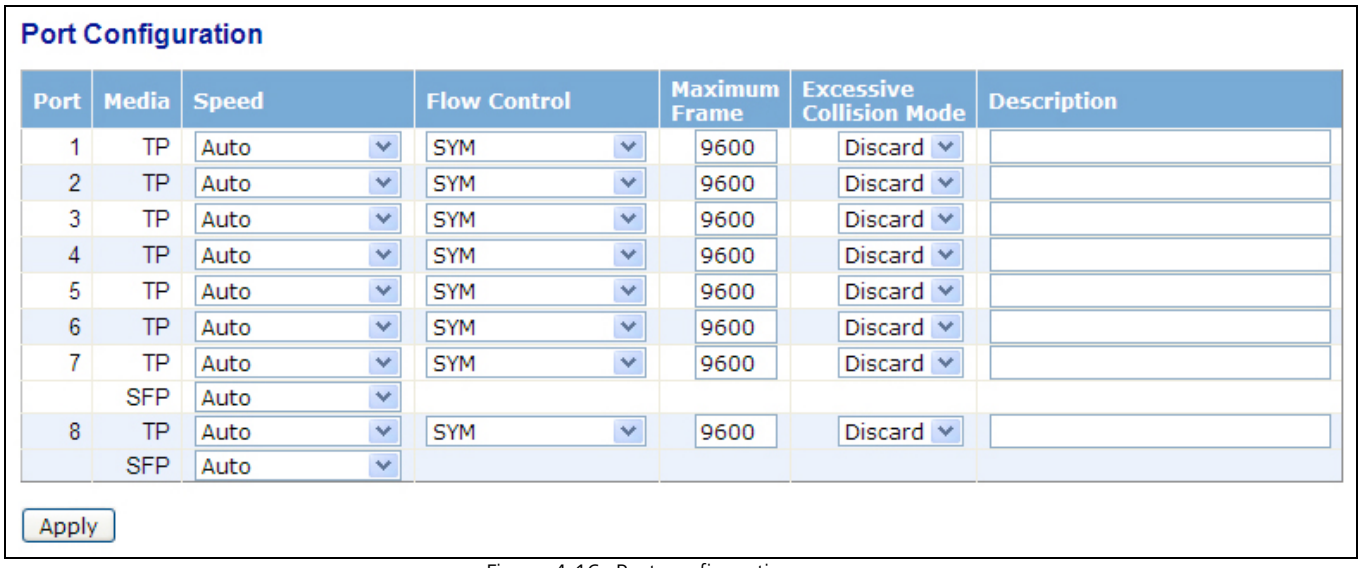


Figure 4-16. Port configuration screen.

Parameter description:
Speed: Set the speed and duplex of the port. For 1 Gbps fiber, the speed is always 1000 Mbps and full duplex. For twisted pair, the speed/duplex is the combination of speed mode (10/100/1000Mbps), and duplex mode (full duplex and half duplex).

1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto-negotiation mode, there is no default value. In Forced mode, the default value depends on your setting.

Flow Control: Choose from two flow control modes: Enable and Disable. If flow control is set to Enable, both users can send a PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle more traffic. When flow control is set Disable, the packet is dropped if the traffic is too much to handle.

Maximum Frame: The maximum packet size is 1518–9600 (Bytes) long.

Excessive Collision Mode: If excessive collisions occur when the connection is half-duplex, choose Discard or Restart.

Discard: The "Discard" mode determines whether the MAC drop frames after an excessive collision has occurred. If set to Discard, a frame is dropped after excessive collisions. This conforms to IEEE Std 802.3 half-duplex flow control operation.

Restart: The "Restart" mode determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Std 802.3, but is useful in non-dropping half-duplex flow control operation.

Description: Description of device ports cannot include # % & ' + \.

4.3.2 Port Status

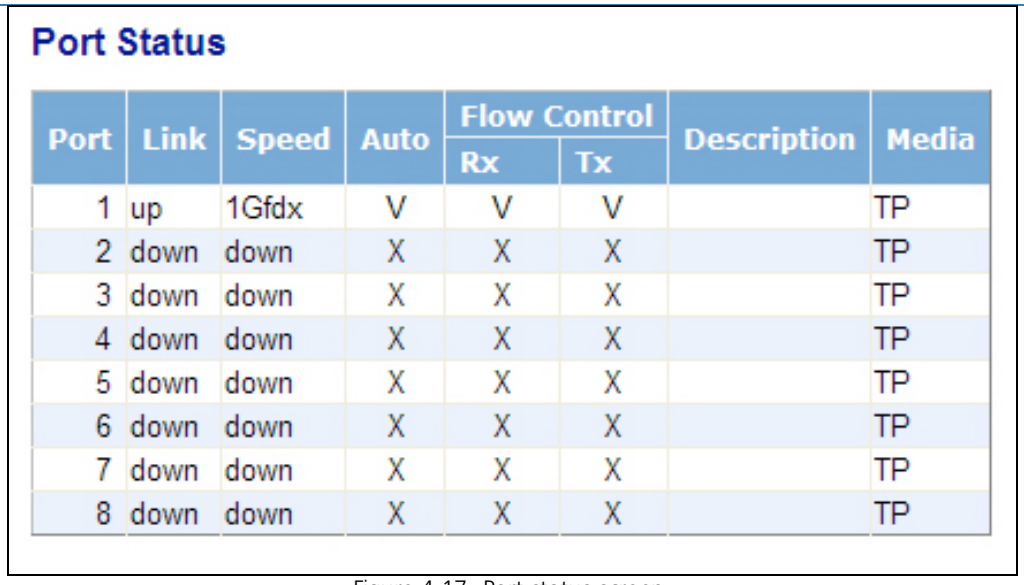
The Port Status function gathers each port's current status information and reports its port number, media, link status, port state, auto-negotiation status, speed/duplex, Rx Pause, and Tx Pause. Media type information for the module ports 7 and 8 is also offered (see Figure 4-14).

Function name:

Port Status

Function Description:

Report the latest updated status of all ports in this switch. When the status of any one of the switch's ports changes, the new value(s) are displayed. The current port status refreshes about every 5 seconds.



Port Status

Port	Link	Speed	Auto	Flow Control		Description	Media
				Rx	Tx		
1	up	1Gfdx	V	V	V		TP
2	down	down	X	X	X		TP
3	down	down	X	X	X		TP
4	down	down	X	X	X		TP
5	down	down	X	X	X		TP
6	down	down	X	X	X		TP
7	down	down	X	X	X		TP
8	down	down	X	X	X		TP

Figure 4-17. Port status screen.

Parameter Description:

Port: Display the port number, from 1–8. Ports 7 and 8 are optional modules.

Link: Show if the link on the port is active or not. If the link is connected to a device that's working, the Link appear as "Up"; otherwise, it will be "Down." This is determined by the hardware on both devices of the connection.

Speed/Duplex Mode: Display the speed and duplex of all port. 10 Mbps, 100 Mbps and 1000 Mbps speeds are supported for TP media, with half duplex and full duplex. If the media is 1Gbps fiber, 1000 Mbps speed is supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in "Auto Speed" mode or 2) user setting in "Force" mode. The local port must preset its capability.

Flow Control: Show each port's flow control status.

There are two types of flow control in Ethernet, Backpressure for half-duplex operation and Pause flow control (IEEE802.3x) for full-duplex operation. The switch supports both of them.

Description: This is provided by users to describe device ports.

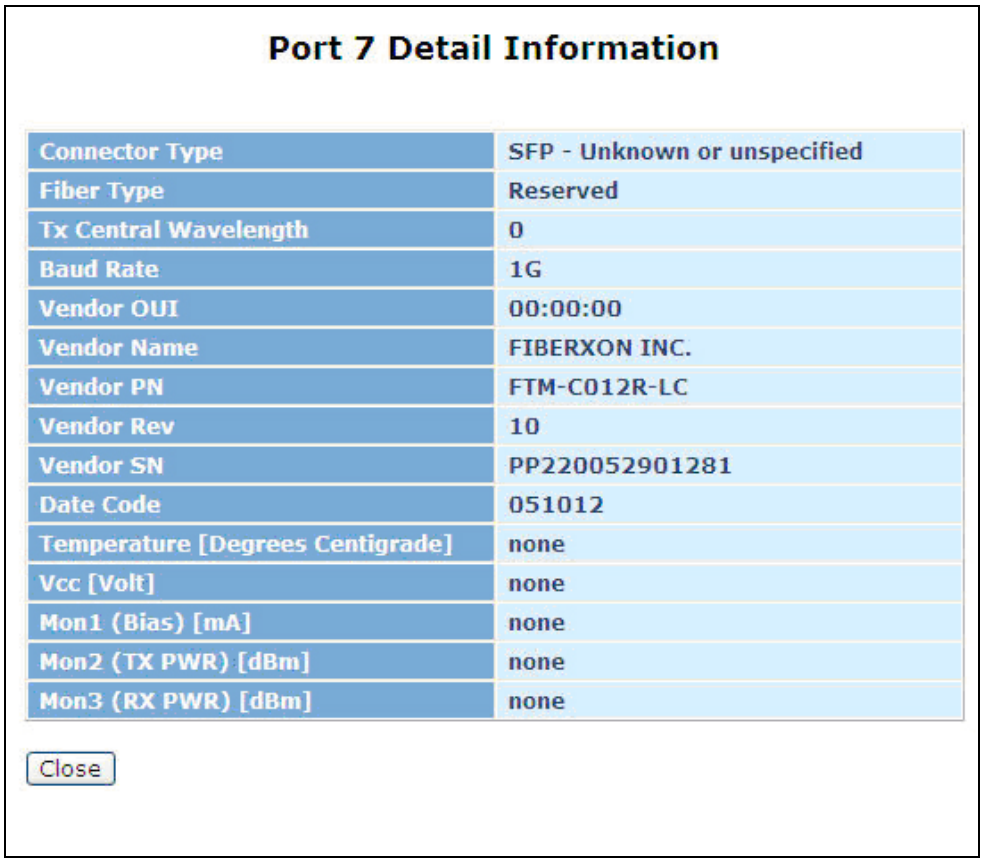


Figure 4-18. Port 7 detail information screen.

Parameter description of Port 7–Port 8:

Connector Type: Displays the connector type, for instance, UTP, SC, ST, LC and so on.

Fiber Type: Displays the fiber mode, for instance, Multi-Mode, Single-Mode.

Tx Central Wavelength: Displays the fiber optical transmitting central wavelength, for instance, 850-nm, 1310-nm, 1550-nm and so on.

Baud Rate: Displays the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.

Vendor OUI: Displays the Manufacturer's OUI code which is assigned by IEEE.

Vendor Name: Displays the company name of the module manufacturer.

Vendor P/N: Displays the product name by module manufacturer.

Vendor Rev (Revision): Displays the module revision.

Vendor SN (Serial Number): Show the serial number assigned by the manufacturer.

Date Code: Show the date this SFP module was made.

Temperature: Show the current temperature of SFP module.

Vcc: Show the working DC voltage of SFP module.

Mon1(Bias) mA: Show the Bias current of SFP module.

Mon2(TX PWR): Show the transmit power of the SFP module.

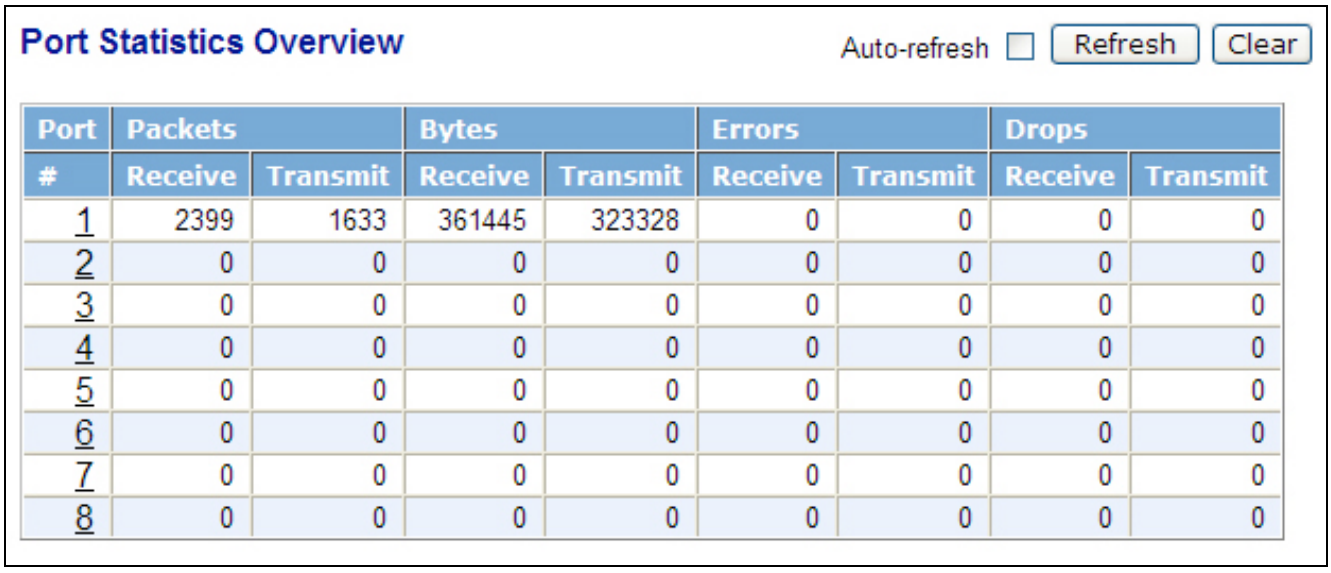
Mon3(RX PWR): Show the receiver power of the SFP module.

4.3.3 Simple Counter

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In Figure 4-15, the window can show all ports' counter information at the same time. Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The Refresh Interval is used to set the update frequency

Function name: Simple Counter
Function description: Display the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision, and Rx Error Packet.



Port	Packets		Bytes		Errors		Drops	
#	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	2399	1633	361445	323328	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Figure 4-19. Port statistics overview screen.

Parameters description:

Packets:

Transmit: The number of packets transmitted.

Receive: The number of packets received.

Bytes:

Transmit: Total transmitted bytes.

Receive: Total received bytes.

Errors:

Transmit: Number of bad packets transmitted.

Receive: Number of bad packets received.

Drops

Transmit: Number of packets transmitted drop.

Receive: Number of packets received drop.

Auto-refresh: The simple counts will be refreshed automatically on the UI screen.

Refresh: The simple counts will be refreshed manually when a user clicks on the "Refresh" button.

Clear: The simple counts will be reset to zero when a user clicks on the "Clear" button.

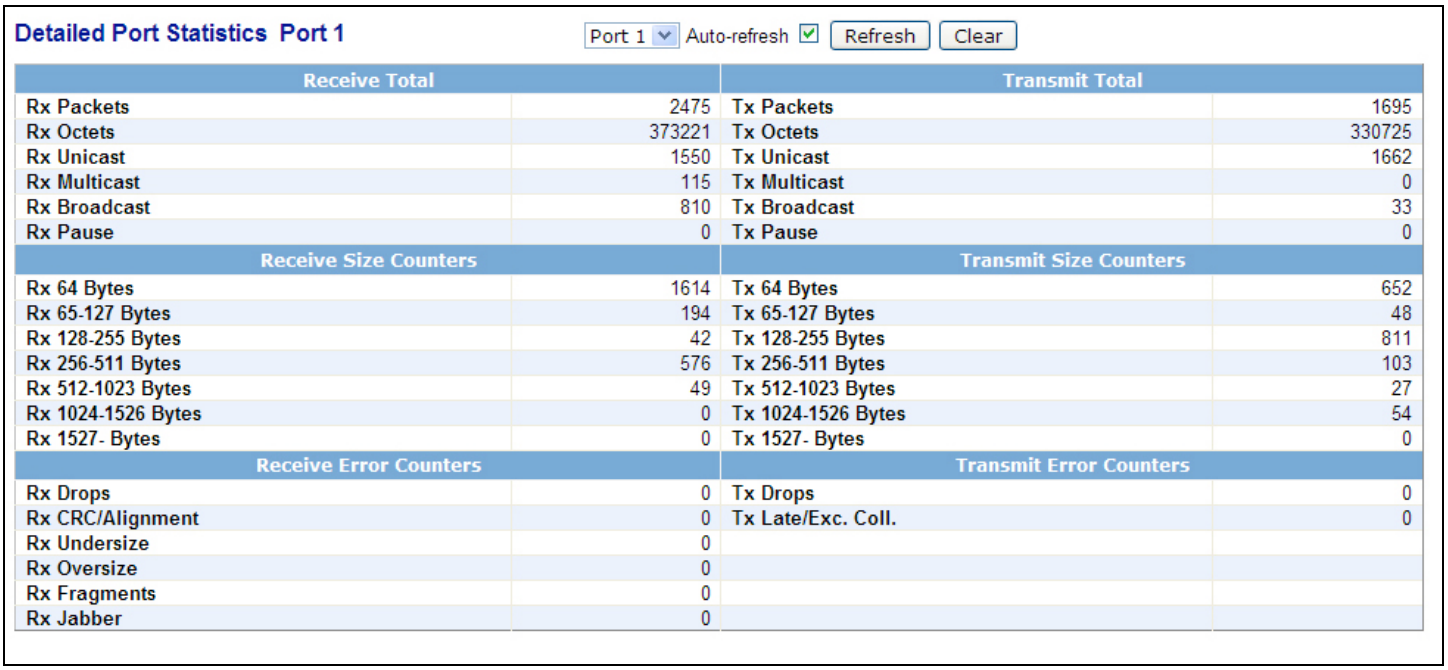
4.3.4 Detail Counter

The Detail Counter function counts the port traffic, whether or not the packet is good or bad. In Figure 4-19, the window can show only one port counter information at the same time. To see another port's counter, you have to pull down the list Select list, then the screen for the port you chose will appear.

Each data field list is 20-digit long. If the counting overflows, the counter will be reset and restart counting. The data is updated at every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

Function name: Detail Counter

Function description: Display the detailed number of each port's traffic. In Figure 4-20, the window can show all port's information at one time.



Receive Total		Transmit Total	
Rx Packets	2475	Tx Packets	1695
Rx Octets	373221	Tx Octets	330725
Rx Unicast	1550	Tx Unicast	1662
Rx Multicast	115	Tx Multicast	0
Rx Broadcast	810	Tx Broadcast	33
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	1614	Tx 64 Bytes	652
Rx 65-127 Bytes	194	Tx 65-127 Bytes	48
Rx 128-255 Bytes	42	Tx 128-255 Bytes	811
Rx 256-511 Bytes	576	Tx 256-511 Bytes	103
Rx 512-1023 Bytes	49	Tx 512-1023 Bytes	27
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	54
Rx 1527- Bytes	0	Tx 1527- Bytes	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		

Figure 4-20. Detailed port statistics port 1 screen.

Parameter description:

Rx Packets: The number of packets received.

RX Octets: Total received bytes.

Rx High Priority Packets: Number of Rx packets classified as high priority.

Rx Low Priority Packets: Number of Rx packets classified as low priority.

Rx Broadcast: Show the number of broadcast packets received.

Rx Multicast: Show the number of multicast packets received.

Tx Packets: The number of packets transmitted.

TX Octets: Total transmitted bytes.

Tx High Priority Packets: Number of Tx packets classified as high priority.

Tx Low Priority Packets: Number of Tx packets classified as low priority.

Tx Broadcast: Show the number of broadcast packets transmitted.

Tx Multicast: Show the number of transmitted multicast packets transmitted.

Rx 64 Bytes: Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes: Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes: Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes: Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes: Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-Bytes: Number of 1024-max_length-byte frames in good and bad packets received.

Tx 64 Bytes: Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes: Number of 65–126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes: Number of 127–255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes: Number of 256–511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes: Number of 512–1023-byte frames in good and bad packets transmitted.

Tx 1024-Bytes: Number of 1024-max_length-byte frames in good and bad packets transmitted.

Rx CRC/Alignment: Number of Alignment errors and CRC error packets received.

Rx Undersize: Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize: Number of long frames (according to max_length register) with valid CRC.

Rx Fragments: Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabber: Number of long frames (according tomax_length register) with invalid CRC.

Rx Drops: Frames dropped due to the lack of receiving buffer.

Rx Errors: Number of error packets received.

Tx Collisions: Number of collision frames transmitted.

Tx Drops: Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx FIFO Drops: Number of frames dropped due to the lack of transmitting buffer.

Auto-refresh: The detail counts will be refreshed automatically on the UI screen.

Refresh: The detail counts will be refreshed manually when users click on the “Refresh” button.

Clear: The detail counts will be reset to zero when users sclick on the “Clear” button.

4.3.5 Power Saving

The Power Saving function reduces the power consumption with "ActiPHY Power Management" and "Perfect Reach Power Management." It efficiently saves the switch Power when the client is idle and detects the cable length to provide different power.

Function name: Power Saving

Function description: The function uses "ActiPHY Power Management" and "Perfect Reach Power Management" to save the switch's power consumption.

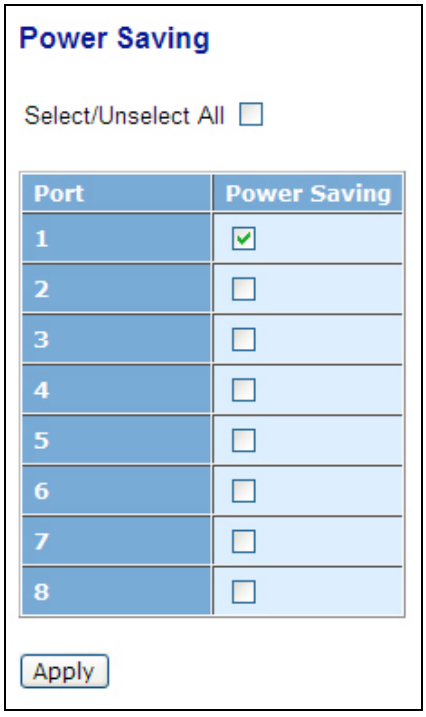


Figure 4-21. Power saving screen.

Parameter description:

Power Saving:

The parameter will consider the length of any Ethernet cable connected and adjust power usage accordingly. Shorter lengths require less power. link-down mode removes power for each port that does not have a device attached.

Default: Disable.

4.4 VLAN

The switch supports Tag-based VLAN (802.1Q) and Port-based VLAN. Support 4094 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as needed. Configure it properly to improve security security and increase performance but reduce VLAN management.

4.4.1 VLAN Mode

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes five modes: Port-based, Tag- based, Metro Mode, Double-tag, and Disable. Choose one from the drop down list. Then click on the <Apply> button, and the settings will take effect immediately.

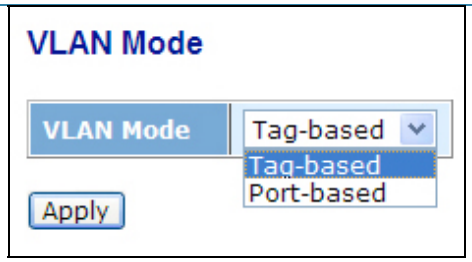


Figure 4-22. VLAN mode.

Parameter description:

VLAN Mode:

Port-based: Port-based VLAN is defined by port. Any packet coming in or going out from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, a port-based VLAN named PVLAN-1 contains port members Port 1 & 2 & 3 & 4. If you are on port 1, you can communicate with port 2&3&4. If you are on port 5, then you cannot talk to them. Each port-based VLAN must be assigned a group name. This switch can support up to maximal 24 port-based VLAN groups.

Tag-based: Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened to determine if it can be forwarded. The switch supports 802.1q. For more details, see Chapter 3.

Each tag-based VLAN must be assigned a VLAN name and a VLAN ID. Valid VLAN IDs are 1–4094. User can create total up to 4094 Tag VLAN groups.

4.4.2 Tag-based Group

Function name: Tag-based Group Configuration

Function description: Tag-based VLAN Groups, You can also easily create, edit and delete a Tag-based VLAN group by pressing the <Add>, <Edit>, and <Delete> function buttons. Or, add a new VLAN group by inputting a new VLAN name and VLAN ID.

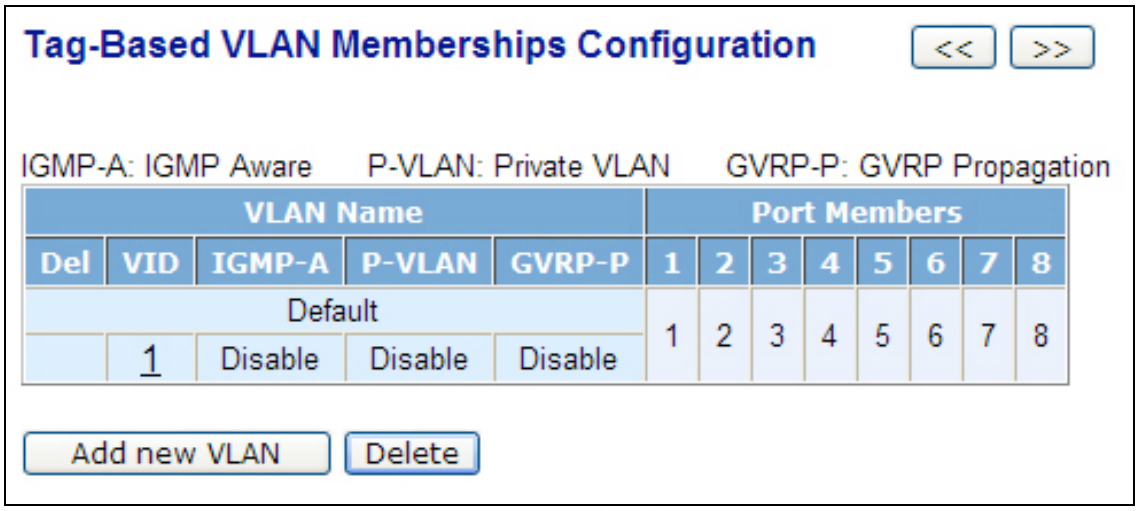


Figure 4-23. Tag-based VLAN memberships configuration screen.

Parameter description:

VLAN Name: The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, "-" and "_" characters. The maximum length is 15 characters.

VLAN ID: VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

IGMP-A: IGMP Aware enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts for its hosts. This switch's IGMP Aware function **"Enable" or "Disable"** can be set by the VLAN group. If the VLAN group IGMP Aware is disabled, the switch will stop the exchange of IGMP messages between the VLAN group members. If the VLAN group IGMP Aware is enabled, the switch will support the exchange of IGMP messages in the VLAN group members and follow with IGMP router port configuration, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP. You enable IGMP on the interfaces that connect the system to its hosts that are farther away from the root of the tree. Refer to Section 3.15.1 for a detailed IGMP Aware function description.

Member Port: This is used to enable or disable if a port is a member of the new added VLAN. "Enable" means it is a member of the VLAN. Click on the check box (☑) beside the port x to enable it.

Add new VLAN: Click on **<Add new VLAN>** to create a new Tag-based VLAN. Input the VLAN name and the VID. Configure the SYM-VLAN function and choose the member by clicking on the check box beside the port No.. Then, press the **<Apply>** button and the setting will take effect.

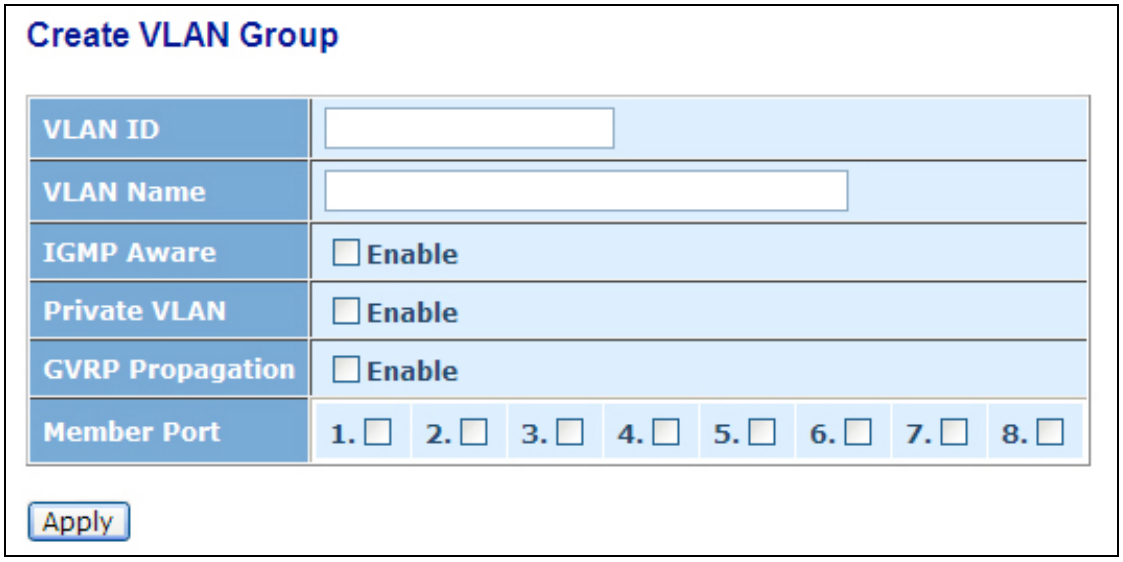


Figure 4-24. Create VLAN group.

Delete Group: Just press the **<Delete>** button to remove the selected group entry from the Tag-based group table.

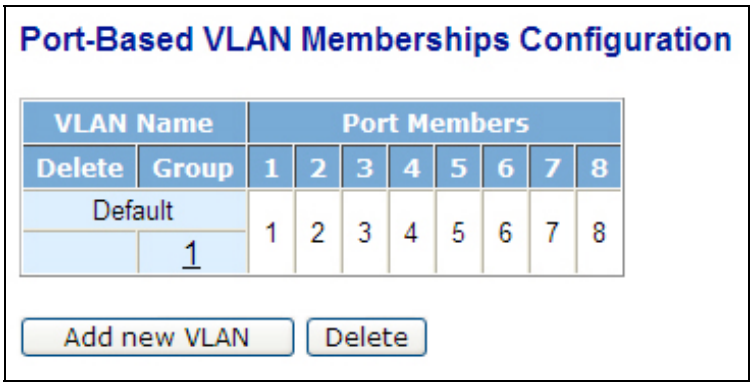


Figure 4-25. Port-based VLAN memberships configuration.

NOTE: If you need use the PVLA (Private VLAN) function on the switch, follow the process described below:

1. Create a VLAN as a primary VLAN, assign the VLAN ID as 2, then instruct the Private VLAN to enable Private VLAN service.

2. Assign port members to the VLAN2.

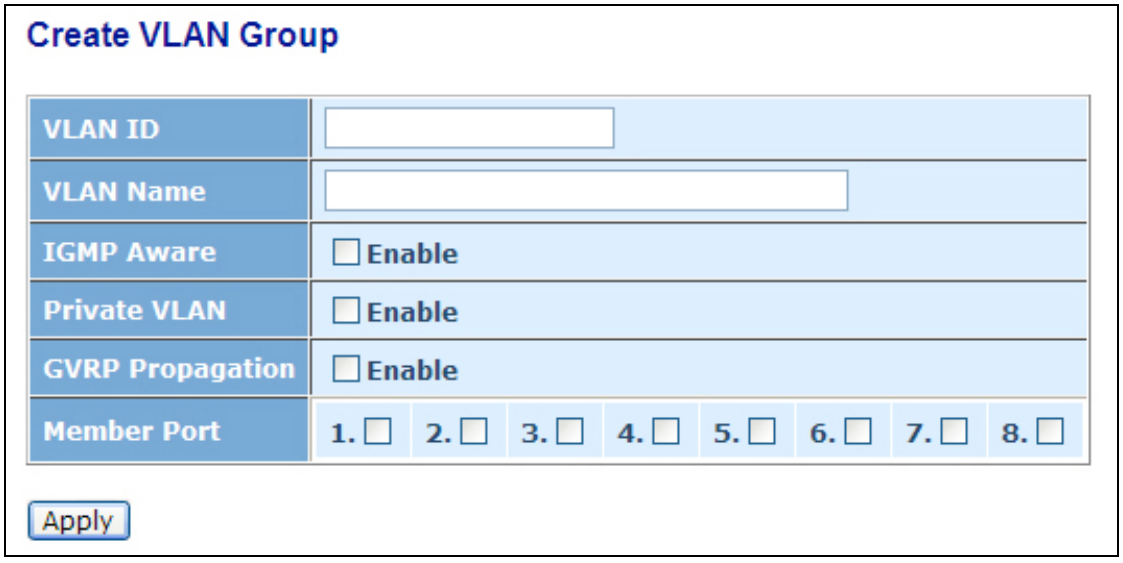


Figure 4-26. Create VLAN group.

3. Assign isolated ports.

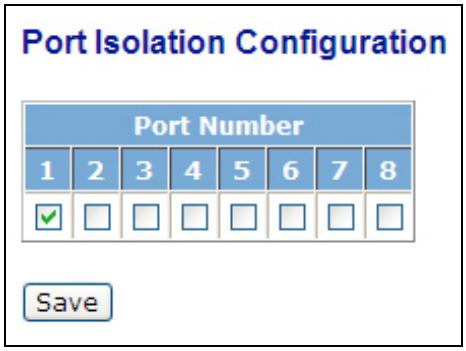


Figure 4-27. Port isolation configuration.

Press the **"Save"** button to complete the PVLAN configuration process.

4.4.3 Port-based Group

Function name: Port-based Group Configuration

Function description: Shows the information for the existing port-based VLAN groups. To create, edit, and delete a Port-based VLAN group, press the <Add>, <Edit>, and <Delete> function buttons. To add a new VLAN group, input a new VLAN name.

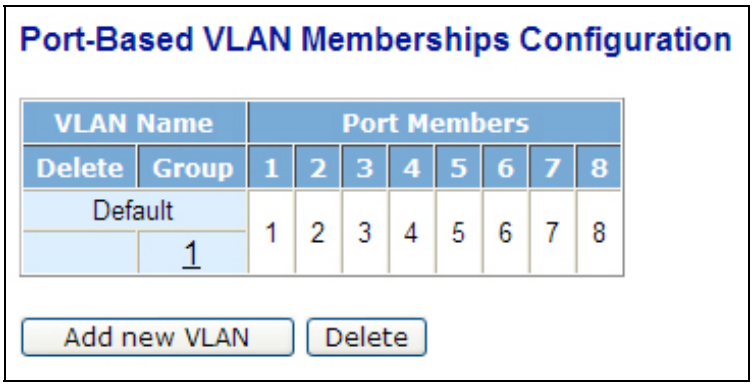


Figure 4-28. Port-based VLAN memberships configuration.

Parameter description:

VLAN Name: The name defined by the administrator is associated with a VLAN group. Valid letters are A–Z, a–z, 0–9, " - " and "_" characters. The maximum length is 15 characters.

Member Port: Enable or disable port members in the new added VLAN. "Enable" means it is a member of the VLAN. Just click on the check box (☑) beside the port x to enable it.

Add new VLAN: Create a new Port-based VLAN. Input the VLAN name and choose the member by clicking on the check box beside the port No., then, press the <Apply> button and the setting will take effect.

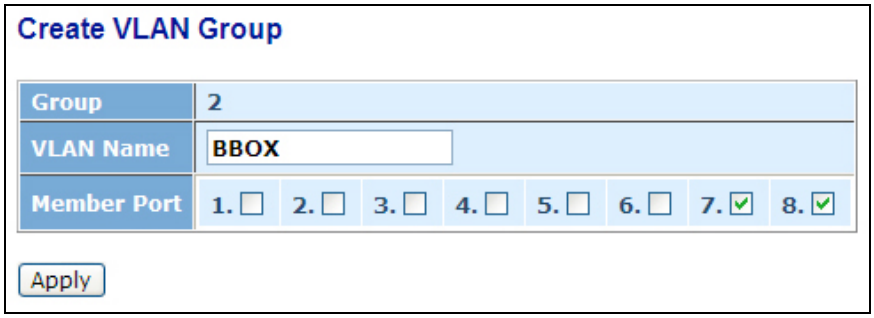


Figure 4-29. Create VLAN group.

Delete Group:

Press the **<Delete>** button to remove the selected group entry from the Port-based group table.

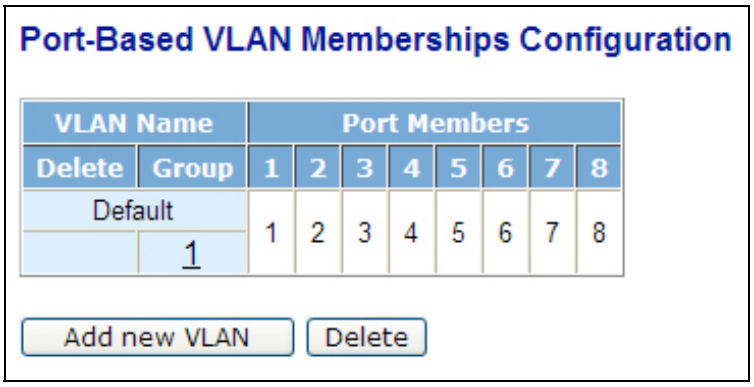


Figure 4-30. Port-based VLAN memberships configuration.

4.4.4 Ports

Function name: VLAN Port Configuration

Function description: In VLAN Tag Rule Setting, users can input the VID number for each port. The VID numbers range from 1 to 4094. Users also can assign ingress filtering rules to each port. There are two ingress filtering rules that apply to the switch. The Ingress Filtering Rule 1 is "forward only packets with VID matching this port's configured VID." The Ingress Filtering Rule 2 is "drop untagged frame." You can also select each port's role: Access, Trunk, or Hybrid.

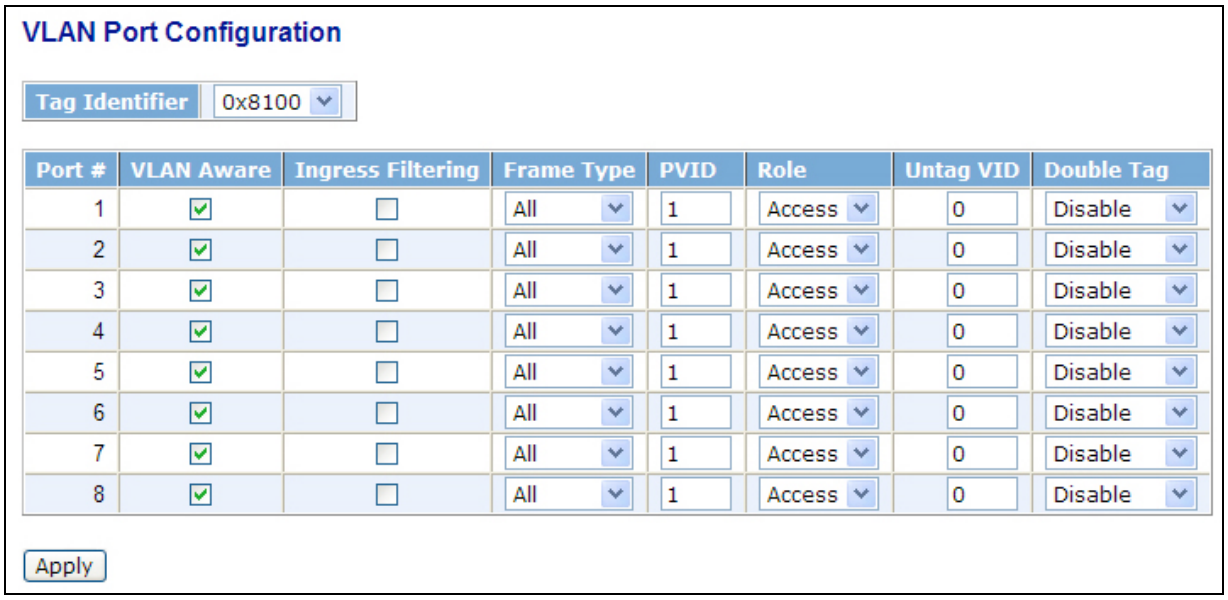


Figure 4-31. VLAN port configuration screen.

Parameter description: Port 1-8: Port number.

VLAN Aware: Forward packets based on IEEE 802.1Q VLAN tag.

Ingress Filtering: Discard other VLAN group packets, only forward packets belonging to this VLAN group.

Frame Type: All: Forward all tagged and untagged packets.

Tagged: Forward tagged packets only and discard untagged packets.

PVID: This PVID range is 1–4094. Before you set a number x as PVID, you must create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the port x's PVID (assume it is VID y) to tag this packet, and the packet then will be forwarded as a tagged packet with VID y.

Role: This is a port egress rule. Choose Access, Trunk, or Hybrid. Access means the outgoing packets carry no VLAN tag header. Trunk means the outgoing packets must carry a VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will not be dropped. Hybrid is similar to Trunk, and both will tag-out. When the port is set to Hybrid, its packets will be untagged if the outgoing packets' tagged VID is the same as the one in this port's Untagged VID.

Untag VID: Valid range is 1–4094. It works only when Role is set to Hybrid.

Double Tag: Double-tag mode belongs to the tag-based mode; however, it would treat all frames as untagged, which means that tags with PVID will be added into all packets. Then, these packets will be forwarded as a Tag-based VLAN. The incoming packets with tag will become the double-tag ones. Scroll to enable the function. The default is Disable.

4.4.5 Management VLAN

Function name: Management VLAN

Function description: Used to assign a specific VLAN for management purpose.

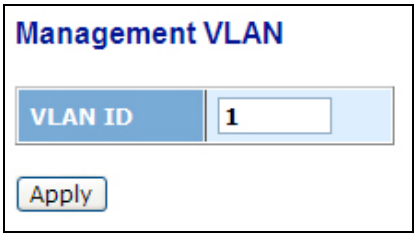


Figure 4-32. Management VLAN screen.

Parameter description: VID: Specific Management VLAN ID.

4.5 MAC

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to a function type. They are described below.

4.5.1 Mac Address Table

Function name: MAC Address Table Information

Function Description: This function can allow the user to set up the MAC Table processing mechanis. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-1000000 seconds, and the setup of this time will have no effect on static MAC addresses.

In addition, the number of MACs that each port can learn are limited.

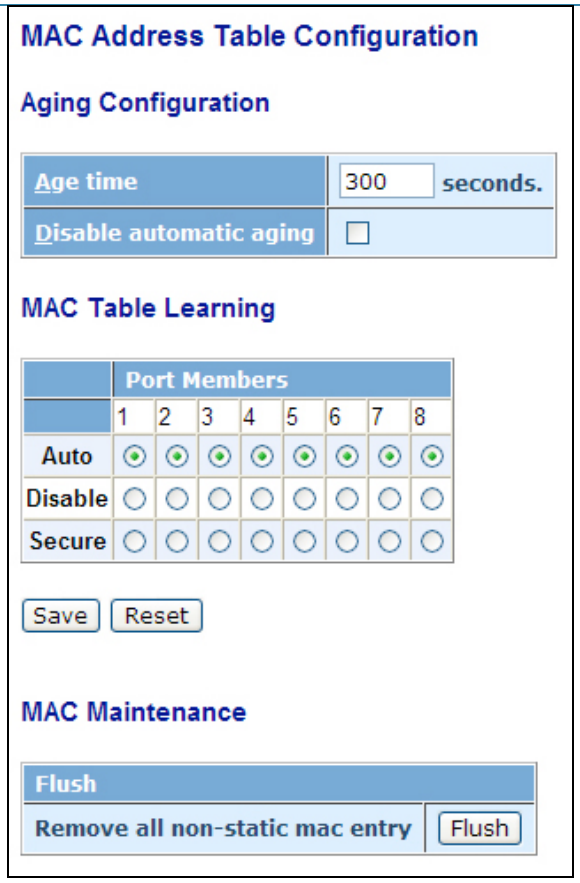


Figure 4-33. MAC address table configuration screen.

Parameter description:

Aging Time: Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.

Disable automatic aging: Stop the MAC table aging timer. The learned MAC address will not age out automatically.

Auto: Enable this port's MAC address dynamic learning mechanism.

Disable: Disable this port's MAC address dynamic learning mechanism, only support static MAC address settings.

Secure: Disable this port's MAC address dynamic learning mechanism and copy the dynamic learning packets to a CPU.

Save: Save MAC Address Table configuration.

Reset: Reset MAC Address Table configuration.

4.5.2 Static Filter

Function name: Static Filter

Function Description: Static Filter is a function that denies the packet forwarding if the packet's MAC Address is listed in the filtering Static Filter table. User maintain the table by filling in MAC Address, VID (VLAN ID), and Alias fields individually. Or delete the existing entry by clicking on the <Delete> button.

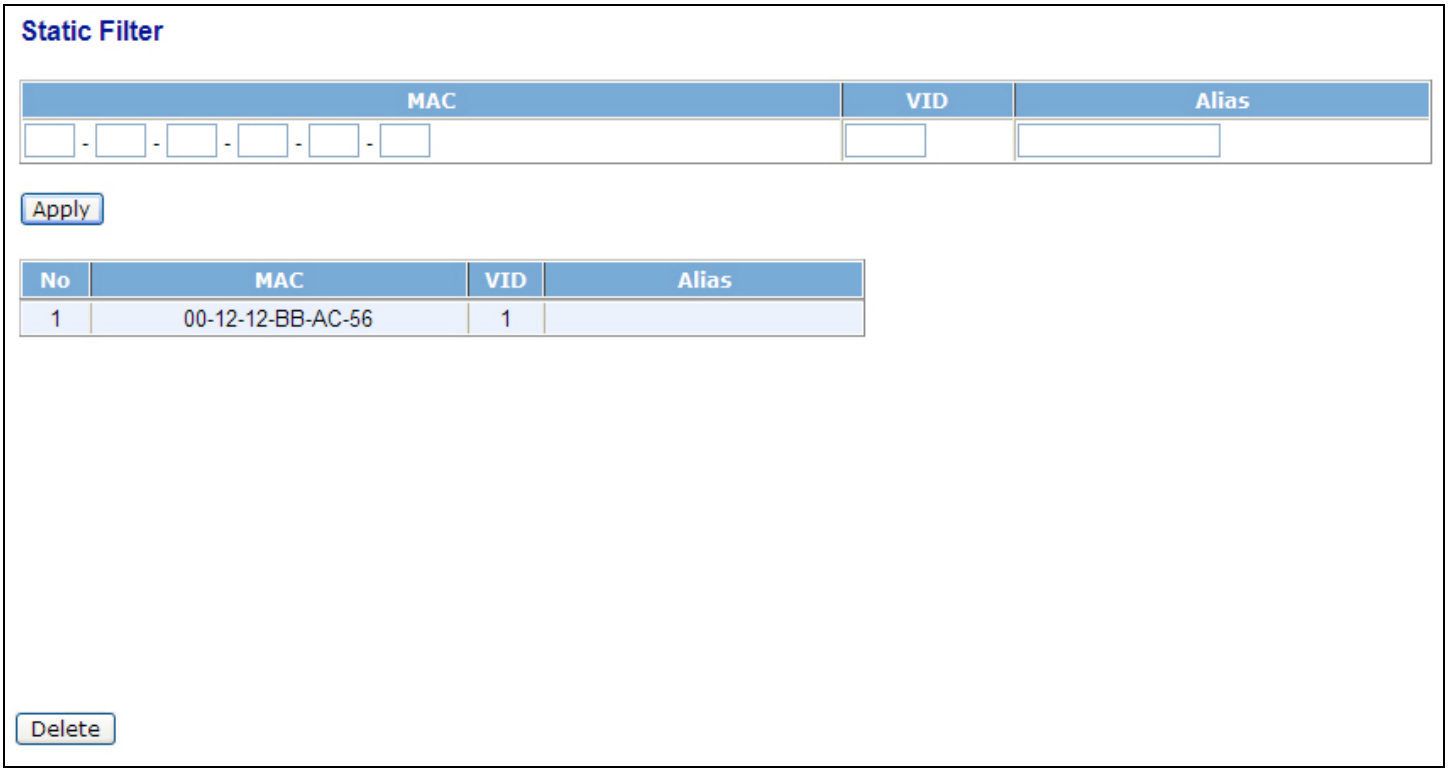


Figure 4-34. Static filter screen.

Parameter description: MAC is a six-byte long Ethernet hardware address that's usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 – 02.

VID: VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1–4094.

Alias: MAC alias name you assign.

4.5.3 Static Forward

Function Name: Static Forward

Function Description: Static Forward is a function that allows the user in the static forward table to access a specified port of the switch. The Static Forward table associated with a specified port of a switch is set up by manually inputting a MAC address and its alias name.

When a MAC address is assigned to a specific port, all of the switch's traffic sent to this MAC address will be forwarded to this port.

To add a MAC address entry in the allowed table, you need to fill in four parameters: MAC address, associated port, VID and Alias. To remove a MAC address, select the existing MAC address entry you want and click on the <Delete> button.

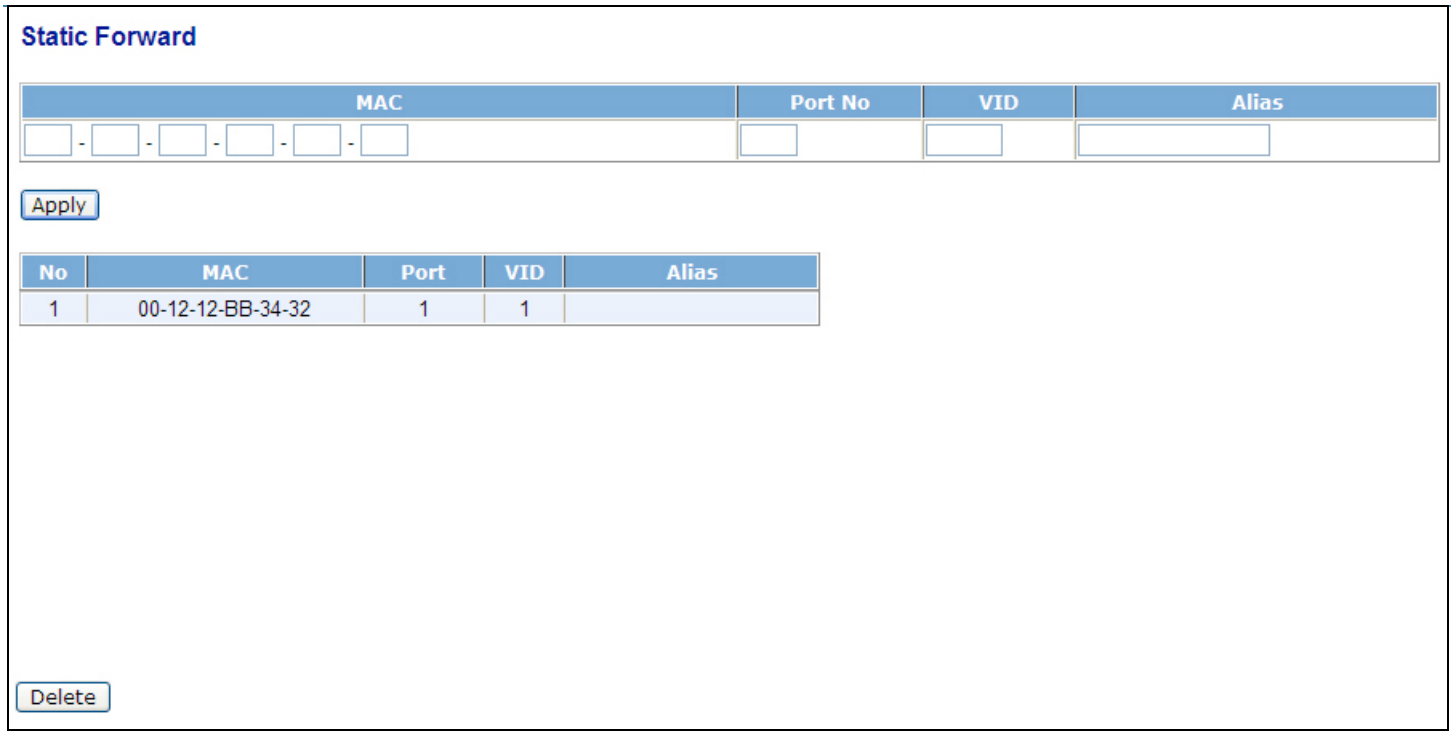


Figure 4-35. Static forward screen.

Parameter description: MAC is a six-byte long Ethernet hardware address that's usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 – 01.

Port No: The port number of the switch is 1–8.

VID: VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1– 4094.

Alias: MAC alias name you assign.

4.5.4 MAC Alias

Function name: MAC Alias

Function description: MAC Alias function is used to let you assign MAC address a plain English name. This will help you tell which MAC address belongs to which user in the illegal access report. At the initial time, it shows all pairs of the existing alias name and MAC address.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit, and MAC Alias Delete. Click on the <Create/Edit> button to add/modify a new or an existing alias name for a specified MAC address, or mark an existed entry to delete it. The alias name must be composed of A-Z, a-z and 0-9 only and can be a maximum 15 characters long.

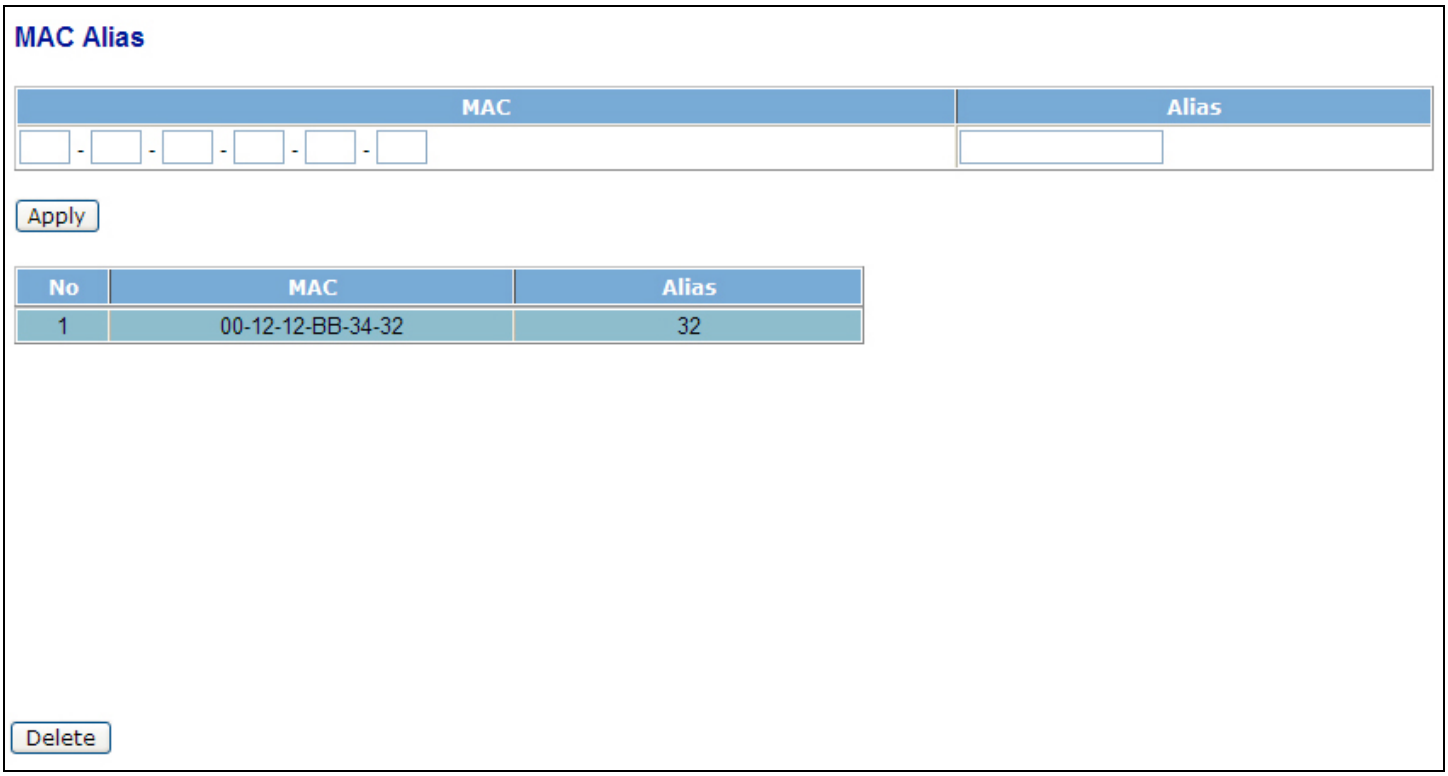


Figure 4-36. MAC alias screen.

Parameter description: MAC Address is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 – 01.

Alias: MAC alias name you assign.

NOTE: If there are too many MAC addresses already in the table, type in the MAC address and alias name directly.

4.5.5 MAC Table

Function name: MAC Table

Function Description: Display the static or dynamic learning MAC entry and the state for the selected port.

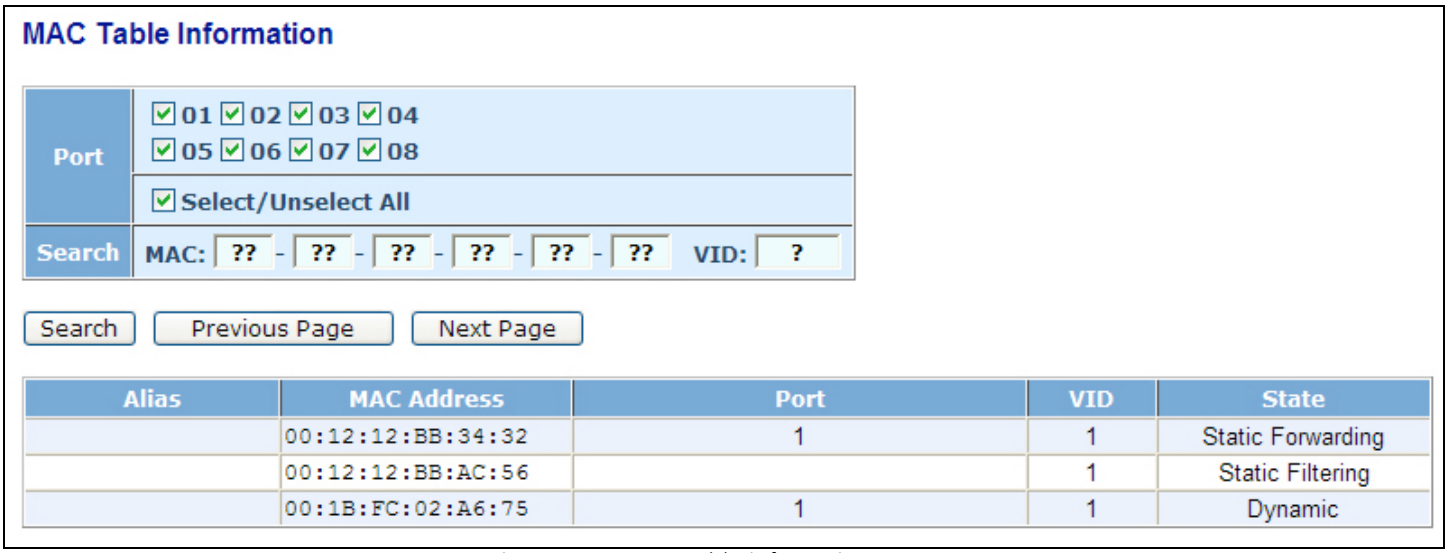


Figure 4-37. MAC table information screen.

Parameter description:

Alias: MAC alias name you assign.

MAC address: Display the MAC address of one entry you selected from the MAC entries table.

Port: The port for the searched MAC Entry.

VID: VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1– 4094.

Status: Dynamic or Static MAC address information.

Refresh: The Refresh function can help you see the current MAC Table status.

Clear: Clears the selected entry.

Previous Page: Move to the previous page.

Next Page: Move to the next page.

4.6 PoE

Function name: PoE Configuration

Function description: In the PoE Port Management function, user can configure the PoE settings.

The switch complies with IEEE 802.3af protocol and is capable of detecting automatically whether the device linked to the port on the switch is a PD (Powered Device) or not. The switch also manages the power supplement based on the Class of the PD, and it will stop supplying the power once the power required by the PD exceeds the Class, or a Short Circuit or over temperature occurs.

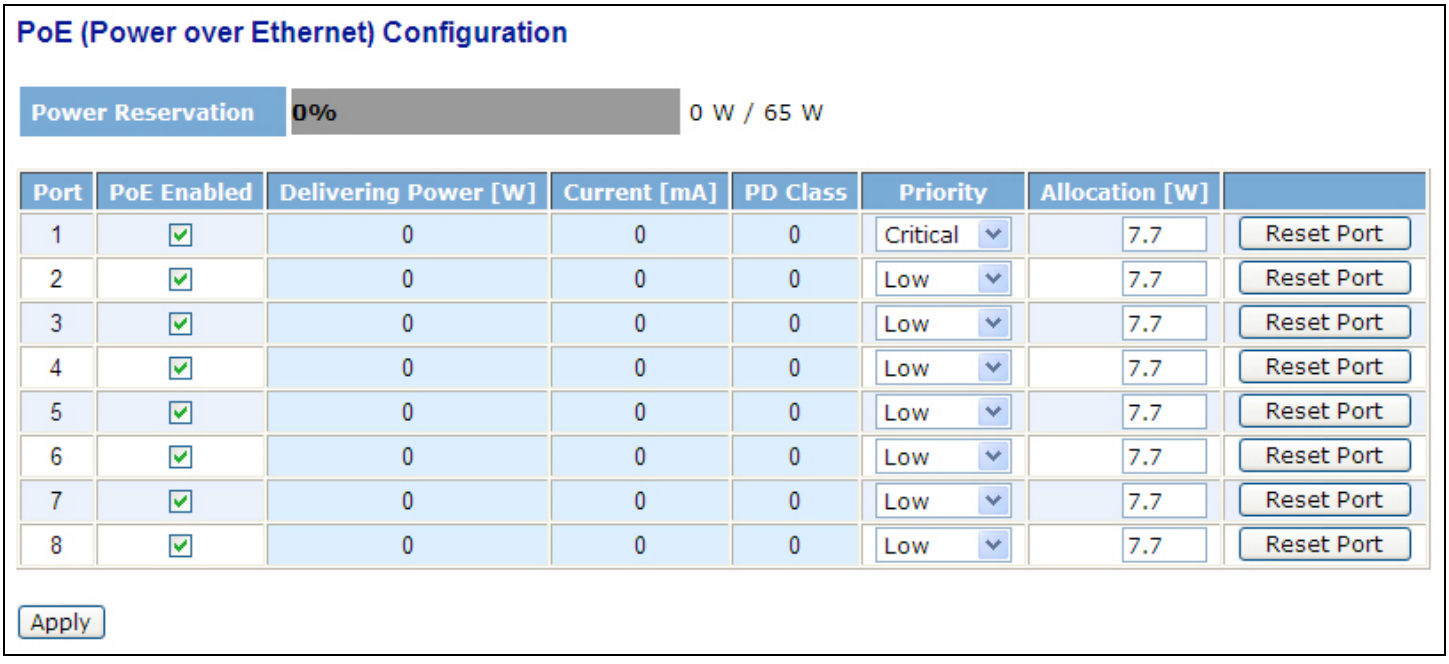


Figure 4-38. PoE configuration.

Parameter description:

Power Reservation: The Power Reservation means the switch is ready to link and supply the power to the PD. The latter means the all ports are supplying a percentage of the power reservation

Port: The port that supplies the power to the PD. The latter means the port is supplying the power.

PoE Enabled: Enables which port supply the power to the PD.

Delivering Power [W]: Displays which port supplies the PD Power and shows the power consumed by the port.
Current (mA): The current supplied to the PD by the port.

PD Class: The Class of the PD linked to the switch's port.

Priority: Choose from three options: Normal, Low, and High. Default is Normal. The switch will stop supplying the power to the port based on the order of the priority Low→Normal→High in case total power required by all PDs linked to the switch exceeds the power limit. IFf the ports have the same priority, then the switch will stop supplementing power from the port with the highest port id (8→1).

Allocation (W): The power consumed by the port.

4.7 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP provides the VLAN registration service through a GARP application. It uses GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machines maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate this information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

In GVRP Configuration function folder, there are three functions supported: GVRP Config, GVRP Counter, and GVRP.

4.7.1 Config

Function name: GVRP Configuration

Function description: GVRP Config is used to configure each port's GVRP operation mode. Seven parameters need to be configured as described below.

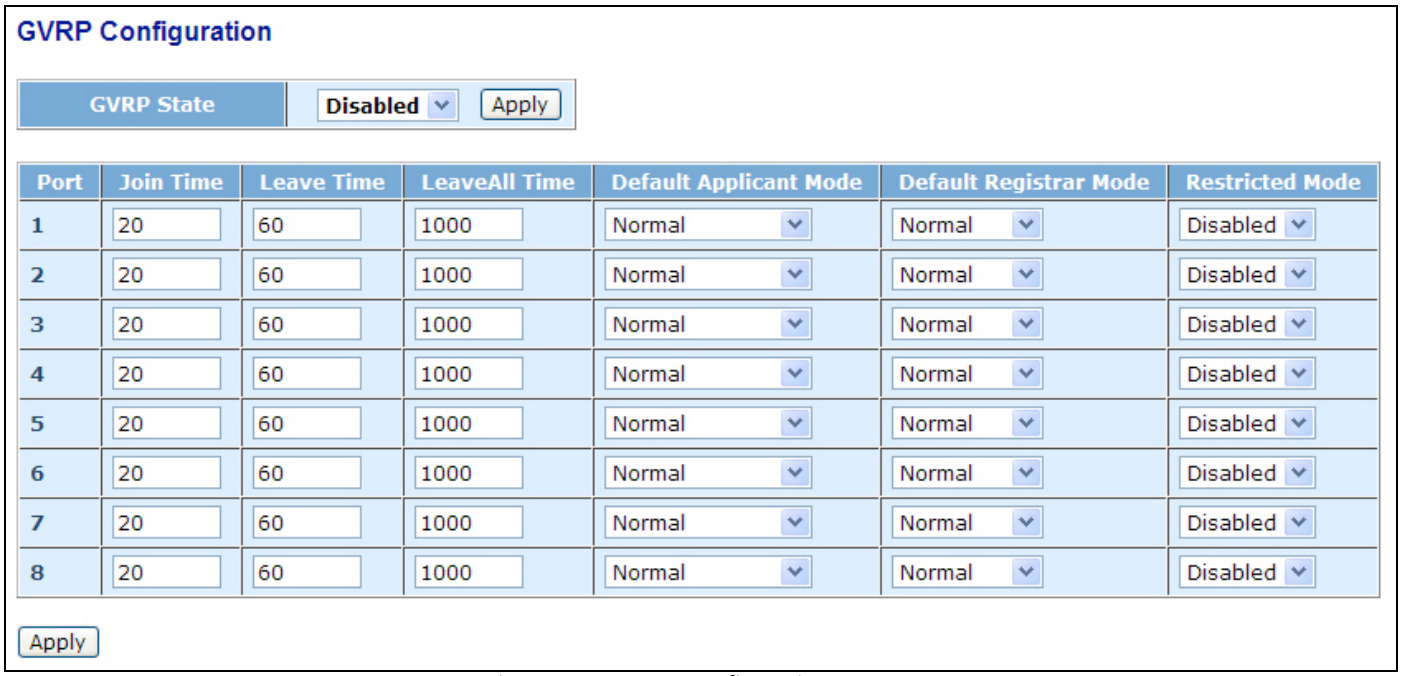


Figure 4-39. GVRP configuration screen.

Parameter description:

GVRP State: This function lets you enable or disable the GVRP function. From the drop-down list, click on the the <Downward> arrow key to choose "Enable" or "Disable." Then, click on the <Apply> button and the system will take effect immediately.

Join Time: Used to declare the Join Time in unit of centisecond. Valid time range: 20–100 centisecond, Default: 20 centisecond.

Leave Time: Used to declare the Leave Time in unit of centisecond. Valid time range: 60–300 centisecond, Default: 60 centisecond.

Leave All Time: A time period to announce that all registered devices are going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000–5000 unit time, Default: 1000 unit time.

Default Applicant Mode: The participent type. Select from two modes: normal participant and non-participant.

Normal: Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.

Non-Participant: In this mode, the switch does not send or reply any GARP messages. It just listens to messages and reacts to the received GVRP BPDU.

Default Registrar Mode: The Registrar type. Choose from three administrative control value modes: normal registrar, fixed registrar, and forbidden registrar.

Normal: Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed: Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden: Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

Restricted Mode: This function restricts a dynamic VLAN from being created when this port receives a GVRP PDU. Choose Enable or Disable.

Disabled: In this mode, a dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

Enabled: In this mode, the switch does not create a dynamic VLAN when this port receives GVRP PDU. Unless a dynamic VLAN GVRP PDU message exists as a static VLAN in the switch, this port will be added into the static VLAN members dynamically.

4.7.2 Counter

Function name: GVRP Counter

Function description: All GVRP counters are mainly divided into Received and Transmitted. These two categories enable you to monitor the GVRP actions. Actually, they are GARP packets.

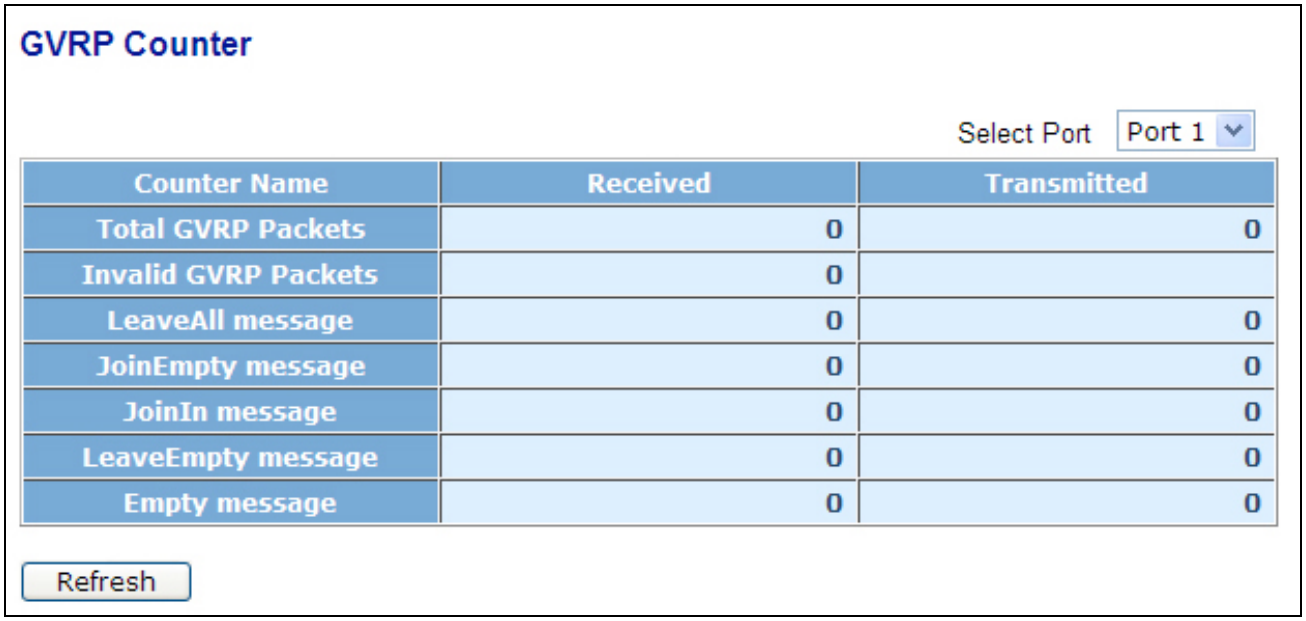


Figure 4-40. GVRP counter screen.

Parameter description:

Total GVRP Packets: Total GVRP BPDU received by the GVRP application.

Invalid GVRP Packets: Number of invalid GARP BPDU received by the GARP application.

LeaveAll Message Packets: Number of GARP BPDU with Leave All message received by the GARP application.

JoinEmpty Message Packets: Number of GARP BPDU with Join Empty message received by the GARP application.

JoinIn Message Packets: Number of GARP BPDU with Join In message received by the GARP application.

LeaveEmpty Message Packets: Number of GARP BPDU with Leave Empty message received by the GARP application.

Empty Message Packets: Number of GARP BPDU with Empty message received by the GARP application.

4.7.3 Group

Function name: GVRP Group VLAN Information

Function description: Show the group members and their information.

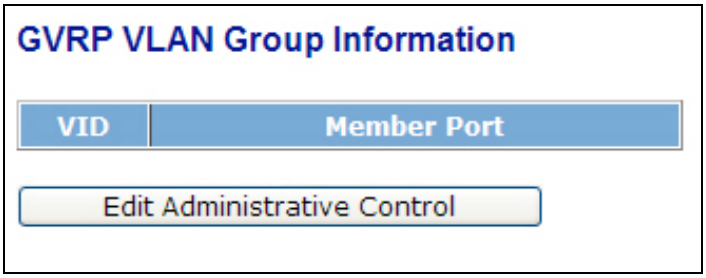


Figure 4-41. GVRP VLAN group information.

Parameter description:

VID: VLAN identifier. When GVRP group is created, each dynamic VLAN group owns its VID. Valid range is 1–4094.

Member Port: Members belonging to the same dynamic VLAN group.

Edit Administrative Control: When you create GVRP group, you can use the Administrative Control function to change the Applicant Mode and the Registrar Mode of a GVRP group member.

4.8 QoS (Quality of Service) Configuration

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. There are 8 QoS Control Lists (QCL) for advanced programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP, and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms that provide excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue has dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

4.8.1 Ports

Function name: Port QoS Configuration

Function description: Configure each port's QoS behavior. There are four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP, and UDP/TCP ports and ranges.

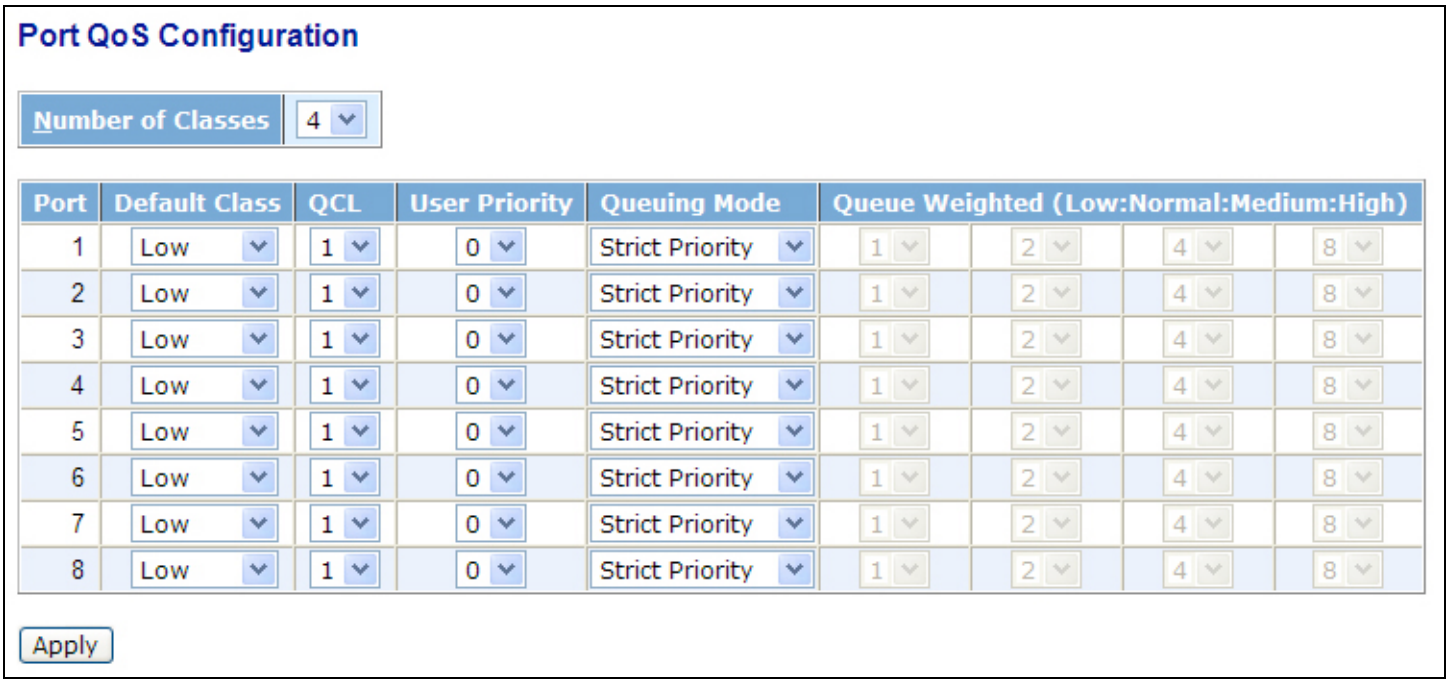


Figure 4-42. Port QoS configuration.

Parameter description:

Number of Classes: 1/2/4

Port: Users can choose ports (1–8) respectively with Priority Class for Per Port Priority function.

Default Class: Users can set up High Priority or Low Priority for each port respectively.

Low/Normal/Medium/High

QCL: The number of QCL rules 1–24. Each port has to apply one of the QCL rules for QoS behavior.

User priority: The user priority value 0~7 (3 bits) is used as an index to the eight QoS class values for VLAN tagged or priority tagged frames.

Queuing Mode: There are two Scheduling Methods, Strict Priority and Weighted Fair. The default is Strict Priority. After you choose a Scheduling Method, click on the Apply button.

Queue Weighted: There are four queues per port and four classes weighted number (1/2/4/8) for each queues. Select the weighted number when the scheduling method is set to “Weighted Fair” mode.

4.8.2 Qos Control List

Function name: QoS Control List Configuration

Function description: The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ether Type, VID, IPv4/IPv6 DSCP, and UDP/TCP ports and ranges.

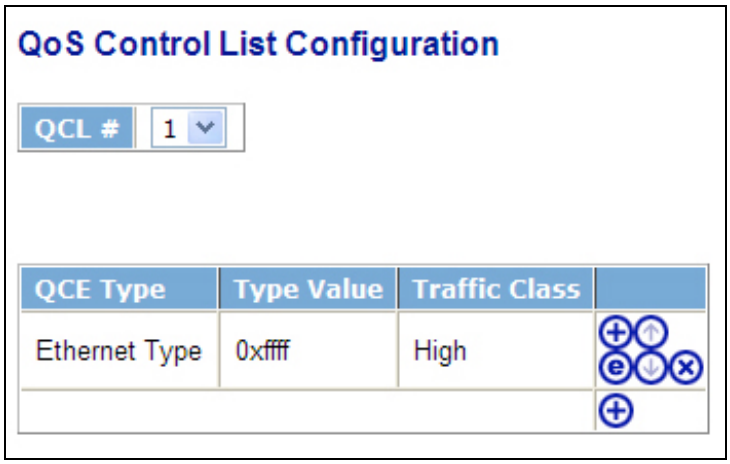


Figure 4-43. QoS control list configuration screen.

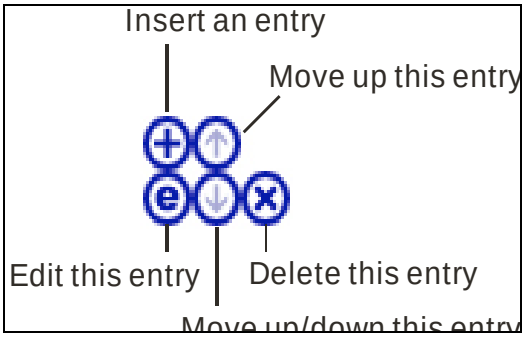


Figure 4-44. Entry priority.

QCE Configuration: The QCL searches of 12 QoS Control Entries (QCEs) from the top of the list to the bottom of the list for a match. The first matching QCE determines the frame's QoS classification. The QCE ordering is important for the resulting QoS classification algorithm. If no matching QCE is found, the default QoS class is used in the port QoS configuration.

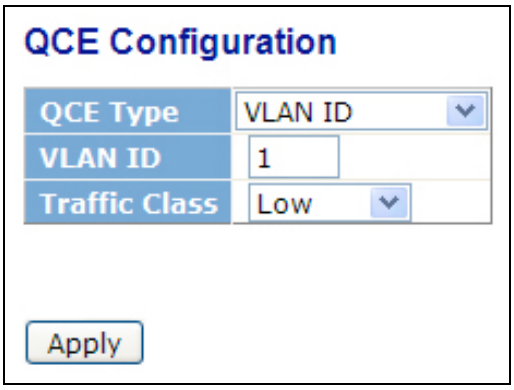


Figure 4-45. QCE configuration screen, QCE type.

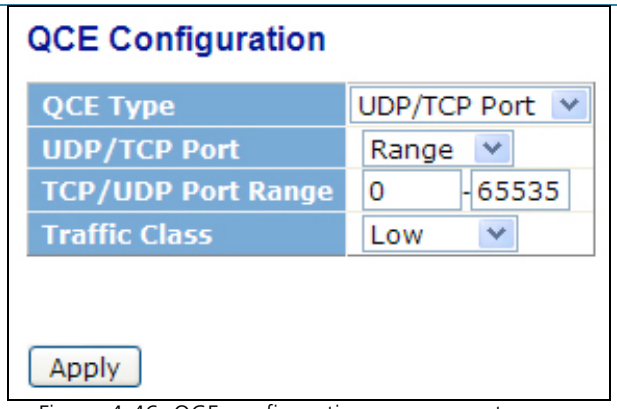


Figure 4-46. QCE configuration screen, port range.

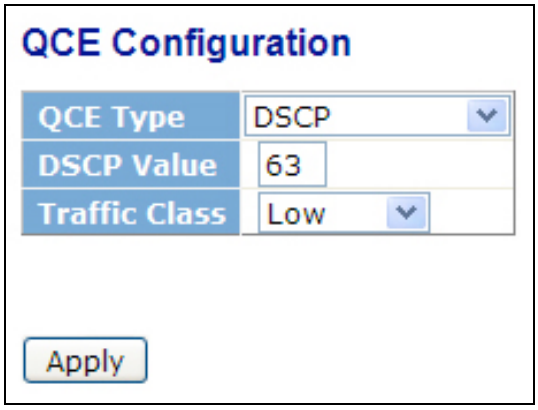


Figure 4-47. QCE configuration screen, DSCP type.

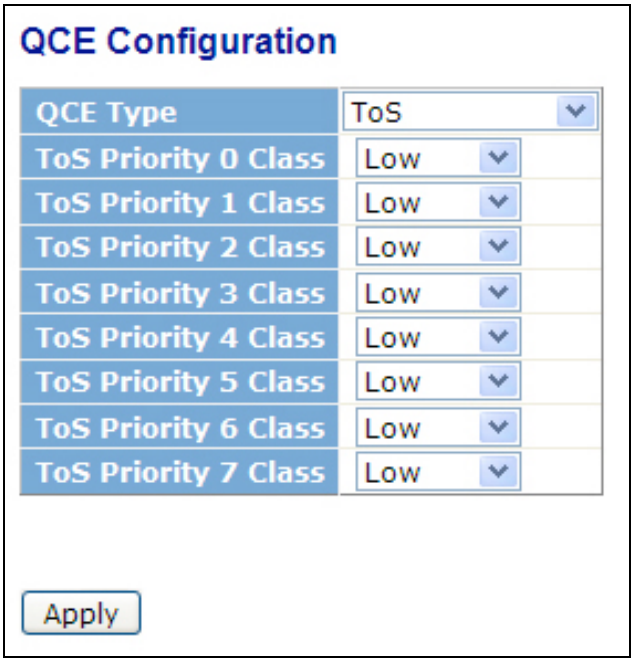


Figure 4-48. QCE configuration screen, ToS priority class.

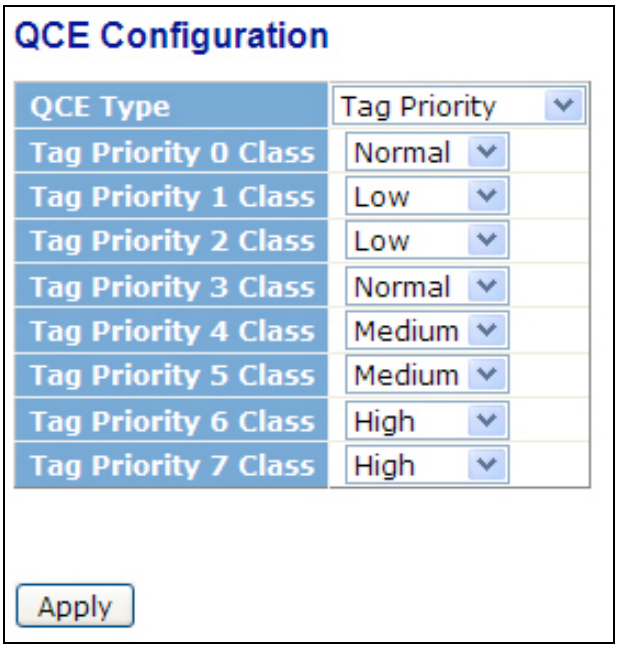


Figure 4-49. QCE configuration screen, tag priority class.

Parameter description:

QCL#:

QCL number: 1–24

QCE Type: Ethernet Type/VLAN ID/UDP/TCP Port/DSCP/ToS/Tag Priority

Ethernet Type Value: The configurable range is 0x600–0xFFFF. Well known protocols already assigned EtherType values. The commonly used values in the EtherType field and corresponding protocols are listed below:

Ethertype (Hexadecimal)	Protocol
0x0800	IP, Internet Protocol
0x0801	X.75 Internet
0x0802	NBS Internet
0x0803	ECMA Internet
0x0804	Chaosnet
0x0805	X.25 Level 3
0x0806	ARP, Address Resolution Protocol.
0x0808	Frame Relay ARP [RFC1701]
0x6559	Raw Frame Relay [RFC1701]
0x8035	DRARP, Dynamic RARP. RARP, Reverse Address Resolution Protocol.
0x8037	Novell Netware IPX

0x809B	EtherTalk (AppleTalk over Ethernet)
0x80D5	IBM SNA Services over Ethernet
0x 80F3	AARP, AppleTalk Address Resolution Protocol.
0x8100	IEEE Std 802.1Q - Customer VLAN Tag Type.
0x8137	IPX, Internet Packet Exchange.
0x 814C	SNMP, Simple Network Management Protocol.
0x86DD	IPv6, Internet Protocol version 6.
0x880B	PPP, Point-to-Point Protocol.
0x 880C	GSMP, General Switch Management Protocol.
0x8847	MPLS, Multi-Protocol Label Switching (unicast).
0x8848	MPLS, Multi-Protocol Label Switching (multicast).
0x8863	PPPoE, PPP Over Ethernet (Discovery Stage).
0x8864	PPPoE, PPP Over Ethernet (PPP Session Stage).
0x88BB	LWAPP, Light Weight Access Point Protocol.
0x88CC	LLDP, Link Layer Discovery Protocol.
0x8E88	EAPOL, EAP over LAN.
0x9000	Loopback (Configuration Test Protocol)
0xFFFF	reserved.

VLAN ID: The configurable VID range: 1–4094

UDP/TCP Port: To select the UDP/TCP port classification method by Range or Specific.

UDP/TCP Port Range: The configurable ports range: 0–65535. You can refer to following UDP/TCP port-numbers information. http://www.iana.org/assignments/port-numbers

UDP/TCP Port No.: The configurable specific port value: 0–65535

DSCP Value: The configurable DSCP value: 0–63

Traffic Class: Low/Normal/Medium/High

4.8.3 Rate Limiters

Function name: Rate Limit Configuration

Function description: Each port includes an ingress policy, and an egress shaper, which can limit the bandwidth of received and transmitted frames. Ingress policer or egress shaper operation is controlled per port in the Rate Limit Configuration.

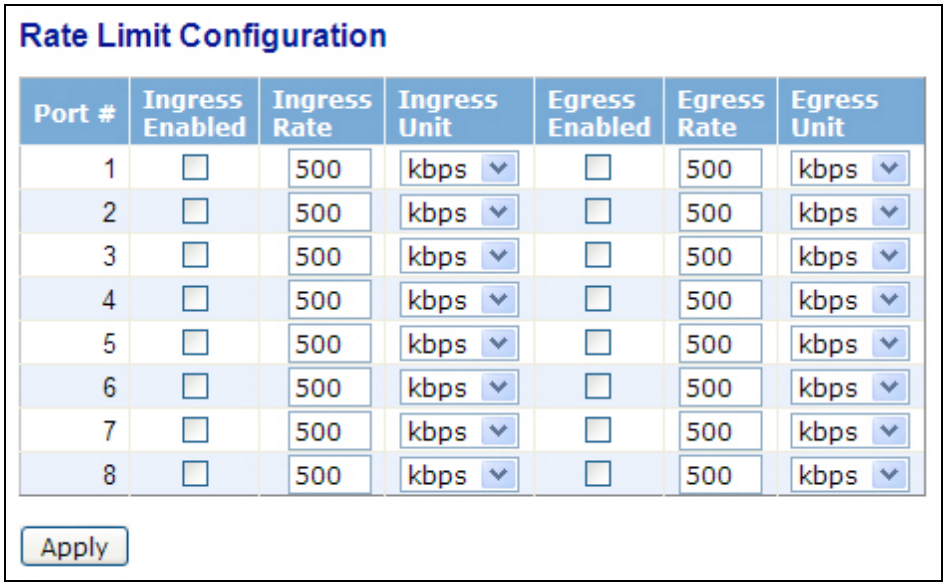


Figure 4-50. Rate limit configuration.

Parameter description:

Port #: Port number.

Ingress Enabled: Ingress enabled to limit ingress bandwidth by policy rate.

Ingress Rate: The configurable ingress rate range: 500 Kbps–1000000 kbps; 1 Mbps–1000 Mbps

Ingress Unit: There are two units for ingress rate limit: kbps/Mbps

Engress Enabled: Engress enabled to limit egress bandwidth by shaper rate.

Engress Rate: The configurable engress rate range: 500 kbps–1000000 kbps; 1 Mbps–1000 Mbps

Engress Unit: There are two units for egress shaper rate limit: kbps/Mbps.

4.8.4 Storm Control

Function name: Storm Control Configuration

Function description: The switch supports storm ingress policy control function to limit the Flooded, Multicast, and Broadcast and prevent storms.

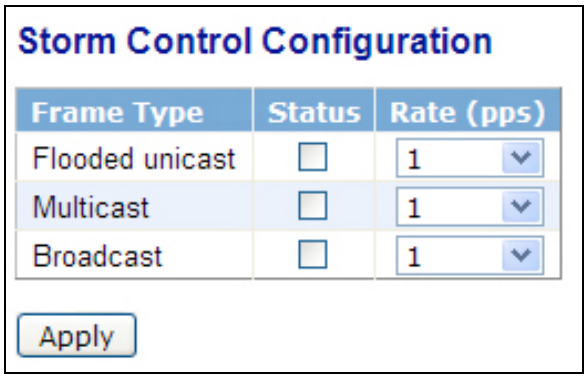


Figure 4-51. Storm control configuration.

Parameter description:

Frame Type: There three storm frame types: Flooded unicast/Multicast/Broadcast

Status: Check on square to enable.

Rate (pps): Refer to the following rate configurable value list (the units are Packets Per Second [pps]):
1/2/4/8/16/32/64/128/256/512/1K/2K/4K/8K/16K/32K/64K/128K/256K/512K/1024K

4.8.5 Wizard

Function name: Wizard

Function description: The QCL configuration Wizard configures the target users' QCL rules for QoS configuration. The wizard provides typical network application rules.

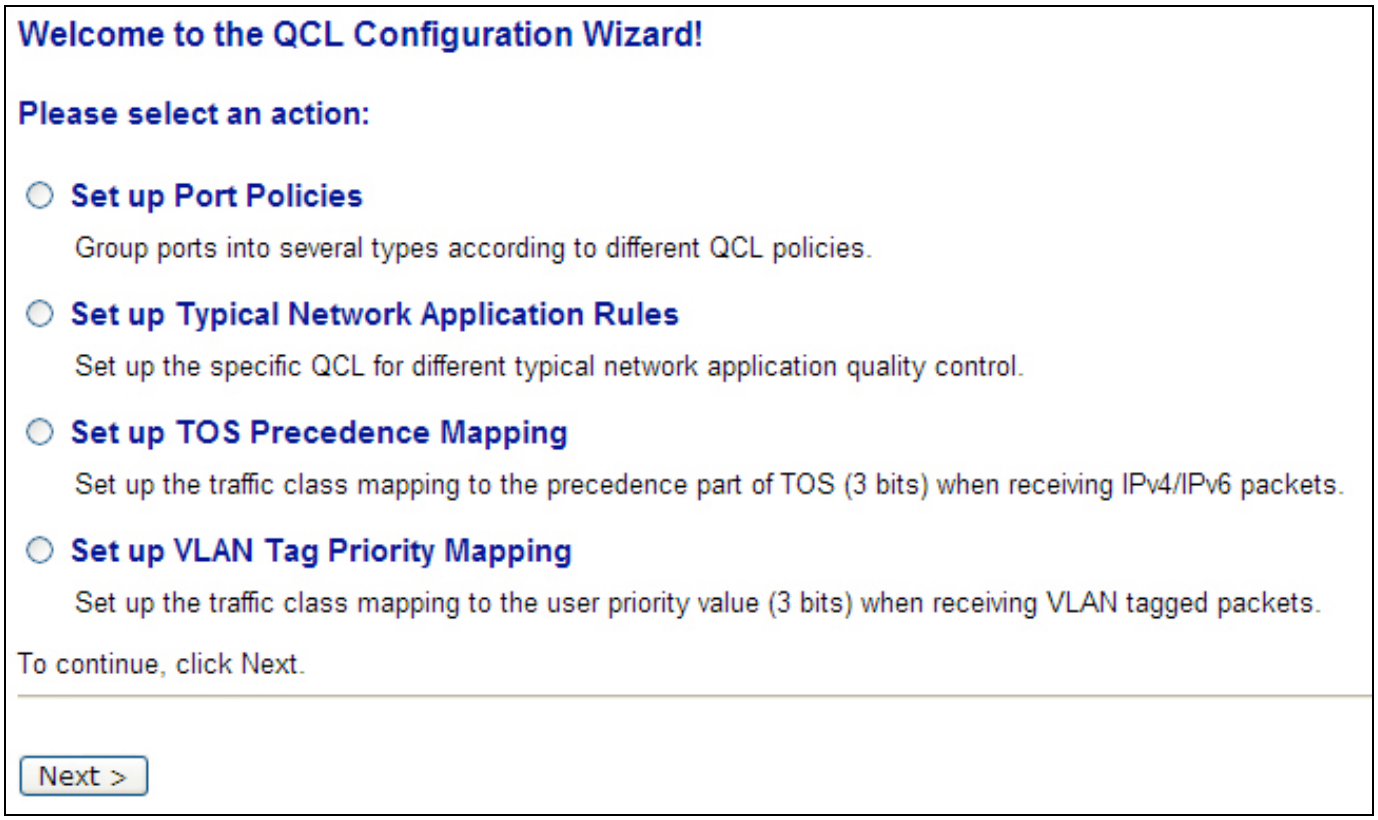


Figure 4-52. QCL configuration screen.

Parameter description:

Please select an Action: User need to select an action from the following items, then click on <Next> to finish QCL configuration:

- Set up Port Policies
- Set up Typical Network Application Rules
- Set up TOS Precedence Mapping
- Set up VLAN Tag Priority Mapping

Next: Go to next step.

Cancel: Abort current configuration back to previous step.

Back: Back to previous screen.

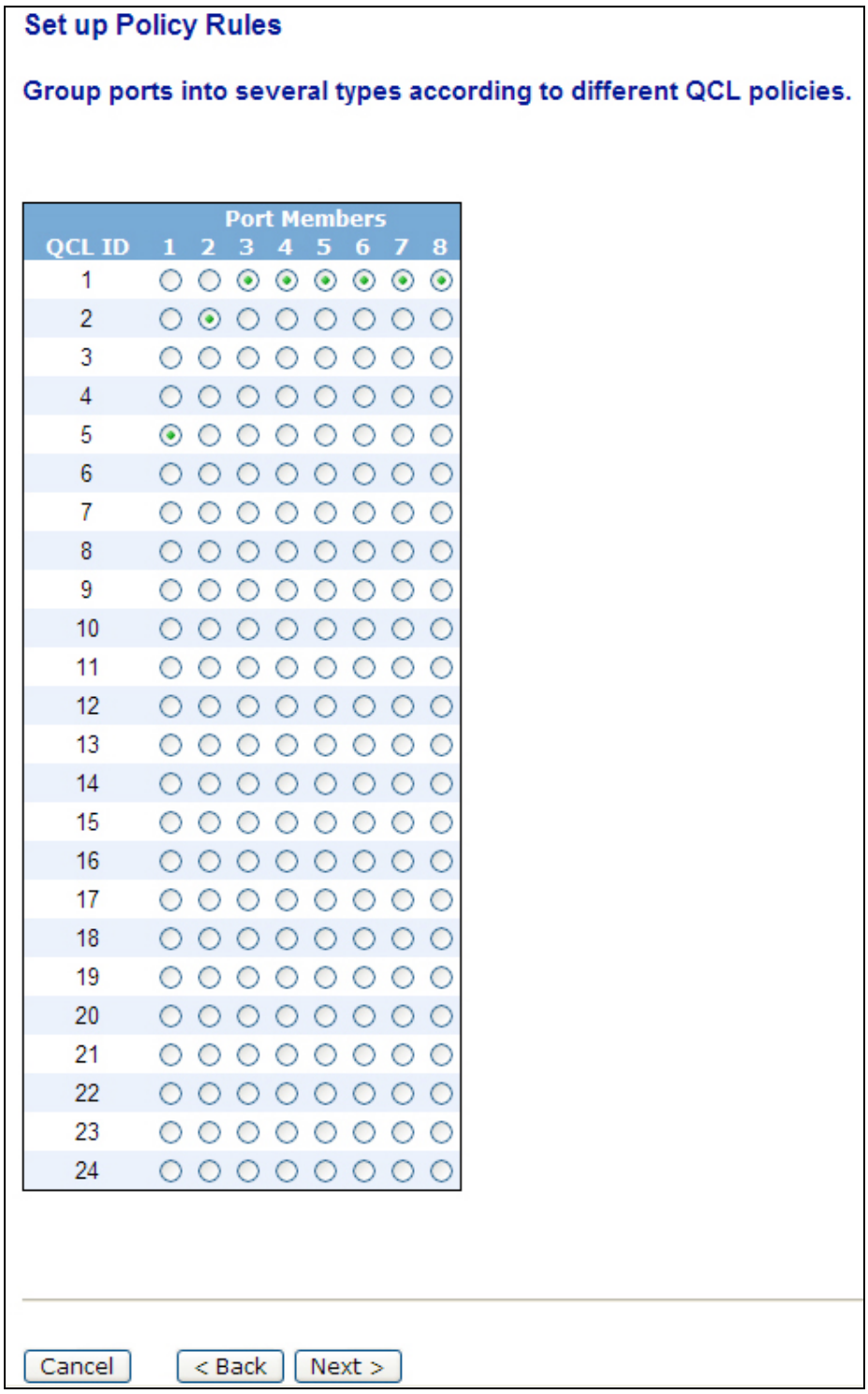


Figure 4-53. Set up Port Policies screen.

Parameter description:

QCL ID: QoS Control List (QCL): 1–24

Port Member: Port Member: 1–24

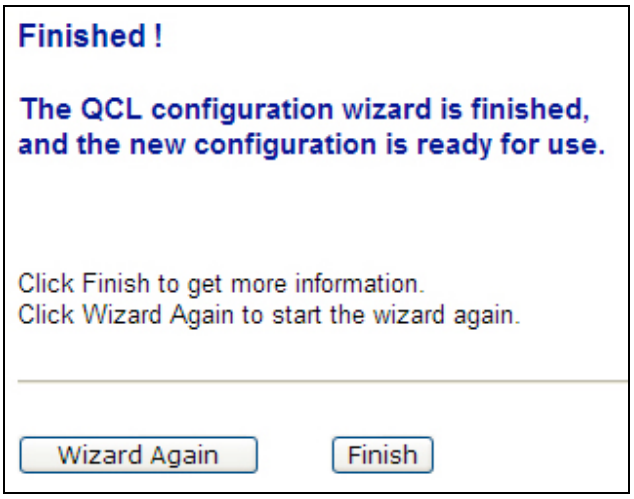


Figure 4-54. Set up Port Policies Finish screen.

Parameter description:
Wizard Again: Click on the <Wizard Again> button to go back to the QCL Configuration Wizard.

Finish: When you click on <Finish>, the parameters will be set according to the wizard configuration and shown on the screen. Click on <Apply> to confirm the changed parameters.

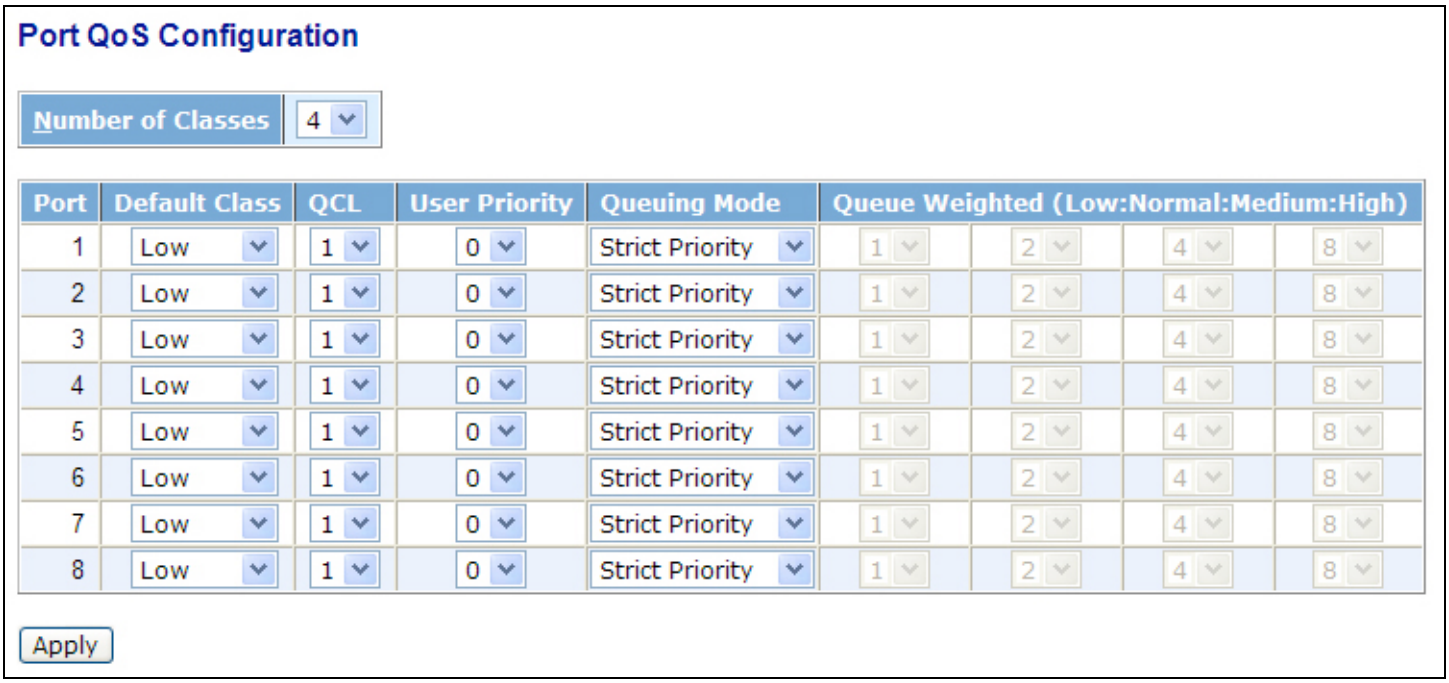


Figure 4-55. Set up Port Policies.

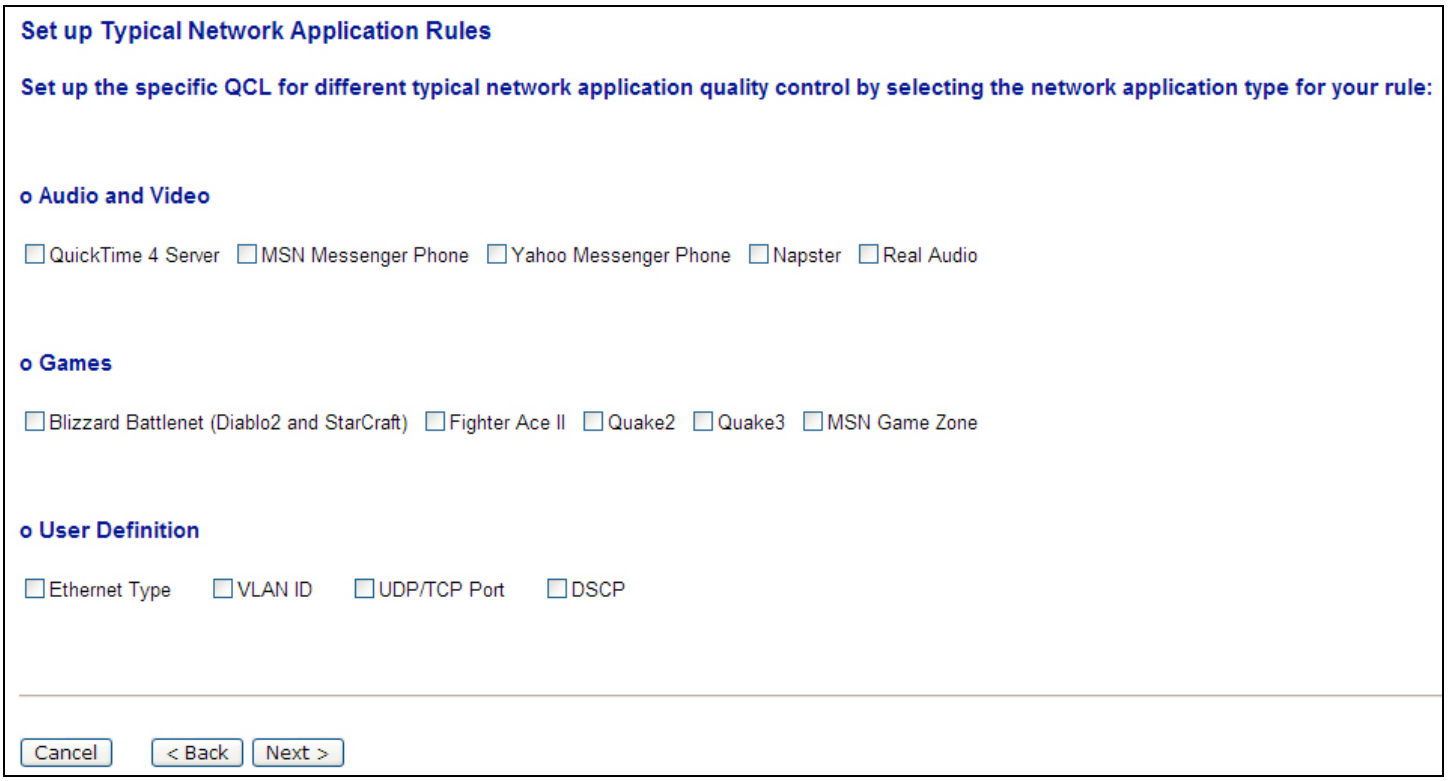


Figure 4-56. Set up Typical Network Application Rules.

Parameter description:

Audio and Video: QuickTime 4 Server/MSN Messenger Phone/Yahoo Messenger Phone/Napster/ Real Audio

Games: Blizzard Battlenet (Diablo2 and StarCraft)/Fighter Ace II/Quake2/Quake3/MSN Game Zone

User Definition: Ethernet Type/VLAN ID /UDP/TCP Port/DSCP

Ethernet Type Value: Type Range: 0x600–0xFFFF

VLAN ID: VLAN ID Range: 1–4094

UDP/TCP Port: Two Mode: Range/Specific

UDP/TCP Port Range: Port Range: 0–65535

UDP/TCP Port No.: Port Range: 0–65535

DSCP Value: DSCP Value Range: 0–63

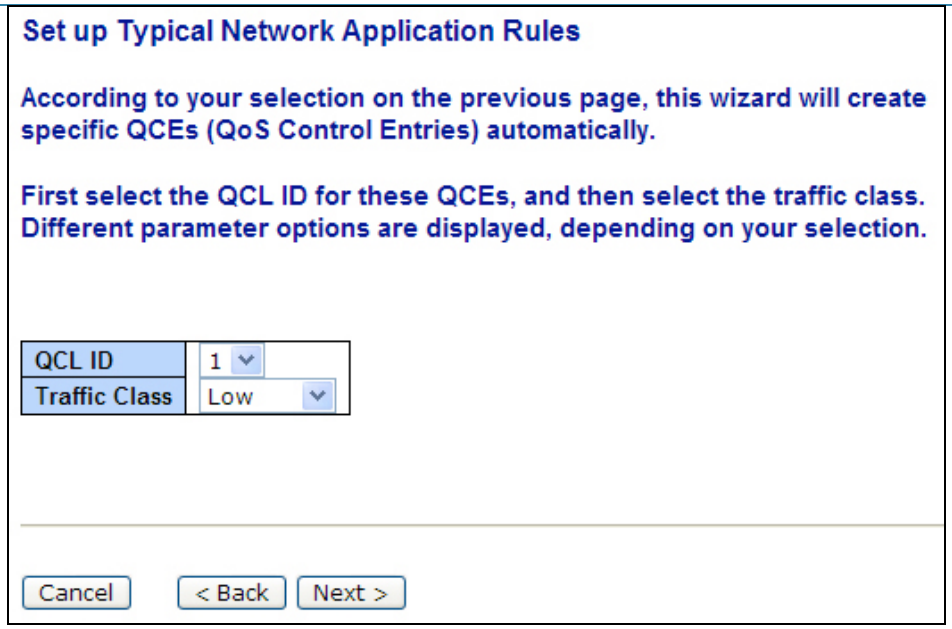


Figure 4-57. Set up Typical Network Application Rules.

Parameter description:

QCL ID: QCL ID Range: 1–24

Traffic Class: There are four classes: Low/Normal/Medium/High

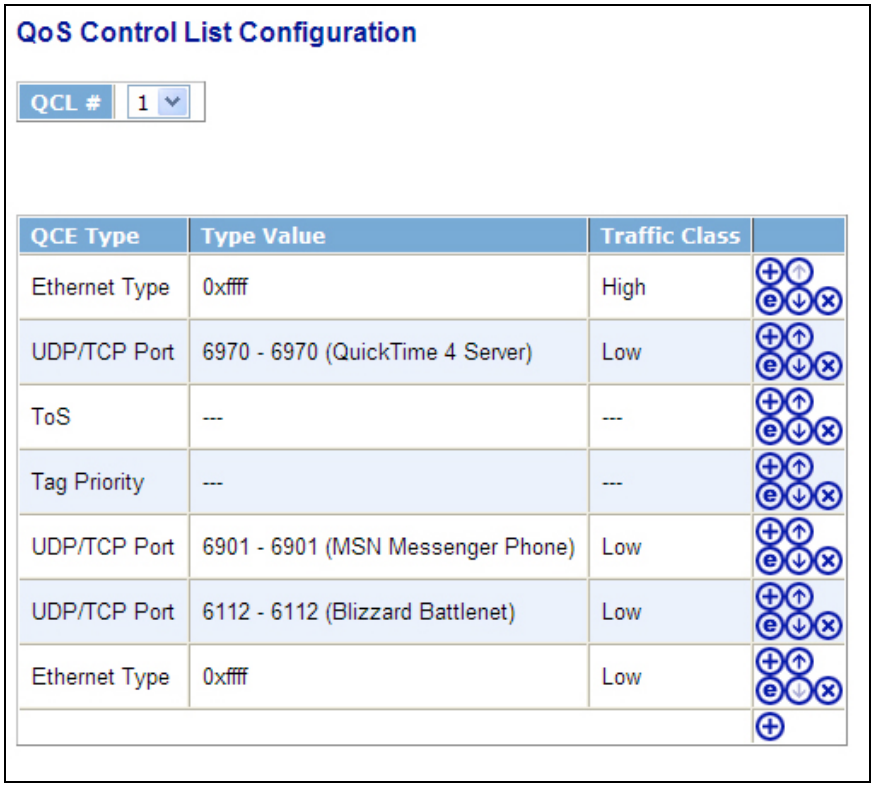


Figure 4-58. Set up Typical Network Application Rules Finish.

Parameter description:
QCL #: QoS Control List (QCL): 1–24

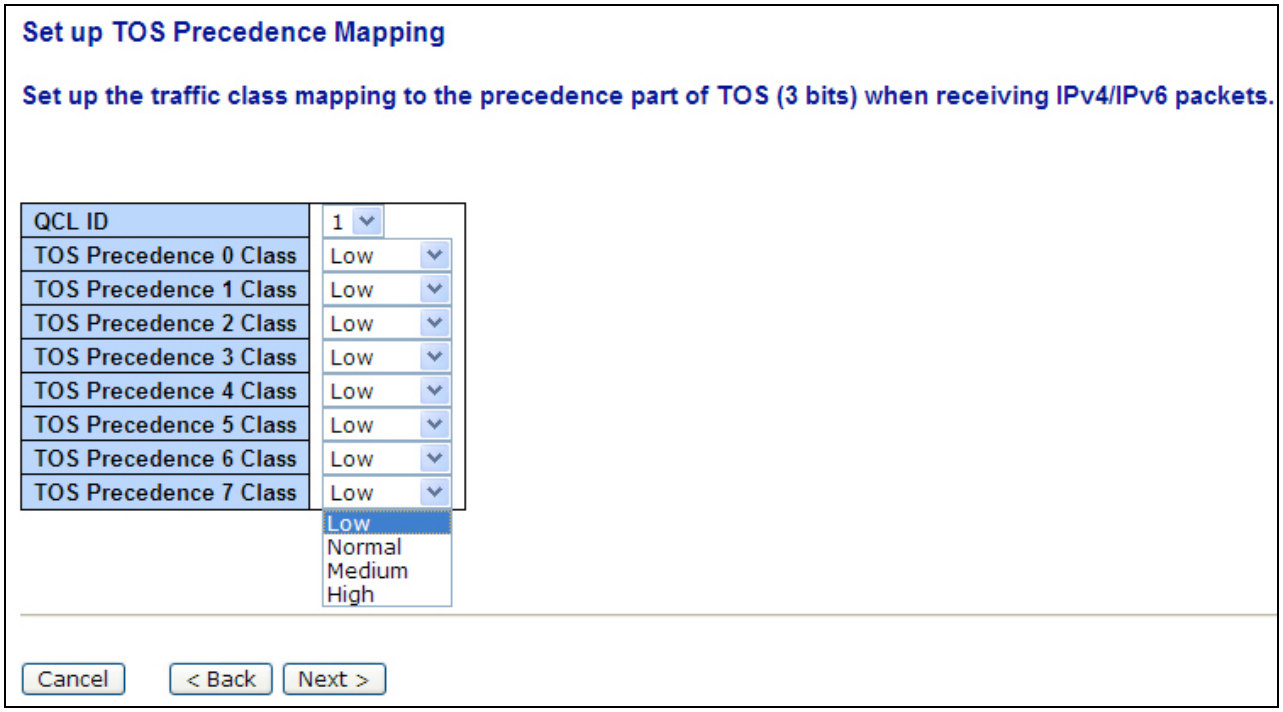


Figure 4-59. Set up TOS Precedence Mapping.

Parameter description:

QCL ID: QoS Control List (QCL): 1–24

TOS Precedence 0–7 Class: Low/Normal/Medium/High

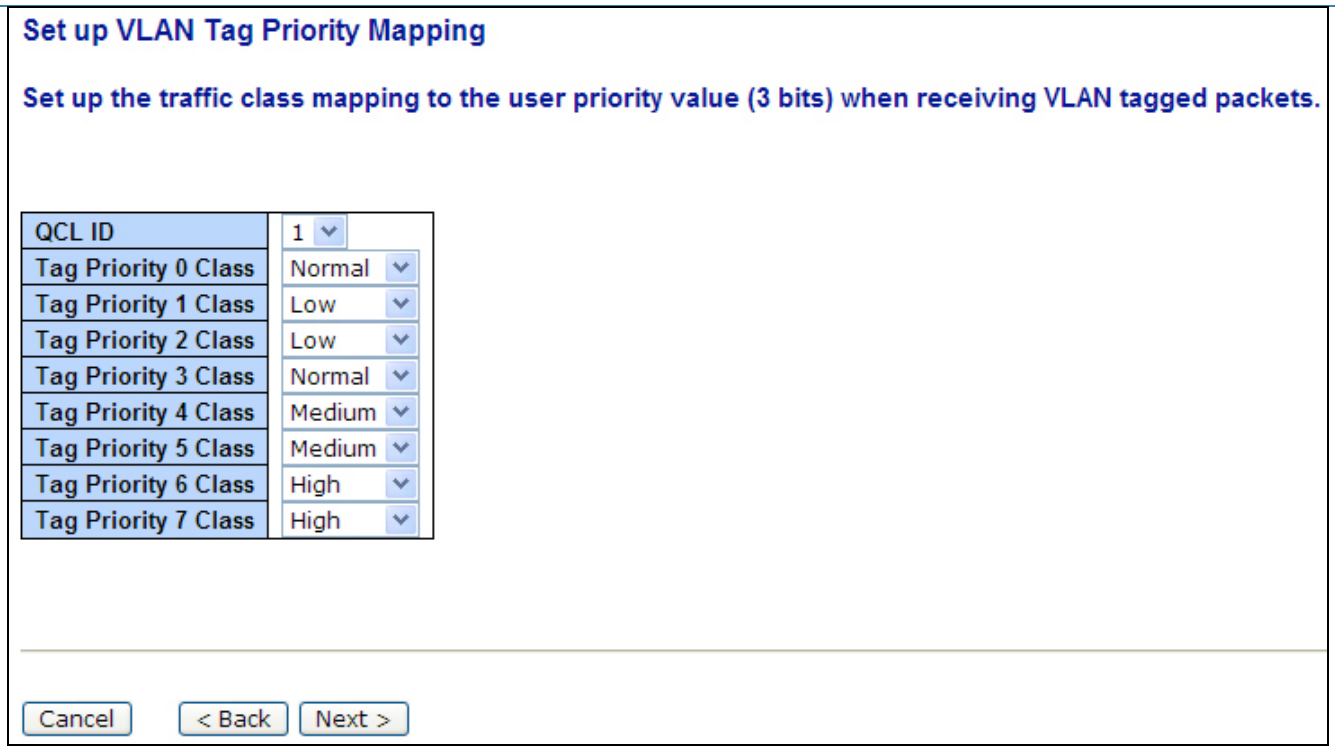


Figure 4-60. Set up VLAN Tag Priority Mapping.

Parameter description:

QCL ID: QoS Control List (QCL): 1–24

Tag Priority 0–7 Class: Low/Normal/Medium/High

4.9 SNMP Configuration

Any Network Management System (NMS) running Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent,. It traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. The SNMP agent running on the switch responds to the request issued by the SNMP manager.

The NMS issues the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP to "Enable," the SNMP agent will start. You can access all supported MIB OIDs, including RMON MIB, via SNMP manager. If the field SNMP is set to "Disable," the SNMP agent will be de-activated, and the related Community Name, Trap Host IP Address, Trap, and all MIB counters will be ignored.

Function name: SNMP Configuration

Function description: This function is used to configure SNMP settings, community name, trap host, and public traps. An SNMP manager must pass the authentication by identifying both community names, then it can access the MIB of the target device. Both parties must have the same community name. Once you complete the setting, click on the **<Apply>** button, and the setting takes effect.

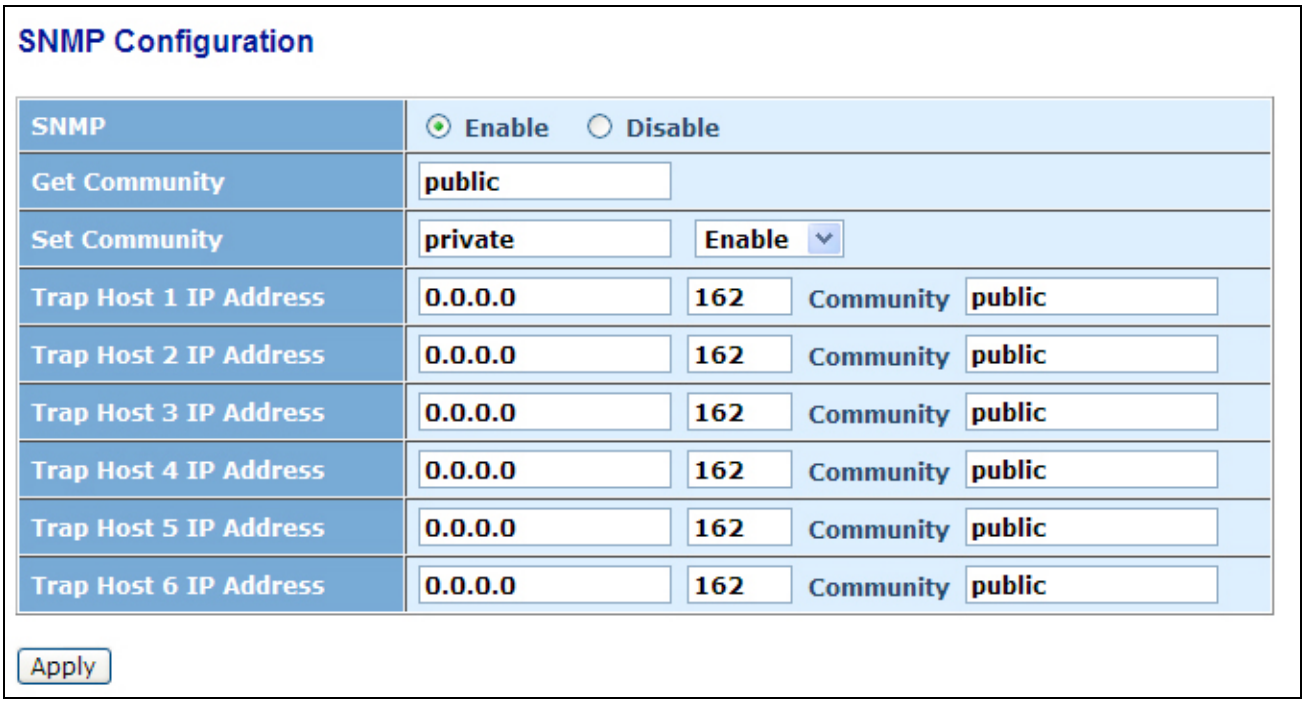


Figure 4-61 Community and trap host setting.

Parameters description:

SNMP: Used to activate or deactivate SNMP. The default is Enable.

Get/Set/Trap Community: Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. In this case, the requesting network management unit cannot access the device with a different community name via SNMP protocol; If they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case-sensitive. No blank spaces are permitted in the community name string. Any printable character is permitted.

The community name for each function works independently. Each function has its own community name. The community name for GET only works for the GET function and can't be applied to other functions such as SET and Trap.

Default SNMP function: Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function : Enable

Default trap host IP address: 0.0.0.0

Default port number :162

Trap: 6 trap hosts supported in the switch. Each has its own community name and IP address and is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. The trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent losing an important trap message.

For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up, and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponding trap will actively send a trap message to the trap host

when a trap occurs. If all public traps are disabled, no public trap message will be sent. The Enterprise (no. 6) trap is classified as a private trap, and is listed in the Trap Alarm Configuration function folder.
Default for all public traps: Enable.

4.10 ACL

The LPB4008A switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way.

The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC, and VLAN parameters, etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port. The policy number is 1–8; however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

4.10.1 Ports

Function name: ACL Port Configuration

Function description: The switch ACL function supports up to 128 Access Control Entries (ACEs), using 128 shared ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any>, assign this ACE for a policy, or assign this ACE for a port. There are 8 policies, each port can select one of policy, then decides which of the following actions would take according to the packet's IPv4, EtherType, ARP Protocol, MAC Parameters, and VLAN parameters:

Packet Deny or Permit

Rate Limiter (Unit: pps)

Port Copy (1–8)

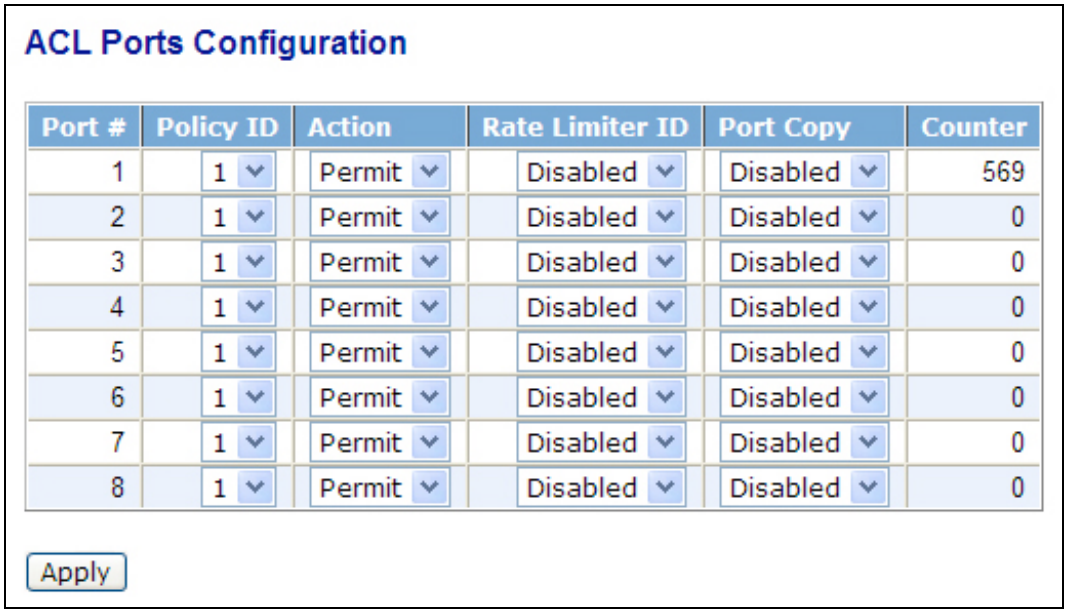


Figure 4-62. ACL ports configuration.

Parameter description:

Port #: Port number: 1–8

Policy ID: Policy ID range: 1–8

Action: Permit or Deny forwarding the met ACL packets

Rate Limiter ID: Disabled: Disable Rate Limitation

Rate Limiter ID Range: 1~16. To select one of rate limiter ID for this port, it will limit met ACL packets by rate limiter ID configuration.

Port Copy: Disabled: Disable to copy the met ACL packets to a specific port.

Port number: 1–8. Copy the met ACL packets to the selected port.

Counter: The counter will increase from its initial value 0, when this port receives one of the met ACL packets, the counter value will increase +1.

4.10.2 Rate Limiters

Function name:

ACL Rate Limiter Configuration

Function description:

There are 16 rate limiter IDs. You can assign one limiter ID for each port. The rate limit configuration unit is Packet Per Second (pps).

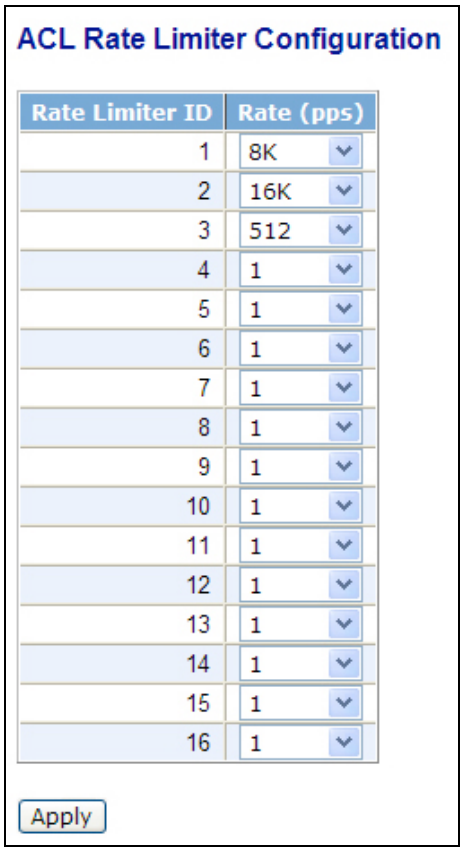


Figure 4-63. ACL rate limiter configuration.

Parameter description:

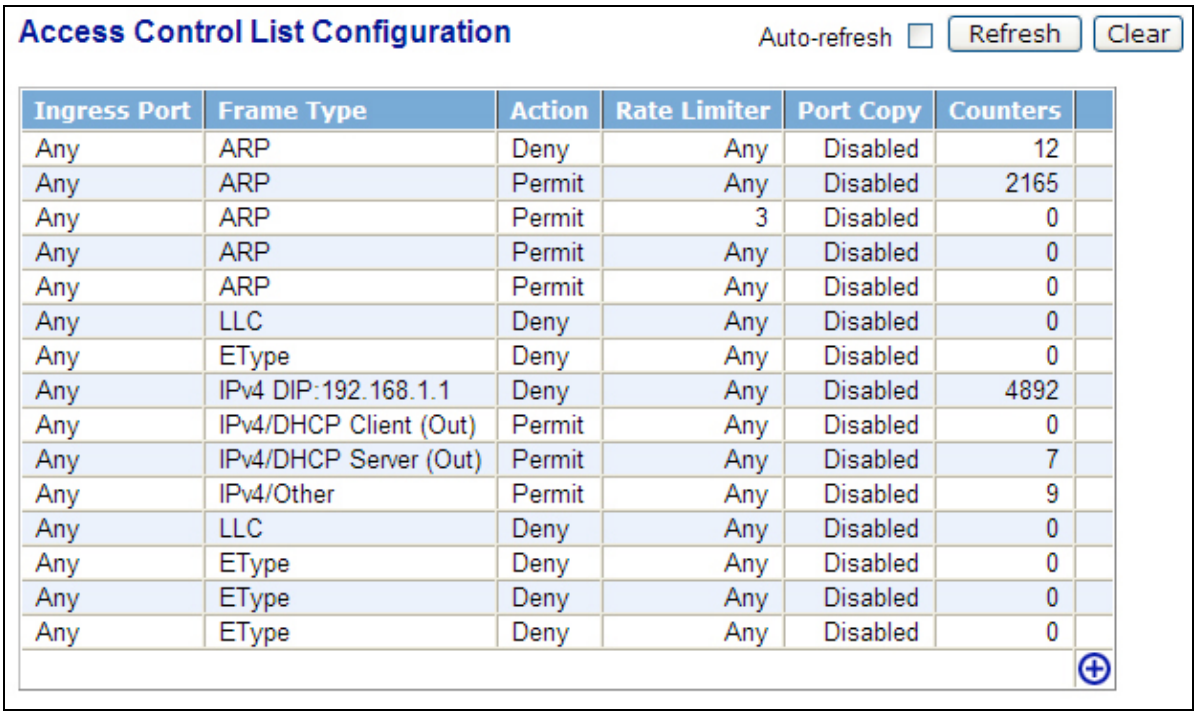
Rate Limiter ID: ID Range: 1–16

Rate(pps): 1/2/4/8/16/32/64/128/256/512/1K/2K/4K/8K/16K/32K/64K/128K/256K/512K/1024K

4.10.3 Access Control List

Function name: ACL Rate Limiter Configuration

Function description: The switch ACL function supports up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any>, assign this ACE for a policy, or assign this ACE for a port. There are 8 policies. Each port can select one policy, then decide which Permit/Deny, Rate Limitation, and Port Copy actions to take according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters, and VLAN parameters.



Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Counters
Any	ARP	Deny	Any	Disabled	12
Any	ARP	Permit	Any	Disabled	2165
Any	ARP	Permit	3	Disabled	0
Any	ARP	Permit	Any	Disabled	0
Any	ARP	Permit	Any	Disabled	0
Any	LLC	Deny	Any	Disabled	0
Any	EType	Deny	Any	Disabled	0
Any	IPv4 DIP:192.168.1.1	Deny	Any	Disabled	4892
Any	IPv4/DHCP Client (Out)	Permit	Any	Disabled	0
Any	IPv4/DHCP Server (Out)	Permit	Any	Disabled	7
Any	IPv4/Other	Permit	Any	Disabled	9
Any	LLC	Deny	Any	Disabled	0
Any	EType	Deny	Any	Disabled	0
Any	EType	Deny	Any	Disabled	0
Any	EType	Deny	Any	Disabled	0

Figure 4-64. Ingress Port.

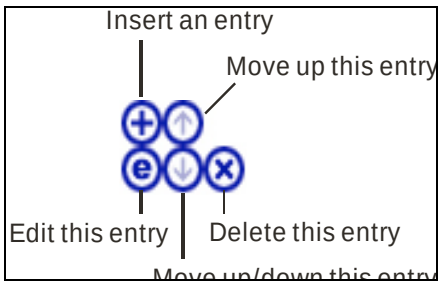


Figure 4-65. Entry screen.

Parameter description:

Ingress Port:

Configurable Range: Any/Policy 1–8 /Port 1–8

Any: Apply this ACE rule for each port ingress classification

Policy 1-8: Apply this ACE rule for specific policy

Port 1-8: Apply this ACE rule for specific port ingress classification

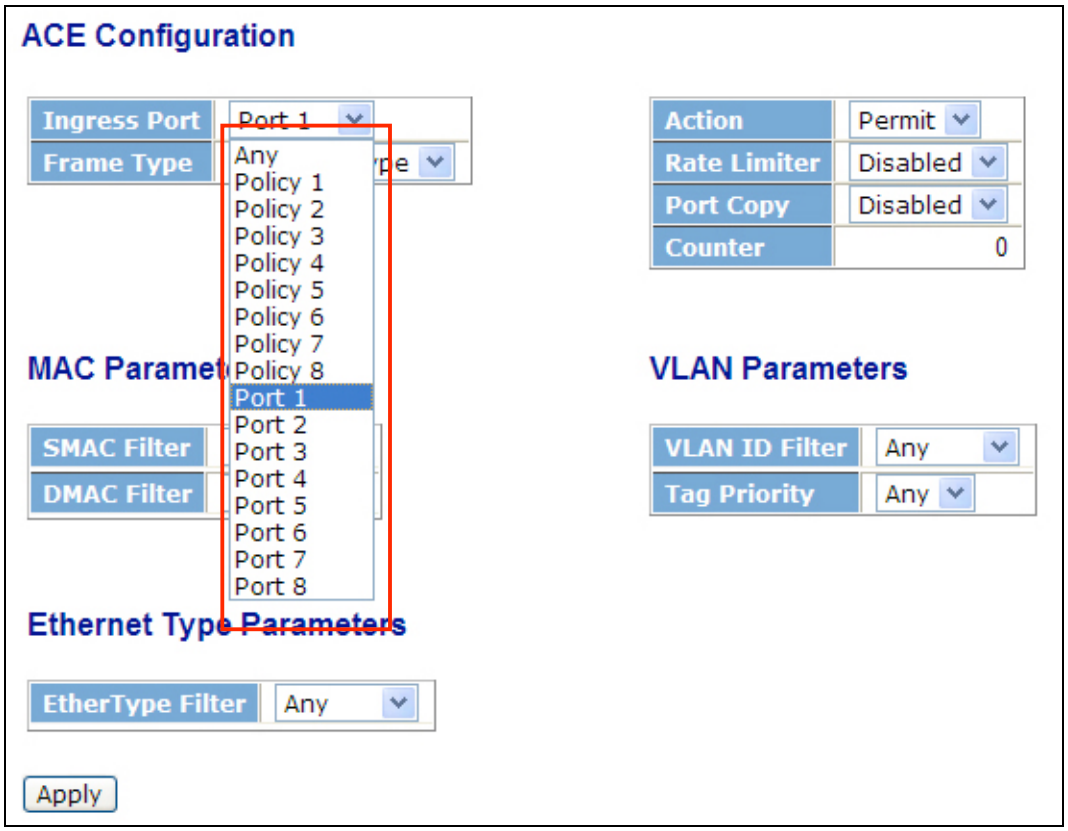


Figure 4-66. Ingress Port.

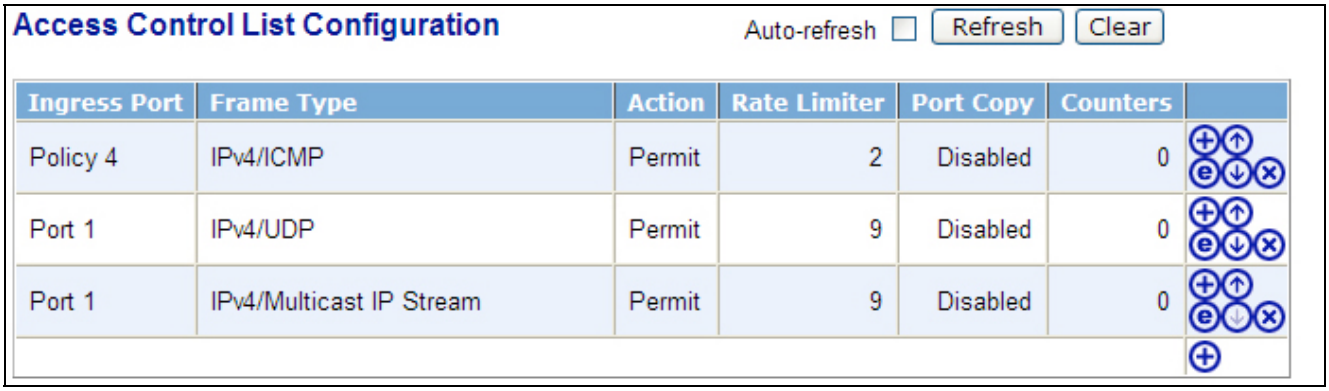


Figure 4-67. Access control list configuration.

Parameter description:

Frame Type: Any/Ethernet Type/ARP/IPv4

Any: Includes all frame types.

Ethernet Type: Includes all Ethernet frame types.

ARP: Includes all ARP protocol frame types.

IPv4: Includes all IPv4 protocol frame types.

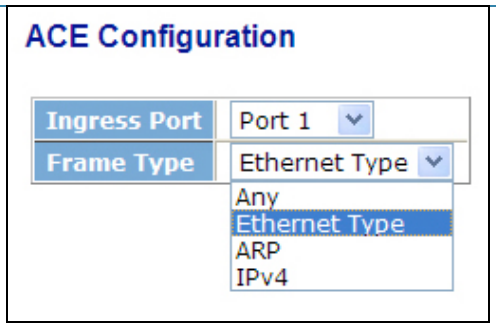


Figure 4-68. Frame Type.

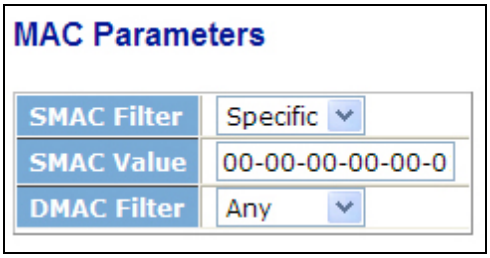


Figure 4-69. SMAC filter value.

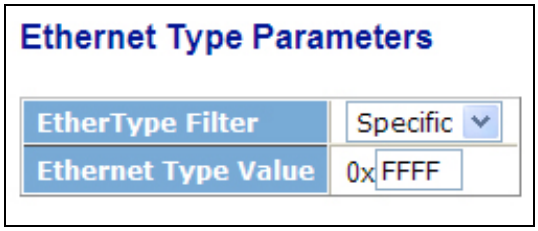


Figure 4-70. Ethernet type parameters screen.

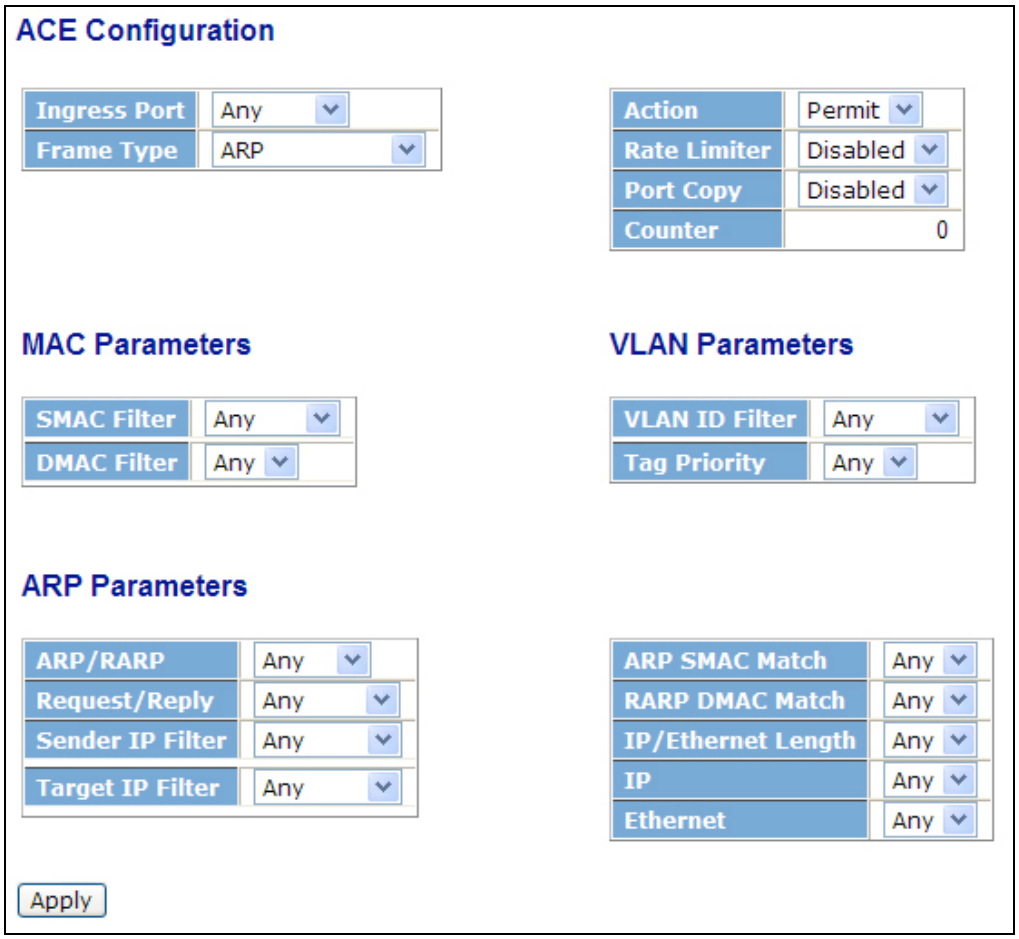


Figure 4-71. ARP parameters.

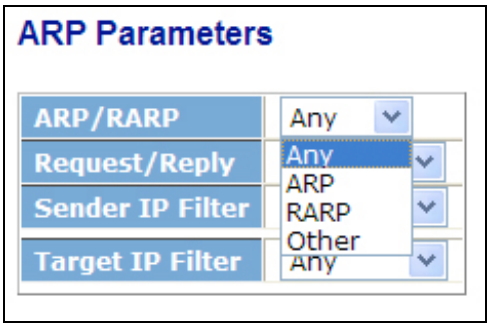


Figure 4-72. ARP request/reply.

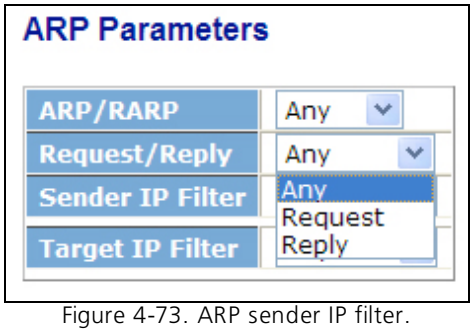


Figure 4-73. ARP sender IP filter.

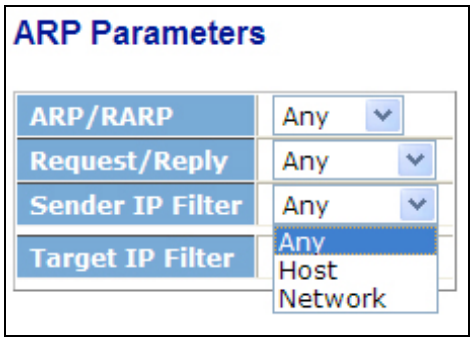


Figure 4-74. ARP target IP filter.

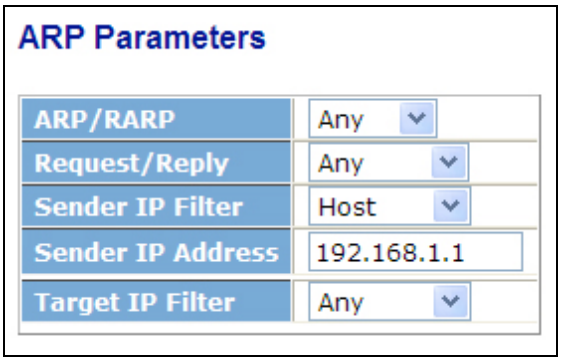


Figure 4-75. ARP sender IP address.

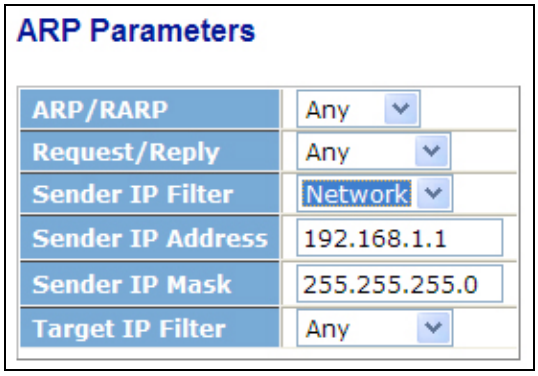


Figure 4-76 ARP sender IP filter.

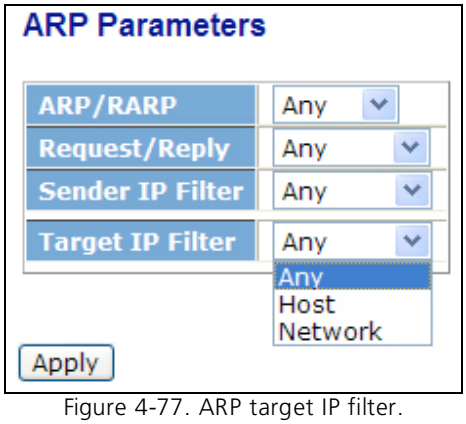


Figure 4-77. ARP target IP filter.

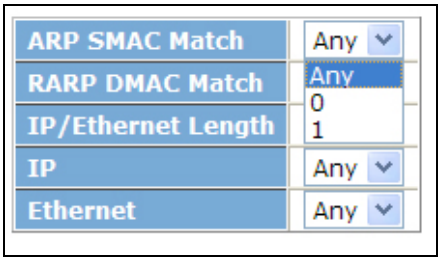


Figure 4-78 ARP RARP DMAC match.

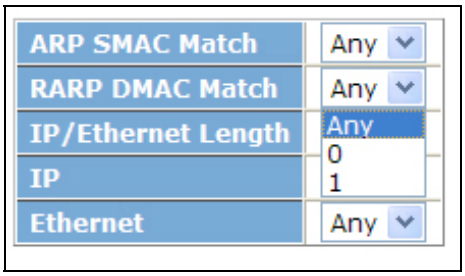


Figure 4-79. ARP IP/Ethernet length.

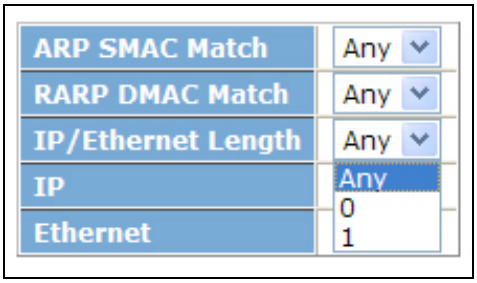


Figure 4-80. ARP IP.

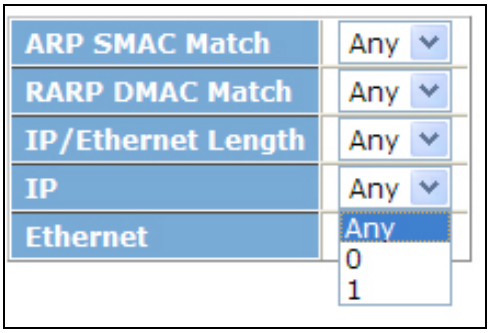


Figure 4-81. ARP Ethernet.

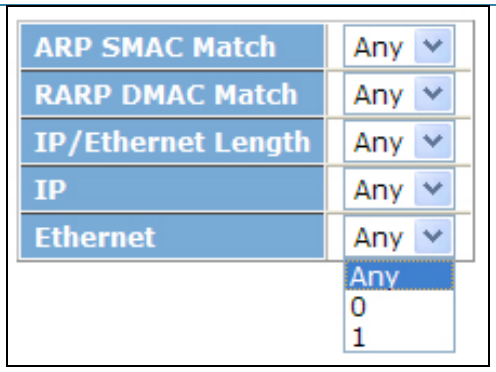


Figure 4-82. ARP Ethernet.

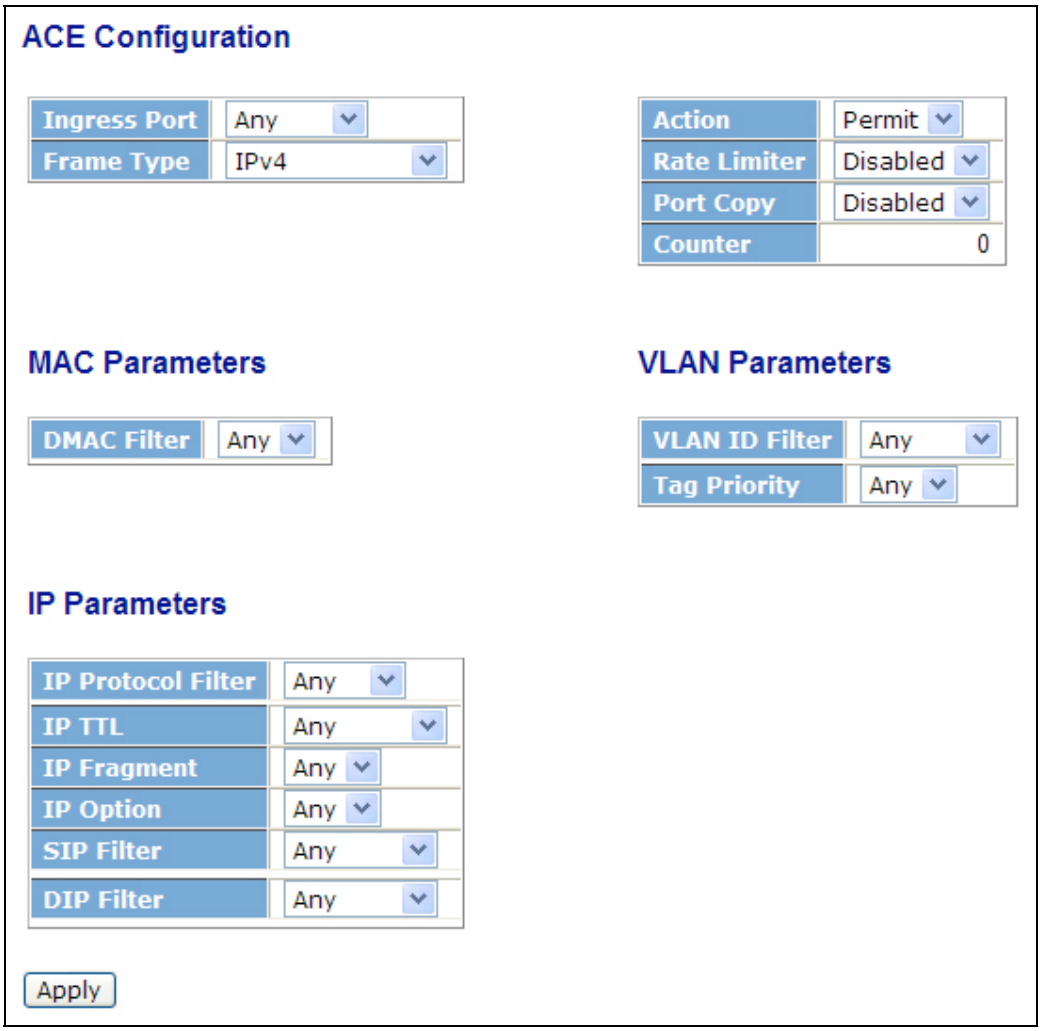


Figure 4-83. IPv4.

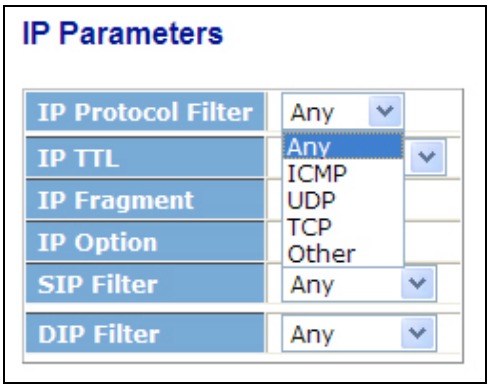


Figure 4-84. IPv4 protocol filter.

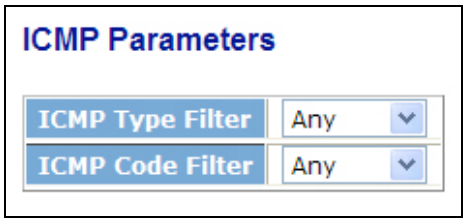


Figure 4-85. IPv4 ICMP parameters.

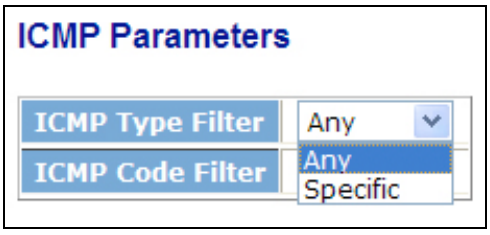


Figure 4-86. IPv4 ICMP type filter.

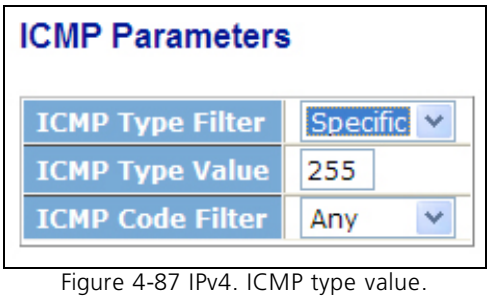


Figure 4-87 IPv4. ICMP type value.

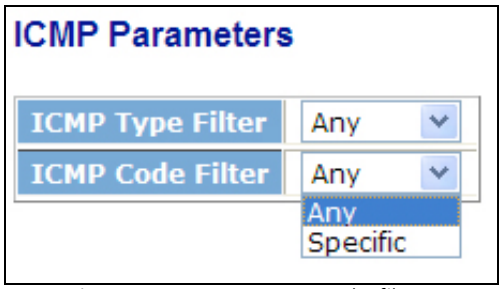


Figure 4-88. IPv4 ICMP code filter.

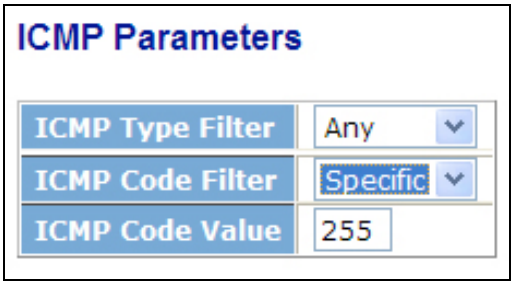


Figure 4-89. IPv4 ICMP code value.

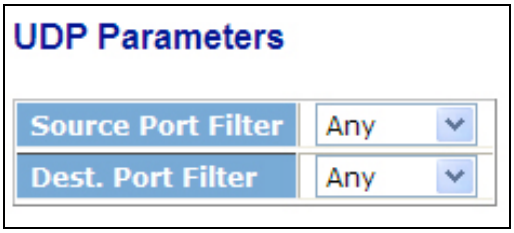


Figure 4-90. IPv4 UDP parameters.

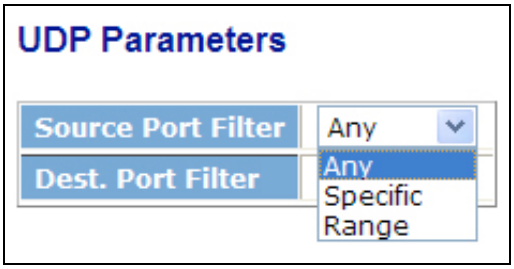


Figure 4-91. IPv4 UDP dest. Port filter.

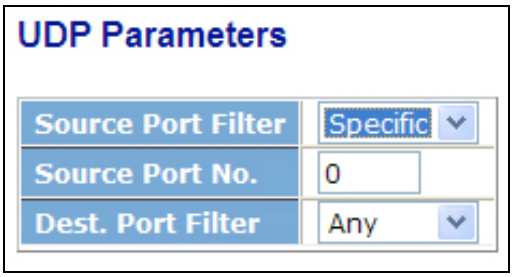


Figure 4-92. IPv4 UDP source port filter.

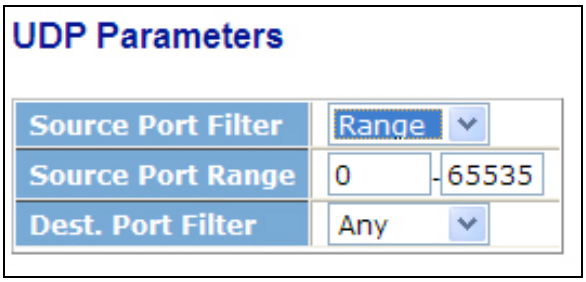


Figure 4-93. IPv4 UDP source port range.

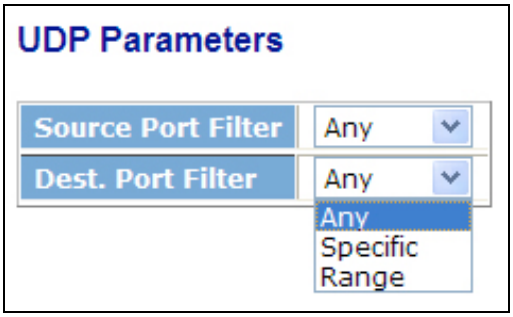


Figure 4-94. IPv4 UDP dest. Port filter.

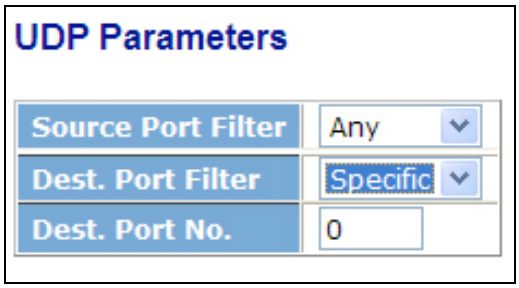


Figure 4-95. IPv4 UDP dest. port number.

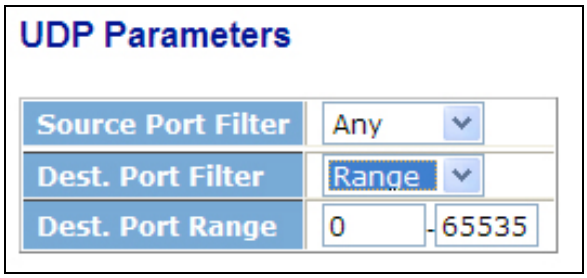


Figure 4-96. IPv4 UDP dest. port range.

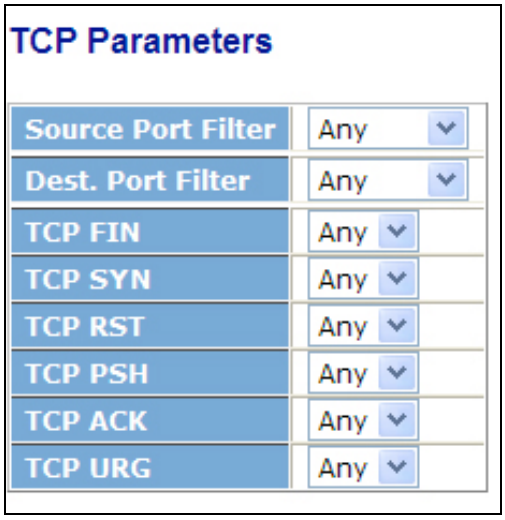


Figure 4-97. IPv4 TCP parameters.

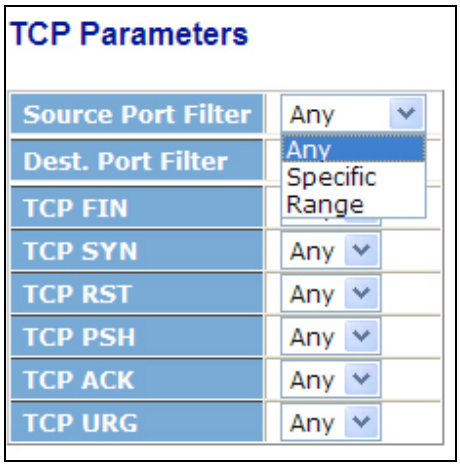


Figure 4-98. IPv4 TCP dest. port filter.

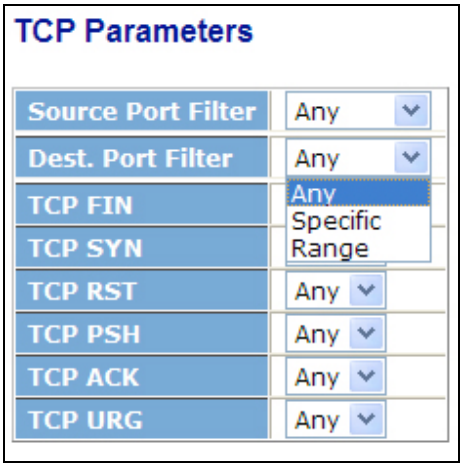


Figure 4-99. IPv4 TCP FIN.

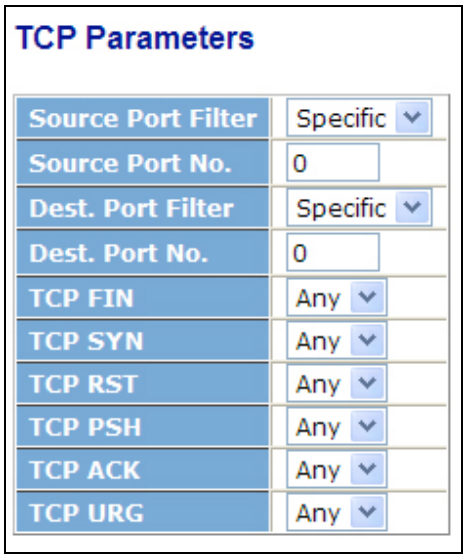


Figure 4-100. TCP parameters.

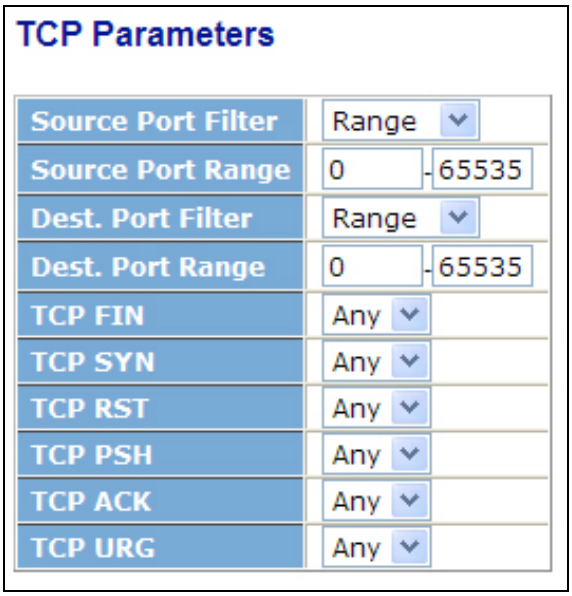


Figure 4-101. IPv4 dest. port range.

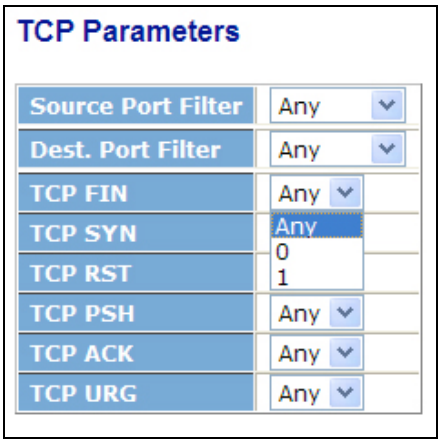


Figure 4-102. IPv4 TCP FIN.

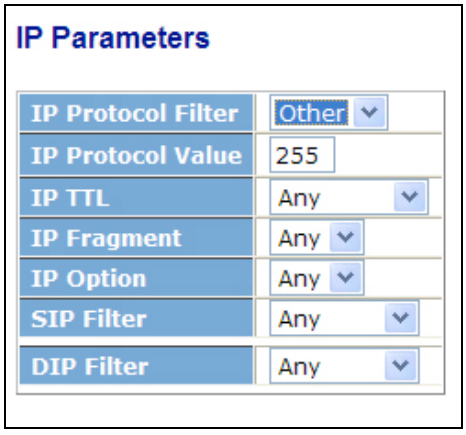


Figure 4-103. IP parameters.

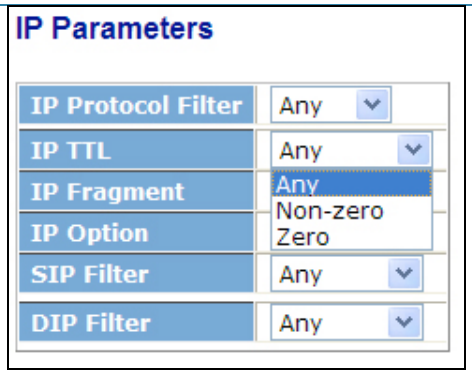


Figure 4-104. IPv4 IP TTL.

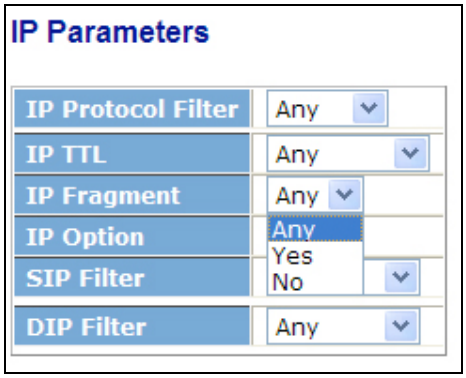


Figure 4-105. IPv4 IP Fragment.

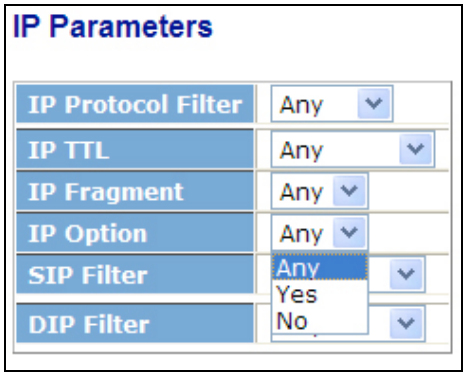


Figure 4-106. IPv4 SIP Filter.

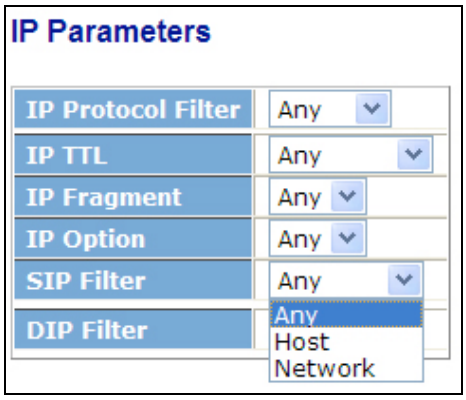


Figure 4-107. IPv4 SIP Filter, Any.

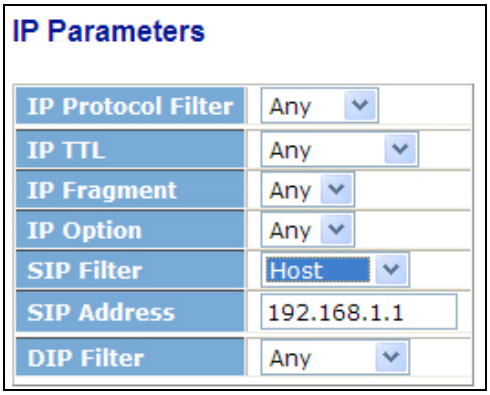


Figure 4-108. IPv4 SIP Filter, Host

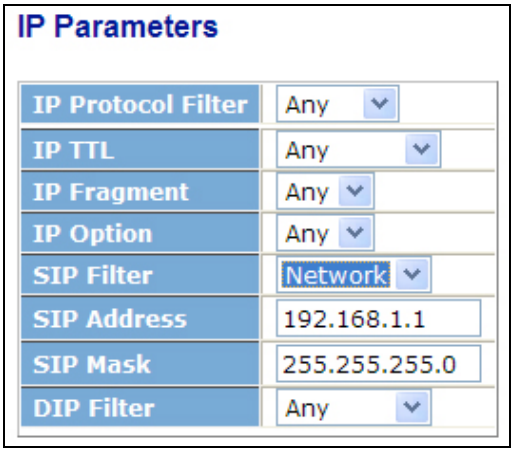


Figure 4-109. IPv4 SIP Filter, Network.

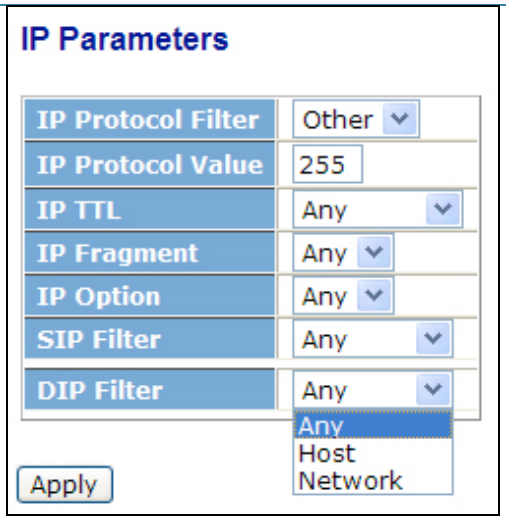


Figure 4-110. IPv4 DIP Filter.

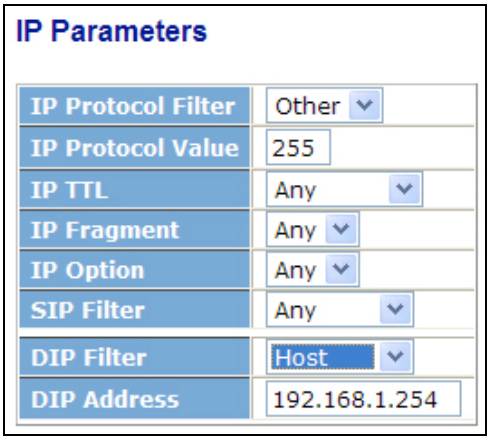


Figure 4-111. IPv4 DIP address.

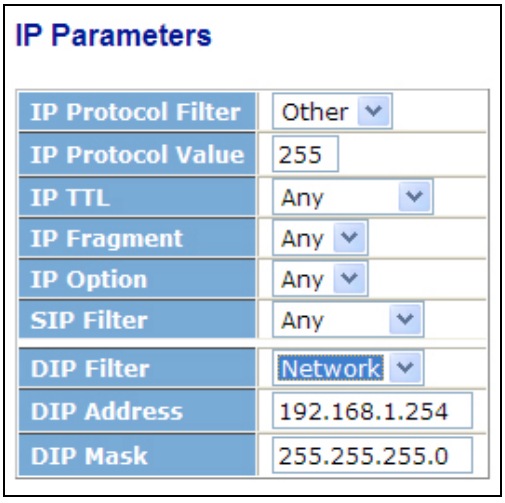


Figure 4-112. IPv4 DIP address.

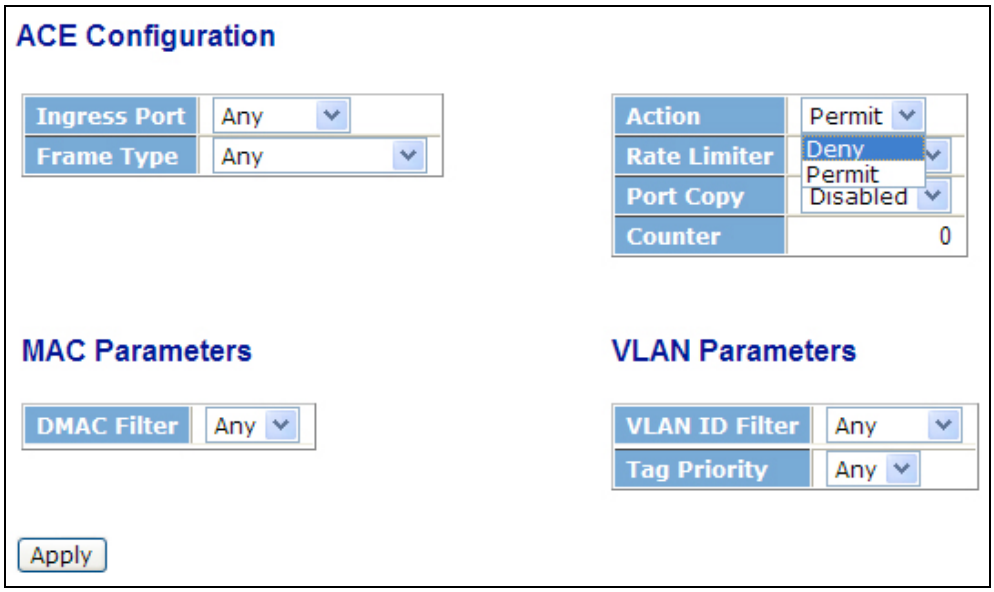


Figure 4-113. Action.

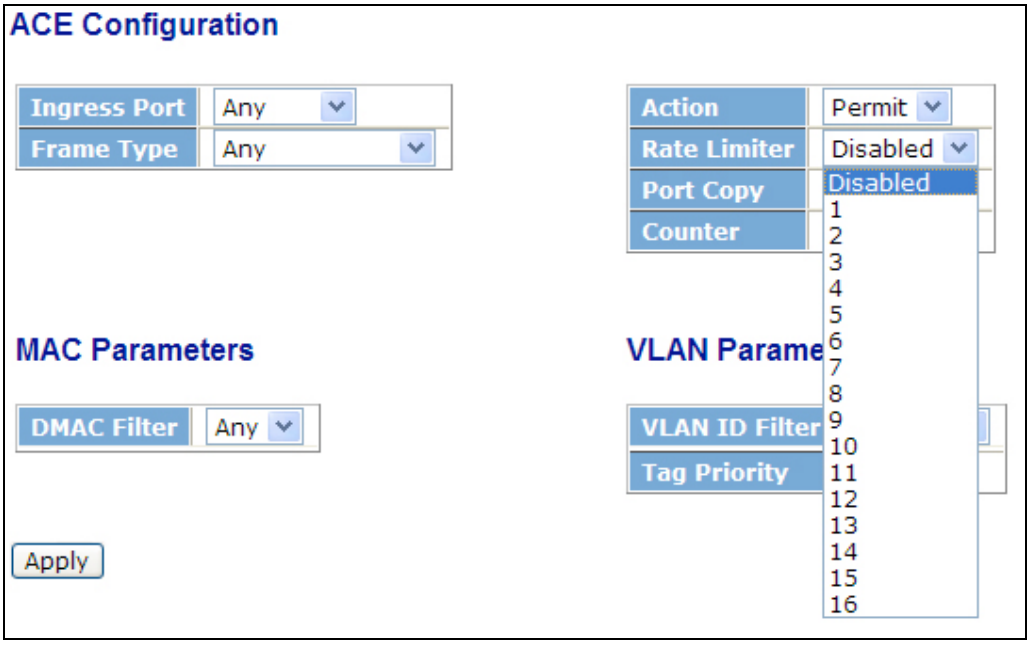


Figure 4-114. Rate Limiter.

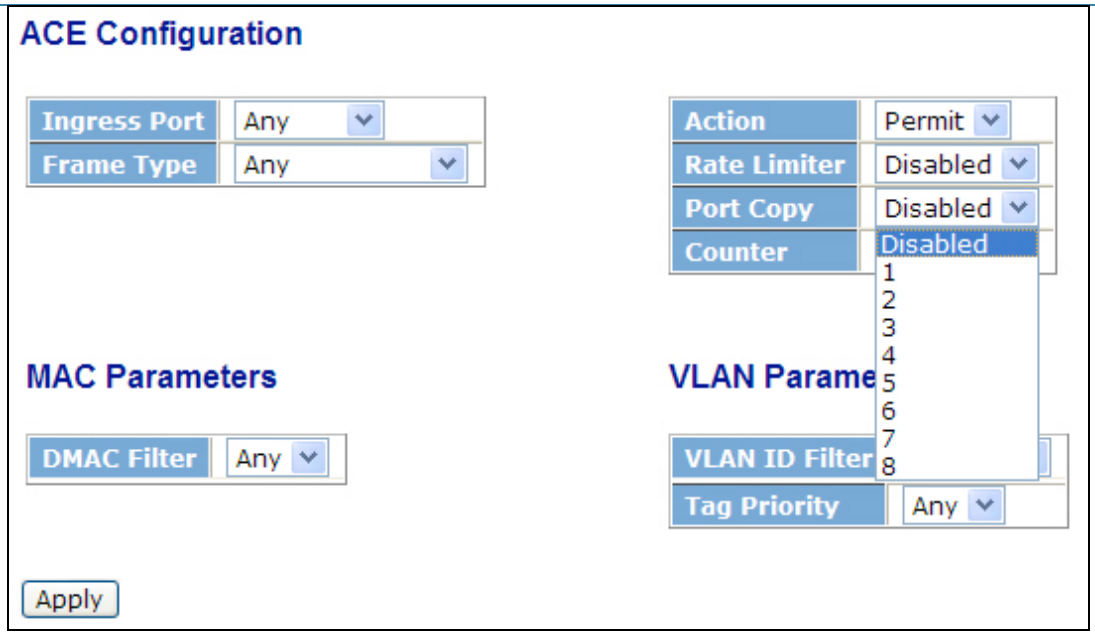


Figure 4-115. Port Copy.

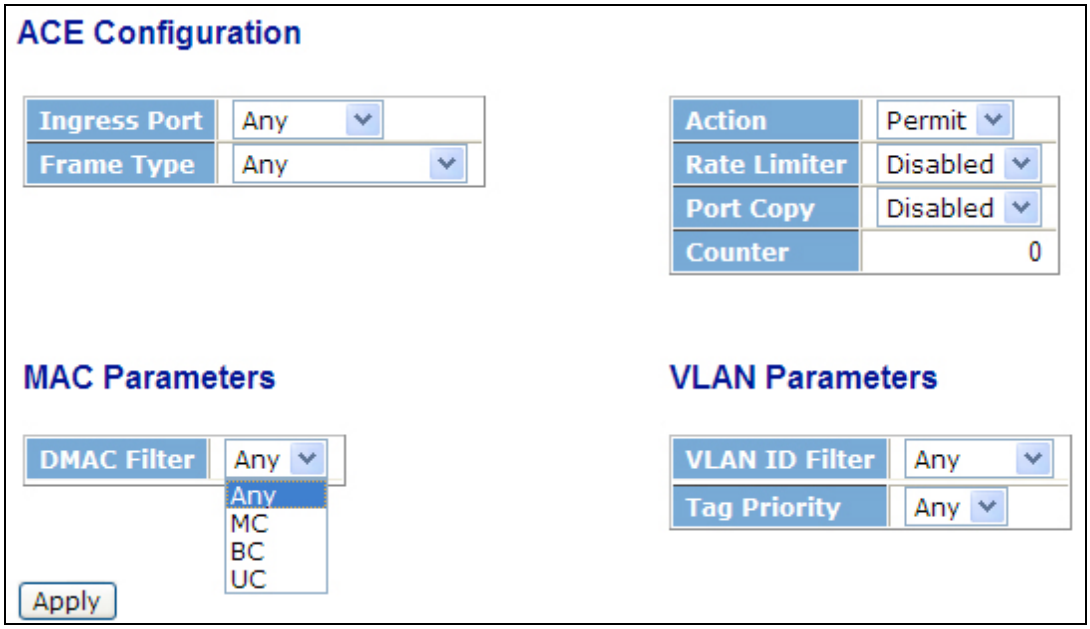


Figure 4-116. DMAC Filter.

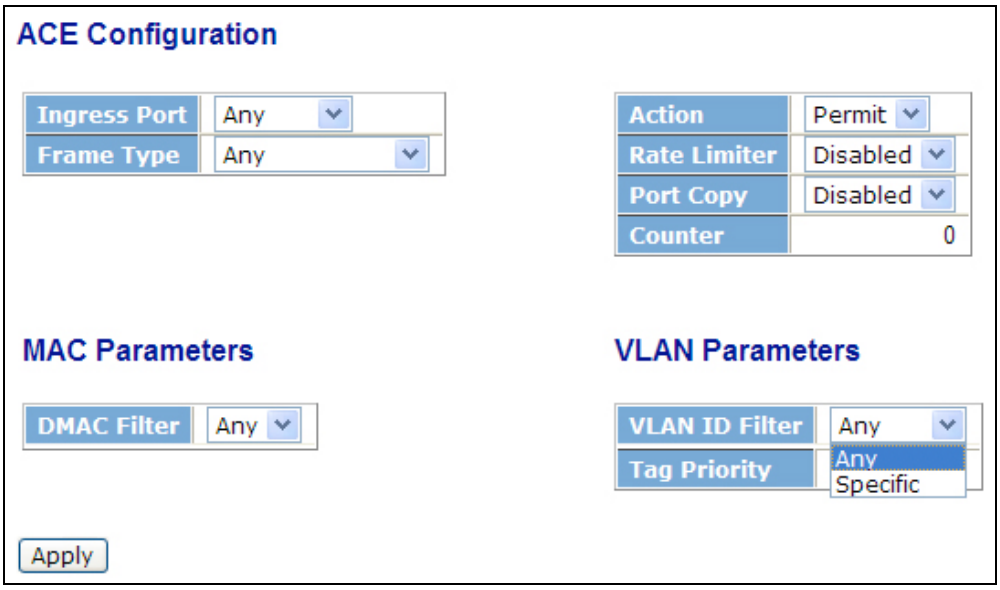


Figure 4-117. VLAN ID Filter.

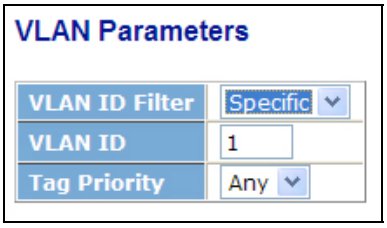


Figure 4-118. VLAN ID Filter.

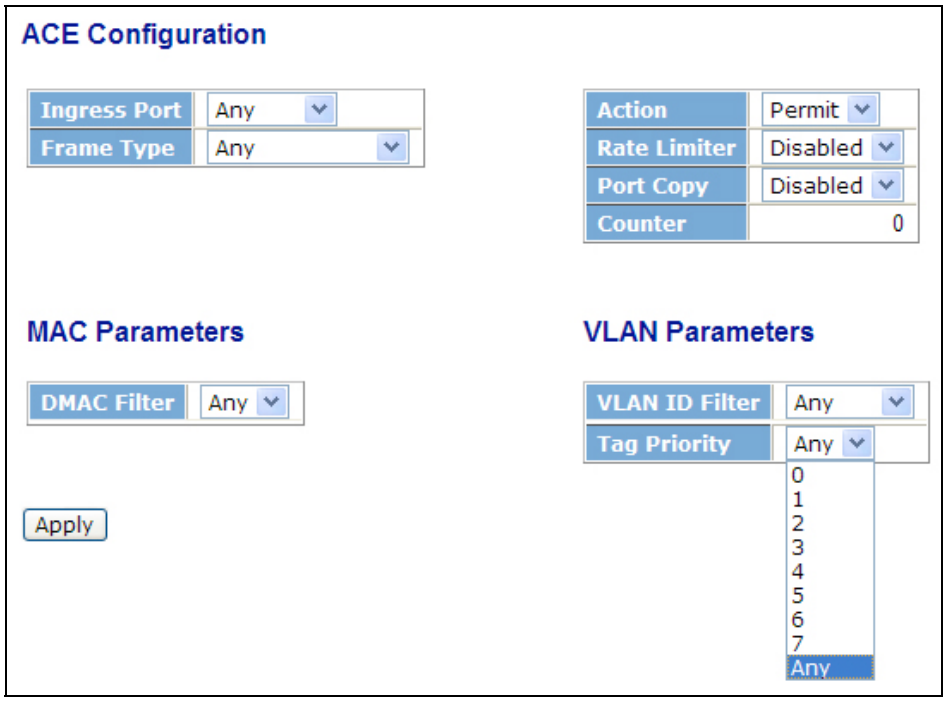


Figure 4-119. Tag Priority.

Function name: ACE Configuration

Function description: The switch ACL function supports up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any>, assign this ACE for a policy, or assign this ACE for a port. There are 8 policies. Each port can select one policy, then decide to Permit/Deny, Rate Limit, and Port Copy according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters.

Parameter description:

Ingress Port: Any/Policy 1-8/Port 1-8

Any: Apply this ACE rule for each port ingress classification

Policy 1–8: Apply this ACE rule for a specific policy

Port 1-24: Apply this ACE rule for a specific port ingress classification

IP Protocol Filter: Any/Ethernet Type/ARP/IPv4

Any: Includes all frame types

Ethernet Type: Includes all Ethernet frame types
ARP: Includes all ARP protocol frame types
IPv4: Includes all IPv4 protocol frame types

MAC Parameters: (When Frame Type = Any)

DMAC Filter: Any/MC/BC/UC

Any: Includes all destination MAC addresses

MC: Includes all Multicast MAC addresses

BC: Includes all Broadcast MAC addresses

UC: Includes all Unicast MAC addresses

MAC Parameters: (When Frame Type = Ethernet Type)

SMAC Filter: Any/Specific

Any: Includes all source MAC addresses

Specific: The source MAC address specific to the SMAC value.

DMAC Filter: Any/MC/BC/UC/Specific

Any: Includes all destination MAC addresses
MC: Includes all Multicast MAC addresses
BC: Includes all Broadcast MAC addresses
UC: Includes all Unicast MAC addresses
Specific: The destination MAC addresses specific to the DMAC value.

MAC Parameters: (When Frame Type = ARP)

SMAC Filter: Any/Specific

Any: Includes all source MAC addresses

Specific: The source MAC addresses specific to the SMAC value.

DMAC Filter: Any/MC/BC/UC

Any: Includes all destination MAC addresses

MC: Includes all Multicast MAC addresses
BC: Includes all Broadcast MAC addresses

UC: Includes all Unicast MAC addresses

MAC Parameters: (When Frame Type = IPv4)

DMAC Filter: Any/MC/BC/UC

Any: Includes all destination MAC addresses

MC: Includes all Multicast MAC addresses

BC: Includes all Broadcast MAC addresses
UC: Includes all Unicast MAC addresses

Ether Type Parameters: (When Frame Type = Ethernet Type)

EtherType Filter: Any/Specific

Any: Includes all Ethernet frame types

Specific: Depends on the Ethernet Type Value.

Ethernet Type Value: 0x600–0xFFFF

ARP Parameters: (When Frame Type = ARP)

ARP/RARP: Any/ARP/RARP/Other

Any: Includes all ARP/RARP protocol frame types

ARP: Includes all ARP protocol frame types

RARP: Includes all RARP frame types

Other: Includes other frame types except ARP/RARP protocol

Request/Reply: Any/Request/Reply

Any: Includes all ARP/RARP Requests and Replies

Request: Includes all ARP/RARP request frames

Reply: Includes all ARP/RARP reply frames

Sender IP Filter: Any/Host/Network

Any: Includes all sender IP addresses

Host: Only one specific sender host IP address

Network: A specific IP subnet segment under the sender IP mask

Sender IP Address: Default: 192.168.1.1

Sender IP Mask: Default: 255.255.255.0

Target IP Filter: Any/Host/Network

Any: Includes all target IP addresses

Host: Only one specific target host IP address

Network: A specific IP subnet segment under the target IP mask

Target IP Address: Default: 192.168.1.254

Target IP Mask: Default: 255.255.255.0

ARP SMAC Match: Any/0/1

Any: Both 0 and 1

0: The ingress ARP frames where the source MAC address does not equal SMAC under the MAC parameter settings.
1: The ingress ARP frames where the source MAC address equasl SMAC address under the MAC parameter settings.

RARP DMAC Match: Any/0/1

Any: Both 0 and 1

0: The ingress RARP frames where the Destination MAC address does not equal DMAC address under the MAC parameter settings.

1: The ingress RARP frames where the Destination MAC address equals DMAC address under the MAC parameter settings.

IP/Ethernet Length: Any/0/1

Any: Both 0 and 1

0: The ingress ARP/PARP frames where the Hardware size does not equal "0x6" or the Protocol size does not equal "0x4."

1: The ingress ARP/PARP frames where the Hardware size equals "0x6" and the Protocol size is "0x4."

IP: Any/0/1

Any: Both 0 and 1

0: The ingress ARP/PARP frames where the Protocol type does not equal "0x800"

1: The ingress ARP/PARP frames where Protocol type equals "0x800"

Ethernet: Any/0/1

Any: Both 0 and 1

0: The ingress ARP/PARP frames where Hardware type does not equal "0x100"

1: The ingress ARP/PARP frames where Hardware type equals "0x100"

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = Any)

IPTTL: (Time To Live) Any/Non-zero/Zero

The quantity of routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever.

Any: Includes all conditions for IPTTL

Non-Zero: IPTTL is Non-Zero

Zero: IIPTTL is zero

IP Fragment: (IP Fragmentation Flag) Any/Yes/No

Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.

Any: Includes all IP fragment cases

Yes: The ingress frame has fragmented packets.
No: The ingress frames does not have fragmented packets

IP Option: A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

Any/Yes/No

Any: Includes all IP option case

Yes: The ingress frame has specific IP options

No: The ingress frame does not have specific IP options

SIP Filter: (SIP Source IP Address) Any/Host/Network

Any: Includes all source IP addresses

Host: Includes only one specific source host IP address

Network: A specific IP subnet segment under the source IP mask

SIP Address: Default: 192.168.1.1

SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address) Any/Host/Network

Any: Includes all destination IP addresses

Host: Includes only one specific destination host IP address

Network: A specific IP subnet segment under the destination IP mask

DIP Address: Default: 192.168.1.254

DIP Mask: Default: 255.255.255.0

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = ICMP)

ICMP Type Filter: Any/Specific

Any: Includes all types of ICMP type values

Specific: Depends on ICMP type value settings for ingress classification

ICMP Type Value: 0-255

ICMP Code Filter: Any/Specific

Any: Includes all ICMP code values

Specific: Depends on ICMP code value setting for ingress classification

ICMP Code Value: 0-255

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = UDP)

Source Port Filter: Any/Specific/Range

Any: Includes all UDP source ports

Specific: Depends on Source Port No. setting for ingress classification

Source Port No.: 0–65535

Source Port Range.: 0–65535

Dest. Port Filter: Any/Specific/Range

Any: Includes all UDP destination ports

Specific: Follows Dest. Port No. setting for ingress classification

Dest. Port No.: (Destination Port Number) 0–65535

Dest. Port Range.: (Destination Port Range) 0–65535

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = TCP)

Source Port Filter: Any/Specific/Range

Any: Includes all TCP source ports

Specific: Depends on Source Port No. setting for ingress classification

Source Port No.: 0–65535

Source Port Range.: 0–65535

Dest. Port Filter: Any/Specific/Range

Any: Includes all TCP destination ports

Specific: Follows Dest. Port No. setting for ingress classification

Dest. Port No.: 065535

Dest. Port Range: 065535

TCP FIN: TCP Control Bit FIN: Means No more data from sender. Any/0/1

Any: Includes all TCP FIN case

0: The TCP control bit FIN is 0

1: The TCP control bit FIN is 1

TCP SYN:

TCP Control Bit SYN: Synchronize sequence numbers. Any/0/1

Any: Includes all TCP SYN case

0: The TCP control bit SYN is 0

1: The TCP control bit SYN is 1

TCP RST:

TCP Control Bit RST: Reset the connection. Any/0/1

Any: Includes all TCP RST case

0: The TCP control bit RST is 0

1: The TCP control bit RST is 1

TCP PSH:

TCP Control Bit PSH: Push Function. Any/0/1

Any: Includes all TCP PSH cases

0: The TCP control bit PSH is 0

1: The TCP control bit PSH is 1

TCP ACK:

TCP Control Bit ACK: Acknowledgment field significant. Any/0/1

Any: Includes all TCP ACK case

0: The TCP control bit ACK is 0

1: The TCP control bit ACK is 1

TCP URG:

TCP Control Bit URG: Urgent Pointer field significant. Any/0/1

Any: Includes all TCP URG cases

0: The TCP control bit URG is 0

1: The TCP control bit URG is 1

IP Protocol Value: The IP Protocol Value is TCP. Options may occupy space at the end of the TCP header and are a multiple of 8 bits long. Currently defined options include:

0 - End of option list

1 - No-Operation

Any: Including all IP protocol value cases

0: The IP protocol value is 0

1: The IP protocol value is 1

IP Parameters: (Frame Type = IPv4 and IP Protocol Filter = Other)

IP Protocol Value: Default: 255

IPTTL: (Time To Live)

The quantity of routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagram from remaining on the Internet forever.

Any: Includes all conditions for IPTTL

Non-Zero: IPTTL is Non-Zero

Zero: IPTTL is zero

IP Fragment: (IP Fragmentation Flag)

Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.

Any: Includes all IP fragment cases

Yes: The ingress frame has fragmented packets.

No: The ingress frames do not have fragmented packet.

IP Option: A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.

Any: Includes all IP option cases

Yes: The ingress frame has specific IP options.

No: The ingress frame does not have specific IP options.

SIP Filter: (SIP Source IP Address)

Any: Includes all source IP addresses

Host: Only one specific source host IP address

Network: A specific IP subnet segment under the source IP mask

SIP Address: Default: 192.168.1.1

SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)

Any: Includes all destination IP addresses

Host: Only one specific destination host IP addresses

Network: A specific IP subnet segment under the destination IP mask

DIP Address: Default: 192.168.1.254

DIP Mask: Default: 255.255.255.0

VLAN Parameters:

VLAN ID Filter: Any/Specific

Any: Includes all VLAN IDs

Specific: According to the following VLAN ID and Tag Priority settings for ingress classification:

VLAN ID: 1–4094

Tag Priority: Any/0–7

Any: Includes all Tag Priority values.

0-7: The Tag Priority Value is a number (0–7)

Action Parameters: When the ingress frame meets the above ACL ingress classification rule you can do the following:

Action: Permit/Deny

Permit: Permit the met ACL ingress classification rule packets forwarding to other ports on the switch.

Deny: Discard the met ACL ingress classification rule packets.

Rate Limiter: Disabled/1–16

Disable: Disable Rate Limiter function

1–16: Apply the Rate Limiter Number setting for met ACL ingress rule packets.

Port Copy: Disabled/1–8

Disable: Disable the Port Copy function

1–8: The packets will be copied to the selected port when they meet the ACL ingress rule.

4.10.4 Wizard

Function name: Wizard

Function description: The wizard function provides four type of typical applications for user to easily configure their application with ACL function.

Figure 4-120. Wizard.

Parameter description:

Please select an Action:

Set up Policy Rules/Set up Port Policies/Set up Typical Network Application Rules/Set up Source MAC and Source IP Binding

Next: Click on <Next> to confirm the current setting and go to the next step automatically.

Cancel: Cancel the current setting and go back to the top layer in the ACL wizard.

Back: Click on <Back> to go back to the previous step.

Wizard Again: Click on <Wizard Again> and the UI will go back to top layer in the wizard.

Finish: Click on <Finish> to finish the ACL Wizard setting to select the parameter settings, then click on <Apply> to confirm all changed parameters settings.

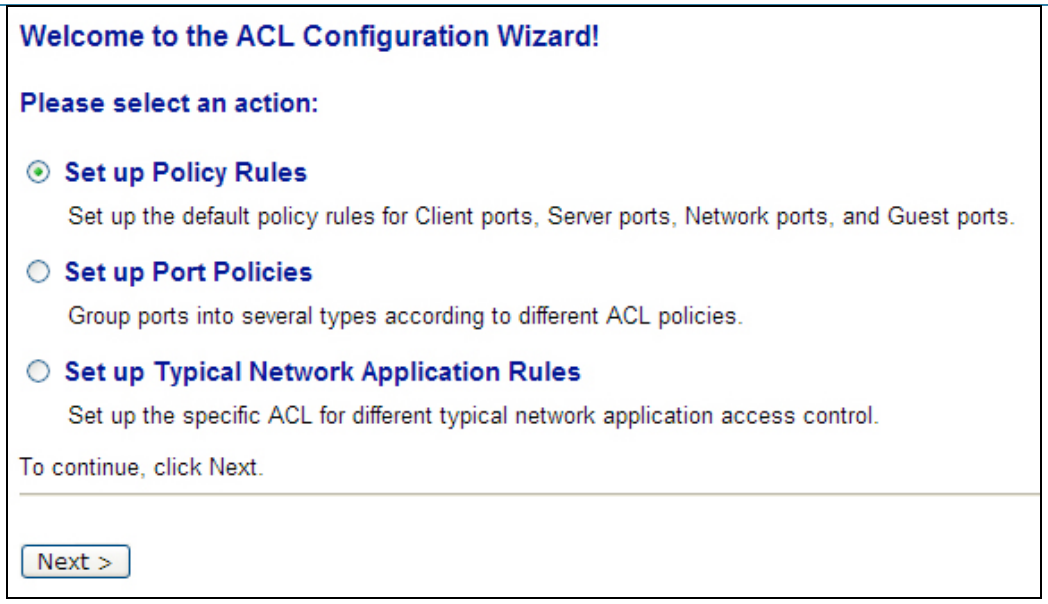


Figure 4-121. Set up Policy Rules.

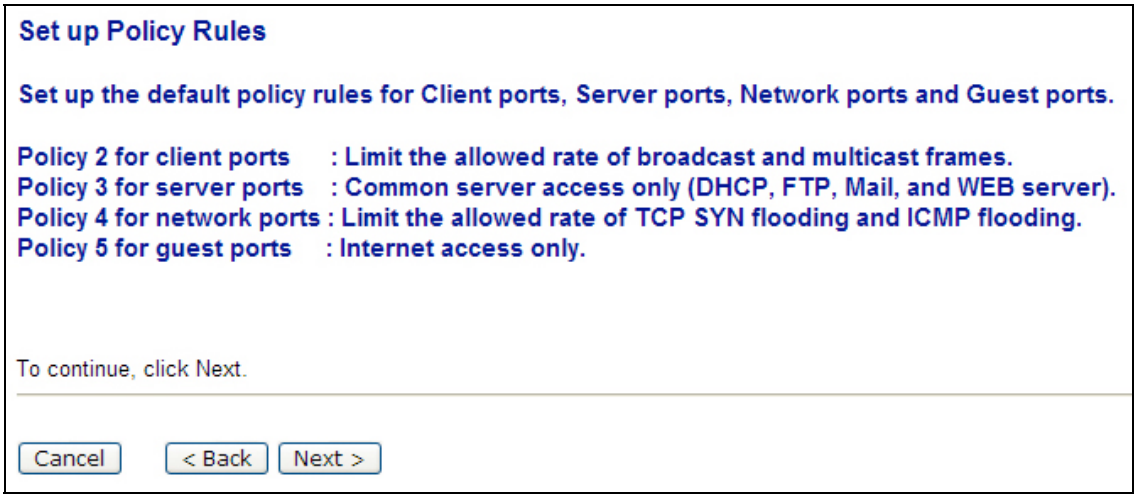


Figure 4-122. Set up Policy Rules.

Figure 4-123. Set up Policy Rules.

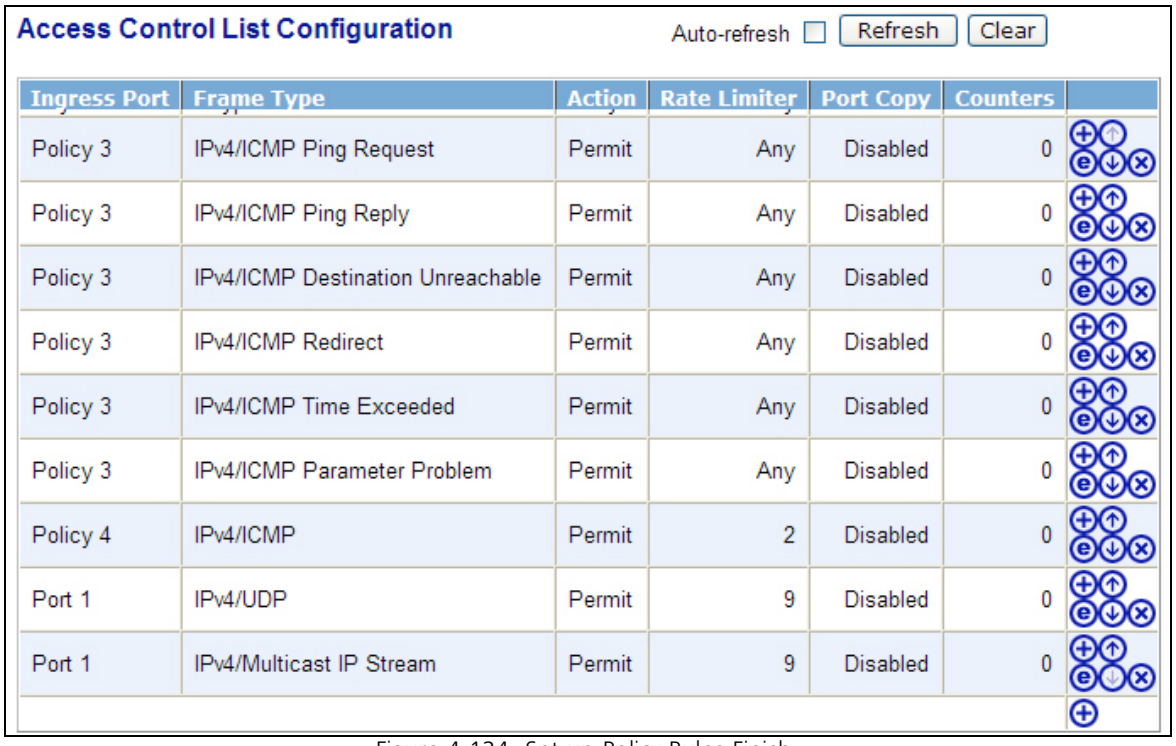


Figure 4-124. Set up Policy Rules Finish.

Figure 4-125. Set up Port Policies.

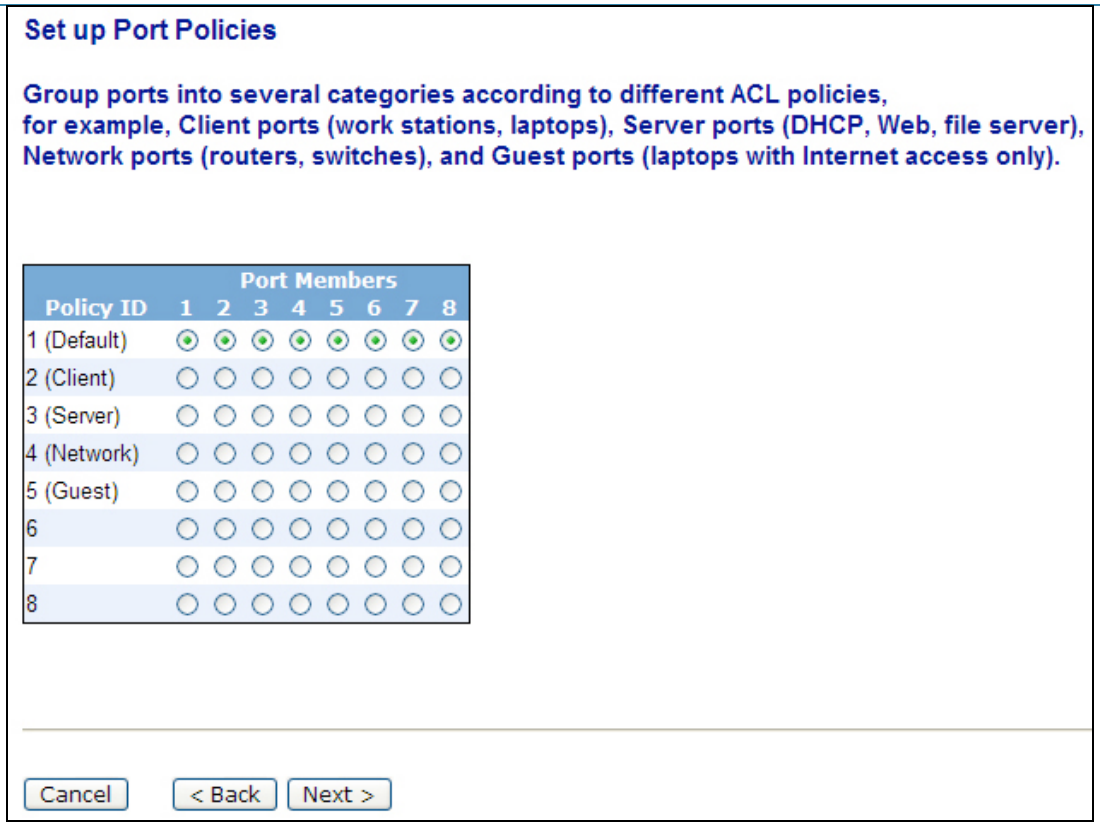


Figure 4-126. Set up Port Policies.

Figure 4-127. Set up Port Policies finished screen.

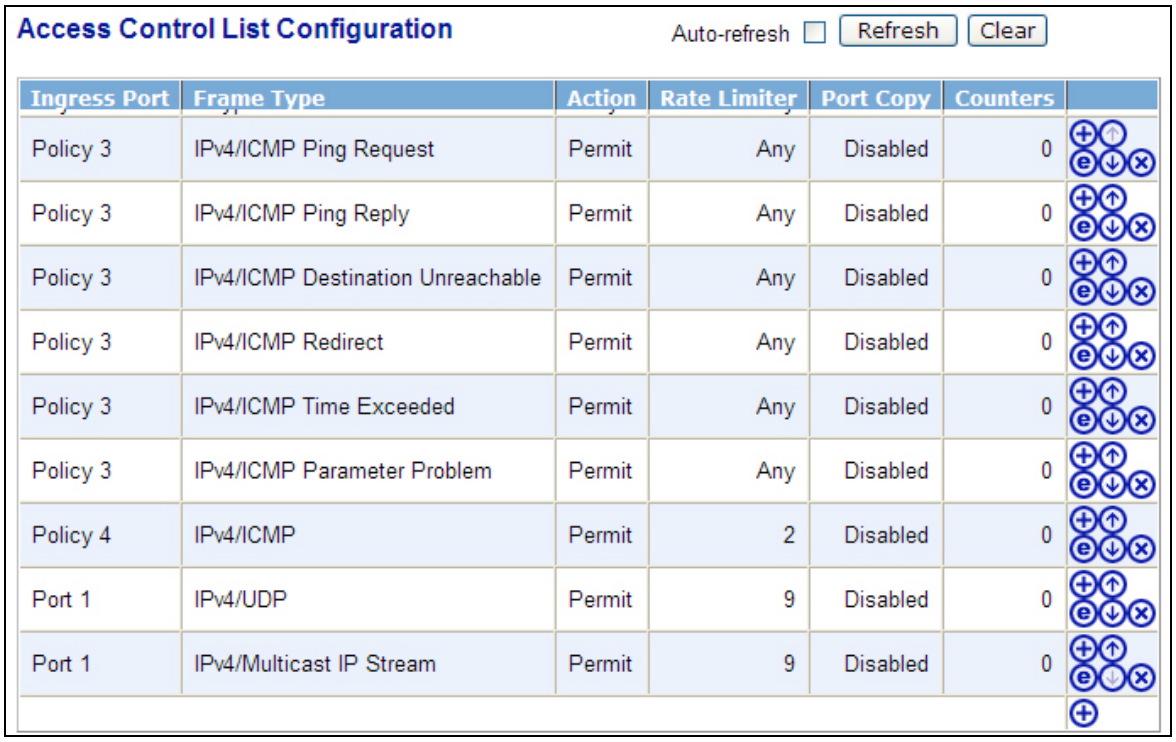


Figure 4-128. Set up Port Policies Finish

Figure 4-129. Set up Typical Network Application Rules.

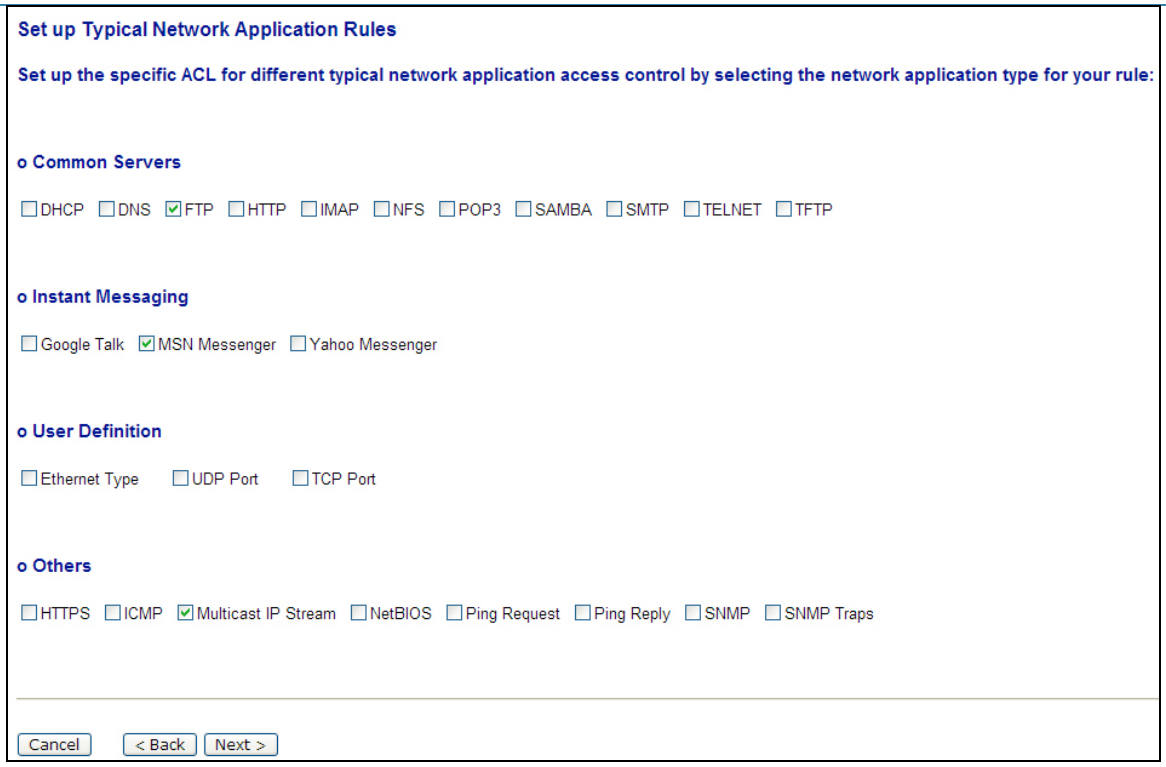


Figure 4-130. Set up Typical Network Application Rules.

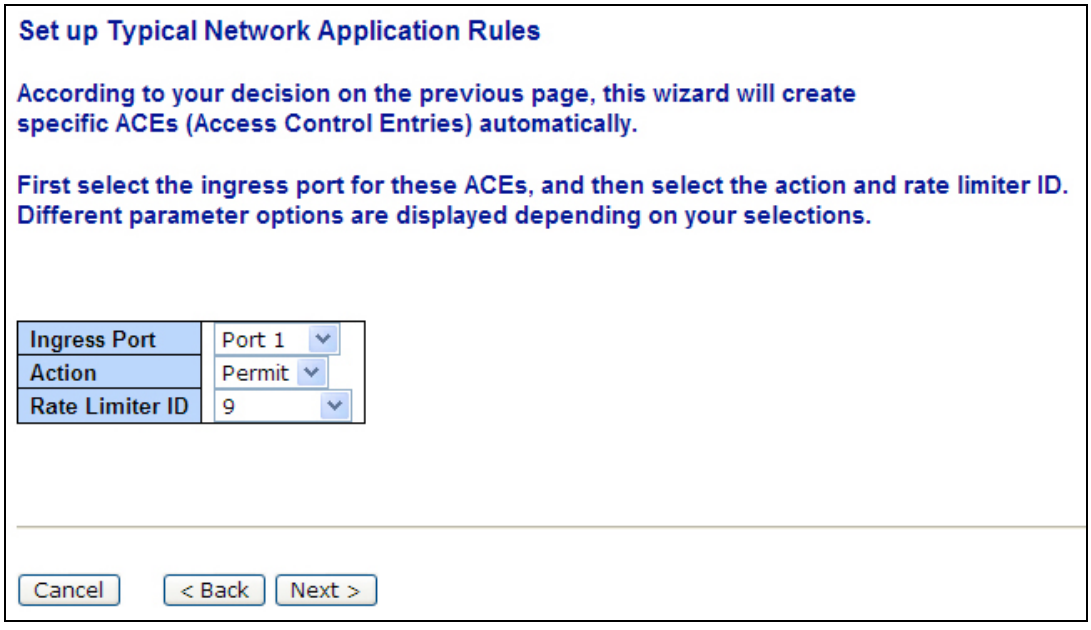


Figure 4-131. Set up Typical Network Application Rules.

Figure 4-132. Set up Typical Network Application Rules.

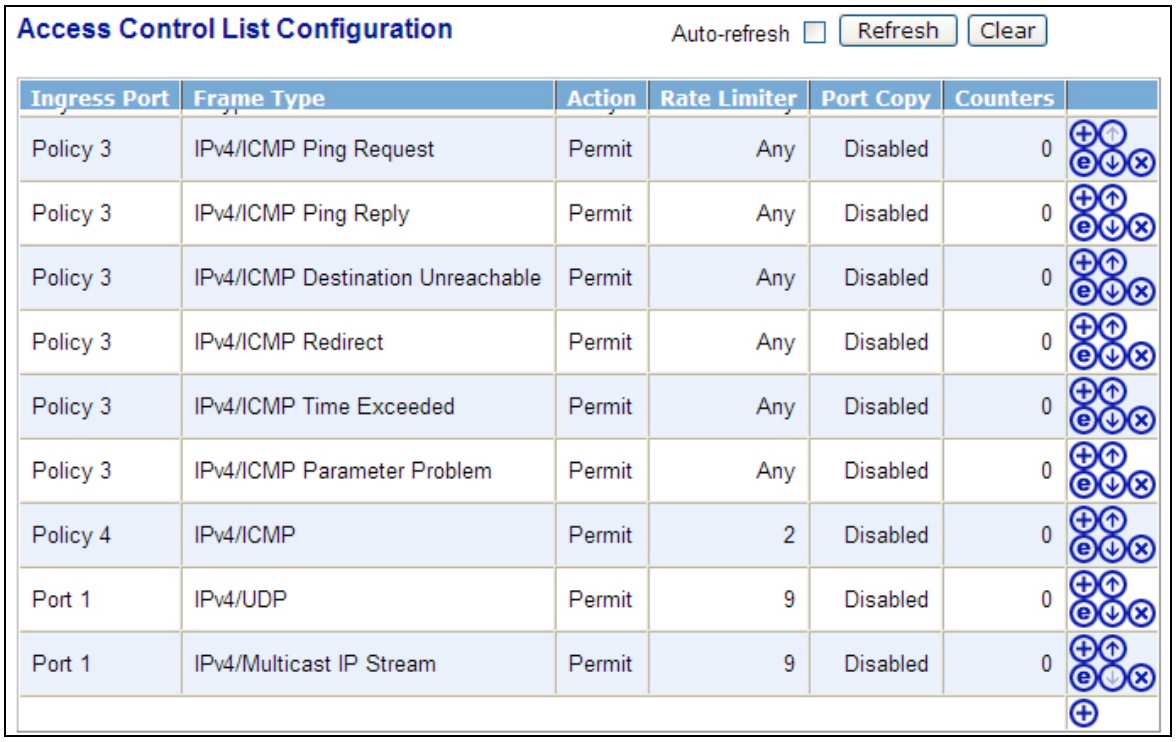


Figure 4-133. Set up Typical Network Application Rules Finish.

Parameter description:

Common Server: 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: TCP Port/ICMP/Multicast IP Stream/NetBIOS/Ping Request/Ping Reply/SNMP/SNMP Traps

Ingress Port: Any/Policy 1–8/Port 1–8

Action: Permit/Deny

Rate Limiter ID: Disabled/1–16

4.11 IP MAC Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC Addresses and port number with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet.

Function name: IP MAC Binding Configuration

Function description: The switch has IP-MAC Binding table. The maximum number of IP-MAC binding table entries is 1024. You can create authorized users manually. The function is global, so a user can enable or disable the function for all ports on the switch.

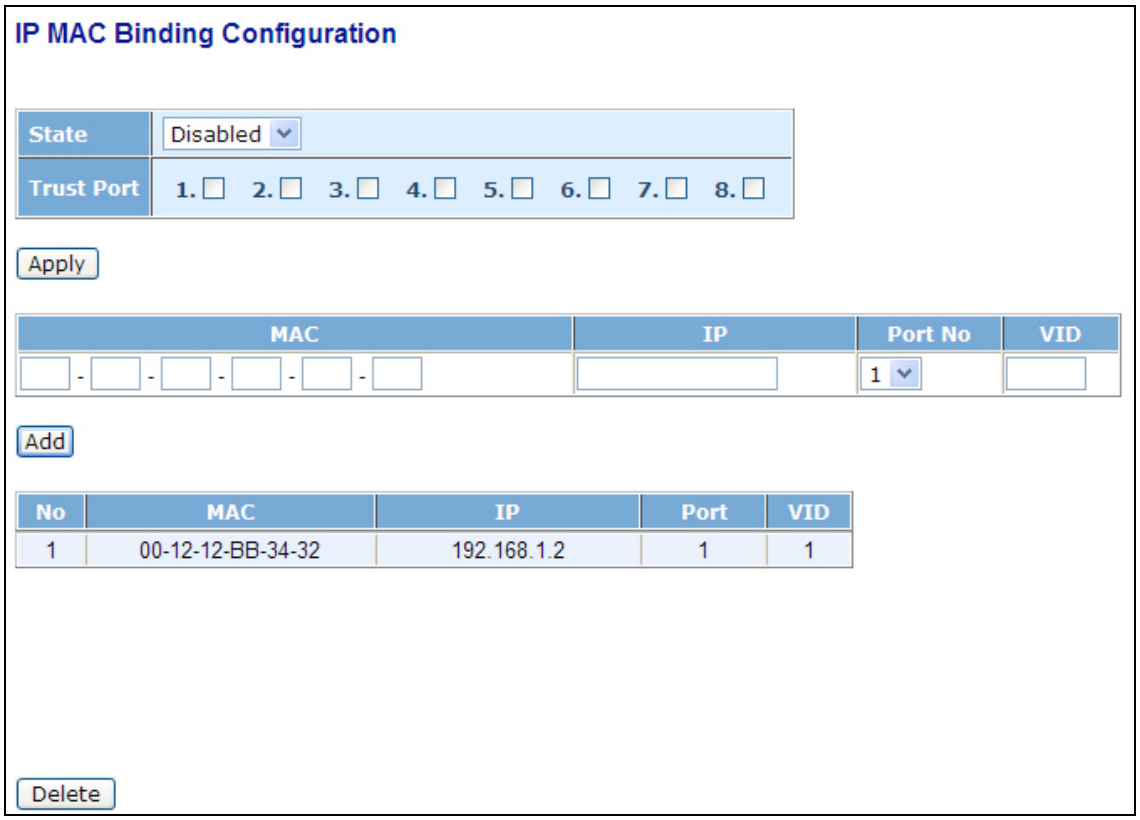


Figure 4-134. IP MAC binding configuration screen.

Parameters description:

State: Disabled/Enabled

Time Interval: 10/20/30

Time interval is for ARP echo, the switch will according to server table entries to send ARP echo.

Server/Client: The maximum number of IP-MAC binding client table is 512 entries. The maximum number of IP-MAC Binding server table is 64 entries.

MAC: Six-byte MAC Address: xx-xx-xx-xx-xx-xx

For example: 00-40-c7-00-00-01

IP: Four-byte IP Address: xxx.xxx.xxx.xxx

For example: 192.168.1.100

Port No: 1–8

VID: VLAN ID: 1–4094

Add: Input MAC, IP, Port and VID, then click on <Add> to create a new entry into the IP MAC Binding table

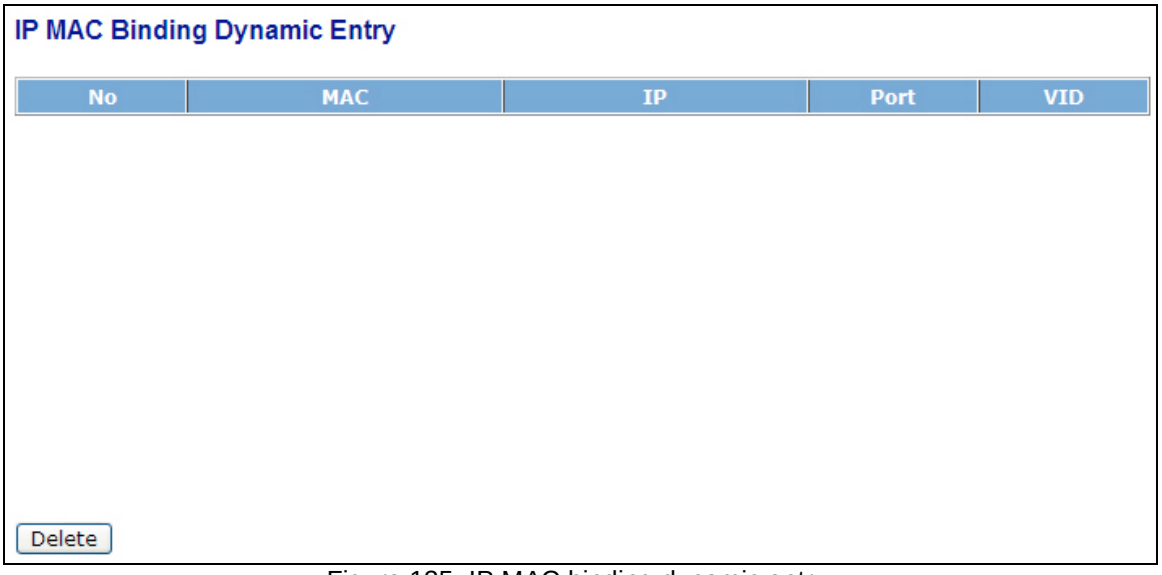


Figure 135. IP MAC binding dynamic entry.

Delete: Select one of entry from the table, then click on <Delete> to delete this entry.

4.12 802.1X Configuration

802.1X port-based network access control provides a method to restrict users from gaining access to the network resources through a 802.1X-enabled port without authentication. If a user wants to connect to the network through a port under 802.1X control, he must input his account name for authentication and gain authorization before sending or receiving any packets from a 802.1X-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1X control, the devices or end stations connected to a controlled port send the authentication request to the authenticator. The authenticator passes the request to the authentication server to authenticate and verify. The server tells the authenticator if the request is authorized for the ports. According to IEEE802.1X, there are three components implemented. They are Authenticator, Supplicant, and Authentication server.

Supplicant: An entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE requests it.

Authenticator: An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of the authentication message exchanged between it and a supplicant PAE.

The authenticator may request that the supplicant re-authenticate itself at a configured time period. Once re-authenticating the supplicant starts, the controlled port stays in the authorized state until re-authentication fails.

A port acting as an authenticator is two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized. An uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by a MAC bridge.

Authentication server: A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

Operation flow is shown in Figure 3-53. When a Supplicant PAE issues a request to an Authenticator PAE, Authenticator and Supplicant exchange an authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message with an authentication

server using EAP encapsulation. Before successfully authenticating, the supplicant can only connect to the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

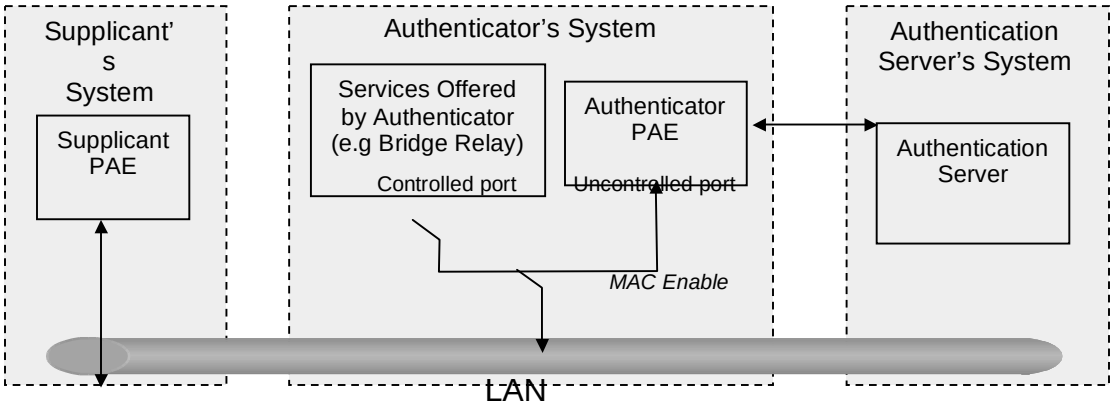


Figure 4-136. Authentication.

Figure 4-137 shows a typical configuration using a single supplicant, an authenticator, and an authentication server. B and C is in the internal network, and D is Authentication server running RADIUS. The switch at the central location acts as an Authenticator connecting to PC A. A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C. It must exchange the authentication message with the authenticator on the port it is connected to via an EAPOL packet. The authenticator transfers the supplicant's credentials to the Authentication server for verification. If authentication is successful, PC A will be allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have perform two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

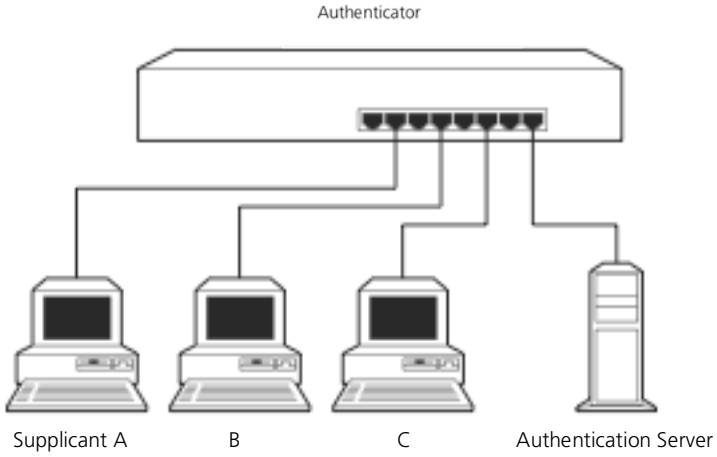


Figure 4-137. Typical configuration.

Figure 4-138 shows the 802.1X authentication procedure. Follow the steps listed below for the login based on 802.1X port access control management. The protocol used on the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. The access is blocked in this stage.

2. Initiating a session. Either the authenticator or the supplicant can initiate the message exchange. If the supplicant initiates the process, it sends an EAPOL-start packet to the authenticator PAE and authenticator will immediately respond with an EAP-Request/Identity packet.

3. The authenticator always periodically sends EAP-Request/Identity packets to the supplicant requesting the identity it wants to authenticate.

4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending it to the authenticator.

5. The Supplicant replies with an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server to confirm its identity.

6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant asking to input the user password via the authenticator PAE.

7. The supplicant converts the user password into the credential information in MD5 format and sends an EAP-Response with this credential information and a specified authentication algorithm (MD5 or OTP) to the Authentication server via the authenticator PAE. The authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or another algorithm.

8. If the user ID and password are correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.

9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. The supplicant is then authorized and the port connected to the supplicant and under 802.1X control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant failed to authenticate. The port it's connected to is in the unauthorized state, so the supplicant and the devices connected to this port won't be allowed to access the network.

10. When the supplicant issues an EAP-Logoff message to Authentication server, the port you are using is unauthorized.

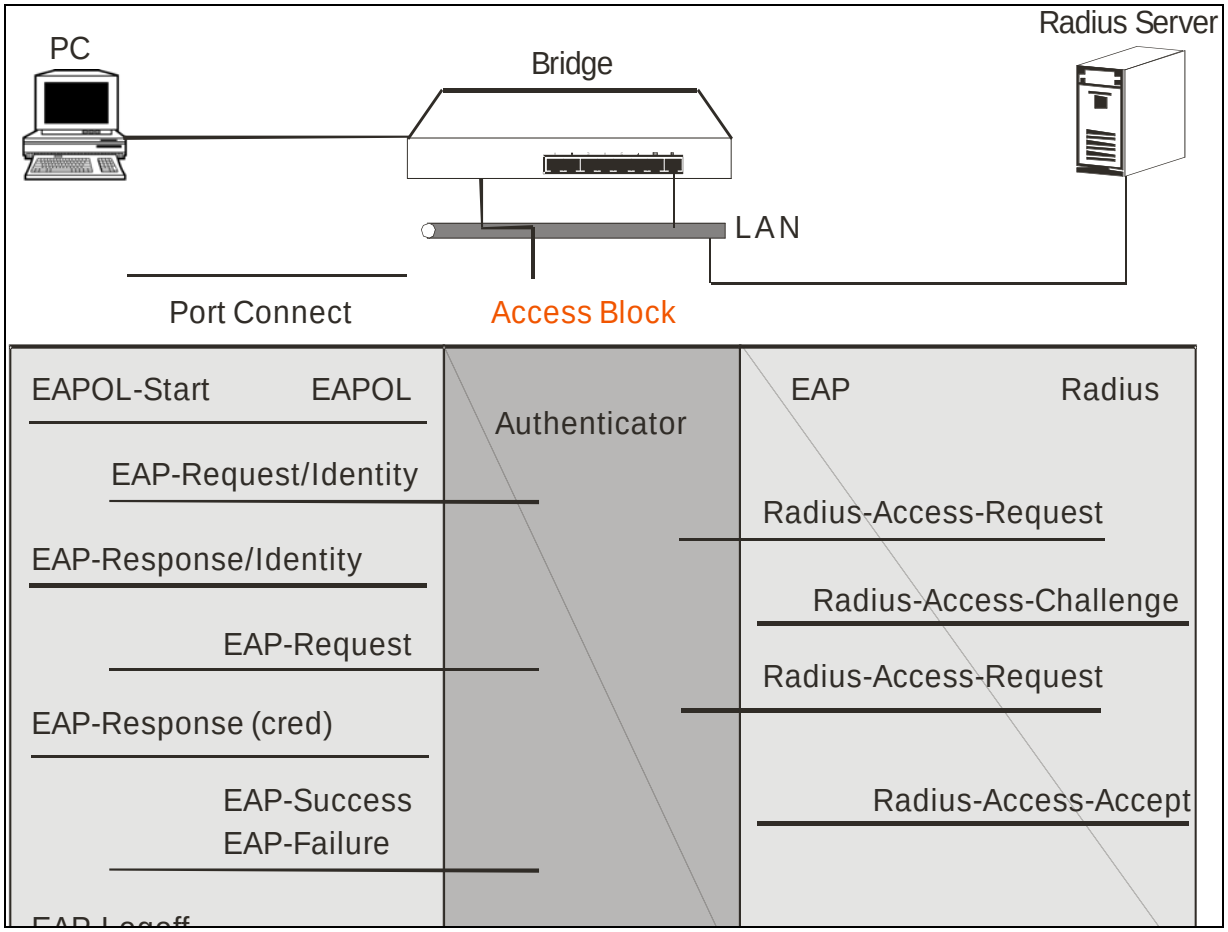


Figure 4-138. Authentication procedure.

MultiHost 802.1X is the only type of authentication supported in the switch. In this mode, once a supplicant is authorized, the devices connected to this port can access the network resources.

The 802.1X Port-based Network Access Control function supported by the switch is somewhat complex,. It just supports basic Multihost mode, which can distinguish between the device's MAC address and its VID. The following table summarizes the authentication status and the port status versus the status of port mode set in 802.1x Port mode, port control state, set in 802.1X port setting. Entry Authorized means a MAC entry is authorized.

Port Mode	Port Control	Authentication Port Status	
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

4.12.1 Server

Function name: 802.1X Server Configuration

Function description: Use this function to configure the global parameters for RADIUS authentication in an 802.1X port security application.

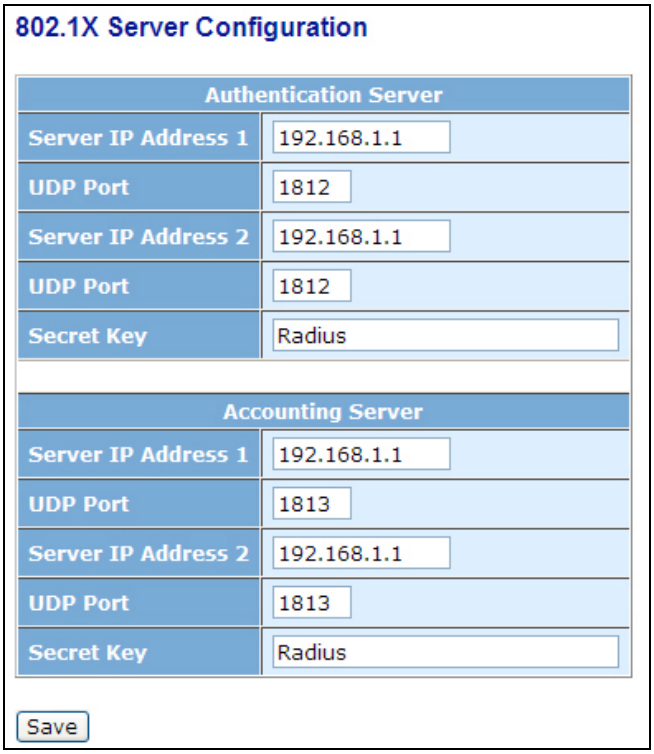


Figure 4-139. 802.1x server configuration screen.

Parameter description: Authentication Server

Server IP Server: Server IP address for authentication.

Default: 192.168.1.1

UDP Port: Default port number is 1812.

Secret Key: The secret key between authentication server and authenticator. It is a string of 1–31 characters. The character string may contain upper case, lower case, and 0-9 and is case-sensitive. Do not enter blank spaces between two characters. The default secret key is Radius.

Accounting Server

Server IP Server: Server IP address for authentication. Default: 192.168.1.1

UDP Port: Default port number is 1812.

Secret Key: The secret key between authentication server and authenticator. It is a string of 1–31 characters. The character string may contain upper case, lower case, and 0-9, and is case-sensitive. Do not place blank spaces between any two characters. Default: Radius

4.12.2 Port Configuration

Function name: 802.1X Port Configuration

Function description: This function is used to configure the parameters for each port in 802.1X port security application. Refer to the following parameters description for details.

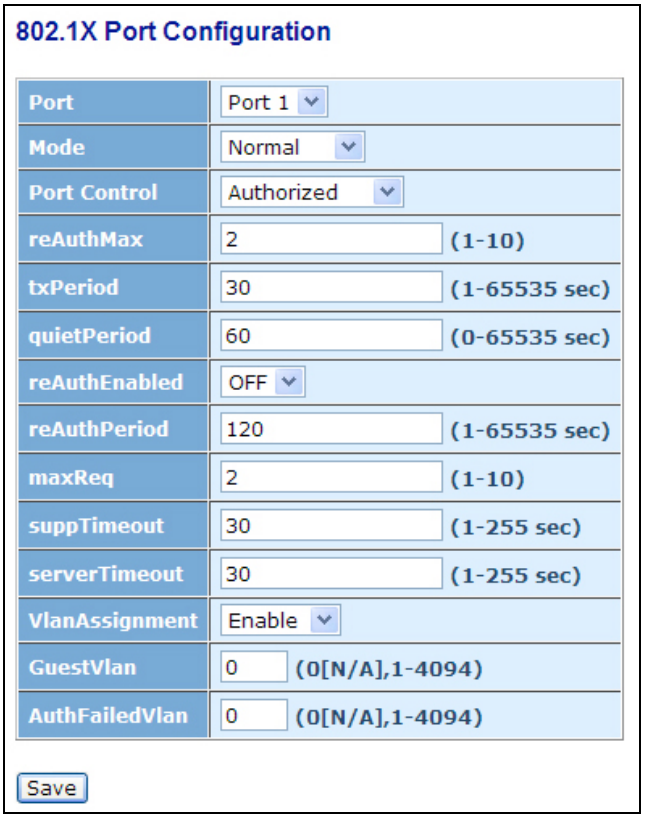


Figure 4-140. 802.1x port configuration.

Parameter description:

Port is the port number you want to select to configure its associated 802.1X parameters, including Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout, and Controlled direction.

Mode: Disable/Normal/Advanced/Clientless

Disable: Disable IEEE 802.1X for this port.

Normal: All clients attached to this port will be authorized when one of the clients is authorized.

Advanced: Each client attached to this port must do 802.1X authentication individually.

Clientless: The clients don't need to install the 802.1X client function. The client PC (for example WINDOW XP) does not need to enable 802.1X client function to do 802.1X authentication. The network administrator needs to configure the Radius server using each client's MAC address for the Radius account ID and password.

Port Control: Use this to set the authorization operation mode. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, and Auto. The default is Auto.

- ForceUnauthorized: The controlled port is forced to stay in the unauthorized state.
- ForceAuthorized: The controlled port is forced to stay in the authorized state.
- Auto: Whether the controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

reAuthMax(1–10): The number of authentication attempts permitted before the port becomes unauthorized. Default: 2

txPeriod (1-65535 s): The amount of time required to transmit the EAPOL PDU between the authenticator and the supplicant. Default: 30

Quiet Period (0-65535 s): A period of time during which we will not attempt to access the supplicant. Default: 60 seconds

reAuthEnabled: Choose whether regular authentication will take place for this port. Default: ON

reAuthPeriod (1-65535 s): A non-zero number of seconds between the periodic re-authentication of the supplicant. Default: 3600

max. Request (1–10): The maximum number of times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range is 1–10. Default: 2 times

suppTimeout (1-65535 s): A timeout condition in the exchange between the authenticator and the supplicant. The valid range is 1–65535. Default: 30 seconds.

serverTimeout (1-65535 s): A timeout condition in the exchange between the authenticator and the authentication server. The valid range is 1–65535. Default: 30 seconds

4.12.3 Status

Function name: 802.1X Status

Function description: Show each port's current IEEE 802.1X authentication operating mode and status.

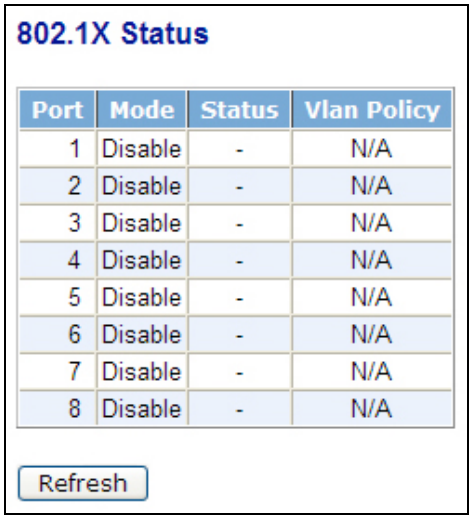


Figure 4-141. 802.1x status.

Parameter description:

Port: Port number: 1–8

Mode: Show this port's IEEE 802.1X operating mode: There are four modes: Disable, Normal, Advance, and Clientless.

Status: Show this port's IEEE 802.1X security current status: Authorized or Unauthorized

4.12.4 Statistics

Function name: 802.1X Port Statistics Port1

Function description: Show the IEEE 802.1X authentication related counters to monitor authenticator status.

802.1X Port Statistics Port 1 Port 1 Auto-refresh Refresh Clear

Authenticator Counters	
authEntersConnecting	0
authEapLogoffsWhileConnecting	0
authEntersAuthenticating	0
authAuthSuccessesWhileAuthenticating	0
authAuthTimeoutsWhileAuthenticating	0
authAuthFailWhileAuthenticating	0
authAuthEapStartsWhileAuthenticating	0
authAuthEapLogoffWhileAuthenticating	0
authAuthReauthsWhileAuthenticated	0
authAuthEapStartsWhileAuthenticated	0
authAuthEapLogoffWhileAuthenticated	0
Backend Authenticator Counters	
backendResponses	0
backendAccessChallenges	0
backendOtherRequestsToSupplicant	0
backendAuthSuccesses	0
backendAuthFails	0
802.1X MIB Counters	
dot1xAuthEapolFramesRx	0
dot1xAuthEapolFramesTx	0
dot1xAuthEapolStartFramesRx	0
dot1xAuthEapolLogoffFramesRx	0
dot1xAuthEapolRespIdFramesRx	0
dot1xAuthEapolRespFramesRx	0
dot1xAuthEapolReqIdFramesTx	0
dot1xAuthEapolReqFramesTx	0
dot1xAuthInvalidEapolFramesRx	0
dot1xAuthEapLengthErrorFramesRx	0
dot1xAuthLastEapolFrameVersion	0
dot1xAuthLastEapolFrameSource	00-00-00-00-00-00

Figure 4-142. 802.1x port statistics port 1.

Parameter description:

Port: Port Number: 1–8

Auto- refresh: Refresh the authenticator counters in the web UI automatically.

Refresh: Click on <Refresh> to update the authenticator counters in the web UI.

Clear: Click on <Clear> to clear all authenticator counters in the web UI.

4.13 Trunking Configuration

Use the Port Trunking Configuration to configure the Link Aggregation settings. You can bundle more than one port with the same speed, full duplex, and the same MAC to be a single logical port. The logical port aggregates these ports' bandwidth. You can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth that's three times as high as a single Fast Ethernet port.

The switch supports two kinds of port trunking:

LACP: Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1–4) to form a logical "trunked port." The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a member of a "trunk group" (also called aggregator). LACP is safer than the other trunking method: static trunk.

The switch LACP does not support the following:

- Link Aggregation across switches
- Aggregation with a non-IEEE 802.3 MAC link
- Half-duplex mode operation
- Aggregate the ports with different data rates

Static Trunk: Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1–4, this Static groupID can be the same as another LACP groupID) to form a logic "trunked port." The benefit of using the Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should aggregate together to form a "logical trunked port." We recommend using Static Trunk on both ends of a link. Note that low speed links will stay in "not ready" state when using static trunk to aggregate high speed links.

There are some system restrictions about the port aggregation function on the switch: In the management point of view, the switch supports a maximum of 8 trunk groups for LACP and an additional 8 trunk groups for Static Trunk. In the system capability view, only 8 "real trunked" groups are supported. An LACP trunk group with more than one ready member portsis a "real trunked" group. An LACP trunk group with only one or less than one ready member-ports is not a "real trunked" group. Any Static trunk group is a "real trunked" group.

Per Trunking Group supports a maximum of 4 ready member ports. Some decisions will automatically be made by the system while you are configuring your trunking ports. Some configuration examples are listed below:

1. 8 ports have already used Static Trunk Group ID 1, the 13th port willing to use the same Static Trunk Group ID will be automatically set to use the "None" trunking method and its Group ID will change to 0. This means the port won't aggregate with other ports.

2. 4 ports all use LACP Trunk Group ID 1. At most, 2 ports can aggregate together and transit into the ready state.

3. A port using the "None" trunking method or Group ID 0 will be automatically set to use the "None" trunking method with Group ID 0.

4.13.1 Port

Function name: Trunk Port Setting/Status

Function description: Port setting/status is used to configure the trunk property for each port in the switch system.

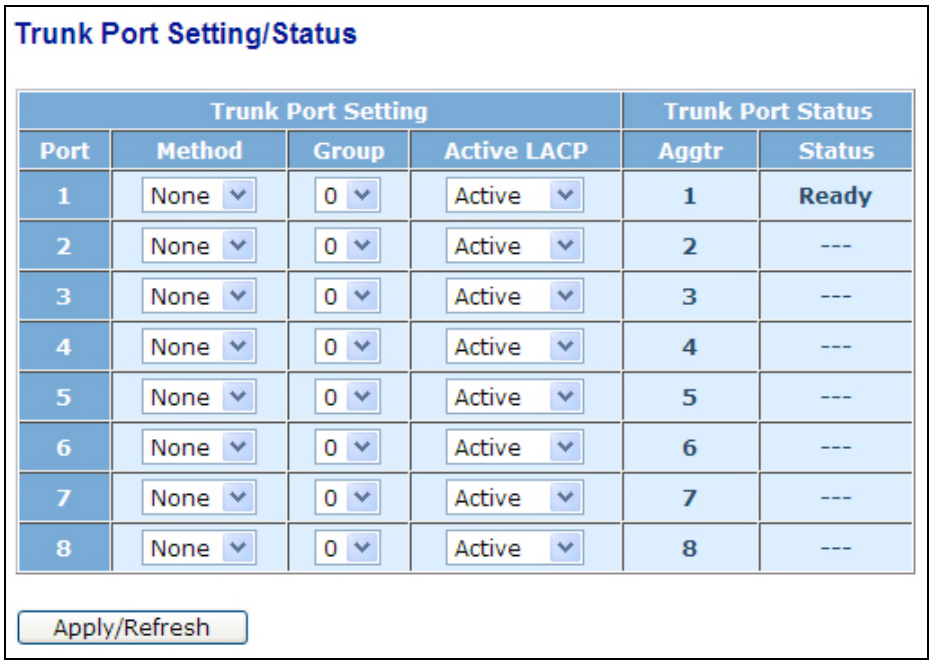


Figure 4-143. Trunk port setting/status screen.

Parameter description:

Port: Port Number: 1–8

Method: This determines the method a port uses to aggregate with other ports.

None: When set to none, the port will not aggregate with any other port.

LACP: A port uses LACP as its trunk method to aggregate with other ports also using LACP.

Static: A port uses Static Trunk as its trunk method to aggregate with other ports also using Static Trunk.

Group: Ports choosing the same trunking method other than "None" must be assigned a unique Group number (that is, a Group ID, valid value is from 1 to 8) to declare that they want to aggregate with each other.

Active LACP: This field is only referenced when a port's trunking method is LACP.

Active: An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

Passive: A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

Aggtr: Aggtr is an abbreviation of "aggregator." Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

Status: This field represents the trunking status of a port that uses a trunking method other than "None." It also represents the management link status of a port that uses the "None" trunking method. "---" means "not ready."

4.13.2 Aggregator View

Function name: Aggregator View

Function description: Displays the current port trunking information from the aggregator point of view.

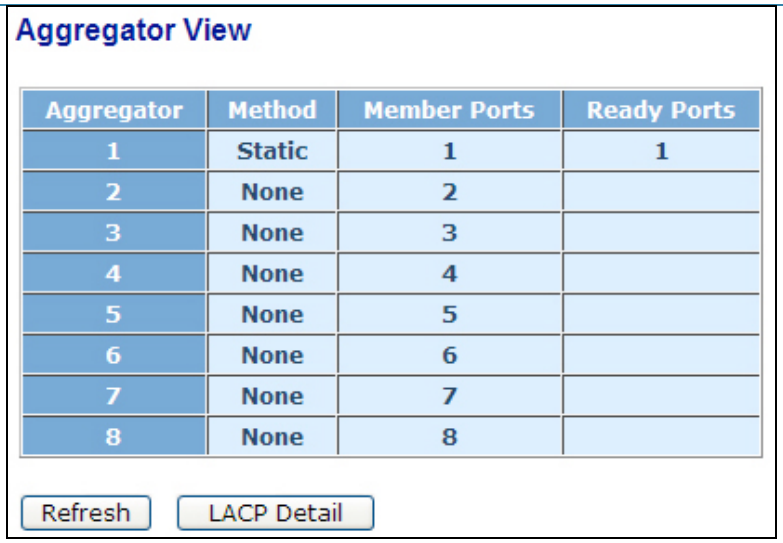


Figure 4-144. Aggregator view screen.

Parameter description:

Aggregator: Shows the aggregator ID (from 1 to 8) of every port. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No.

Method: Shows the method a port uses to aggregate with other ports.

Member Ports: Show all member ports of an aggregator (port).

Ready Ports: Show only the ready member ports within an aggregator (port).

4.13.3 Aggregation Mode Configuration

Function name: Aggregation Mode Configuration

Function description: Use to configure the current port aggregate mode with 4 types.

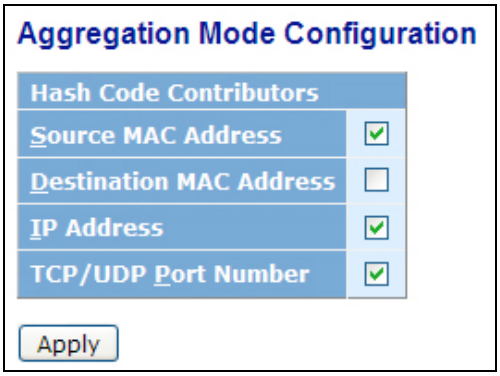


Figure 4-145. Aggregation mode configuration.

Parameter description:

Source MAC Address: Enables source MAC address for Aggregate Mode.

Destination MAC Address: Enables destination MAC address for Aggregate Mode.

IP Address: Enables IP address for Aggregate Mode.

TCP/UDP Port Number: Enables TCP/UDP Port Number for Aggregate Mode.

4.13.4 LACP System Priority

Function name: LACP System Priority

Function description: Sets the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP that will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The user can set the System Priority. Its range is from 1 to 65535. Default: 32768

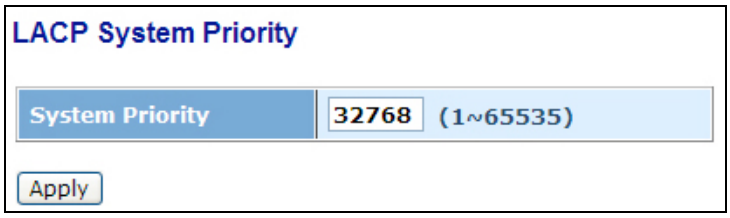


Figure 4-146. LACP system priority.

Parameter description:

System Priority: Show the System Priority part of a system ID (1–65535)

4.14 STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, make sure that only one path is active between any two nodes on the network at a time. Users can enable Spanning Tree Protocol on the switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

4.14.1 Status

Function name: STP Status

Function description: In the Spanning Tree Status, the user can read 12 parameters to know the STP current status. The 12 parameters' descriptions are listed in the following table.

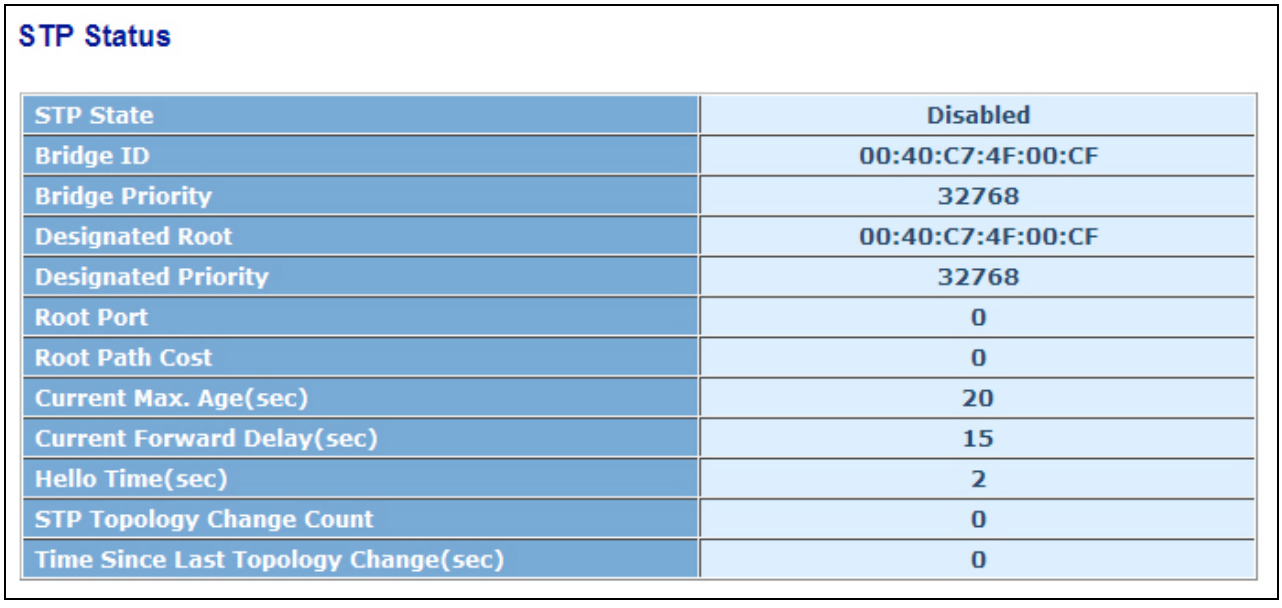


Figure 4-147. STP status.

Parameter description:

STP State: Show the current STP Enabled / Disabled status. Default is "Disabled."

Bridge ID: Show the switch's bridge ID (it stands for the switch's MAC address.)

Bridge Priority: Show this switch's current bridge priority setting. Default is 32768.

Designated Root: Show root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.

Designated Priority: Show the current root bridge priority.

Root Port: Show the port number connected to root bridge with the lowest path cost.

Root Path Cost: Show the path cost between the root port and the designated port of the root bridge.

Current Max. Age: Show the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from the root bridge until the maximum age time counts down to 0, the bridge will malfunction and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine which bridge is the root. Maximum Age time is assigned by the root bridge in units of seconds. The default is 20 seconds.

Current Forward Delay: Shows the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a bridge port.

Hello Time: Shows the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending a hello message every "hello time" seconds to the bridge attached to its designated port.

STP Topology Change Count: STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will reset to 0..

Time Since Last Topology Change: Time Since Last Topology Change is the accumulated time elapsed in unit of seconds since the last STP Topology Change was made. When Topology Change is initiated again, this counter will reset to 0. It will also count again once the STP topology Change is completed.

4.14.2 Configuration

The STP, Spanning Tree Protocol, includes RSTP. In the Spanning Tree Configuration, there are six parameters open for the user to configure. Each parameter description is listed below.

Function name: STP Configuration

Function description: You can set the following Spanning Tree parameters to control STP function enable/disable, select mode RSTP/STP, and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is "Disable."

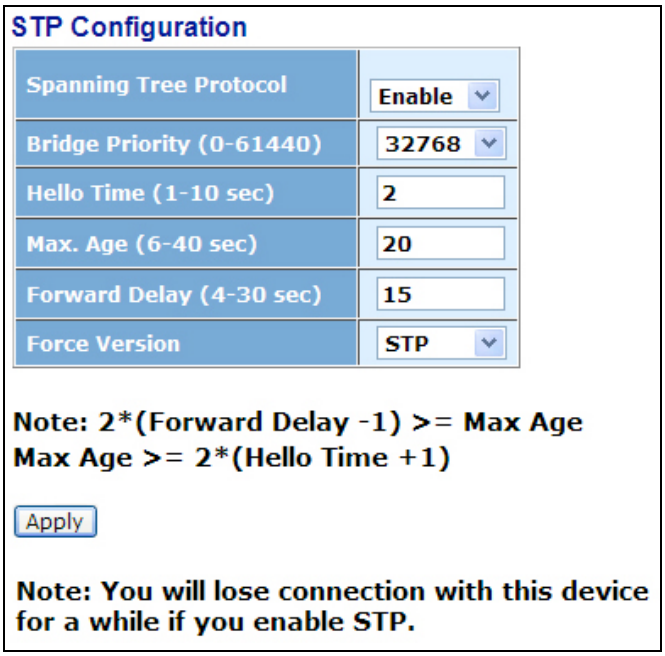


Figure 4-148. STP configuration.

Parameter description:

Spanning Tree Protocol: Set 802.1W Rapid STP function to Enable or Disable. The default is "Disable.

Bridge Priority: The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the LPB4008A as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0–61440. The default is 32768.

Hello Time: Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. When the LPB4008A is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1–10 in units of seconds. The default is 2 seconds.

Max. Age: When the LPB4008A is the root bridge, the entire LAN will apply the figure set by this switch as their maximum age time. When a bridge receives a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge as a malfunction and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6– 40 seconds. The default is 20 seconds.

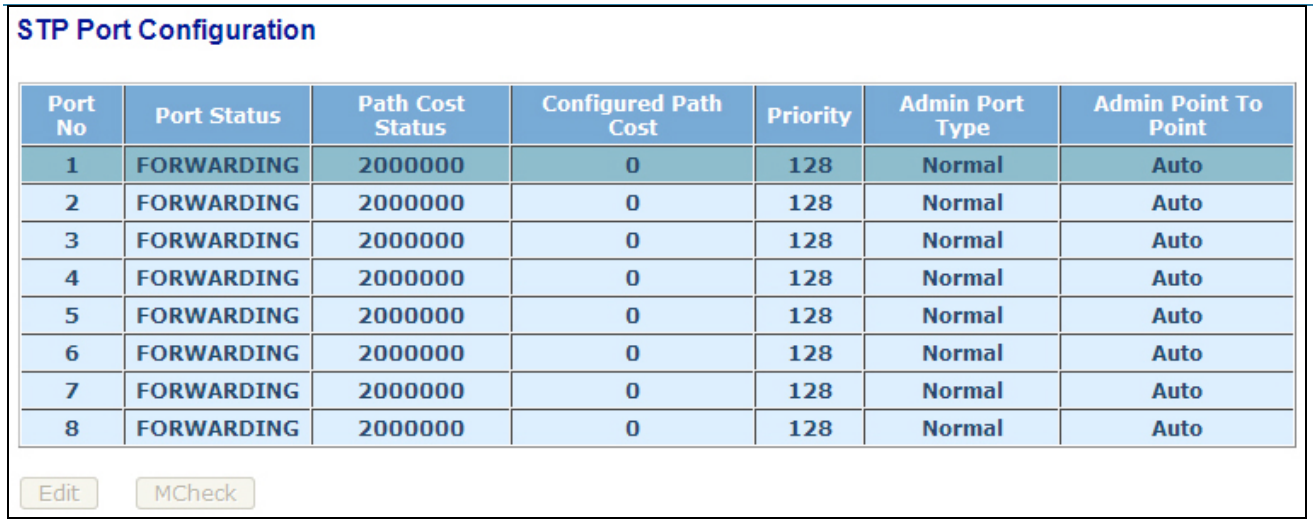
Forward Delay: You can set the root bridge forward delay time. This figure is set by the root bridge only. The forward delay time is defined as the time spent from the Listening state moving to the Learning state and also from the Learning state moving to the Forwarding state of a port in bridge. The forward delay time contains two states, going from the Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then the total forward delay time will be 30 seconds. The STP convergent time will be more than 30 seconds because of some other factors. The valid value is 4–30 seconds, and the default is 15 seconds.

Force Version: Two options are offered for the user's choosing STP algorithm. One is RSTP and the other is STP. If you choose STP, RSTP will run as a legacy STP. The switch supports RSTP (802.1w), which is backward compatible with STP (802.1d).

4.14.3 STP Port Configuration

Function name: STP Port Setting

Function description: In the STP Port Setting, one item selection and five parameters settings are offered for each user's setup. Users can disable and enable each port by selecting each Port Status item. Users also can set the "Path Cost" and "Priority" of each port by filling in the desired value. And set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.



STP Port Configuration

Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	FORWARDING	2000000	0	128	Normal	Auto
2	FORWARDING	2000000	0	128	Normal	Auto
3	FORWARDING	2000000	0	128	Normal	Auto
4	FORWARDING	2000000	0	128	Normal	Auto
5	FORWARDING	2000000	0	128	Normal	Auto
6	FORWARDING	2000000	0	128	Normal	Auto
7	FORWARDING	2000000	0	128	Normal	Auto
8	FORWARDING	2000000	0	128	Normal	Auto

Edit MCheck

Figure 4-149. STP port configuration.

Parameter description:

Port Status displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states (according to the 802.1w specification):

▪ DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.

NOTE: Three other states (Disable state, BLOCKING state, and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

▪ LEARNING state indicates this port can now contribute its learning knowledge but still cannot forward packets.

▪ FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.

Path Cost Status: The value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would most likely become the Root Port.

Configured Path Cost: The range is 0– 200,000,000. In the switch, if path cost is set to zero, the STP will get the recommended value resulting from auto-negotiation of the link accordingly and display this value in the Path Cost Status field. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

802.1w RSTP as the recommended value: (Valid range: 1– 200,000,000)
10 Mbps: 2,000,000

100 Mbps: 200,000

1 Gbps: 20,000

Default: 0

Priority: Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0–240. The default is 128.

Admin Edge Port: If a user selects "Yes," this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transition to the forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology remains unchanged. Unlike the designated port or root port though, an edge port will transition to a normal spanning-tree port immediately if it receives a BPDU. The default is No.

Admin Point To Point: A port is a point-to-point link, from RSTP's view, if it is in full-duplex mode. It is a shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will cause the port to transition to forwarding state.

There are three parameters, Auto, True, and False, used to configure the type of the point-to-point link. If you configure this parameter to be Auto, it means RSTP will use the duplex mode resulting from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. The result may be half-duplex, in this case, the port will not fast transition to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transitioned to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port. Default: Auto

M Check: Migration Check. It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click on the **<M Check>** button to send a RSTP BPDU from the port you specified.

4.15 MSTP

The implementation of MSTP is according to IEEE 802.1Q 2005 Clause 13—Multiple Spanning Tree Protocol. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. Proper configuration of MSTP in an 802.1Q VLAN environment can ensure a loop-free data path for a group of VLANs within an MSTI. Redundant path and load balancing in a VLAN environment is also achieved via this feature. .A spanning tree instance called CIST (Common and Internal Spanning Tree) always exists. Up to 64 more spanning tree instances (MSTIs) can be provisioned.

4.15.1 Status

Function name: MSTP State

Function description: Enable or disable MSTP. Select a version of Spanning Tree MSTP operating protocol.

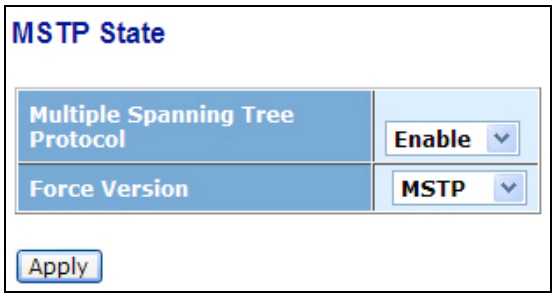


Figure 4-150. MSTP state.

Parameter description: Multiple Spanning Tree Protocol: Disabled / Enabled

Force Version: STP / RSTP / MSTP

4.15.2 Region Config

Function name: MSTP Region Config

Function description: Configures the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

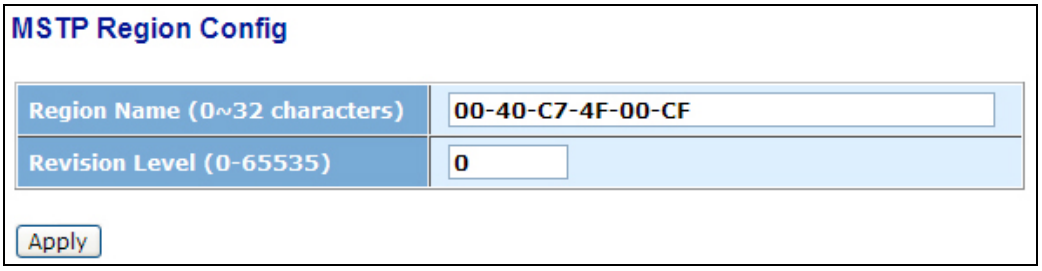


Figure 4-151. MSTP region configuration.

Parameter description:
Region Name: 0-32 characters (A variable length text string encoded within a fixed field of 32 octets, that conforms to RFC 2271's definition of SnmpAdminString.)

Revision Level: 0-65535

4.15.3 Instance View

Function name: MSTP Instance Config

Function description: Provides an MST instance table that includes information (an MSTI's VLAN membership) of all spanning instances provisioned in the particular MST region that the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.

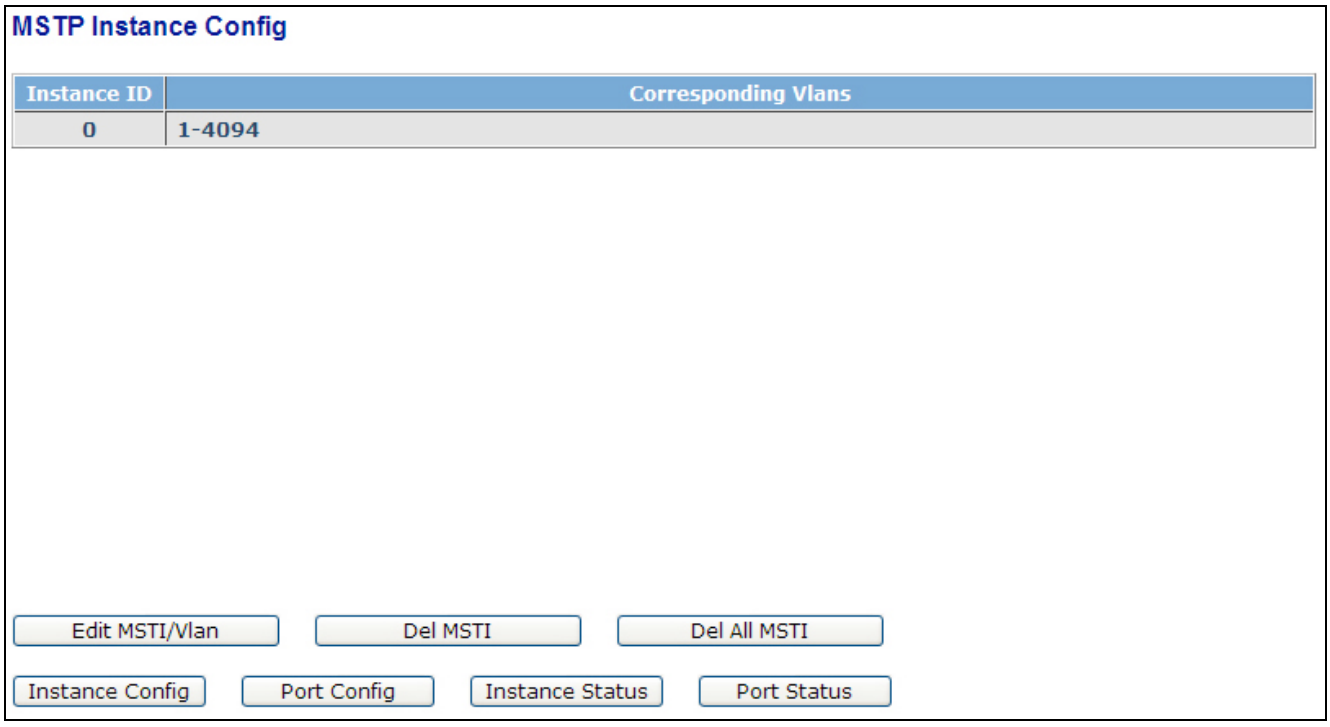


Figure 4-152. MSTP instance configuration.

Parameter description:

Instance ID: Every spanning tree instance needs to have a unique instance ID within 0–4095. Instance 0 (CIST) always exists and cannot be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one VLAN must be provisioned for an MSTI to declare the need for the MSTI to exist.

Corresponding VLANs: 0–4095. Multiple VLANs can belong to an MSTI. All VLANs that are not provisioned through this will be automatically assigned to Instance 0 (CIST).

Edit MSTI/VLAN: (Figure 4-153) Add an MSTI and provide its VLAN members or modify VLAN members for a specific MSTI.

Del MSTI: Delete an MSTI.

Del All MSTI: Deleting all provisioned MSTIs at a time.

Instance Configuration: (Figure 4–154) Provision spanning tree performance parameters per instance.

Port Config: (Figure 4–155) Provision spanning tree performance parameters per instance per port.

Instance Status: (Figure 4-156) Show the status report of a particular spanning tree instance.

Port Status: (Figure 4-157) Show the status report of all ports regarding a specific spanning tree instance.

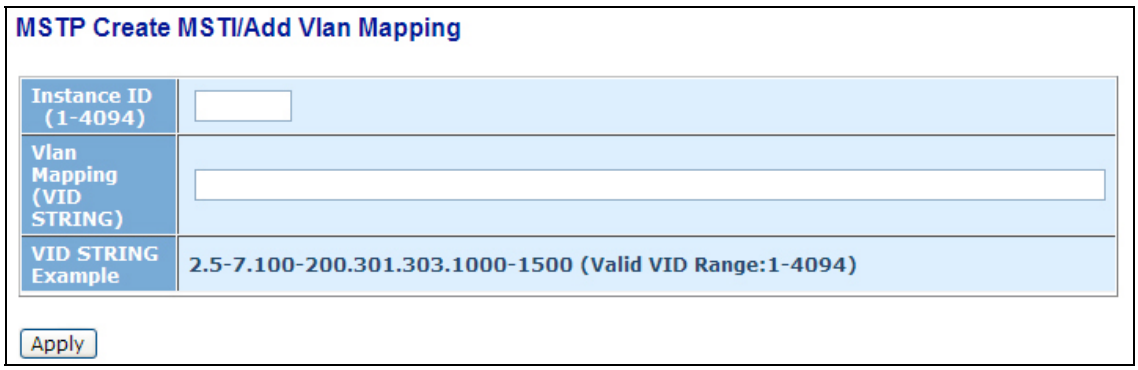


Figure 4-153. Edit MSTI / Vlan

Parameter description:

Vlan Mapping: VID STRING

VID STRING Example: 2.5-7.100-200.301.303.1000-1500 (Valid VID Range: 1–4094)

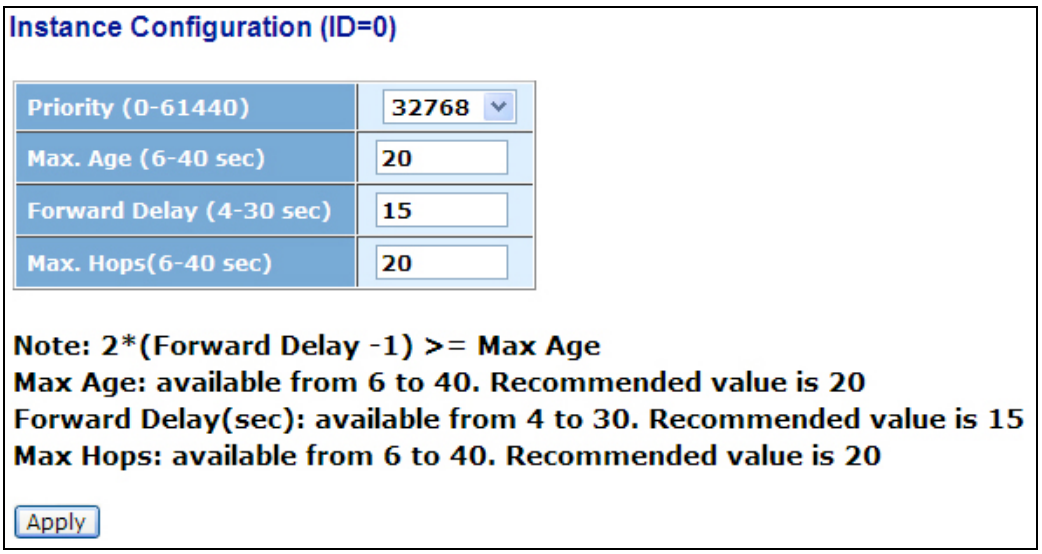


Figure 4-154. Instance Config.

Parameter description:

Priority: The priority parameter used in the CIST(Common and Internal Spanning Tree) connection.

0/4096/8192/12288/16384/20480/24576/28672/32768/36864/40960/45056/49152/53248/57344/61440

MAX. Age: 6–40 sec. The same definition as in the RSTP protocol.

Forward Delay: 4–30 sec. The same definition as in the RSTP protocol.

MAX. Hops: 6–40 sec. A new parameter for the multiple spanning tree protocol. It is used in internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message decreases by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid.

Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root).

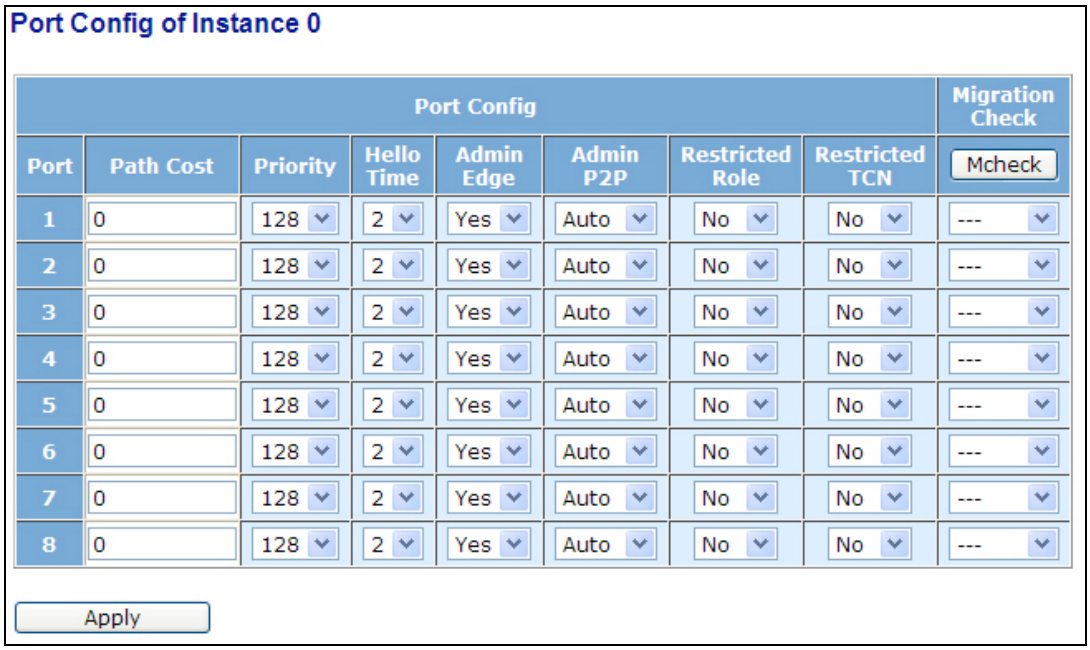


Figure 4-155. Port Config.

Parameter description:

Port: 1–8

Path Cost: 1– 200,000,000

This has the same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Priority: 0/16/32/48/64/80/96/112/128/144/160/176/192/208/224/240

This has the same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Hello Time: 1/2

In contrast with RSTP, Hello Time in MSTP is a per port setting for the CIST.

Admin Edge: Yes/No

This has the same definition as in the RSTP specification for the CIST ports.

Admin P2P: Auto/True/False

This has the same definition as in the RSTP specification for the CIST ports.

Restricted Role: Yes/No

"Yes" 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 is selected. This parameter is "No" by default. If set, it can cause lack of spanning tree connectivity. It is 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.

Restricted TCN: Yes/No

"Yes" causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is "No" by default. If set it can cause temporary loss of connectivity after changes in a spanning tree's 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. It checks the status of MAC operation for the attached LANs transitions frequently.

Mcheck: The same definition as in the RSTP specification for the CIST ports.

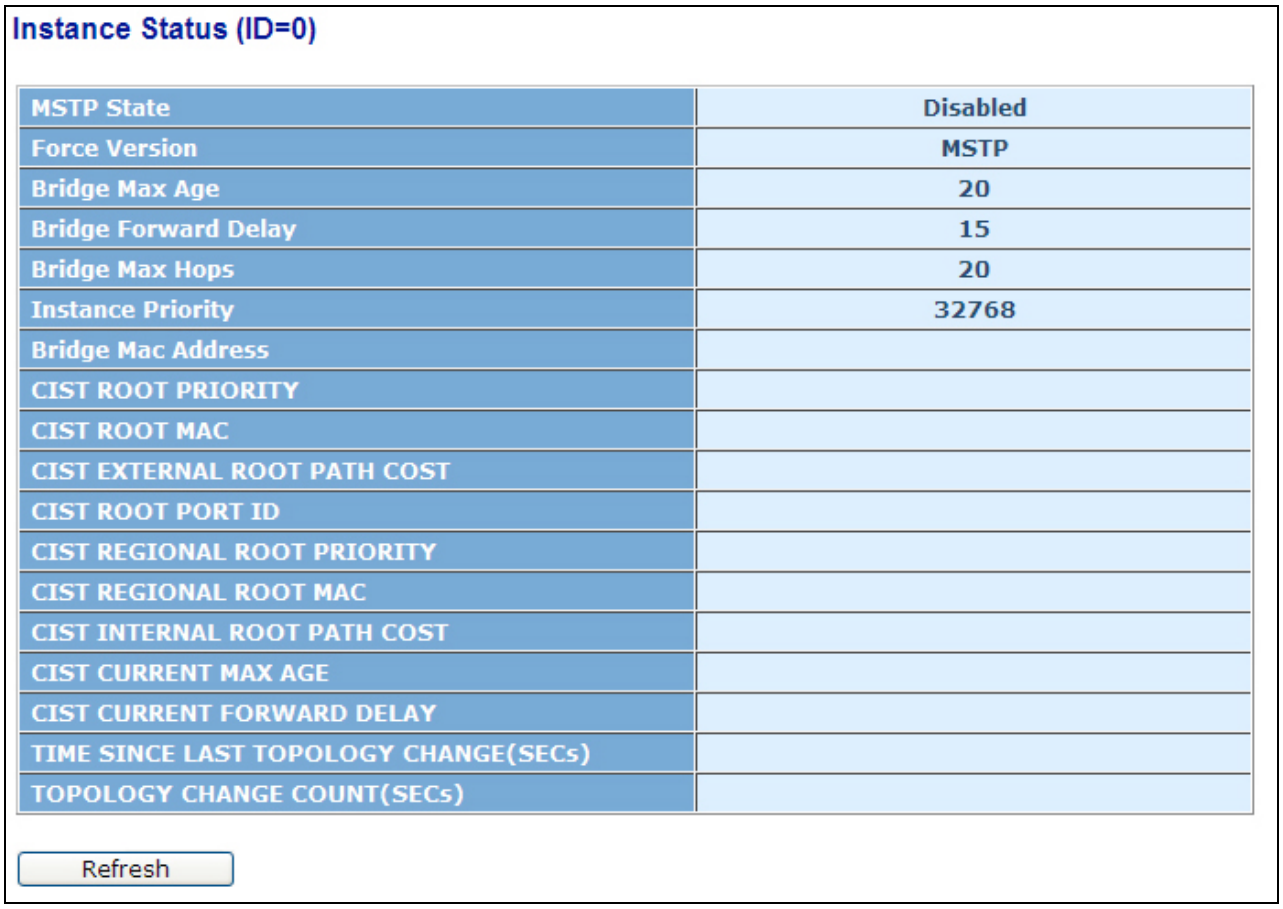


Figure 4-156. Instance Status.

Parameter description:

MSTP State: MSTP protocol is Enable or Disable

Force Version: Shows the current spanning tree protocol version configured.

Bridge Max Age: Shows the bridge's Max Age setting.

Bridge Forward Delay: Shows the bridge's Forward Delay setting.

Bridge Max Hops: Shows the bridge's Max Hops setting.

Instance Priority: Spanning tree priority value for a specific tree instance (CIST or MSTI).

Bridge Mac Address: The bridge's Mac Address.

CIST ROOT PRIORITY: The CIST root bridge's spanning tree priority value.

CIST ROOT MAC: The CIST root bridge's MAC address.

CIST EXTERNAL ROOT PATH COST: Root path cost value from the point of view of the bridge's MST region.

CIST ROOT PORT ID: The port ID of the bridge's root port. In MSTP, a peer port of a root port may reside in a different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.

CIST REGIONAL ROOT PRIORITY: Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region is the root bridge of the CST (Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST (Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.

CIST REGIONAL ROOT MAC: Mac Address of the CIST regional root bridge.

CIST INTERNAL ROOT PATH COST: Root path cost value from the point of view of the bridges inside the IST.

CIST CURRENT MAX AGE: Max Age of the CIST Root bridge.

CIST CURRENT FORWARD DELAY: Forward Delay of the CIST Root bridge.

TIME SINCE LAST TOPOLOGY CHANGE (SECs): Time Since Last Topology Change is the elapsed time in units of seconds for a bunch of "Topology Change and (or) Topology Change Notification receiving" to occur. When a new series of Topology Changes occur again, this counter will be reset to 0.

TOPOLOGY CHANGE COUNT (SECs): The per spanning tree instance Topology Change Count expresses the time spent in units of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once there is no topology change occurring and no more topology change notifications are received, the Topology Change count will be reset to 0.

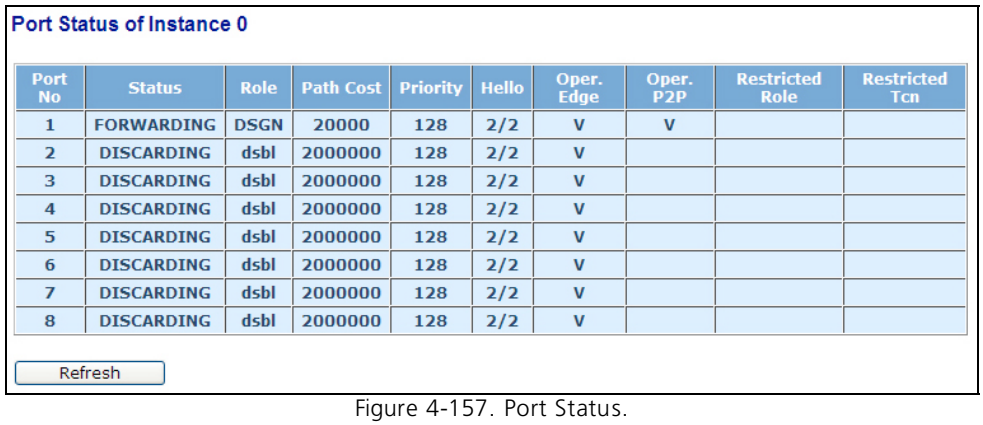


Figure 4-157. Port Status.

Parameter description:

Port No: 1–8

Status: The forwarding status.has the same definition as the RSTP specification. Possible values are "FORWARDING," "LEARNING," and "DISCARDING."

Status: The port's role in the spanning tree topology. Possible values are "dsbl"(disable port), "alt"(alternate port) , "bkup"(backup port), "ROOT"(root port), "DSGN"(designated port), and "MSTR"(master port). The last 3 are possible port roles for a port to transition to FORWARDING state.

Path Cost: Display port path cost value for each port in a particular spanning tree instance.

Priority: Display port priority value for each port in a particular spanning tree instance.

Hello: per port Hello Time display.

Current Hello Time/Hello Time Setting

Oper. Edge: Whether or not a port is an Edge Port.

Oper. P2P: Whether or not a port is a Point-to-Point Port.

Restricted Role: Same as mentioned in "Port Config"

Restricted Tcn: Same as mentioned in "Port Config"

4.16 Mirror

Function name: Mirror Configuration

Function description: Mirror Configuration monitors the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively. The traffic received by Port B will be copied to Port A for monitoring.

NOTE: When you configure the mirror function, avoid setting a port to be a sniffer port and aggregated port at the same time.

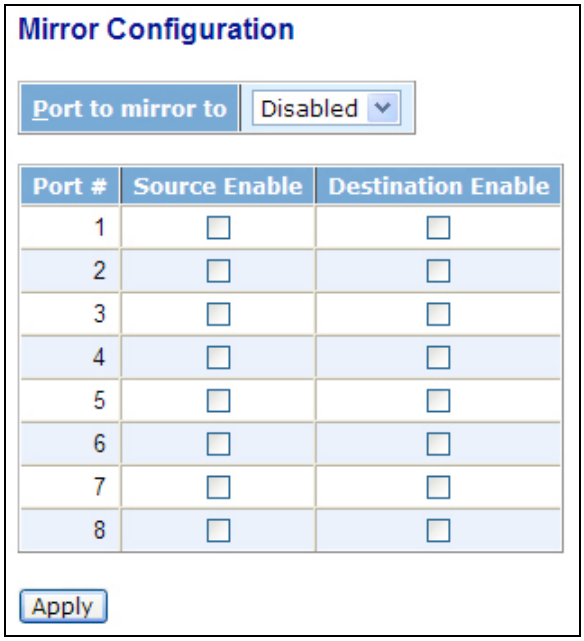


Figure 4-158. Mirror configuration.

Parameter description:

Port to mirror to: Range: Disabled/Port 1–8

Port #: Range: 1–8

Source Enable: Source enable means the monitored port ingress traffic will be copied to a monitoring port.

Destination Enable: The destination enable means the monitored port egress traffic will be copied to a monitoring port.

4.17 Multicast

This function establishes which multicast groups forward the multicast packet to the member ports. This avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as broadcast packets. Without IGMP Snooping, the multicast packet forwarding function functions in the same way as broadcast packet forwarding.

A switch supports IGMP Snooping with query, report and leave. A type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the Multicast table's information when a member (port) joins or leaves an IP Multicast Destination Address. Once a switch receives an IP multicast packet, it will forward the packet to the members who were joined in a specified IP multicast group.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that was not built in advance.

4.17.1 IGMP Mode

Function name: IGMP Mode Configuration

Function description: IGMP mode enables the switch to issue the IGMP function. This enables IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the *upstream interface*. The router on the upstream interface should be running IGMP.

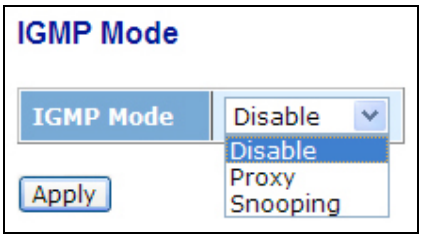


Figure 4-159. IGMP Mode.

Parameter description:

IGMP Mode: Choose the IGMP mode "Disable," "Proxy," or "Snooping,' from the drop-down menu.

4.17.2 IGMP Proxy

Function name: IGMP Proxy Configuration

Function description: IGMP proxy enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The switch acts as a *proxy* for its hosts.

Enable IGMP proxy on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

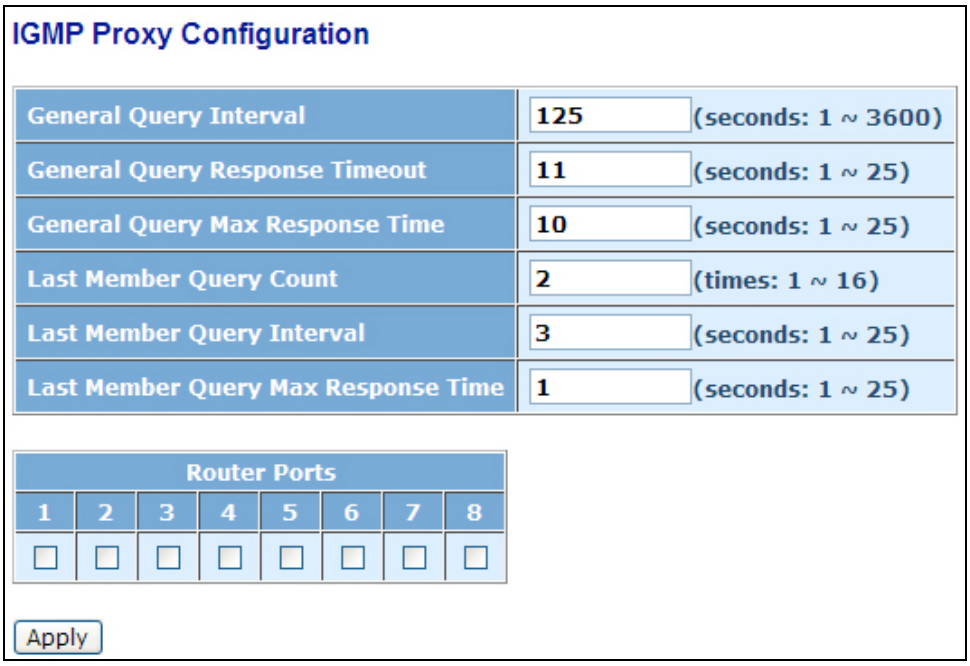


Figure 4-160. IGMP Proxy.

Parameter description:

IGMP Proxy Enable: This function supports IGMP Proxy Enable on the Switch.

Enable: Choose "IGMP Proxy Enable" to enable IGMP Proxy on Switch. Default: Disable

Unregister IPMC Flooding Enable: Set unregister to prevent the traffic from appearing in the multicast table for flooding.

General Query Interval: Set the switch's general sending query period time. (Available: 1–3600 seconds)

General Query Response Timeout: Set the switch's timeout value. (Available: 1–25 seconds)

General Query Max Response Time: Set the max response code value of the general query packet. (Available: 125 seconds)

Last Member Query Count: Set the frequency. When the Switch receives IGMP leave then switch send specific query frequency. (Available: 1~16 secs)

Last Member Query Interval: Set the frequency that the Switch will send specific queries. (Available: 1–25 seconds)

Last Member Query Max Response Time: Set the max response code value in the specific query packet. (Available: 1–25 seconds)

Update Interval of Router Port: To set the time interval that the interface receives IGMP query packets. (Available: 1–3600 seconds)

Router Ports: Set which interface connects to the IGMP Router, and the switch that send/sreceives IGMP report/leave port. Router ports may be only one or more than one. Apply: To save all configurations.

4.17.3 IGMP Snooping

Function name:

IGMP Snooping Configuration

Function description:

IGMP Snooping enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The switch acts with Snooping mode for its hosts. Enable IGMP Snooping on the switch.

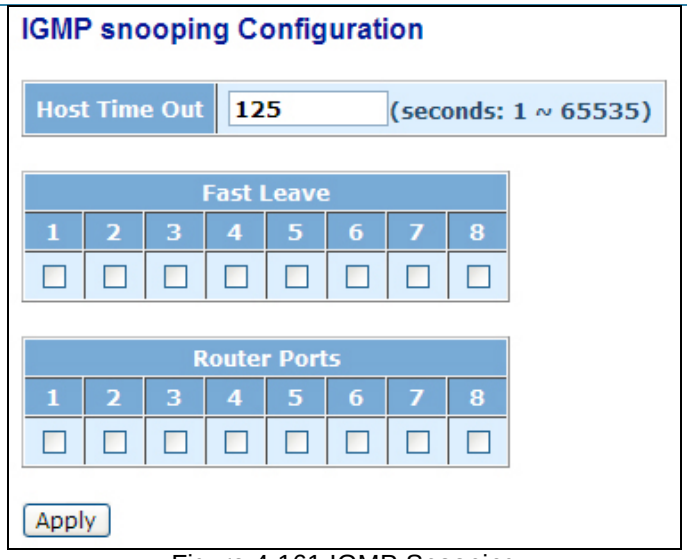


Figure 4-161 IGMP Snooping

Parameter description:

Host Time Out: Set IGMP Snooping enable and the Host packet received by Switch timeout period. The units are seconds and time range is from 1 to 65535. The default is 125 seconds.

Fast Leave: Set which port will enable the Fast leave mode in IGMP snooping mode.

Router Ports: Set which port wil be a Router Port in IGMP snooping mode.

4.17.4 IGMP Group Membership

Function name:

IGMP Group Membership

Function description:

To show the IGMP group members information, the you can edit the parameters for IGMP groups and members in the web user interface.

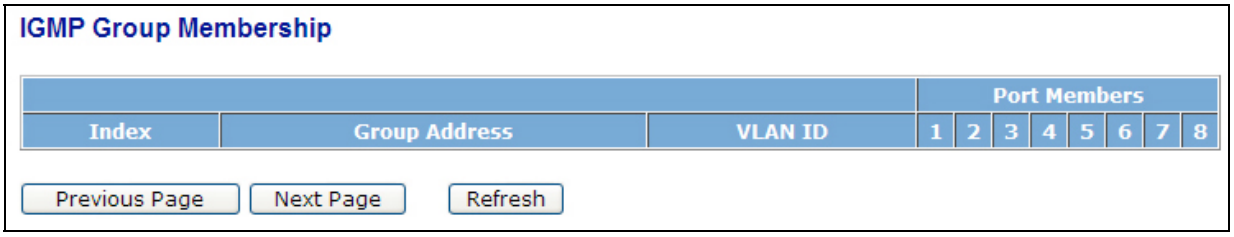


Figure 4-162. IGMP group membership.

Parameter description:

Index: Display the current built-up multicast group entry index.

Group Address: Display the current built-up multicast Group Address.

VLAN ID: Display the current built-up multicast VLAN ID.

Port Members: Display the current built-up multicast port members.

Previous Page: Display the previous page context.

Next Page: Display the next page context.

Refresh: Update the multicast group membership.

4.17.5 MVR

Function name:

MVR configuration (Multicast VLAN Registration)

Function description:

Multicast VLAN Registration (MVR) routes packets received in a multicast source VLAN to one or more receive VLANs. Clients are in the receive VLANs and the multicast server is in the source VLAN. Multicast routing has to be disabled when MVR is enabled.

NOTE: Use this function with a tag based VLAN mode.

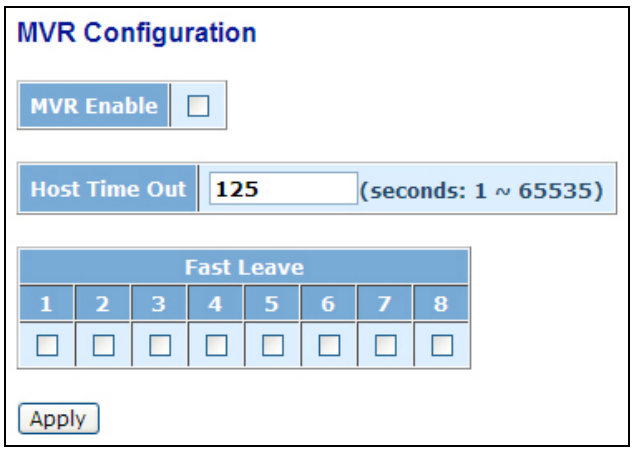


Figure 4-163. MVR configuration.

Parameter description:

MVR Enable: Set the MVR function enable.

Host Time Out: To set the MVR function enable and the Host packet received by the Switch timeout period. The units are seconds and the time range is from 1 to 65535. The default is 125 seconds.

Fast Leave: Set which port will enable the Fast leave mode with IGMP snooping mode.

4.17.6 MVID

Function name:

MVID configuration (Multicast VLAN Registration ID assign entry)

Function description:

Set the MVR Group member ID (MVID) entry with the Member port and Router Port.

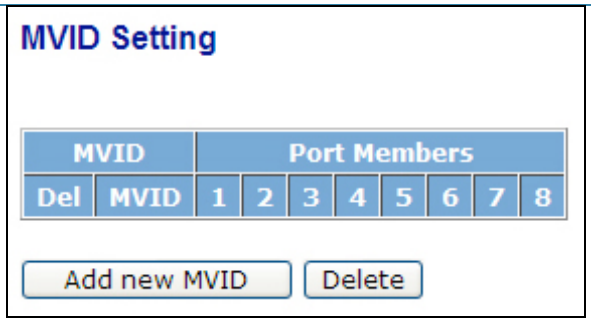


Figure 4-164. MVID configuration.

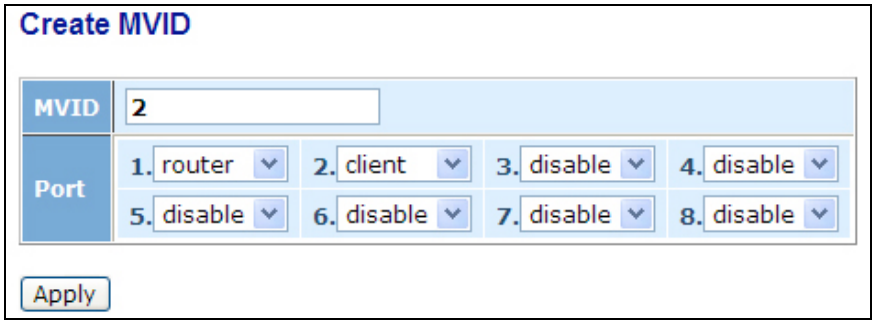


Figure 4-165. MVID configuration.

Parameter description:

Add new MVID: Creates a new MVID entry.

MVID: Sets the MVR Group ID.

Member Port: Sets which port will join the MVR Group member.

Router Port: Sets which port will become the MVR Group router port.

4.17.7 Group Allow

Function name: MVID Group Allow

Function description: The Group Allow function allows the Multicast VLAN Registration to set up the IP multicast group filtering conditions. IGMP items that behave the same as the items you set up will be joined to form the multicast group.

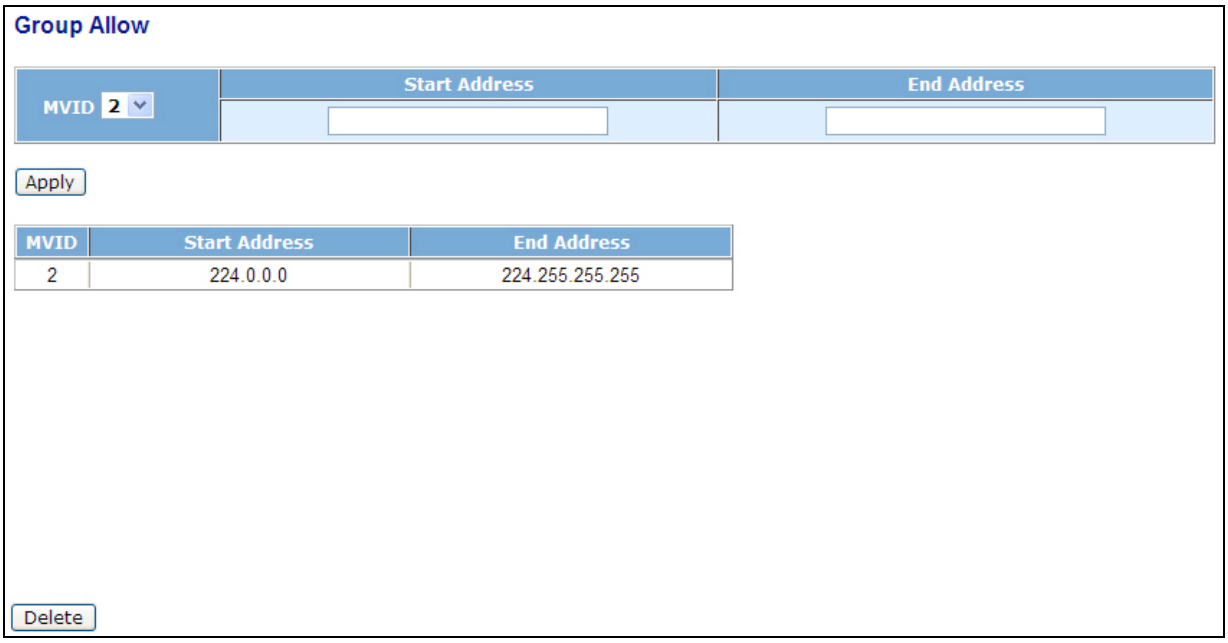


Figure 4-166. MVID Group Allow configuration.

Parameter description:

IP Address Range: The switch supports two kinds of options for managed valid IP range, including "Any" and "Custom." The default is "Any." If you chose Custom," you can assign an effective IP range. The valid range is 224.0.0.0–239.255.255.255.

MVID: The switch supports two kinds of options for managed valid MVID, including "Any" and "Custom." The default is "Any." When you choose "Custom," you can fill in the VID number. The valid VID range is 1–4094.

4.17.8 MVR Group Membership

Function name: MVR Group Membership

Function description: Displays the MVR Group Membership information.

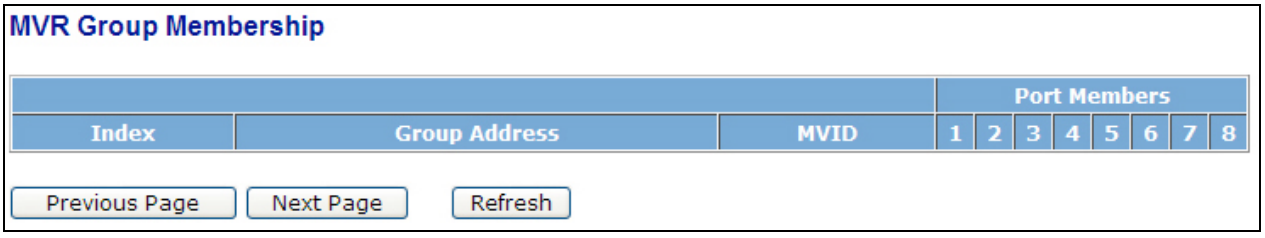


Figure 4-167. MVID Group Membership.

Parameter description:

Refresh: The Refresh function shows the current MVR group Membership status.

Previous Page: Move to the previous page.

Next Page: Move to the next page.

4.18 Alarm Configuration

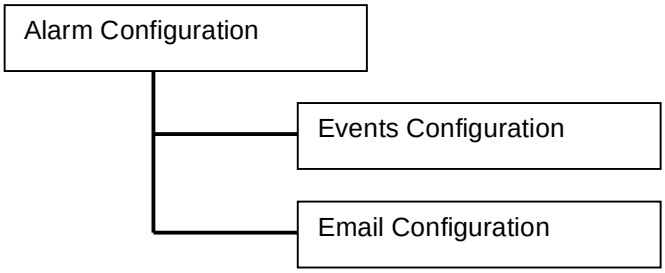


Figure 4-168. Alarm configuration menu tree.

4.18.1 Events

Function name: Events Configuration

Function description: The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occur. The switch offers 24 different trap events to users for switch management. The trap information can be sent out using email (short message system) and trap. The message will be sent while users check the checkbox (☑) for the trap event individually on the web page as shown below.

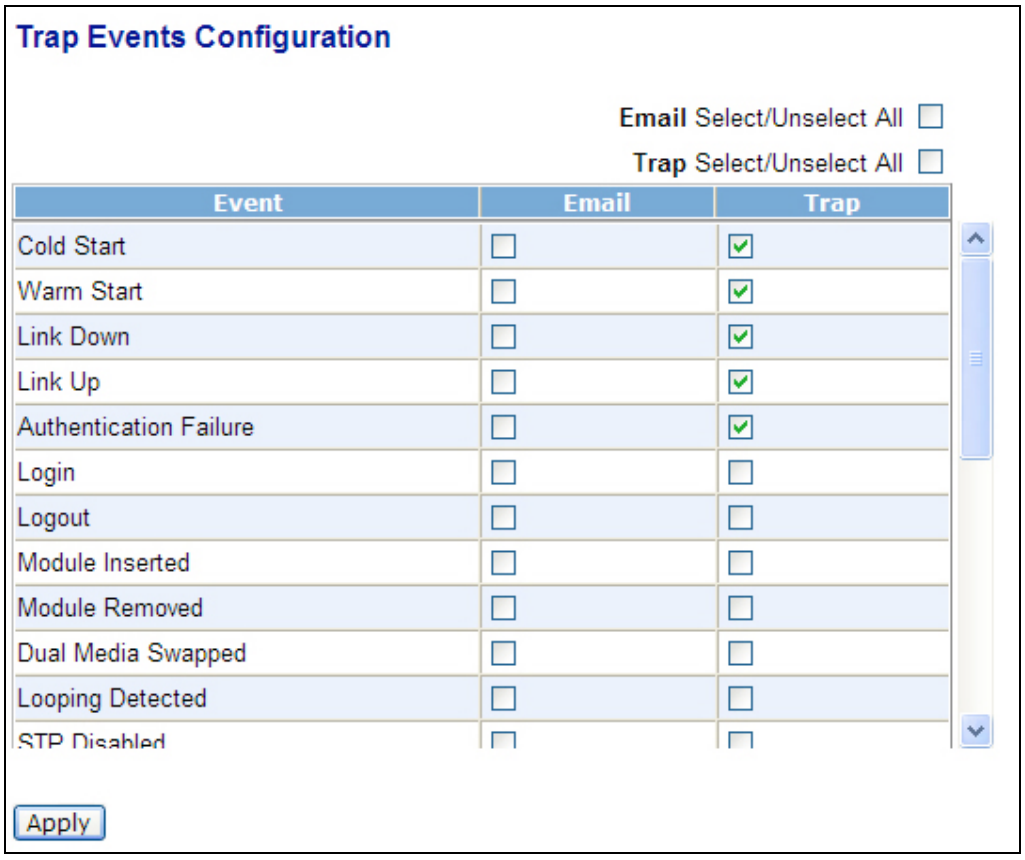


Figure 4-168. Trap Events Configuration page.

Parameter description:

Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

STP: STP Topology Changed, STP Disabled, STP Enabled

LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure
GVRP: GVRP Disabled, GVRP Enabled

VLAN: VLAN Disabled, Port-based VLAN Enabled, Tag-based VLAN Enabled, Metro-mode Vlan Enabled, Double-tag Vlan Enabled

Module Swap: Module Inserted, Module Removed, Dual Media Swapped

4.18.2 Email

Function name: Email Configuration

Function description:

Alarm configuration is used to configure which users should receive the alarm message via email. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration (See Fig. 3-61). Then, users can read the trap information from the email. This function provides 6 email addresses at most. The 24 different trap events will be sent out to SNMP Manager when a trap event occurs. After checking trap events, fill in your desired email addresses and mobile phone numbers. Then, click on the <Apply> button to complete the alarm configuration. It will take effect in a few seconds.

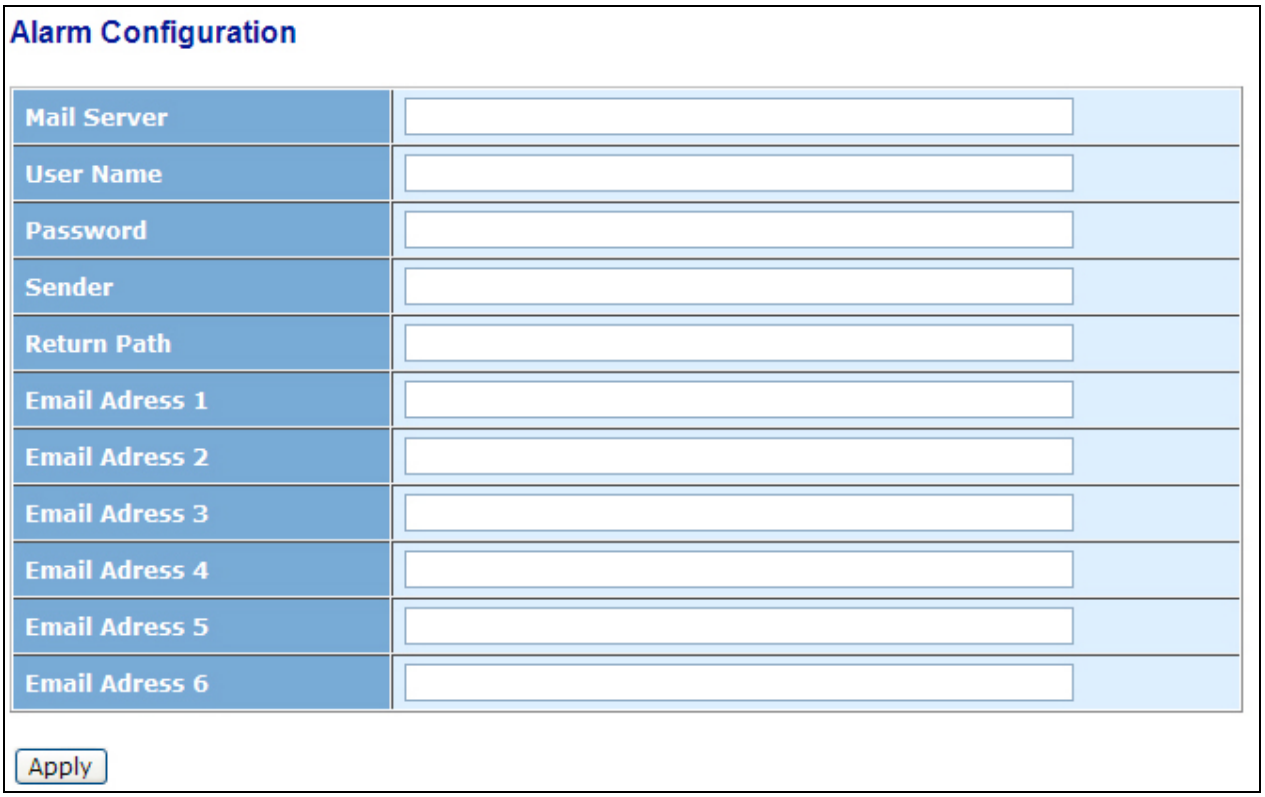


Figure 4-169. Alarm Configuration screen.

Parameter description:

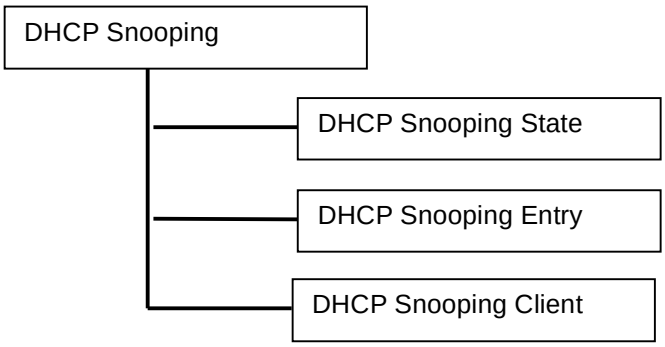
Email: Mail Server: the IP address of the server transferring your email.

Username: your username on the mail server.

Password: your password on the mail server.

Email Address 1–6: email address that will receive the alarm message.

4.19 DHCP Snooping



DHCP snooping menu tree.

4.19.1 DHCP Snooping State

Function name: DHCP Snooping State

Function description:

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

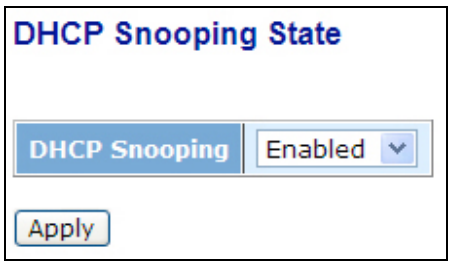


Figure 4-170. DHCP Snooping State.

Parameter description:

DHCP Snooping state: The parameter disables or enables the DHCP snooping function on the switch. The default is Disabled.

NOTE: Click on the " Apply" button when you finish the configuration.

4.19.2 DHCP Snooping Entry

Function name:

DHCP Snooping Entry

Function description:

DHCP snooping Entry allows a switch to add a trusted DHCP server and 2 trusted ports to the DHCP snooping entry. You can use this information to track an IP address back to a physical port and enable or disable the DHCP Option 82.

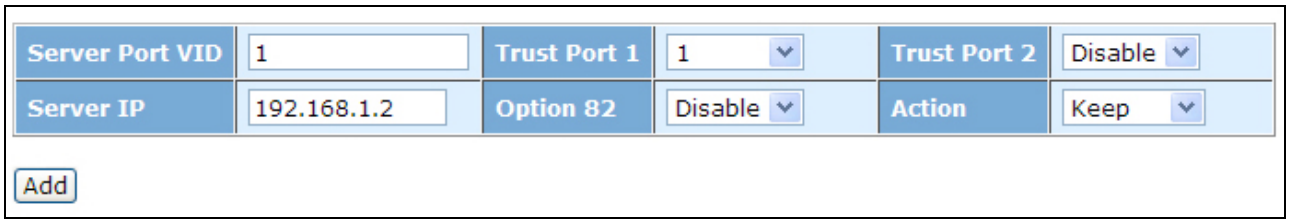


Figure 4-171. DHCP Snooping State.

Parameter description:

VID: When DHCP snooping is enabled on the specified VLAN, DHCP packet filtering will be performed on any un-trusted ports within the VLAN. It sets an available VLAN ID to enable the DHCP snooping on VLAN interface.

Trust Port 1: If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. It sets a trusted port 1 from 0 to 24. 0 is disabled.

Trust port 2: Sets a trusted port 2 from 0 to 8. 0 is disabled.

Trust VID: Sets a trusted VLAN ID VID from 1 to 4094.

Server IP: Sets a trusted DHCP Server IP address for DHCP Snooping.

Option 82: Sets the DHCP Option 82 function on the switch. The default is Disable.

Action: Sets the switch's filtering options when its receives a client DHCP request. Options include: keep/drop/replace.

NOTE: Filtering rules are implemented as follows:

If the DHCP snooping is disabled, all DHCP packets are forwarded.

If DHCP snooping is enabled and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded to a trusted port.

If DHCP snooping is enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it processes the packet as follows:

- If the DHCP packet is a reply packet from a DHCP server, the packet is dropped.

- If the DHCP packet is from a client, such as a DISCOVER, REQUEST INFORM, DECLINE or RELEASE message, the packet is forwarded if
MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's
hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

If the DHCP packet is not a recognizable type, it is dropped.

If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

If a DHCP packet is from a server is received on a trusted port, it will be forwarded to both trusted and un-trusted ports in the same VLAN.

4.19.3 DHCP Snooping Client

Function name: DHCP Snooping Client

Function description:

Shows the DHCP snooping client.

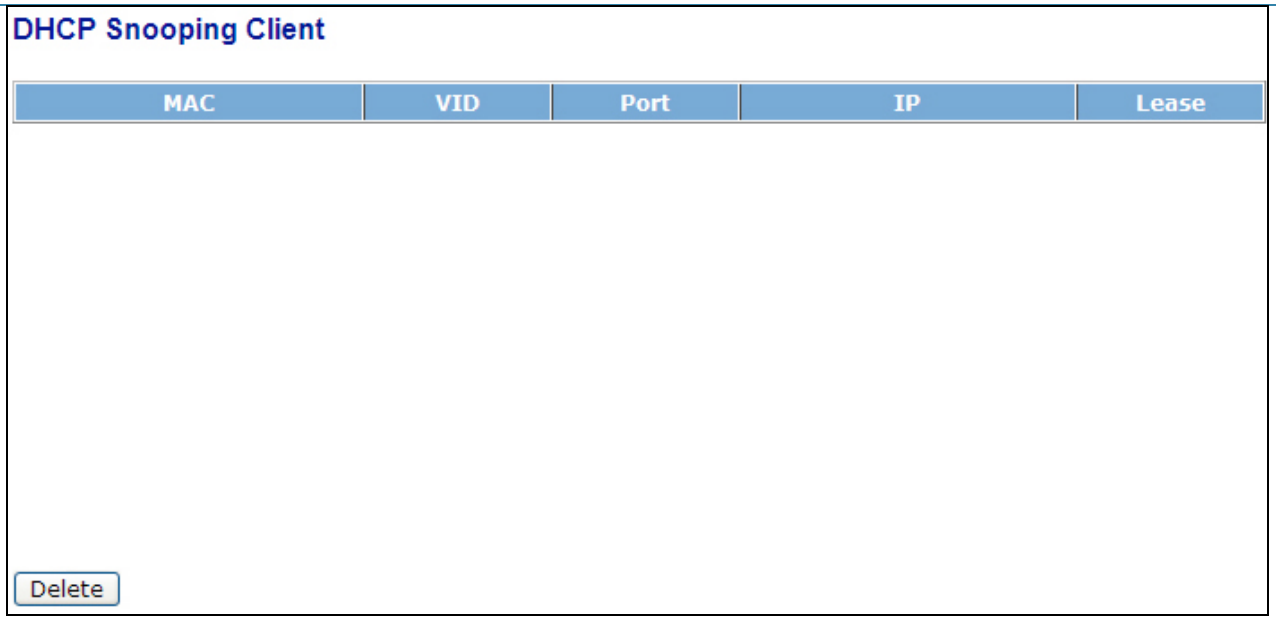


Figure 4-172. DHCP Snooping Client.

Parameter description:

MAC: Shows the DHCP snooping client's MAC address.

VID: Shows the DHCP snooping client's VLAN ID.

Port: Shows the DHCP snooping client's port.

IP: Shows the DHCP snooping client's IP address.

Lease: Shows the DHCP snooping client's lease.

4.20 LLDP

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

4.20.1 LLDP State

Function name: LLDP State

Function description:

The LLDP state function, enables you to set the LLDP configuration and the detail parameters per port. The settings will take effect immediately.

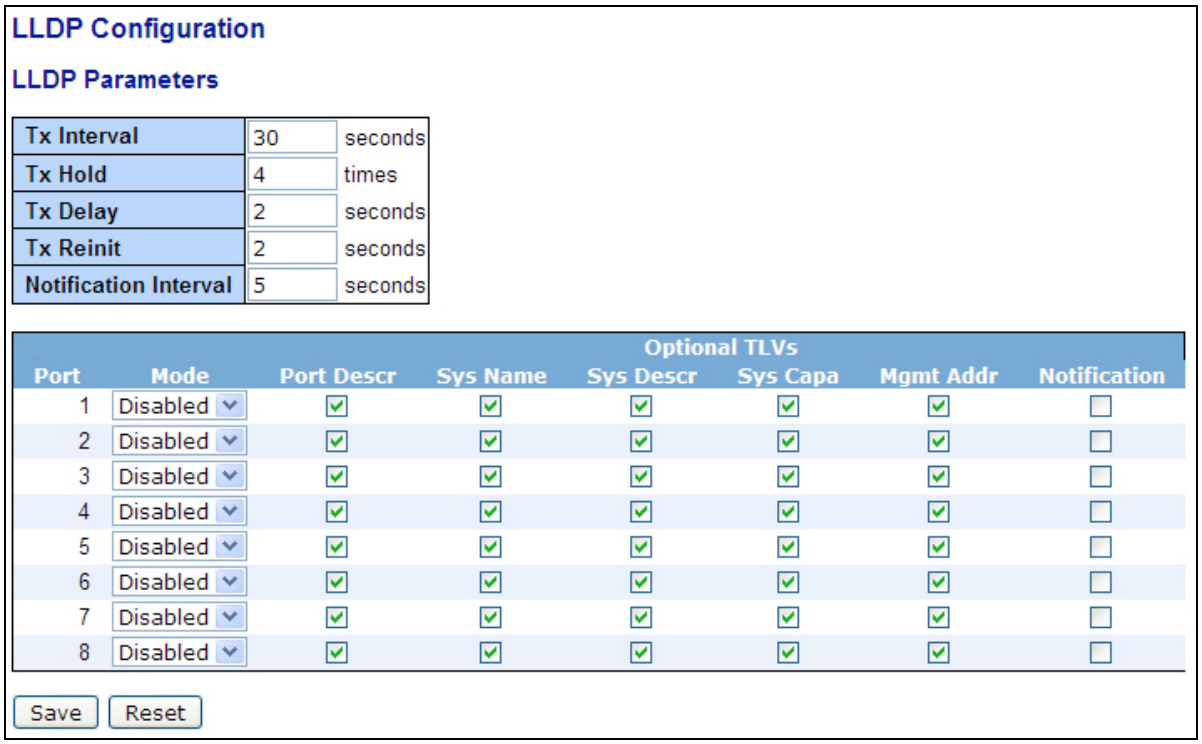


Figure 4-173. LLDP parameter.

Parameter:
Tx Interval: Changes the interval between consecutive transmissions of LLDP advertisements on any given port. (Default: 30 seconds)

Tx Hold: Specifies the amount of time the receiving device holds a Link Layer Discovery Protocol (LLDP) packet before discarding it. (Default: 4 times)

Tx Delay: Specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local system's MIB. (Default: 2 seconds)

Tx Reinit: Specifies the minimum time an LLDP port waits before reinitializing LLDP transmission. (Default: 2 seconds
)
Notification Interval: A network management application can periodically check the switch MIB to detect any missed change notification traps. Refer to IEEE 802.1AB-2005 or later for more information. (Default: 5 seconds)

Mode: Enables or disables the LLDP mode per port. There are four types, including Disable, Tx_Rx, Tx only, and Rx only.

Port Descr: Enables or disables the outbound LLDP advertisements. This includes an alphanumeric string describing the port.

Sys Name: Enables or disables the outbound LLDP advertisements. This includes the system's assigned name

Sys Descr: Enables or disables outbound LLDP advertisements. This includes an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

Sys Capa: Enables or disables outbound advertisements. This includes a bitmask of system capabilities (device functions) that are supported. Also includes information on whether the capabilities are enabled.

Mgmt Addr: Enables or disables outbound advertisements, including information about the management address. Use this to include a specific IP address in the outbound LLDP advertisements for specific ports.

Notification: Enables or disables outbound advertisements, including information on Notification.

4.20.2 LLDP Entry

Function name: LLDP Entry

Function description:

The LLDP Entry function allows a switch to display which ports build the LLDP available entry. Use this information to track LLDP packets back to a physical port and enable or disable the LLDP.

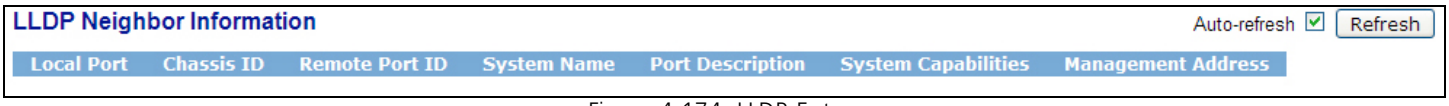


Figure 4-174. LLDP Entry.

Parameter description:

Local port: Displays the switch local port.

Chassis ID: Displays the Chassis ID which connect to the switch and what the neighbor Chassis ID.

Remote Port ID: Displays the Remote Port ID which connect to the switch and what the neighbor's remote port ID.

System name: Displays the system name which connect to the switch and which device supports the LLDP

Port Description: Displays an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

System Capabilities: Display includes a bitmask of system capabilities (device functions) that are supported. Also includes information on whether the capabilities are enabled.

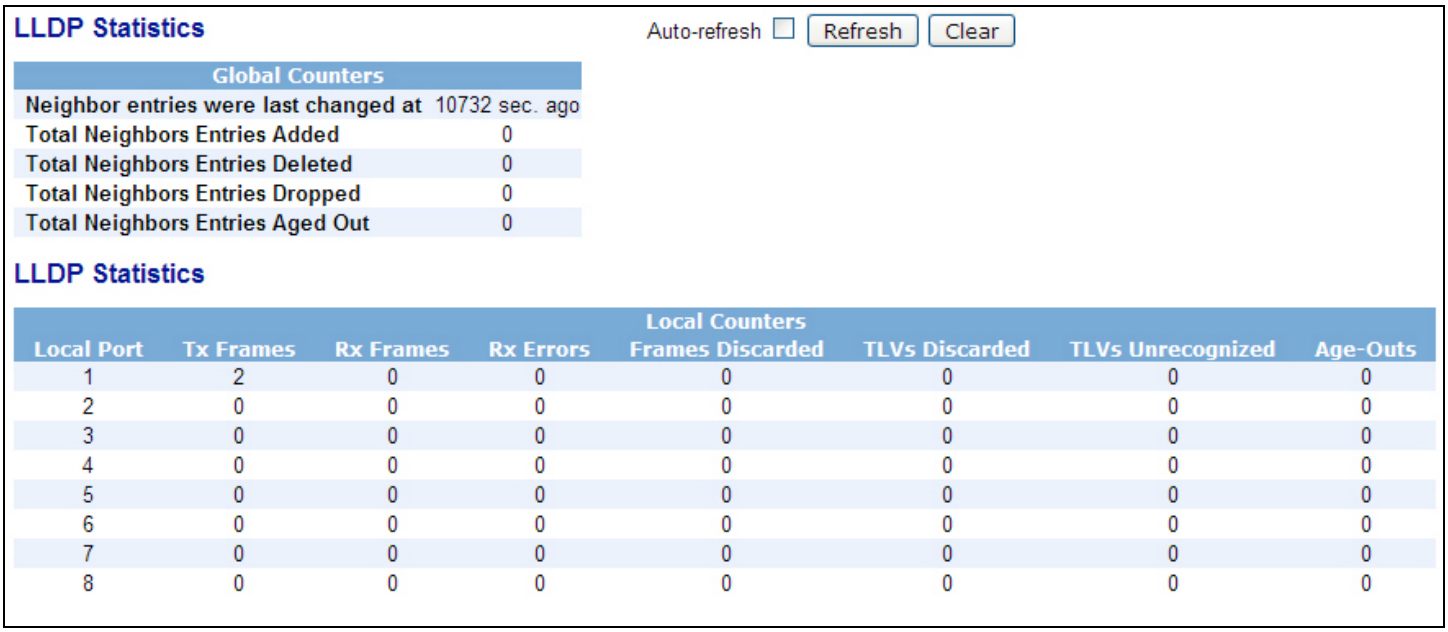
Management Address: Display includes a specific IP address in the outbound LLDP advertisements for specific ports.
Auto - refresh: Refresh the authenticator counters in the web UI automatically.

Refresh: Click on the <Refresh> button to update the authenticator counters in the web UI.

4.20.3 LLDP Statistics

Function name: LLDP Statistics

Function description: Display the detailed counting number of each port's LLDP traffic.



LLDP Statistics

Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbor entries were last changed at	10732 sec. ago
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics

Local Counters							
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Age-Outs
1	2	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0

Figure 4-175. LLDP statistics.

Parameter description:

Neighbor entries were last changed at: The time period since neighbor entries were changed.

Total Neighbors Entries Added: The total neighbors' entries added are received.

Total Neighbors Entries Deleted: The total neighbors' entries deleted are received.

Total Neighbors Entries Dropped: The total neighbors' entries dropped are received.

Total Neighbors Entries Aged Out: The total neighbors' entries aged out are received.

Local port: Show the local port on the switch.

Tx Frames: The number of frames transmitted.

Rx Frames: The number of frames transmitted.

Frames Discarded: Show the number of frames discarded.

TLVs Discarded: Show the number of TLVs discarded.

TLVs Unrecognized: Show the number of TLVs unrecognized.

Age Outs: Show the number of Age Outs.

4.21 Save/Restore

The switch supports three copies of configuration, including the default configuration, working configuration, and user configuration are listed and described below.

Default Configuration:

This is an ex-factory setting and cannot be altered. In Web UI, two restore default functions are offered for the user to restore the default setting of the switch. One is "Restore Default Configuration, including default IP address." The IP address will restore to the default "192.168.1.1." Another function is "Restore Default Configuration without changing current IP address." This means that the IP address will keep the same one that you had saved before by performing this function.

Working Configuration:

The configuration you are currently using. This can be changed at any time. The configurations you are using are saved into this configuration file. This is updated each time you press the **<Apply>** button.

User Configuration:

The configuration file for the specified or backup purposes. It can be updated after confirming the configuration. You can retrieve it by performing Restore User Configuration.

4.21.1 Factory Defaults

Function name: Restore Default Configuration (includes default IP address)

Function description:

Restore Default Configuration function can retrieve ex-factory settings to replace the start configuration. The IP address of the switch will also be restored to 192.168.1.1.

Figure 4-176. Factory defaults reset screen.

4.21.2 Save Start

Function name:

Save As Start Configuration

Function description:

Save the current configuration as a start configuration file in flash memory.

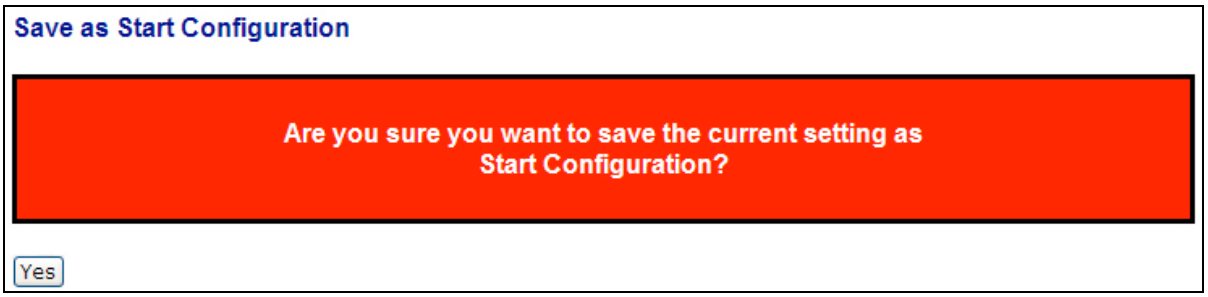


Figure 4-177. Save as start configuration prompt.

4.21.3 Save User

Function name: Save As User Configuration.

Function description:

Save the current configuration as a user configuration file in flash memory.

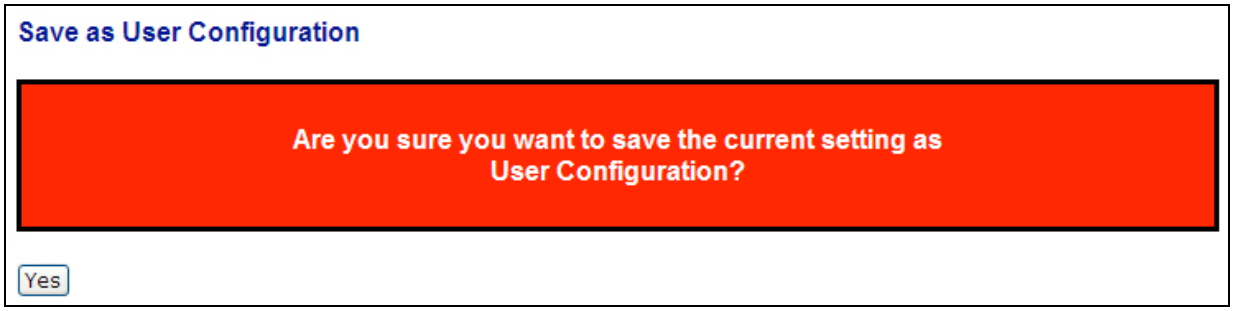


Figure 4-178. Save the current setting as user configuration prompt.

4.21.4 Restore User

Function name: Restore User Configuration

Function description:

The Restore User Configuration function can retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When restoring the configuration, the system's start configuration is updated and its system settings will change after rebooting the system.

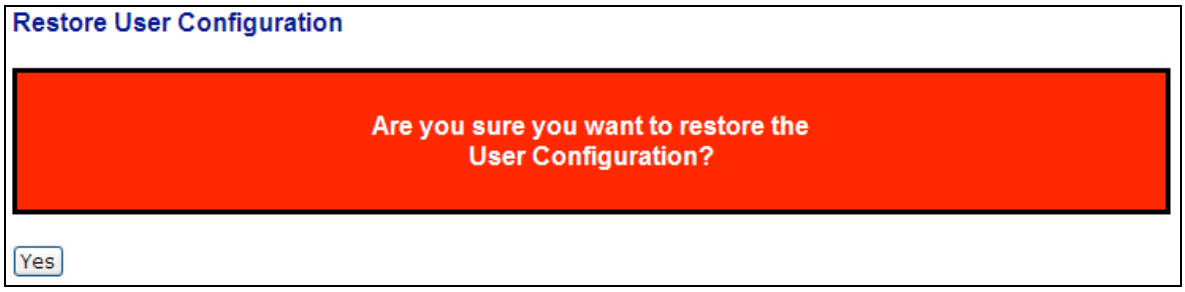


Figure 4-179. Restore user configuration prompt.

4.22 *Export/Import*

Function name: Export/Import

Function description:

With this function, users can back up or reload the configuration files of Save As Start or Save As User via TFTP.

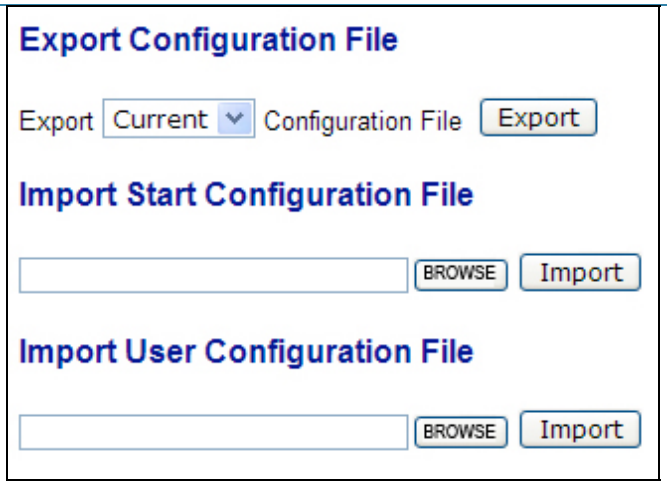


Figure 4-180. Export/Import configuration file.

Parameter description:

Export File Path:

Export Start: Export Save As Start's config file stored in the flash.

Export User-Conf: Export Save As User's config file stored in the flash.

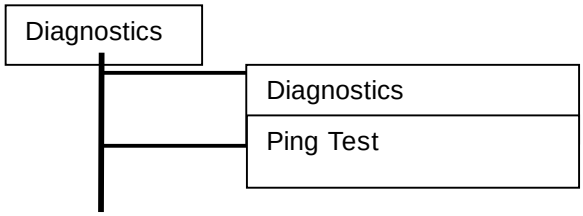
Import File Path:

Import Start: Import Save As Start's config file stored in the flash.

Import User-Conf: Import Save As User's config file stored in the flash.

4.23 Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics. Each of them is described in detail in the following sections.



4.23.1 Diag

Function name: Diagnostics

Function description:

The Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is healthly or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM, test and Flash test.

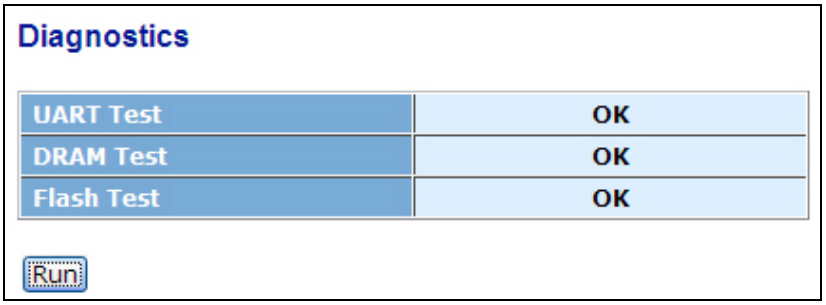


Figure 4-181. Diagnostics screen.

4.23.2 Ping

Function name:

Ping Test

Function description:

Ping Test function detects if the target device is alive or not through ICMP protocol with report messages. The switch provides Ping Test function to let you know if the target device is available or not. Simply fill in a known IP address and then click on the <Ping> button. After a few seconds, the switch will report that the pinged device is alive or dead in the Ping Result field.

Parameter description:

IP Address: An IP address with version v4, e.g. 192.168.1.1.

Default Gateway: IP address of the default gateway.

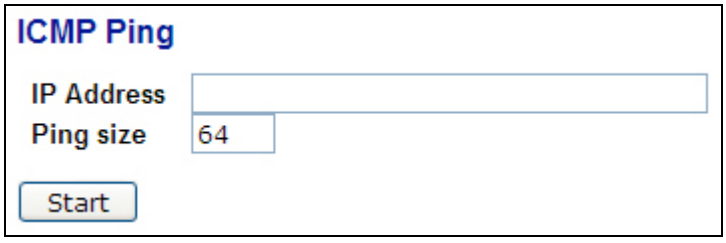


Figure 4-182. ICMP ping screen.

Figure 4-183. ICMP ping output screen.

4.24 Maintenance

This section introduces the reset and firmware upgrade functions for the firmware upgrade and key parameters change system maintenance requirements.

4.24.1 Warm Restart

Function name: Warm Restart

Function description:

There are many ways to reset the switch, including power up, hardware reset and software reset. Press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, then you must reboot to have the new configuration take effect. To reset the software to “reboot” in the main menu, click on the “Yes” button in Figure 4-184.

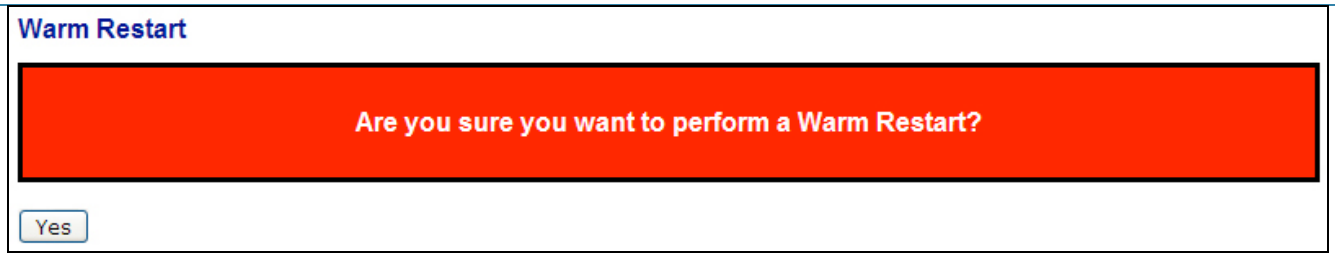


Figure 4-184. Warm restart prompt.

4.24.2 Software Upload

Function name: Software Upload

Function description: Click on <Browse> to select a specific LPB4008A firmware file from the Web management PC, then click on <Upload> to confirm the firmware upgrade. The new firmware will be uploaded into the switch and write to flash memory. You have to reboot the switch for the new firmware to take effect after the firmware upgrades successfully.

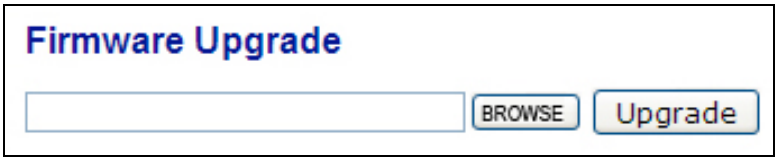


Figure 4-185. Firmware upgrade screen.

4.25 Logout

Manually logout by performing the Logout function. Or you can configure it to logout automatically.

Function name: Logout

Function description:

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout in five minutes. Besides this manually logout.

Figure 4-186. Logout screen.

Parameter description:

Logout: Click on <Logout> to leave the web UI management function.

5. Operation of CLI Management

5.1 CLI Management

Refer to Chapter 3 for basic installation. The following briefly describes the network connection.

- Locate the correct DB9 null modem cable with female DB9 connector. Null modem cable comes with the management switch. Refer to Chapter 8 for null modem cable configuration.

- Attach the DB9 female connector to the male DB9 serial port connector on the Management board.

- Attach the other end of the DB9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.

- At "Com Port Properties" Menu, configure the parameters as shown below:

Baud rate	115200
Stop bits	1
Data bits	8
Parity	N
Flow control	none

5.2 Login

The command-line interface (CLI) is a text-based interface. Users can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin

Password: admin

After you login successfully, the prompt will be shown as "**#**" if you are the first person to login and your authorization is administrator; otherwise it may show "**$**". See the following two figures. The former means you are an administrator and have access rights to the system. The latter means you area guest and are only allowed to view the system without permission to configure settings for this switch.

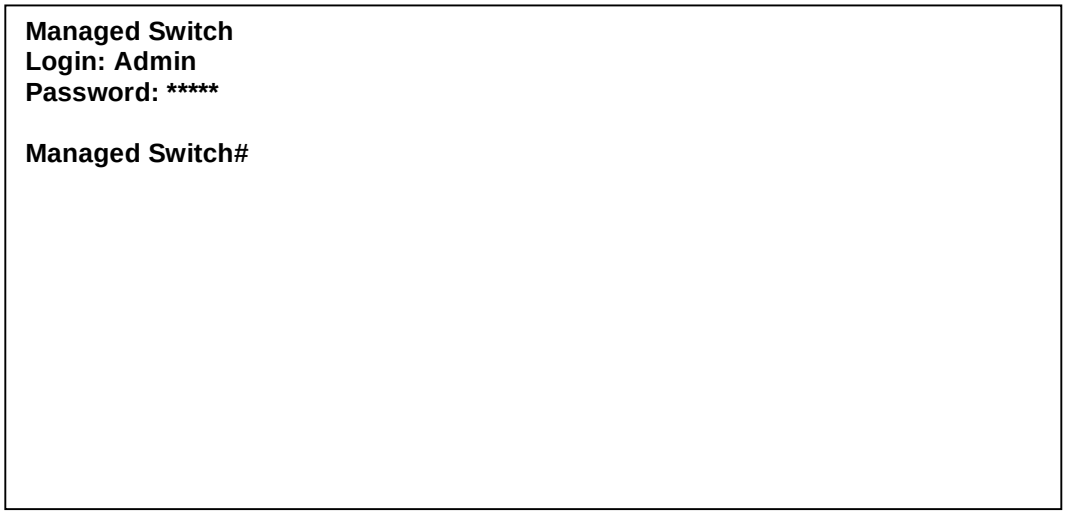


Figure 5-1.

5.3 Commands of CLI

To see the commands of the mode, input "**?**" after the prompt, then all commands will be listed in the screen. All commands can be divided into two categories, including global commands and local commands. You can use global commands regardless of the mode you are in. The modes are "exit," "end," "help," "history," "logout," "save start," "save user," "restore default," and "restore user". For more details, refer to Section 5.3.1.

Command instructions that reside in the corresponding modes are local commands. The same command with the same command name may occur but perform a totally different function in different modes. For example, "show" in IP mode displays the IP information; however, it displays the system information in system mode. For more details, refer to Section 5.3.2.

```
Managed Switch
Login: Admin
Password: *****

Managed Switch# help
 -------------------------<<Local Commands>>-------------------------
 802.1X              Enter into 802.1X mode
 Account             Enter into account mode
 Acl                 Enter into acl mode
 Alarm               Enter into alarm mode
 Autologout          Change auto logout time
 Config-File         Enter into config file mode
 DHCP_Snooping       Enter into DHCP snooping mode
 Diagnostics         Enter into diagnostics mode
 Firmware            Enter into firmware mode
 Gvrp                Enter into gvrp mode
 Hostname            Change hostname
```

Figure 5-3. Managed switch help screen.

5.3.1 *Global Commands of CLI*

end

Syntax: end

Description: Back to the top mode. When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.

Argument: None.

Possible value: None.

Example:

LPB4008A# alarm

LPB4008A(alarm)# events

LPB4008A(alarm-events)# end

LPB4008A#

Exit

Syntax: exit

Description: Back to the previous mode. When you enter this command, your current position will move back to the previous mode. If you use this command in the top mode, you remain in top mode.

Argument: None.

Possible value: None.

Example:

LPB4008A# trunk

LPB4008A(trunk)# exit

LPB4008A#

Help

Syntax: help

Description: Show available commands. Some commands are the combination of more than two words. When you enter this command, the CLI shows the complete commands. The command helps you classify the commands between the local commands and the global ones.

Argument: None.

Possible value: None.

Example:

LPB4008A# ip

LPB4008A(ip)# help

Commands available:

```
------------<< Local commands >>------------
set ip                  Set ip,subnet mask and gateway
set dns         Set dns
enable dhcp     Enable DHCP, and set dns auto or manual
disable dhcp    Disable DHCP
show                    Show IP Configuration
------------<< Global commands >>------------
exit                    Back to the previous mode
end                     Back to the top mode
help                    Show available commands
history         Show a list of previously run commands
logout                  Logout the system
save start              Save as start config
save user       Save as user config
restore default Restore default config
restore user            Restore user config
```

history

Syntax: history [#]

Description: Shows a list of previous commands that you have run. When you enter this command, the CLI shows a list of commands that you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI will list total records up to 256. If an optional argument is given, the CLI would only show records indicated by the argument.

Argument: [#]: show last number of history records. (optional)

Possible value: [#]: 1, 2, 3, …., 256

Example:

```
LPB4008A(ip)# history

 Command history:
  0. trunk
  1. exit
  2. LPB4008A# trunk
  3. LPB4008A(trunk)# exit
  4. LPB4008A#
  5. ?
  6. trunk
  7. exit
  8. alarm
  9. events
 10. end
 11. ip
 12. help
 13. ip
 14. history

LPB4008A(ip)# history 3
 Command history:
 13. ip
 14. history
 15. history 3

LPB4008A(ip)#
```

Logout

Syntax: logout

Description: When you enter this command via a Telnet connection, logout of the system and disconnect. If you connect the system through a direct serial port with RS-232 cable, logout of the system and return to the initial login prompt when you run this command.

Argument: None.

Possible value: None.

Example:

```
LPB4008A# logout
```

restore default

Syntax: restore default

Description: When you use this function in CLI, the system will show you the information “Do you want to restore the default IP address?(y/n)”. If you choose Y or y, the IP address will restore to default “192.168.1.1”. If you choose N or n, the IP address will be the same one that you saved before.
If restoring default successfully, the CLI prompts you to reboot immediately or not. If you press Y or y, the system reboots immediately; if not, it will return to the CLI system. After restoring the default configuration, all the changes in the startup configuration will be lost. After rebooting, the entire startup configuration will reset to the factory default.

Argument: None.

Possible value: None.

Example:

LPB4008A# restore default

Restoring …

Restore Default Configuration Successfully

Press any key to reboot system.

restore user

Syntax: restore user

Description: Restore the startup configuration as a user defined configuration. If restoring default successfully, the CLI prompts if you need to reboot immediately or not. If you press Y or y, the system will reboot immediately; if not, you return to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration are lost. After rebooting, the entire startup configuration replaces a user defined one.

Argument: None.

Possible value: None.

Example:

LPB4008A# restore user

Restoring …

Restore User Configuration Successfully

Press any key to reboot system.

save start

Syntax: save start

Description: Save the current configuration as the startup one. When you enter this command, the CLI saves your current configuration into the non-volatile FLASH. If you want the configuration to work after rebooting, save the configuration using the command ‘save stat’.

Argument: None.

Possible value: None.

Example:

LPB4008A# save start

Saving start…

Save Successfully

LPB4008A#

save user

Syntax: save user

Description: To save the current configuration as the user-defined configuration. When you enter this command, the CLI saves your current configuration into the non-volatile FLASH as a user-defined configuration.

Argument: None.

Possible value: None.

Example:

LPB4008A# save user

Saving user...

Save Successfully

LPB4008A#

5.3.2 *Local Commands of CLI*

802.1X

set maxReq

Syntax: set maxReq <port-range> <vlaue>

Description: The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.

Argument: <port range> : syntax 1,5-7, available from 1 to 8

<value>: max-times , range 1–10

Possible value: <port range> : 1 to 8

<value>: 1-10, default is 2

Example:

LPB4008A(802.1X)# set maxReq 2 2

set mode

Syntax: set mode <port-range> <mode>

Description: Set up the 802.1X authentication mode of each port.

Argument: <port range>: syntax 1,5-7, available from 1 to 8

<mode>: set up 802.1X mode

0: disable the 802.1X function

1: set 802.1X to Multi-host mode

Possible value: <port range>: 1 to 8

<mode>: 0 or 1

Example:

LPB4008A(802.1X)# set mode 2 1

LPB4008A(802.1X)#

set port-control

Syntax: set port-control <port-range> <unauthorized| authorized| auto>

Description: Set up 802.1X status of each port.

Argument: <port range>: syntax 1,5-7, available from 1 to 8

<authorized>: Set up the status of each port

0: ForceUnauthorized

1: ForceAuthorized

2: Auto

Possible value: <port range>: 1 to 8

<authorized>: 0, 1 or 2

Example:

LPB4008A(802.1X)# set port-control 2 2

set quietPeriod

Syntax: set quietPeriod <port-range> <value>

Description: A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

Argument: <port range>: syntax 1, 5-7, available from 1 to 8

<value>: timer, range 0-65535

Possible value: <port range>: 1 to 8

<value>: 0-65535, default is 60

Example:

LPB4008A(802.1X)# set quietPeriod 2 30

set reAuthEnabled

Syntax: set reAuthEnabled <port-range> <on | off >

Description: A constant that defines whether regular reauthentication will take place on this port.

Argument: <port range>: syntax 1, 5-7, available from 1 to 8

<on | off >: 0: OFF Disable reauthentication

1: ON Enable reauthentication

Possible value: <port range>: 1 to 8

< on | off l>: 0 or 1, default is 1

Example:

LPB4008A(802.1X)# set reAuthEnabled 2 1

set reAuthMax

Syntax: set reAuthMax <port-range> <value>

Description: The number of reauthentication attempts that are permitted before the port becomes Unauthorized.

Argument: <port range>: syntax 1, 5-7, available from 1 to 8

<value>: max. value, range 1–10

Possible value: <port range>: 1 to 8

<value>: 1-10, default is 2

Example:

LPB4008A(802.1X)# set reAuthMax 2 2

set reAuthPeriod

Syntax: set reAuthPeriod <port-range> <value>

Description: A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.

Argument: <port range>: syntax 1, 5-7, available from 1 to 8

<value>: timer, range 1-65535

Possible value: <port range>: 1 to 8

<value>: 1-65535, default is 3600

Example:

LPB4008A(802.1X)# set reAuthPeriod 2 3600

set serverTimeout

Syntax: set serverTimeout <port-range> <value>

Description: A timer used by the Backend Authentication state machine to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument: <port range>: syntax 1, 5-7, available from 1 to 8

<value>: timer, range 1-65535

Possible value: <port range>: 1 to 8

<value>: 1-65535, default is 30

Example:

LPB4008A(802.1X)# set serverTimeout 2 30

set auth-server

Syntax: set auth-server <ip-address> <udp-port> <secret-key>

Description: Configure the settings related to the 802.1X Radius Server.

Argument: <ip-address>: the IP address of Radius Server

<udp-port>: the service port of Radius Server(Authorization port)

<secret-key>: set up the value of secret-key, and the length of secret-key is from 1 to 31

Possible value: <udp-port >: 1~65535, default is 1812

Example:

LPB4008A(802.1X)# set auth-server 192.168.1.115 1812 WinRadius

set suppTimeout

Syntax: set suppTimeout <port-range> <value>

Description: A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument: <port range>: syntax 1, 5-7, available from 1 to 8

<value>: timer , range 1-65535

Possible value: <port range>: 1 to 8

<value>: 1-65535, default is 30

Example:

LPB4008A(802.1X)# set suppTimeout 2 30

set txPeriod

Syntax: set txPeriod <port-range> <value>

Description: A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted

Argument: <port range>: syntax 1, 5-7, available from 1 to 8

<value>: timer, range 1-65535

Possible value: <port range>: 1 to 8

<value>: 1-65535, default is 30

Example:

LPB4008A(802.1X)# set txPeriod 2 30

show status

Syntax: show status

Description: Displays the mode of each port.

Argument: None

Possible value: None

Example:

LPB4008A(802.1X)# show status

```
 Port      Mode
======  ============
  1       Disable
  2       Multi-host
  3       Disable
  4       Disable
  5       Disable
  6       Disable
```

show port-config

Syntax: show port-config <port-range>

Description: Displays the parameter settings of each port.

Argument: <port range> : syntax 1,5-7, available from 1 to 8

Possible value: <port range> : 1 to 8

Example:

LPB4008A(802.1X)# show port-config 1, 2

```
port  1) Mode                : Disabled

port control  : Auto
        reAuthMax           : 2
        txPeriod                        : 30
        Quiet Period        : 60
        reAuthEnabled       : ON
        reAuthPeriod        : 120
        max. Request        : 2
        suppTimeout         : 30
        serverTimeout       : 30

port  2) Mode               : Disabled
port control  : Auto
        reAuthMax            : 2
        txPeriod                        : 30
        Quiet Period        : 60
        reAuthEnabled       : ON
        reAuthPeriod        : 120
        max. Request        : 2
        suppTimeout         : 30
        serverTimeout       : 30
```

show statistics

Syntax: show statistics <#>

Description: Displays each port's statistics.

Argument: <#> syntax 1, 5-7, available from 1 to 8

Possible value: <#> 1 to 8

show server

Syntax: show server

Description: Show the Radius server configuration

Argument: None

Possible value: None

Example:

LPB4008A(802.1X)# show server

Authentication Server
_____

IP Address : 192.168.1.1

UDP Port : 1812

Secret Key : Radius

Accounting Server
_____
IP Address: 192.168.1.1

UDP Port : 1812

Secret Key : Radius

B. account

add

Syntax: add <name>
Description: Create a new guest user. When you create a new guest user, you must type in the password and confirm it.
Argument: <name>: new account name
Possible value: A string must be at least 5 characters.
Example:
LPB4008A(account)# add aaaaa
Password:
Confirm Password:
LPB4008A(account)#

Del

Syntax: del <name>

Description: Delete an existing account.

Argument: <name>: existing user account

Possible value: None.

Example:

LPB4008A(account)# del aaaaa

Account aaaaa deleted

Modify

Syntax: modify <username>

Description: Change the username and password of an existing account.

Argument: <name>: existing user account

Possible value: None.

Example:

LPB4008A(account)# modify aaaaa

username/password: the length is from 5 to 15.

Current username (aaaaa):bbbbb

New password:

Confirm password:

Username changed successfully.

Password changed successfully.

Show

Syntax: show

Description: Shows system account, including account name and identity.

Argument: None.

Possible value: None.

Example:

LPB4008A(account)# show

Account Name	Identity
admin	Administrator
guest	guest

C. acl

ace

Syntax: ace <index>

Description: Displays the ace configuration.

Argument: <index>: the access control rule index value

Possible value: None.

Example:

LPB4008A(acl)# ace 2

index: 2

rule: switch

vid: any

tag_prio: any

dmac: any

frame type: arp

arp type: Request/Reply (opcode): any

source ip: any

destination ip: any

ARP flag

ARP SMAC Match: any

RARP DMAC Match: any

IP/Ethernet Length: any

IP: any

Ethernet: any

action: 1

rate limiter: 0

copy port: 0

action

Syntax: action <port> <permit|deny> <rate_limiter> <port copy>

Description: Set the access control per port as a packet filter action rule.

Argument: <port>: 1-8

<permit/deny>: permit: 1, deny: 0

<rate_limiter>: 0-16 (0: disable)

<port copy>: 0-8 (0:disable)

Possible value: <port>: 1-8

<permit/deny>: 0-1

<rate_limiter>: 0-16

<port copy>: 0-8

Example:

LPB4008A(acl)# action 5 0 2 2

LPB4008A(acl)# show

port	policy id	action	rate limiter	port copy	counter a class map
5	1	deny	2		2
7	1	permit	0		0
8	1	permit	0		0

```
rate limiter   rate(pps)
------------ ------------
      1              1
      2              1
      3              1
      4              1
      5              1

      ......         ......

LPB4008A(acl)#
```

delete

Syntax: delete <index>

Description: Delete the ACE (Access Control Entry) configuration on the switch.

Argument: <index>: the access control rule index value

Possible value: None.

Example:

LPB4008A(acl)# delete 1

LPB4008A(acl)#

Move

Syntax: move <index1> <index2>

Description: Move the ACE (Access Control Entry) configuration between index1 and index2..

Argument: None.

Possible value: None.

Example:

LPB4008A(account)# move 1 2

Policy

Syntax: policy <policy> <ports>

Description: Set acl port policy on the switch

Argument: <policy>: 1-8

<ports>: 1-24

Possible value: <policy>: 1-8

<ports>: 1-24

Example:

LPB4008A(acl)# policy 3 10

LPB4008A(acl)#

Ratelimiter

Syntax: ratelimiter <id> <rate>

Description: Set access control rule with rate limiter on the switch.

Argument: <id>: 1-16

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1000, 2000, 4000,8000, 16000, 32000, 64000, 128000, 256000, 512000, 1024000

Possible value: <id>: 1-16

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000, 128000, 256000, 512000, 1024000

Example:

LPB4008A(acl)# ratelimiter 3 16000

LPB4008A(acl)#

set

```
Syntax: set [<index>] [<next index>]
        [switch | (port <port>) | (policy <policy>)]
        [<vid>] [<tag_prio>] [<dmac_type>]
        [(any) |
         (etype [<etype>] [<smac>]) |
         (arp [<arp type>] [<opcode>]
              (any | [<source ip>] [<source ip mask>])
              (any | [<destination ip>] [<destination ip mask>])
              [<source mac>] [<arp smac match flag>]
              [<raro dmac match flag>] [<ip/ethernet length flag>]
              [<ip flag>] [<ethernet flag>]) |
         (ip [(<source ip> <source ip mask>) | any]
             [(<destination ip> <destination ip mask>) | any]
             [<ip ttl>] [<ip fragment>] [<ip option>]
             [(icmp <icmp type> <icmp code>) |
              (udp <source port range> <destination port range>) |
              (tcp <source port range> <destination port range>
                   <tcp fin flag> <tcp syn flag> <tcp rst flag>
                   <tcp psh flag> <tcp ack flag> <tcp urg flag>) |
              (other <ip protocol value>) |
              (any)]
        ]
        [<action>] [<rate limiter>] [<port copy>]
```

Description: To set access control entry on switch

Show

Syntax: show

Description: Show all access control entry settings on the switch.

Argument: none

Possible value: none

Example:

LPB4008A(acl)# show

port	policy id	action	rate limiter	port copy	counter a class map
5	1	deny	2	2	0
7	1	permit	0	0	0
8	1	permit	0	0	0

rate limiter	rate(pps)
1	1
2	1
3	1
4	1
5	1
……	……

LPB4008A(acl)#

D. alarm

a. email
b.

del mail-address

Syntax: del mail-address <#>

Description: Remove the E-mail address configuration.

Argument: <#>: email address number, range: 1 to 6

Possible value: <#>: 1 to 6

Example:

LPB4008A(alarm-email)# del mail-address 2

del server-user

Syntax: del server-user

Description: To remove the server configuration, user account, and password.

Argument: None.

Possible value: None.

Example:

LPB4008A(alarm-email)# del server-user

set mail-address

Syntax: set mail-address <#> <mail address>

Description: Set up the email address.

Argument: <#>: email address number, range: 1 to 6

<mail address>: email address

Possible value: <#>: 1 to 6

Example:

LPB4008A(alarm-email)# set mail-address 1 abc@mail.abc.com

set server

Syntax: set server <ip>

Description: Set up the IP address of the email server.

Argument: <ip>: email server ip address or domain name

Possible value: None.

Example:

LPB4008A(alarm-email)# set server 192.168.1.6

set user

Syntax: set user <username>

Description: Set up the account and password of the email server.

Argument: <username>: email server account and password

Possible value: None.

Example:

LPB4008A (alarm-email)# set user admin

Show

Syntax: show

Description: Display the configuration of e-mail.

Argument: None.

Possible value: None.

Example:

```
LPB4008A(alarm-email)# show
Mail Server         : 192.168.1.6
Username             : admin
Password            : ****************
Email Address 1   : abc@mail.abc.com
Email Address 2:
Email Address 3:
```

Email Address 4:
Email Address 5:
Email Address 6:

b. events

del all

Syntax: del all <range>

Description: Disable email and trap events trap.

Argument: <range>: del the range of events, syntax 1, 5-7

Possible value: <range>: 1~24

Example:

LPB4008A(alarm-events)# del all 1-3

del email

Syntax: del email <range>

Description: Disable the events email.

Argument: <range>: del the range of email, syntax 1, 5-7

Possible value: <range>: 1~24

Example:

LPB4008A(alarm-events)# del email 1-3

del trap

Syntax:

del trap <range>

Description:

Disable the events trap.

Argument:

<range>:del the range of trap, syntax 1,5-7

Possible value:

<range>: 1~24

Example:

LPB4008A(alarm-events)# del trap 1-3

set all

Syntax: set all <range>

Description: To enable email and events trap.

Argument: <range>: set the range of events, syntax 1, 5-7

Possible value: <range>: 1~24

Example:

LPB4008A(alarm-events)# set all 1-3

set email

Syntax: set email <range>

Description: Enable the events email.

Argument: <range>: set the range of email, syntax 1, 5-7

Possible value: <range>: 1~24

Example:

LPB4008A(alarm-events)# set email 1-3

set trap

Syntax: set trap <range>

Description: Enable the events trap.

Argument: <range>: set the range of trap, syntax 1, 5-7

Possible value: <range>: 1~24

Example:

LPB4008A(alarm-events)# set trap 1-3

Show

Syntax: show

Description: Display the alarm event configuration.

Argument: None.

Possible value: None.

Example:

LPB4008A(alarm-events)# show

```
   Events                  Email   Trap
-------------------------------------------
1  Cold Start                       v
2  Warm Start                       v
3  Link Down                        v
4  Link Up                           v
5  Authentication Failure       v
6  Login
7  Logout
8  Module Inserted
9  Module Removed
10 Dual Media Swapped
11 Looping Detected
12 STP Disabled
13 STP Enabled
14 STP Topology Changed
15 LACP Disabled
```

16 LACP Enabled
17 LACP Member Added
18 LACP Aggregates Port Failure
19 GVRP Disabled
20 GVRP Enabled
21 VLAN Disabled
22 Port-based Vlan Enabled
23 Tag-based Vlan Enabled
24 IP MAC Binding Enabled
25 IP MAC Binding Disabled
26 IP MAC Binding Client Authenticate error
27 IP MAC Binding Server Authenticate error

show (alarm)

Syntax: show

Description: Show alarm displays the configuration of Events, or E-mail.

Argument: None.

Possible value: None.

Example:

LPB4008A(alarm)# show events

LPB4008A(alarm)# show email

E. autologout

Autologout

Syntax: autologout <time>

Description: Set up the autologout timer.

Argument: <time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.

Possible value: <time>: 0,1-3600

Example:

LPB4008A# autologout 3600

Set autologout time to 3600 seconds

F. config-file

Export

Syntax: export <current | user> < ip address>

Description: To run the export function.

Argument: < Usage> set up current or user

< ip address> the TFTP server ip address

Possible value: none

Example:

LPB4008A(config-file)# export current 192.168.1.63

Export successful.

import

Syntax: import <current | user> < ip address>

Description: Run the import start function.

Argument: None

Possible value: None

Example:

LPB4008A(config-file)# import current 192.168.1.63

Import successful.

G. firmware

Upgrade

Syntax: upgrade <ip_address> <file_path>

Description: Set up the image file that will be upgraded.

Argument: <ip address>: TFTP server ip address

<filepath>: upgrade file path

Possible value: <ip address>: TFTP server ip address

<filepath>: upgrade file path

Example:

LPB4008A(firmware)# upgrade 192.168.2.4 fgs2924R_LPB4008A_v2.03.img

H. gvrp

set state

Syntax: set state < 0 | 1>

Description: Disable/enable the gvrp function.

Argument: 0: disable the gvrp function

1: enable the gvrp function

Possible value: 0: disable the gvrp function

1: enable the gvrp function

Example:

LPB4008A(gvrp)# set state 1

group applicant

Syntax: group applicant <vid> <port> < 0 | 1>

Description: Enter any gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of an existing gvrp group per port.

Argument: <vid>: enter which gvrp group you created, using value vid. Available range: 1 to 4094

<port>: 1 to 8

< 0 | 1>:

Possible value: <vid>: 1~4094

<port>: 1 to 8

Example:

LPB4008A(gvrp)# group applicant 2 5 0

GVRP group information

Current Dynamic Group Number: 1

VID Member Port
---- --
2   5

set applicant

Syntax: set applicant <port> < 0 | 1 >

Description: Set default applicant mode for each port.

Argument: <port>: port range, syntax 1, 5-7, available from 1 to 8

<0>: set applicant as normal mode

<1>: set applicant as non-participant mode

Possible value: <port>: 1 to 8

< 0 | 1 >: normal or non-participant

Example:

LPB4008A(gvrp)# set applicant 1-10 non-participant

set registrar

Syntax: set registrar <port> < 0 | 1 | 2>

Description: Set default registrar mode for each port.

Argument: <port>: port range, syntax 1,5-7, available from 1 to 8

<0>: set registrar as normal mode

<1>: set registrar as fixed mode

<2>: set registrar as forbidden mode

Possible value: <range>: 1 to 8

< 0 | 1 | 2>: normal or fixed or forbidden

Example:

LPB4008A(gvrp)# set registrar 1-5 fixed

set restricted

Syntax: set restricted <port> <0 | 1 | 2>

Description: Set the restricted mode for each port.

Argument: <port>: port range, syntax 1,5-7, available from 1 to 8

<0>: set restricted normal

<1>: set restricted fixed

<2>: set restricted forbidden

Possible value: <port>: 1 to 8

< 0| 1| 2>: normal, fixed or forbidden

Example:

LPB4008A(gvrp)# set restricted 1-10 1

LPB4008A(gvrp)# show config
GVRP state: Enable

Port	Join Time	Leave Time	LeaveAll Time	Applicant	Registrar	Restricted
1	20	60	1000	Normal	Normal	Enable
2	20	60	1000	Normal	Normal	Enable
3	20	60	1000	Normal	Normal	Enable
4	20	60	1000	Normal	Normal	Enable
5	20	60	1000	Normal	Normal	Enable
6	20	60	1000	Normal	Normal	Enable
7	20	60	1000	Normal	Normal	Enable
8	20	60	1000	Normal	Normal	Enable

set timer

Syntax: set timer <port> <JoinTime> <leaveTime> <leaveAllTime>
Description: Set gvrp join time, leave time, and leaveall time for each port.
Argument: <port> : port range, syntax 1,5-7, available from 1 to 8
<JoinTime>: join timer, available from 20 to 100
<LeaveTime>: leave timer, available from 60 to 300
<LeaveAllTime>: leaveall timer, available from 1000 to 5000. Leave Time must equal double Join Time at least.
Possible value: <port>: 1 to 8
<JoinTime>: 20 to 100
<LeaveTime>: 60 to 300
<LeaveAllTime>: 1000 to 5000
Example:
LPB4008A(gvrp)# set timer 2-8 25 80 2000

show

Syntax: show
Description: Display the gvrp configuration.
Argument: None
Possible value: None
Example:

```
LPB4008A(gvrp)# show
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time    Applicant    Registrar Restricted
---- --------- ---------- ------------- ---------- ---------- ----------
  1      20         60         1000       Normal         Normal      Disable
  2      25         80         2000       Normal         Normal      Disable
  3      25         80         2000       Normal         Normal      Disable
  4      25         80         2000       Normal         Normal      Disable
  5      25         80         2000       Normal         Normal      Disable
  6      25         80         2000       Normal         Normal      Disable
  7      25         80         2000       Normal         Normal      Disable
  8      25         80         2000       Normal         Normal      Disable
```

counter

Syntax: counter <port>
Description: Display the port's number.
Argument: <port>: port number
Possible value: <port>: available from 1 to 8
Example:

```
LPB4008A(gvrp)# counter 2
Received

Total GVRP Packets          : 0
Invalid GVRP Packets        : 0
LeaveAll message            : 0
JoinEmpty message           : 0
JoinIn message              : 0
LeaveEmpty message          : 0
Empty message               : 0

Transmitted
Total GVRP Packets          : 0
Invalid GVRP Packets        : 0
LeaveAll message            : 0
JoinEmpty message           : 0
JoinIn message              : 0
LeaveEmpty message          : 0
Empty message               : 0
```

group grpinfo

Syntax: group grpinfo <vid>

Description: Show the gvrp group.

Argument: <vid>: Set the vlan id from 1 to 4094.

Possible value: <vid>: 1 to 4094

Example:

```
LPB4008A(gvrp)# group grpinfo 2

GVRP group information

VID  Member Port
---- ------------------------------------------------
```

hostname

hostname

Syntax: hostname <name>

Description: Set up the switch's hostname.

Argument: <name>: hostname, max. 40 characters.

Possible value: <name>: hostname, max. 40 characters.

Example:

LPB4008A# hostname Company

Company#

J. igmp

set drp

Syntax: set drp <port >

Description: Set router ports to disable.

Argument: <port >: syntax 1, 5-7, available from 1 to 8

Possible value: <port >: 1 to 8

Example:

LPB4008A(igmp)# set drp 1-10

set erp

Syntax: set erp <port>

Description: Set router ports to enable.

Argument: <port>: syntax 1, 5-7, available from 1 to 8

Possible value: <port>: 1 to 8

Example:

LPB4008A(igmp)# set erp 1

set flood

Syntax: set flood <state>

Description: Set up disable/enable unregister ipmc flooding.

Argument: <state>: 0: disable, 1:enable

Possible value: <state>: 0 or 1

Example:

LPB4008A(igmp)# set flood 1

show gm

Syntax: show gm

Description: Display group membership.

Argument: None.

Possible value: None.

Example:

LPB4008A(igmp)# show gm

show igmpp

Syntax: show igmpp

Description: Display igmp proxy setting.

Argument: None.

Possible value: None.

Example:

LPB4008A(igmp)# show igmpp

K. IP

disable dhcp

Syntax: disable dhcp

Description: Disable the system's DHCP function.

Argument: None

Possible value: None

Example:

LPB4008A(ip)# disable dhcp

enable dhcp

Syntax: enable dhcp <manual|auto>

Description: Enable the system's DHCP function and set DNS server via manual or auto mode.

Argument: <manual|auto>: set dhcp by using manual or auto mode.

Possible value: <manual|auto> : manual or auto

Example:

LPB4008A(ip)# enable dhcp manual

Set dns

Syntax: set dns <ip>

Description: Set the DNS server's IP address.

Argument: <ip>: dns ip address

Possible value: 168.95.1.1

Example:

LPB4008A (ip)# set dns 168.95.1.1

set ip

Syntax: set ip <ip> <mask> <gateway>

Description: Set the system IP address, subnet mask, and gateway.

Argument: <ip>: ip address

<mask>: subnet mask

<gateway>: default gateway

Possible value: <ip>: 192.168.1.2 or others

<mask>: 255.255.255.0 or others

<gateway>: 192.168.1.253 or others

Example:

LPB4008A(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253

Show

Syntax: show

Description: Display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address, and current IP address.

Argument: None

Possible value: None

Example:

LPB4008A(ip)# show

DHCP : Disable
IP Address : 192.168.2.237
Current IP Address : 192.168.2.237
Subnet mask : 255.255.255.0
Gateway : 192.168.2.252
DNS Setting : Manual

DNS Server : 168.95.1.1

L. ip_mac_binding

set entry

Syntax: set entry < 0 | 1> < mac> < ip> < port no> < vid>

Description: Set ip mac binding entry.

Argument: < 0 | 1>: 0: Client, 1: Server

<mac>: mac address

<ip>: ip address

<port>: syntax 1, 5-7, available from 1 to 8

<vid>: vlan id, 1 to 4094

Possible value: < 0 | 1>: 0: Client, 1: Server

<mac>: format: 00-02-03-04-05-06

<ip>: ip address

<port>: 1 to 8

<vid>: 1 to 4094

Example:

LPB4008A(ip_mac_binding)# set entry 1 00-11-2f-de-7b-a9 192.168.2.2 1 1

delete ip

Syntax: delete ip < 0 | 1> <ip>

Description: Delete ip mac binding entry by ip.

Argument: <0 | 1>: 0: client, 1: server

<ip>: ip address

Possible value: None

Example:

LPB4008A(ip_mac_binding)# delete ip 1 192.168.2.2

set state

Syntax: show

Description: Display the mac alias entry.

Argument: None

Possible value: None

Example:

```
LPB4008A(mac-table-alias)# show

MAC Alias List
     MAC Address            Alias
----- ----------------- ----------------
1)    00-02-03-04-05-06    aaa
2)    00-33-03-04-05-06    ccc
3)    00-44-33-44-55-44    www
```

M. loop-detection

Disable

Syntax: disable <#>

Description: Disable the loop detection function for the switch ports.

Argument: <#>: set up the range of the ports to search for, syntax 1, 5-7, available form 1 to 8.

Possible value: <#>: 1 to 8

Example:

```
LPB4008A(loop-detection)# disable 1-8

LPB4008A(loop-detection)# show

Detection Port       Locked Port
  Port Status          Port Status
---------------------------------
    1  Disable         1  Normal
    2  Disable         2  Normal
    3  Disable         3  Normal
    4  Disable         4  Normal
    5  Disable         5  Normal
    6  Disable         6  Normal
    7  Disable         7  Normal
    8  Disable         8  Normal
```

Enable

Syntax: enable <#>

Description: Enable the detection function for the switch ports.

Argument: <#>: set up the range of the ports to search for, syntax 1, 5-7, available form 1 to 8

Possible value: <#>:1 to 8

Example:

```
LPB4008A(loop-detection)# enable 1-8

LPB4008A(loop-detection)# show

Detection Port       Locked Port
  Port Status          Port Status
---------------------------------
```

1	Enable	1	Normal
2	Enable	2	Normal
3	Enable	3	Normal
4	Enable	4	Normal
5	Enable	5	Normal
6	Enable	6	Normal
7	Enable	7	Normal
8	Enable	8	Normal

Resume

Syntax: resume <#>

Description: Resume locked ports on switch.

Argument: <#>: set up the range of the ports to search for, syntax 1,5-7, available form 1 to 8

Possible value: <#>: 1 to 8

Example:

LPB4008A (loop-detection)# resume 1-8

LPB4008A (loop-detection)# show

Detection Port		Locked Port	
Port	Status	Port	Status
1	Enable	1	Normal
2	Enable	2	Normal
3	Enable	3	Normal
4	Enable	4	Normal
5	Enable	5	Normal
6	Enable	6	Normal
7	Enable	7	Normal
8	Enable	8	Normal

show

Syntax: show
Description: Display loop detection configure.

Argument: None

Possible value: None

Example:

LPB4008A (loop-detection)# show

Detection Port		Locked Port	
Port	Status	Port	Status
1	Enable	1	Normal
2	Enable	2	Normal
3	Enable	3	Normal
4	Enable	4	Normal

5	Enable	5	Normal
6	Enable	6	Normal
7	Enable	7	Normal
8	Enable	8	Normal

N. Mac

a. alias

del

Syntax: del <mac>

Description: Delete mac alias entry.

Argument: <mac>: set up the MAC format: xx-xx-xx-xx-xx-xx

Possible value: <mac>: set up the MAC format: xx-xx-xx-xx-xx-xx

Example:

LPB4008A(mac-alias)# set 23-56-r5-55-3f-03 test3

LPB4008A(mac-alias)# show

MAC Alias

No	MAC	Alias
1	23-56-00-55-3F-03	test3
2	23-56-00-55-EF-03	test13
3	23-56-00-55-EF-33	test1

LPB4008A(mac-alias)# del 23-56-00-55-3F-03

LPB4008A(mac-alias)# show

MAC Alias

No	MAC	Alias
1	23-56-00-55-EF-03	test13
2	23-56-00-55-EF-33	test1

set

Syntax: set <mac> < alias>

Description: Set mac alias entry.

Argument: <mac>: mac address, xx-xx-xx-xx-xx-xx

<alias>: mac alias name, max 15 characters

Possible value: <mac>: set up the MAC format: xx-xx-xx-xx-xx-xx

<alias> : mac alias name, max 15 characters

Example:

LPB4008A(mac-alias)# set 23-56-r5-55-3f-03 test3

```
LPB4008A(mac-alias)# show

MAC Alias
 No      MAC                       Alias
==========================================
  1      23-56-00-55-3F-03         test3
  2      23-56-00-55-EF-03         test13
  3      23-56-00-55-EF-33         test1
```

show

Syntax: show

Description: Display MAC alias entry.

Argument: None

Possible value: none

Example:

```
LPB4008A(mac-alias)# show

MAC Alias
 No      MAC                       Alias
==========================================
  1      23-56-00-55-3F-03         test3
  2      23-56-00-55-EF-03         test13
  3      23-56-00-55-EF-33         test1
```

mac-table

flush

Syntax: flush

Description: Delete dynamic MAC entry.

Argument: none

Possible value: none

Example:

```
LPB4008A(mac-mac-table)# flush

LPB4008A(mac-mac-table)# show

 No      Type      VLAN     MAC               Port Members
------------------------------------------------------------------------------
  1      Static       1     FF-FF-FF-FF-FF-FF  1,2,3,4,5,6,7,8
```

show

Syntax: show

Description: Show all MAC table information.

Argument: none

Possible value: none

Example:

LPB4008A(mac-mac-table)# show

No	Type	VLAN	MAC	Port Members
1	Static	1	FF-FF-FF-FF-FF-FF	1,2,3,4,5,6,7,8

c. maintenance
d.

set age-time

Syntax: set age-time <#>

Description: Set MAC table age out time of the dynamic learning MAC.

Argument: <#>: age-timer in seconds, 0, 10, 1000000. The value zero disables aging.

Possible value: <#>: 0, 10 to 1000000.

Example:

LPB4008A(mac-table-maintain)# set age-time 300

LPB4008A(mac-maintenance)# show

E api_ai 26/vtss_

Aging Configuration: Enter into sta

Age time: 300 mode

MAC Table Learning

Port	Learning Mode-<< Global commands >
2	Auto
3	Auto
4	Auto
5	Auto
6	Auto
7	Auto

set learning

Syntax: set learning <range> <auto|disable|secure>

Description: Set MAC table learning.

Argument: <range syntax>: 1, 5-7, available from 1 to 8

<auto >: auto learning

<disable >: disable learning

<secure >: learn frames are discarded

Possible value: <range syntax>: 1, 5-7, available from 1 to 8

<auto>: auto learning

<disable>: disable learning

<secure>: learn frames are discarded.

Example:

LPB4008A(mac-table-maintain)# set learning 1-24 auto

LPB4008A(mac-maintenance)# show

E api_ai 26/vtss_

Aging Configuration: Enter into sta

Age time: 300mode

MAC Table Learning
Port Learning Mode-<< Global commands >
 2 Auto
 3 Auto
 4 Auto
 5 Auto
 6 Auto
 7 Auto
 8 Auto

show

Syntax: show

Description: To display mac table maintenance

Argument: None.

Possible value: None

Example:

LPB4008A(mac-maintenance)# show

1 Static

Aging Configuration:FF 1,2,3,4,5,6,7,8

Age time: 3004,15,16,17,1

MAC Table Learning
Port Learning Mode
 2 Auto
 3 Auto
 4 Auto
 5 Auto
 6 Auto
 7 Auto
 8 Auto

static-mac

add

Syntax: add <mac> <port> <vid> [alias]

Description: Add the static mac entry.

Argument: <mac>: mac address, format: 00-02-03-04-05-06

<port>: 0-8. The value "0" means this entry is a filtering entry.

<vid>: vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based.

[alias]: mac alias name, max. 15 characters

Possible value: <mac>: mac address

<port>: 0-8

<vid>: 0, 1-4094

[alias]: mac alias name

Example:

LPB4008A(mac-static-mac)# add 00-02-03-04-05-06 3 0 aaa

LPB4008A(mac-static-mac)#

del

Syntax: del <mac> <vid>

Description: Delete the static MAC entry.

Argument: <mac>: mac address, format: 00-02-03-04-05-06

<vid>: vlan id. 0, 1-4094. VID must be zero if vlan mode is not tag-based

Possible value: <mac>: mac address

<vid>: 0, 1-4094

Example:

LPB4008A(mac-static-mac)# del 00-02-03-04-05-06 0

LPB4008A(mac-static-mac)#

show filter

Syntax: show filter

Description: Display the static filtering MAC entry.

Argument: None

Possible value: None

Example:

LPB4008A(mac-static-mac)# show filter

Static Filtering Etnry: (Total 1 item(s))

1) mac: 00-33-03-04-05-06, vid: -, alias: ccc

LPB4008A(mac-static-mac)#

show forward

Syntax: show forward

Description: Display the static forwarding mac entry.

Argument: None

Possible value: None

Example:

LPB4008A(mac-static-mac)# show forward

Static Forwarding Etnry: (Total 1 item(s))

1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa

LPB4008A(mac-static-mac)#

O. mirror

set mirror

Syntax: set mirror < #>

Description: Set mirror port and enable/disable mirror function.

Argument: <#>: port, available from 1 to 8 and 0.

1 to 8: available port number

0: disable mirror function

Possible value: <#>: 1 to 8

Example:

LPB4008A(mirror)# set mirror 2

set monitor-destination

Syntax: set monitor-destination <range>

Description: Set monitor destination port. The packets sent by this port will be copied to the monitoring port.

Argument: <range>: the port that is chosen for monitored port of the mirror function, syntax 1,5-7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

LPB4008A(mirror)# set monitor-destination 2-8

LPB4008A(mirror)# show

2	V
3	V
4	V
5	V
6	V
7	V
8	V

set monitor-source

Syntax: set monitor-source <range>

Description: Set up the monitoring port of the mirror function. Users can observe the packets that the monitored port received via this port.

Argument: <range>: the monitoring port that is chosen for the mirror function. Only one port can be configured, available from 1 to 8.

Possible value: <range>:1 to 8

Example:

LPB4008A(mirror)# set monitor-source 8

LPB4008A(mirror)# show

Port to mirror to: 1

Port	Source Enable	Destination Enable
2		V
3		V
4		V
5		V
6		V
7		V
8		V

LPB4008A(mirror)#

Show

Syntax: show

Description: Display the mirror configuration's setting status.

Argument: None

Possible value: None

Example:

LPB4008A(mirror)# show

Port to mirror to: 1

Port	Source Enable	Destination Enable
2		V
3		V
4		V
5		V
6		V
7		V
8		V

LPB4008A(mirror)#

disable

Syntax: disable

Description: Disable mstp function.

Argument: None

Possible value: None

Example:

LPB4008A (mstp)# disable

enable

Syntax: enable

Description: Enable mstp function.

Argument: None

Possible value: None

Example:

LPB4008A (mstp)# enable

migrate-check

Syntax: migrate-check <port-range>

Description: Force the port to transmit RST BPDUs.

Argument: Usage: migrate-check <port range>

port range syntax: 1,5-7, available from 1 to 8

Possible value: Usage: migrate-check <port range>

port range syntax: 1,5-7, available from 1 to 8

Example:

LPB4008A (mstp)# migrate-check 1-2

set config

Syntax: set config <Max Age><Forward Delay><Max Hops>

Description: Set max age,forward delay,max hops.

Argument: <Max Age>: available from 6 to 40. Recommended value is 20.

<Forward Delay(sec)>: available from 4 to 30. Recommended value is 15.

<Max Hops>: available from 6 to 40. Recommended value is 20.

Possible value: <Max Age>: available from 6 to 40. Recommended value is 20.

<Forward Delay(sec)>: available from 4 to 30. Recommended value is 15.

<Max Hops>: available from 6 to 40. Recommended value is 20.

Example:

LPB4008A(mstp)# set config 20 15 20

LPB4008A(mstp)#

set msti-vlan

Syntax: set msti-vlan <instance-id><vid-string>

Description: Map Vlan ID(s) to an MSTI

Argument: <instance-id>: MSTI id available from 1 to 4095

<vid-string>: syntax example: 2.5-7.100-200

Possible value: <instance-id>: available from 1 to 4094

Example:

LPB4008A(mstp)# set msti-vlan 2 2.5

msti 2 had been successfully created and(or)

vlan(s) have been added to map to this msti.

LPB4008A(mstp)#

set p-cost

Syntax: set p-cost <instance_id> <port range> <path cost>

Description: Set port path cost per instance

Argument: <port range> syntax: 1, 5-7, available from 1 to 8

<path cost>: 0, 1-200000000. The value zero means auto status

Possible value: <port range>: available from 1 to 8

<path cost>: The value zero means auto status, 0-2000000000

Example:

LPB4008A(mstp)# set p-cost 2 8-10 0

LPB4008A(mstp)#

set p-edge

Syntax: set p-edge <port range> <admin edge>

Description: Set per port admin edge

Argument: <port range> syntax: 1,5-7, available from 1 to 8

<admin edge>: 0->non-edge port,1->edge ports

Possible value: <port range> syntax: 1,5-7, available from 1 to 8

<admin edge>: 0->non-edge port,1->edge ports

Example:

LPB4008A(mstp)# set p-edge 10-12 0

LPB4008A(mstp)#

set p-hello

Syntax: set p-hello <port range> <hello time>

Description: Set per port hello time

Argument: <port range>: syntax: 1, 5-7, available from 1 to 8

<hello time>: only 1~2 are valid values

Possible value: <port range>: syntax: 1, 5-7, available from 1 to 8

<hello time>: only 1~2 are valid values

Example:

LPB4008A(mstp)# set p-hello 4-7 1

LPB4008A(mstp)#

set p-p2p

Syntax: set p-p2p <port range> <admin p2p>

Description: Set per port admin p2p

Argument: <port range> syntax: 1, 5-7, available from 1 to 8

<admin p2p>: Admin point to point, <auto|true|false>

Possible value: <port range> syntax: 1, 5-7, available from 1 to 8

<admin p2p>: Admin point to point, <auto|true|false>

Example:

LPB4008A(mstp)# set p-p2p 7-8 auto

LPB4008A(mstp)#

set priority

Syntax: set priority <instance-id><Instance Priority>

Description: Set instance priority

Argument: <instance-id>: 0->CIST; 1-4095->MSTI

<Instance Priority>: must be a multiple of 4096, available from 0 to 61440

Possible value: <instance-id>: 0->CIST; 1-4095->MSTI

<Instance Priority>: 0 to 61440

Example:

LPB4008A(mstp)# set priority 0 4096

LPB4008A(mstp)# enable

MSTP started

LPB4008A(mstp)# show instance 0

mstp status : enabled

force version : 3

instance id: 0

bridge max age : 20

bridge forward delay : 15

bridge max hops : 20

instance priority : 4096

bridge mac : 00:40:c7:5e:00:09

CIST ROOT PRIORITY : 4096

CIST ROOT MAC : 00:40:c7:5e:00:09

CIST EXTERNAL ROOT PATH COST : 0

CIST ROOT PORT ID : 0

CIST REGIONAL ROOT PRIORITY : 4096

CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09

CIST INTERNAL ROOT PATH COST : 0

CIST CURRENT MAX AGE : 20

CIST CURRENT FORWARD DELAY : 15

TIME SINCE LAST TOPOLOGY CHANGE(SECs) : 2

TOPOLOGY CHANGE COUNT(SECs) : 0

LPB4008A(mstp)#

set r-role

Syntax: set r-role <port range> <restricted role>

Description: Set per port restricted role.

Argument: <port range> syntax: 1, 5-7, available from 1 to 8

<restricted role>: 0->false, 1->True

Possible value: <port range>: 1 to 8

<restricted role>: 0->false, 1->True

Example:

LPB4008A(mstp)# set r-role 1-4 1

```
LPB4008A(mstp)# set r-role 5-8 0

LPB4008A(mstp)# show ports 0

==== =========== ====== ========= ===== ===== ==Operational== =Restricted=
Port Port Status Role   Path Cost Pri   Hello Edge-Port       P2P  Role  Tcn
==== =========== ====== ========= ===== ===== ========= ===== ====== =====
  1  FORWARDING  DSGN   200000            128   2/2       V
  2  DISCARDING  dsbl   2000000   128     2/2   V
  3  DISCARDING  dsbl   2000000   128     2/2   V
  4  DISCARDING  dsbl   2000000   128     2/2   V
  5  FORWARDING  DSGN   200000            128   2/2       V              V
  6  DISCARDING  dsbl   2000000   128     2/2   V
  7  FORWARDING  DSGN   20000     128     2/2   V              V
  8  DISCARDING  dsbl   2000000   128     2/2   V              V
LPB4008A(mstp)#
```

set r-tcn

Syntax: set r-tcn <port range> <restricted tcn>

Description: Set per port restricted tcn

Argument: <port range> syntax: 1, 5-7, available from 1 to 8

<restricted tcn>: 0->false,1->True

Possible value: <port range>: 1 to 8

<restricted tcn>: 0->false,1->True

Example:

```
LPB4008A(mstp)# set r-tcn 1-4 1

LPB4008A(mstp)# set r-tcn 5-8 1

LPB4008A(mstp)# show pconf 0

Port      Path      Cost      Priority  Hello     Edge-Port         P2P       Role      Tcn
  system              Enter in
==== ========= ======== ===== ========= ===== ====== =====...(q to quit)
  2       0        128    2     true     auto           false             false
  3        0       128    2     true     auto           false             true
  4        0       128    2     true     auto           false             true
  5        0       128    2     true     auto           false             false
  6        0       128    2     true     auto           false             false
  7        0       128    2     true     auto           false             false
  8        0       128    2     true     auto           true              false
  LPB4008A(mstp)#
```

set region-name

Syntax: set region-name <string>

Description: Set mstp region name (0–32 bytes).

Argument: <string>:a null region name

Possible value: <string>:1-32

Example:

```
LPB4008A(mstp)# set region-name test2
```

LPB4008A(mstp)# show region-info

Name : test2

Revision : 0

Instances : 0

LPB4008A(mstp)#

set revision-level

Syntax: set rev <revision-level>

Description: Set mstp revision-level (0–65535)

Argument: <revision-level>: 0~65535

Possible value: <revision-level>: 0~65535

Example:

LPB4008A(mstp)# set revision-level 30000

LPB4008A(mstp)# show region-info

Name: test2

Revision: 30000

Instances: 0

LPB4008A(mstp)#

set version

Syntax: set version <stp|rstp|mstp>

Description: Set force-version

Argument: <revision-level>: 0~65535

Possible value: <revision-level>: 0~65535

Example:

GS-2924(mstp)# set version mstp

show instance

Syntax: show instance <instance-id>

Description: Show instance status.

Argument: <instance-id>: 0->CIST; 1-4095->MSTI

Possible value: <instance-id>: 0->CIST; 1-4095->MSTI

Example:

LPB4008A(mstp)# show instance 0

mstp status : enabled

force version : 2

instance id: 0

bridge max age : 20

bridge forward delay : 15

bridge max hops : 20

instance priority : 4096

bridge mac : 00:40:c7:5e:00:09

CIST ROOT PRIORITY : 4096

CIST ROOT MAC : 00:40:c7:5e:00:09

CIST EXTERNAL ROOT PATH COST : 0

CIST ROOT PORT ID : 0

CIST REGIONAL ROOT PRIORITY : 4096

CIST REGIONAL ROOT MAC : 00:40:c7:5e:00:09

CIST INTERNAL ROOT PATH COST : 0

CIST CURRENT MAX AGE : 20

CIST CURRENT FORWARD DELAY : 15

TIME SINCE LAST TOPOLOGY CHANGE(SECs) : 2569

TOPOLOGY CHANGE COUNT(SECs) : 0

LPB4008A(mstp)#

show pconf

Syntax: show pconf <instance-id>

Description: Show port configuration.

Argument: instance-id: 0->CIST; 1-4095->MSTI

Possible value: <instance-id>: 0->CIST; 1-4095->MSTI

Example:

```
LPB4008A(mstp)# show pconf 0
  set r-role          Se
  2         0    128     2      true     auto  false false
  3         0    128     2      true     auto  false  true
  4         0    128     2      true     auto  false  true
  5         0    128     2      true     auto  false false
  6         0    128     2      true     auto  false false
  7         0    128     2      true     auto  false false
  8         0    128     2      true     auto   true false

LPB4008A(mstp)#
```

show ports

Syntax: show ports <instance-id>

Description: Show port status.

Argument: instance-id: 0->CIST; 1-4095->MSTI

Possible value: <instance-id>:0->CIST; 1-4095->MSTI

Example:

LPB4008A(mstp)# show ports 0

show region-info

Syntax: show region-info

Description: Show region config.

Argument: none

Possible value: none

Example:

LPB4008A(mstp)# show region-info

Name : test2

Revision : 30000
Instances : 0

LPB4008A(mstp)#

show vlan-map

Syntax: show vlan-map <instance-id>

Description: Show vlan mapping of an instance.

Argument: <nstance-id>: 0->CIST; 1-4095->MSTI

Possible value: <instance-id>: 0->CIST; 1-4095->MSTI

Example:

LPB4008A(mstp)# show vlan-map 0

instance 0 has those vlans :

0-4095

LPB4008A(mstp)#

Q. policy

Add

Syntax: add [name <value>] [ip <value>] [port <value>] [type <value>] action <value>

Description: Add a new management policy entry.

Argument: Synopsis: add name George ip 192.168.1.1-192.168.1.90 port 2-5, 8 type h,s action a

Synopsis: add name Mary ip 192.168.2.1-192.168.2.90 action deny

Possible value: None

Example:

LPB4008A(policy)# add name Mary ip 192.168.3.1-192.168.3.4 action deny

LPB4008A(policy)# show

```
1) Name        : george        IP Range                : 192.168.1.1-192.168.1.90
   Action      : Accept        Access Type             : HTTP SNMP
   Port        : 2 3 4 5 8

 2) Name       : rule1           IP Range          : 192.168.2.1-192.168.2.30
   Action      : Deny            Access Type       : HTTP TELENT SNMP
   Port         : 11 12 13 14 15

 3) Name       : Mary             IP Range         : 192.168.3.1-192.168.3.4
   Action      : Deny            Access Type       : Any
   Port                  : Any
LPB4008A(policy)#
```

Delete

Syntax: delete <index>

Description: Delete a management policy entry.

Argument: <index>: a specific or range management policy entry(s) e.g. delete 2,3,4-7

Possible value: <index>: a specific or range management policy entry(s)

Example:

LPB4008A(policy)# add name rule2 ip 192.168.4.23-192.168.4.33 port 6-8 type s,t

action d

LPB4008A(policy)# show

```
 1) Name       : rule1           IP Range          : 192.168.4.5-192.168.4.22
   Action      : Deny            Access Type       : HTTP TELENT SNMP
   Port                  : 2 3 4 5

 2) Name       : rule2           IP Range          : 192.168.4.23-192.168.4.33
   Action      : Deny            Access Type       : TELENT SNMP
   Port                  : 6 7 8
```

LPB4008A(policy)# delete 2

LPB4008A(policy)# show

```
 1) Name       : rule1           IP Range          : 192.168.4.5-192.168.4.22
   Action      : Deny            Access Type       : HTTP TELENT SNMP
   Port   : 2 3 4 5
```

LPB4008A(policy)#

Show

Syntax: show

Description: Show management policy list.

Argument: none

Possible value: none

Example:

LPB4008A(policy)# show

```
 1) Name        : rule1          IP Range        : 192.168.4.5-192.168.4.22
    Action      : Deny           Access Type     : HTTP TELENT SNMP
    Port                : 2 3 4 5
 2) Name         : rule2         IP Range        : 192.168.4.23-192.168.4.33
    Action      : Deny           Access Type     : TELNET SNMP
    Port                : 6 7 8
```

R. port

clear counter

Syntax: clear counter

Description: Clear all ports' counter (include simple and detail port counter) information.

Argument: None

Possible value: None

Example:

LPB4008A (port)# clear counter

set description

Syntax: set description <port-range> <description>

Description: Set port description.

Argument: <port range> syntax: 1, 5-7, available from 1 to 8

<description>: set port description, max 47 characters

Possible value: <port range>: 1 to 8

<description>: max 47 characters

Example:

LPB4008A(port)# set description 3-8 salesdepartment

LPB4008A(port)# show config

```
          Speed/    Flow     Maximum Excessive          Synopsis: add name George ip 192.168.1.1-
Port      Duplex    Control  Frame   Collision  Description
          type
  2       Auto      Disabled 9600    Discard
  3       Auto      Disabled 9600    Discard            salesdepartment
  4       Auto      Disabled 9600    Discard            salesdepartment
  5       Auto      Disabled 9600    Discard            salesdepartment
  6       Auto      Disabled 9600    Discard            salesdepartment
  7       Auto      Disabled 9600    Discard            salesdepartment
  8       Auto      Disabled 9600    Discard            salesdepartment
```

set excessive-collision

Syntax: set excessive-collision <port-range> <discard|restart>

Description: Set port description.

Argument: <port range> syntax: 1, 5-7, available from 1 to 8

Possible value: <port range>: 1 to 8

Example:

LPB4008A(port)# set excessive-collision 6-10 restart

LPB4008A(port)# show config

```
      Speed/Flow                          Maximum Excessive

Port  Duplex    Control    Frame      Collision  Description a list of previously run command  set priority
----- --------- ---------- ---------- ---------- ---------------------------------DISCAR
  2   Auto      Disabled   9600       Discard
  3   Auto      Disabled   9600       Discard    salesdepartment
  4   Auto      Disabled   9600       Discard    salesdepartment
  5   Auto      Disabled   9600       Discard    salesdepartment
  6   Auto      Disabled   9600       Restart    salesdepartment
  7   Auto      Disabled   9600       Restart    salesdepartment
  8   Auto      Disabled   9600       Restart    salesdepartment
```

set flow-control

Syntax: set flow-control <port-range> <enable|disable>

Description: Set per-port flow control.

Argument: <port-range>: syntax 1, 5-7, available from 1 to 8

Possible value: <port-range>: 1 ~ 8

Example:

LPB4008A(port)# set flow-control 1-8

LPB4008A(port)# show config

1	Auto	Disabled	9600	Doscard	
2	Auto	Disabled	9600	Discard	
3	Auto	Enabled	9600	Discard	salesdepartment
4	Auto	Enabled	9600	Discard	salesdepartment
5	Auto	Enabled	9600	Discard	salesdepartment
6	Auto	Enabled	9600	Restart	salesdepartment
7	Auto	Enabled	9600	Restart	salesdepartment
8	Auto	Enabled	9600	Restart	salesdepartment

set max-frame

Syntax: set max-frame <port-range> <value>

Description: Set per-port maximum frame size.

Argument: <port range> syntax: 1, 5-7, available from 1 to 8

<value>: Allowed value are 1518-9600 bytes.

Possible value: <port range> syntax: 1 to 8

<value>: 1518-9600 bytes.

Example:
LPB4008A(port)# set max-frame 3-6 1518
LPB4008A(port)# show config

	Speed/	Flow	Maximum	Excessive commands	
2	Auto	Disabled	9600	Discard	
3	Auto	Enabled	1518	Discard	salesdepartment
4	Auto	Enabled	1518	Discard	salesdepartment
5	Auto	Enabled	1518	Discard	salesdepartment
6	Auto	Enabled	1518	Restart	salesdepartment
7	Auto	Enabled	9600	Restart	salesdepartment
8	Auto	Enabled	9600	Restart	salesdepartment

set speed

Syntax: set speed <port-range> <disable|auto|1Gfull|100full|100half|10full|10half

Description: Set port capability.

Argument: <port-range>: syntax 1, 5-7, available from 1 to 8

<port-speed>: auto: set auto-negotiation mode

10half: set speed/duplex 10M Half

10full: set speed/duplex 10M Full

100half: set speed/duplex 100M Half

100full: set speed/duplex 100M Full

1Gfull: set speed/duplex 1G Full

Possible value: <port-range>: 1 to 8

<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull

Example:

```
LPB4008A (port)# set speed 3 auto
LPB4008A (port)# show status
                 Speed/
Port Link        Duplex          Rx Pause        Tx Pause        Description
---- ---- --------- -------- -------- --------------------------------
  1  Up               100M/Full       Disabled                Disabled
  2  Down     Down          Disabled                Disabled
  3  Up               100M/Full       Disabled                Disabled
  4  Down     Down          Disabled                Disabled
  5  Down     Down          Disabled                Disabled
  6  Down     Down          Disabled                Disabled
  7  Up               1G/Full         Disabled                Disabled
  8  Down     Down          Disabled                Disabled
```

show config

Syntax: show config

Description: Display each port's configuration information.

Argument: None.

Possible value: None.

Example:

```
LPB4008A(port)# show config
       Speed/    Flow      Maximum  Excessive
Port  Duplex   Control   Frame       Collision  Description
---- --------- -------- ------- --------- --------------------------------
  1    Auto      Disabled  9600        Discard
  2    1G/Full   Disabled  9600        Discard
  3    Auto      Disabled  9600        Discard
  4    1G/Full   Disabled  9600        Discard
  5    1G/Full   Disabled  9600        Discard
  6    Auto      Disabled  9600        Discard
  7    Auto      Disabled  9600        Discard
  8    Auto      Disabled  9600        Discard
```

show detail-counter

Syntax: show detail-counter <port>

Description: Display the display detail port counter.

Argument: <port>: port, available from 1 to 8

Possible value: <port>: 1 ~ 8

Example:

```
LPB4008A          (port)#   show              detail-counter 3
Rx Multicast      6         Tx Multicast      641
Rx Broadcast      94        Tx Broadcast      5251
Rx Pause           0        Tx Pause                  0

Receive Size                Counters          Transmit Size Counters
--------------------------------              ------------------------------------
Rx 64 Bytes                 7381      Tx 64 Bytes                 4351
Rx 65-127 Bytes              291      Tx 65-127 Bytes                     2342
Rx 128-255 Bytes            118       Tx 128-255 Bytes             605
Rx 256-511 Bytes             53       Tx 256-511 Bytes                    1081
Rx 512-1023 Bytes            33       Tx 512-1023 Bytes            144
Rx 1024-1526 Bytes           28       Tx 1024-1526 Bytes          11453
Rx 1527- Bytes                0       Tx 1527- Bytes                    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
```

show sfp

Syntax: show sfp <port>

Description: Display the SFP module information.

Argument: <port>: SFP port of the switch, available from 7, 8

Possible value: <port>: 7- 8

Example:

```
LPB4008A(port)# show sfp 7
Port 7 SFP information
-------------------------------------------------------------------------
Connector Type              : SFP - Unknown or unspecified
Fiber Type                          : Reserved
Tx Central Wavelength       : 0
Baud Rate                           : 1G
Vendor OUI                  : 00:00:00
Vendor Name                 : FIBERXON INC.
Vendor PN                   : FTM-C012R-LC
Vendor Rev                  : 10
Vendor SN                           : PP220052901281
Date Code                   : 051012
Temperature                 : none
Vcc                         : none
Mon1 (Bias) mA              : none
Mon2 (TX PWR)               : none
Mon3 (RX PWR)               : none
LPB4008A(port)#
```

show simple-counter

Syntax: show simple-counter

Description: To display each port's traffic counting summary.

Argument: None.

Possible value: None.

Example:

LPB4008A (port)# show simple-counter

set max-frame Set per-port maximum frame size

1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0

LPB4008A(port)#

show status

Syntax: show status
Description: Display the port's current status.
Argument: None.
Possible value: None.
Example:
LPB4008A(port)# show status
Speed/1G/Full Disable

Port	Link	Duplex	Rx Pause	Tx Pause	Description
3	Auto	Disabled	9600	Discard	
2	Down	Down	Disabled	Disabled	
3	Up	100M/Full	Disabled	Disabled	
4	Down	Down	Disabled	Disabled	
5	Down	Down	Disabled	Disabled	
6	Down	Down	Disabled	Disabled	
7	Up	1G/Full	Disabled	Disabled	
8	Down	Down	Disabled	Disabled	

LPB4008A(port)#

S. qos

a. ports

set class

Syntax: set class <#>

Description: Set the number of classes.

Argument: #: Number of classes, available 1, 2, 4

Possible value: <#>: 1, 2, 4

Example:

LPB4008A(qos-ports)# set class 2

LPB4008A(qos-ports)#

set port

Syntax: set port <range> <default class> <qcl> <user priority> <queuing mode> <low queue weighted> <normal queue weighted>

<medium queue weighted> <high queue weighted>

Description: Set port information.

Argument: <range syntax>: 1, 5-7, available from 1 to 8

<default class option>: low | normal | medium | high

<qcl>: available from 1 to 24

<user priority>: available from 0 to 7

<queuing mode>: strict | weighted

<low queue weighted>: 1/2/4/8

<normal queue weighted>: 1/2/4/8

<medium queue weighted>: 1/2/4/8

<high queue weighted>: 1/2/4/8

Possible value: <range syntax>: 1 to 8

<default class option>: low | normal | medium | high

<qcl>: 1 to 24

<user priority>: 0 to 7

<queuing mode>: strict | weighted

<low queue weighted>: 1/2/4/8

<normal queue weighted>: 1/2/4/8

<medium queue weighted>: 1/2/4/8

<high queue weighted>: 1/2/4/8

Example:

```
LPB4008A(qos-ports)# set port 2 medium 1 3 weithted 2 2 2 2

LPB4008A(qos-ports)# show

 2  Medium 1        3      Weighted Fair     2/2/2/2
 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

LPB4008A(qos-ports)#
```

Show

Syntax: show

Description: Show port information.

Argument: none

Possible value: none

Example:

```
LPB4008A(qos-ports)# show

Number of Classes:2
  2  Medium 1         3       Weighted Fair     2/2/2/2
  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                  1/2/4/8
  7  Low       1         0       Strict Priority       1/2/4/8
  8  Low       1         0       Strict Priority       1/2/4/8
  9  Low       1         0       Strict Priority       1/2/4/8
 10  Low      1         0       Strict Priority       1/2/4/8
```

b. qcl

set

Syntax: set <dscp> < tos> < tagpriority> <qce type> <value> <class>

Description: Add the QCE entry in the specific QCL.

Argument: <dscp>: dscp field, syntax 1,5-7, available from 0 to 63

<tos>: tos priority, available from 1 to 8

<tagpriority>: tag priority, available from 1 to 8

<qce type>: Ethernet

<value>: 0xfff0

<class>: high

Possible value: <dscp>: dscp field, syntax 1,5-7, available from 0 to 63

<tos>: tos priority , available from 1 to 8

<tagpriority>: tag priority, available from 1 to 8
<qce type>: Ethernet

<value>: 0xfff0

<class>: high

Example:

```
LPB4008A(qos-qcl)# set 2 0 3 ethernet 0xfff0 high

LPB4008A(qos-qcl)# show 2 1

QCE Type:           Ethernet Type

Ethernet Type Value:0xfff0

Traffic Class:      High

LPB4008A(qos-qcl)#
```

move

Syntax: move <qcl> <qce> <new qce>

Description: Move up the specific QCE entry in the specific QCL

Argument: <qcl>: the qcl number, available from 1 to 24.

<qce>: the original qce number, available from 1 to 12.

<new qce>: the new qce number, available from 1 to 12.

Possible value: <qcl>: available from 1 to 24.

<qce>: available from 1 to 12.

<new qce>: available from 1 to 12.

Example:

LPB4008A(qos-qcl)# move 2 1 1

Delete

Syntax: delete <qcl> <qce range>

Description: Delete the specific QCE entry in the specific QCL.

Argument: <qcl>: the qcl number, available from 1 to 24.

<qce range>: 1, 5-7, available from 1 to 12

Possible value: <qcl>: available from 1 to 24.

<qce range>: available from 1 to 12

Example:

LPB4008A(qos-qcl)# delete 2 1

c. rate

set

Syntax: set <range> <policer enabled> <rate> <unit> <shaper enabled> <rate> <unit>

Description: Set rate limit configuration.

Argument: <range syntax>: 1,5-7, available from 1 to 8

<policer enabled>: 1 means enable and 0 means disable

<rate>: allowed values are 500kbps-1Gkps

<unit>: 'k' means kbps and 'm' means mbps

<shaper enabled>: 1 means enable and 0 means disable

<rate>: allowed values are 500kbps-1Gkps

<unit>: 'k' means kbps and 'm' means mbps

Possible value: range syntax: 1, 5-7, available from 1 to 8

policer enabled: 1 means enable and 0 means disable

shaper enabled: 1 means enable and 0 means disable

rate: allowed values are 500kbps-1Gkps

unit: 'k' means kbps and 'm' means mbps

Example:

LPB4008A(qos-rate)# set 2 1 1000 m 1 1000 m

LPB4008A(qos-rate)# show

2	V	1000	Mbps	V	1000	Mbps
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
9		500	kbps		500	kbps
10		500	kbps		500	kbps

storm

set broadcast

Syntax: set broadcast <status> <rate>

Description: Set broadcast storm control configuration.

Argument: <status>: 1 means enable and 0 means disable

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

Possible value: <status>: 1 means enable and 0 means disable

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

Example:

LPB4008A(qos-storm)# set broadcast 1 512

LPB4008A(qos-storm)# show

Frame Type	Status	Rate(Packet Per Second)
Flooded unicast		1
Multicast		1
Broadcast	V	512

set multicast

Syntax: set multicast <status> <rate>

Description: Set multicast storm control configuration.

Argument: <status>: 1 means enable and 0 means disable

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

Possible value: <status>: 1 means enable and 0 means disable

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

Example:

LPB4008A(qos-storm)# set multicast 1 64

LPB4008A(qos-storm)# show

```
Frame Type        Status              Rate(Packet Per Second)
-------------------------------------------------
Flooded unicast                 1
Multicast         V            64
Broadcast         V           512
```

set unicast

Syntax: set unicast <status> <rate>

Description: Set flooded unicast storm control configuration.

Argument: <status>: 1 means enable and 0 means disable

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

Possible value: <status>: 1 means enable and 0 means disable

<rate>: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k

Example:

LPB4008A(qos-storm)# set unicast 1 128

LPB4008A(qos-storm)# show

```
Frame Type       Status    Rate(Packet Per Second)
-------------------------------------------------
Flooded unicast  V       128
Multicast        V         64
Broadcast        V       512
```

Show

Syntax: show

Description: Show storm control configuration.

Argument: none

Possible value: none

Example:

LPB4008A(qos-storm)# show

```
Frame Type       Status    Rate (Packet Per Second)
-------------------------------------------------
Flooded unicast  V         128
Multicast        V           64
Broadcast        V         512
```

T. reboot

reboot

Syntax: reboot

Description: Reboot the system.

Argument: None.

Possible value: None.

Example:

LPB4008A# reboot

U. snmp

Disable

Syntax: disable set-ability

disable snmp

Description: Disable is used to de-activate snmp or set-community.

Argument: None.

Possible value: None.

Example:

LPB4008A(snmp)# disable snmp

LPB4008A(snmp)# disable set-ability

Enable

Syntax: enable set-ability

enable snmp

Description: Enable is used to activate snmp or set-community.

Argument: None.

Possible value: None.

Example:

LPB4008A(snmp)# enable snmp

LPB4008A(snmp)# enable set-ability

Set

Syntax: set get-community <community>

set set-community <community>

set trap <#> <ip> [port] [community]

Description: Set is used to set up get-community, set-community, trap host ip, host port and trap-community.
Argument: <#>: trap number

<ip>: ip address or domain name

<port>: trap port

<community>: trap community name

Possible value: <#>: 1 to 6

<port>: 1~65535

Example:

LPB4008A(snmp)# set get-community public

LPB4008A(snmp)# set set-community private

LPB4008A(snmp)# set trap 1 192.168.1.1 162 public

Show

Syntax: show

Description: Show displays the SNMP configuration.

Argument: None.

Possible value: None.

Example:

LPB4008A(snmp)# show

SNMP : Enable

Get Community: public

Set Community: private [Enable]

Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public

Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public

V. stp

MCheck

Syntax: MCheck <range>

Description: Forces the port to transmit RST BPDUs.

Argument: <range>: syntax 1,5-7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

LPB4008A(stp)# Mcheck 1-8

Disable

Syntax: disable

Description: Disables the STP function.

Argument: None.

Possible value: None.

Example:

LPB4008A(stp)# disable

Enable

Syntax: enable

Description: Enables the STP function.

Argument: None.

Possible value: None.

Example:

LPB4008A(stp)# enable

set config

Syntax: set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

Description: Set up the STP parameters.

Argument: <Bridge Priority>: priority must be a multiple of 4096, available from 0 to 61440.

<Hello Time>: available from 1 to 10.

<Max. Age>: available from 6 to 40.

<Forward Delay>: available from 4 to 30.

Note: 2*(Forward Delay -1) >= Max Age

Max Age >= 2*(Hello Time +1)

Possible value: <Bridge Priority>: 0 to 61440

<Hello Time>: 1 to 10

<Max. Age>: 6 to 40

<Forward Delay>: 4 to 30

Example:

LPB4008A(stp)# set config 61440 2 20 15

set port

Syntax: set port <range> <path cost> <priority> <edge_port> <admin p2p>

Description: Set up the STP port information.

Argument: <range>: syntax 1, 5-7, available from 1 to 8

<path cost>: 0, 1-200000000. The value zero means auto status

<priority>: priority must be a multiple of 16, available from 0 to 240

<edge_port>: Admin Edge Port, <yes|no>

<admin p2p>: Admin point to point, <auto|true|false>

Possible value: <range>:1 to 8

<path cost>: 0, 1-200000000

<priority>: 0 to 240

<edge_port>: yes/no

<admin p2p>: auto/true/false

Example:

LPB4008A(stp)# set port 1-16 0 128 yes auto

set version

Syntax: set version <stp|rstp>

Description: Set up the STP version.

Argument: <stp|rstp>:stp/rstp

Possible value: <stp|rstp>:stp/rstp

Example:

LPB4008A(stp)# set version rstp

show config

Syntax: show config

Description: Display the STP configuration
.
Argument: None.

Possible value: None.

Example:

LPB4008A(stp)# show config

STP State Configuration :

Spanning Tree Protocol : Enabled

Bridge Priority (0-61440) : 61440

Hello Time (1-10 sec) : 2

Max. Age (6-40 sec) : 20

Forward Delay (4-30 sec) : 15

Force Version : RSTP

show port

Syntax: show port

Description: Display the STP port information.

Argument: None.

Possible value: None.

Example:

LPB4008A# stp

LPB4008A(stp)# show port

```
Port Port Status      Path Cost    Priority    Admin Edge Port   Admin Point To Point
==== =========== ========== ======== ================ ====================
  1  DISCARDING    2000000    128         No                Auto
  2  DISCARDING    2000000    128         No                Auto
  3  DISCARDING    2000000    128         No                Auto
...(q to quit)
```

show status

Syntax: show status

Description: Display the STP status.

Argument: None.

Possible value: None.

Example:

LPB4008A(stp)# show status

STP Status :

STP State : Enabled

Bridge ID : 00:40:C7:D8:09:1D

Bridge Priority : 61440

Designated Root : 00:40:C7:D8:09:1D

Designated Priority : 61440

Root Port : 0

Root Path Cost : 0

Current Max. Age(sec) : 20

Current Forward Delay(sec) : 15

Hello Time(sec) : 2

STP Topology Change Count : 0

Time Since Last Topology Change(sec) : 848

W. system

set contact

Syntax: set contact <contact string>

Description: Set the switch's contact description.

Argument: <contact>:string length up to 40 characters.

Possible value: <contact>: A, b, c, d, … ,z and 1, 2, 3, …. etc.

Example:

LPB4008A(system)# set contact Taipei

set device-name

Syntax: set device-name <device-name string>

Description: Set the switch's device name description.

Argument: <device-name>: string length up to 40 characters.

Possible value: <device-name>: A, b, c, d, … ,z and 1, 2, 3, …. etc.

Example:

LPB4008A(system)# set device-name CR-2600

set location

Syntax: set location <location string>

Description: Set the switch's location description.

Argument: <location>: string length up to 40 characters.

Possible value: <location>: A, b, c, d, … ,z and 1, 2, 3, …. etc.

Example:

LPB4008A(system)# set location Taipei

Show

Syntax: show

Description: Display the switch's basic information.

Argument: None.

Possible value: None.

Example:

LPB4008A(system)# show

Model Name : LPB4008A

System Description : L2 Managed Switch

Location :

Contact :

Device Name : LPB4008A

System Up Time : 0 Days 0 Hours 4 Mins 14 Secs

Current Time : Tue Jan 17 16:28:46 2006

BIOS Version : v1.05

Firmware Version : v2.08

Hardware-Mechanical Version : v1.01-v1.01

Serial Number : 030C02000003
Host IP Address : 192.168.1.1

Host MAC Address : 00-40-c7-e7-00-10

Device Port : UART * 1, TP * 22, Dual-Media Port(RJ45/SFP) * 2

RAM Size : 16 M

Flash Size : 2 M

X. traplog

clear

Syntax: clear

Description: Clear the trap log.

Argument: none

Possible value: none

Example:

LPB4008A(traplog)# clear

LPB4008A(traplog)# show

No time desc

---- --------------------------- -------------------------------------

show

Syntax: show

Description: Display the trap log.

Argument: None.

Possible value: None.

Example:

LPB4008A(tftp)# show

2 Mon Mar 17 15:18:38 2008gvrp mode> <qce type> .

Dual Media Swapped [Port:1][SwapTo:TP]ge hostnamexit / 4 / 8

3 Mon Mar 17 15:18:38 2008nto igmp mode, available from Link Up [Port:1]Enter into ip mode

6 Mon Mar 17 15:18:38 2008 Dual Media Swapped [Port:5][SwapTo:TP]

7 Mon Mar 17 15:18:38 2008 Link Up [Port:5]

8 Mon Mar 17 15:18:48 2008 Login [admin]

Y. time

set daylightsaving

Syntax: set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>

Description: Set up the daylight savings time.

Argument: hr: daylight saving hour, range: -5 to +5

MM: daylight saving start Month (01-12)

DD: daylight saving start Day (01-31)

HH: daylight saving start Hour (00-23)

mm: daylight saving end Month (01-12)

dd: daylight saving end Day (01-31)

hh: daylight saving end Hour (00-23)

Possible value: hr: -5 to +5

MM: (01-12)

DD: (01-31)

HH: (00-23)

mm: (01-12)

dd: (01-31)

hh: (00-23)

Example:

LPB4008A(time)# set daylightsaving 3 10/12/01 11/12/01

Save Successfully

set manual

Syntax: set manual <YYYY/MM/DD> <hh:mm:ss>

Description: Set up the current time manually.

Argument: YYYY: Year (2000-2036), MM: Month (01-12)

DD: Day (01-31), hh: Hour (00-23)

mm: Minute (00-59), ss: Second (00-59)

Possible value: YYYY: (2000-2036), MM: (01-12)

DD: (01-31), hh: (00-23)

mm: (00-59), ss: (00-59)

Example:

LPB4008A(time)# set manual 2004/12/23 16:18:00

set ntp

Syntax: set ntp <ip> <timezone>
Description: Set up the current time via an NTP server.
Argument: <ip>: ntp server ip address or domain name
<timezone>: time zone (GMT), range: -12 to +13
Possible value: <timezone>: -12,-11..., 0, 1...,13
Example:
LPB4008A(time)# set ntp clock.via.net 8
Synchronizing...(1)
Synchronization success

Show

Syntax: show

Description: Show the time configuration, including “Current Time,” “NTP Server,” ” Timezone,” ” Daylight Saving,” “Daylight Saving Start,” and “Daylight Saving End”

Argument: None.

Possible value: None.

Example:

LPB4008A(time)# show

Current Time : Thu Thu 14 15:04:03 2005

NTP Server : 209.81.9.7

Timezone : GMT+8:00

Day light Saving : 0 Hours

Day light Saving Start : Mth: 1 Day: 1 Hour: 0

Day light Saving End : Mth: 1 Day: 1 Hour: 0

LPB4008A(time)#

Z. trunk

del trunk

Syntax: del trunk <port-range>

Description: Delete the trunking port.

Argument: <port-range>: port range, syntax 1,5-7, available from 1 to 8

Possible value: <port-range>: 1 to 8

Example:

LPB4008A(trunk)# del trunk 1

set priority

Syntax: set priority <range>

Description: Set up the LACP system priority.

Argument: <range>: available from 1 to 65535.

Possible value: <range>: 1 to 65535, default: 32768

Example:

LPB4008A(trunk)# set priority 33333

set trunk

Syntax: set trunk <port-range> <method> <group> <active LACP>

Description: Set up the status of trunk, including the group number and mode of the trunk as well as the LACP mode.

Argument: <port-range> : port range, syntax 1,5-7, available from 1 to 8

<method>: static: adopt the static link aggregation

lacp: adopt the dynamic link aggregation- link aggregation control protocol

<group>: 1-8.

<active LACP>: active: set the LACP to active mode

passive: set the LACP to passive mode

Possible value: <port-range>: 1 to 8

<method>: static / lacp

<group>: 1-8.

<active LACP>: active / passive

Example:

LPB4008A(trunk)# set trunk 1-4 lacp 1 active

show aggtr-view

Syntax: show aggtr-view

Description: Display the aggregator list.

Argument: None.

Possible value: None.

Example:

LPB4008A(trunk)# show aggtr-view

Aggregator 1) Method: None

Member Ports: 1

Ready Ports: 1

Aggregator 2) Method: LACP

Member Ports: 2

Ready Ports:

: :

show lacp-detail

Syntax: show lacp-detail <aggtr>

Description: Display the LACP trunk group's detailed information.

Argument: <aggtr>: aggregator, available from 1 to 8

Possible value: <aggtr>: 1 to 8

Example:

LPB4008A(trunk)# show lacp-detail 2

Aggregator 2 Information:

Actor Partner

System Priority MAC Address System Priority MAC Address

32768 00-40-c7-e8-00-02 32768 00-00-00-00-00-00

Port Key Trunk Status Port Key

---

2 257 --- 2 0

show lacp-priority

Syntax: show lacp-priority

Description: Display the LACP Priority value.

Argument: None.

Possible value: None.

Example:

LPB4008A(trunk)# show lacp-priority

LACP System Priority : 32768

show status

Syntax: show status

Description: Display each port's aggregator status and settings.

Argument: None.

Possible value: None.

Example:

LPB4008A(trunk)# show status

Trunk Port Setting				Trunk Port Status		
port	Method	Group	Active LACP	Aggtregator	Status	
1	None	0	Active	1	Ready	
2	LACP	1	Active	2	---	
3	LACP	1	Active	3	---	
4	LACP	1	Active	4	---	
5	LACP	1	Active	5	---	
6	LACP	1	Active	6	---	
7	LACP	1	Active	7	---	

A1. Vlan

del port-group

Syntax: del port-group <name>

Description: Delete the port-based vlan group.

Argument: <name>: which vlan group you want to delete.

Possible value: <name>: port-vlan name

Example:

LPB4008A(vlan)# del port-group VLAN-2

del tag-group

Syntax: del tag-group <vid>
Description: Delete the tag-based vlan group.
Argument: <vid>: which vlan group you want to delete, available from 1 to 4094
Possible value: <vid>: 1 to 4094
Example:

LPB4008A(vlan)# del tag-group 2

disable drop-untag

Syntax: disable drop-untag <range>

Description: Don't drop the untagged frames.

Argument: <range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

LPB4008A(vlan)# disable drop-untag 5-10

disable sym-vlan

Syntax: disable sym-vlan <range>

Description: Drop frames from the non-member port.

Argument: <range>: which port(s) you want to set, syntax 1,5-7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

LPB4008A(vlan)# disable sym-vlan 5-10

enable drop-untag

Syntax: enable drop-untag <range>

Description: Drop the untagged frames.

Argument: <range>: which port(s) you want to set, syntax 1, 5-7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

LPB4008A(vlan)# enable drop-untag 5-10

enable sym-vlan

Syntax: enable sym-vlan <range>

Description: Drop frames from the non-member port.

Argument: <range> : which port(s) you want to set, syntax 1,5-7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

LPB4008A(vlan)# enable sym-vlan 5-10

set mode

Syntax: set mode < port | tag > [up-link]

Description: Set switch VLAN mode, including port-based and tag-based modes.

Argument: <tag>: set tag-based vlan

<port>: set port-based vlan

Possible value: < port | tag >: port,tag

Example:

LPB4008A(vlan)# set mode

Usage: set mode <port|tag>

tag: set tag-based vlan

port: set port-based vlan

LPB4008A(vlan)#

set double-tag

Syntax: set double-tag <range> <0|1|2>

Description: Set double-tag per port and enable Q-in-Q VLAN function on switch.

Argument: <range >: 1, 5-7, available from 1 to 8

0: disable

1: service provider port

2: customer port

Possible value: <range>: 1 to 8

Example:

LPB4008A(vlan)# set double-tag 3 1

LPB4008A(vlan)#

set port-group

Syntax: set port-group <name> <range>

Description: To add or edit a port-based VLAN group.

Argument: <name>: port-vlan name

<range>: syntax 1,5-7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

LPB4008A(vlan)# set port-group VLAN-1 2-5,6,15-13

set port-role

Syntax: set port-role <range> <access|trunk|hybrid> [vid]

Description: Set egress rule: configure the port roles.

Argument: <range>: which port(s) you want to set, syntax 1, 5-7, available from 1 to 8

<access>: Do not tag frames

<trunk>: Tag all frames

<hybrid>: Tag all frames except a specific VID

<vid>: untag-vid for hybrid port

Possible value: <range>: 1 to 8

<vid>: 1 to 4094

Example:

LPB4008A(vlan)# set port-role 5 hybrid 6

set pvid

Syntax: set pvid <range> <pvid>

Description: Set the pvid of vlan.

Argument: <range>: which port(s) you want to set PVID(s), syntax 1,5-7, available from 1 to 8

<pvid>: which PVID(s) you want to set, available from 1 to 4094

Possible value: <range>: 1 to 8

<pvid>: 1 to 4094

Example:

LPB4008A(vlan)# set pvid 3,5,6-8 5

set tag-group

Syntax: set tag-group <vid> <name> <range> <#>

Description: Add or edit the tag-based vlan group.

Argument: <vid>: vlan ID, range from 1 to 4094

<name>: tag-vlan name

<range>: vlan group members, syntax 1,5-7, available from 1 to 8

<#>: sym/asym vlan setting. 1: symmetric vlan, 0: asymmetric vlan

Possible value: <vid>: 1 to 4094

<range>: 1 to 8

<#>: 0 or 1

Example:

LPB4008A(vlan)# set tag-group 2 VLAN-2 2-5,6,15-13 0

show group

Syntax: show group

Description: Display the vlan mode and vlan group.

Argument: None.

Possible value: None.

Example:

LPB4008A(vlan)# show group

Vlan mode is double-tag.

1) Vlan Name : default

Vlan ID : 1

Sym-vlan : Disable

Member : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

2) Vlan Name : VLAN-2
Vlan ID : 2

Sym-vlan : Disable

Member : 2 3 4 5 6 13 14 15

show port

Syntax: show port

Description: Display pvid, ingress/egress rule.

Argument: None.

Possible value: None.

Example:

LPB4008A(vlan)# show pvid

Port	PVID	Rule1	Rule2	Port Rule	Untag Vid
1	1	Disable	Disable	Access	-
2	1	Disable	Disable	Access	-
3	5	Disable	Disable	Access	-
4	1	Disable	Disable	Access	-
5	5	Enable	Disable	Hybrid	6
6	5	Enable	Disable	Access	-
7	5	Enable	Disable	Access	-
8	5	Enable	Disable	Access	-

6. Troubleshooting

Q: Resolving No Link Condition

A: The possible causes for a no link LED status are as follows:

- The attached device is not powered on.
- The cable may not be the correct type or is faulty.

- The installed building premise cable is faulty.

- The port may be faulty.

Q: Computer A can connect to Computer B, but cannot connect to Computer C through the Managed Switch.

A: The network port of Computer C may be faulty. Check the link/act status of Computer C on the LED indicator. Try another network device on this connection.

The network configuration of Computer C may be wrong. Verify the network configuration on Computer C.

Q: The uplink connection function fails to work.

A: Make sure you are using connection ports on that Managed Switch.
Check the uplink setup of the Managed Switch to verify the uplink function is enabled.

Q: The console interface doesn't appear on the console port connection.

A: The COM port default parameters are [Baud Rate: 115200, Data Bits: 8, Parity Bits: None, Stop Bit: 1, Flow Control: None]. Make sure that the COM port is set property in the terminal program. If the parameters are changed, set the COM configuration to the new setting.

Make sure that RS-232 cable is connected on the console port of the Managed Switch and COM port of PC.

Make sure the PC's COM is enabled.

Q: How do I configure the Managed Switch?

A: The "Hyperterm" is the terminal program in Windows OS. Users can also use any other terminal programs in Linux/Unix to configure the Managed Switch. Refer to your terminal program's user guide. But the COM port parameters' settings (baud rate/data bits/parity bits/ flow control) must be the same as the Managed Switch console port's settings.

7. Null Modem Cable Specifications

The DB9 cable is used for connecting a terminal or terminal emulator to the Managed Switch's RS-232 port to access the command-line interface.

The table below shows the pin assignments for the DB9 cable.

Function	Mnemonic	Pin
Carrier	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

The 9-pin null-modem cable's pin assignment is as follows:

CD 1 .....4 DTR
DSR 6--| 1 CD
DTR 4.....|--6 DSR
RXD 2 .....3 TXD
TXD 3 .....2 RXD
GND 5.....5 GND
RTS 7 .....8 RTS
CTS 8..... 7 RTS
Reserve 9 ..... 9 Reserve