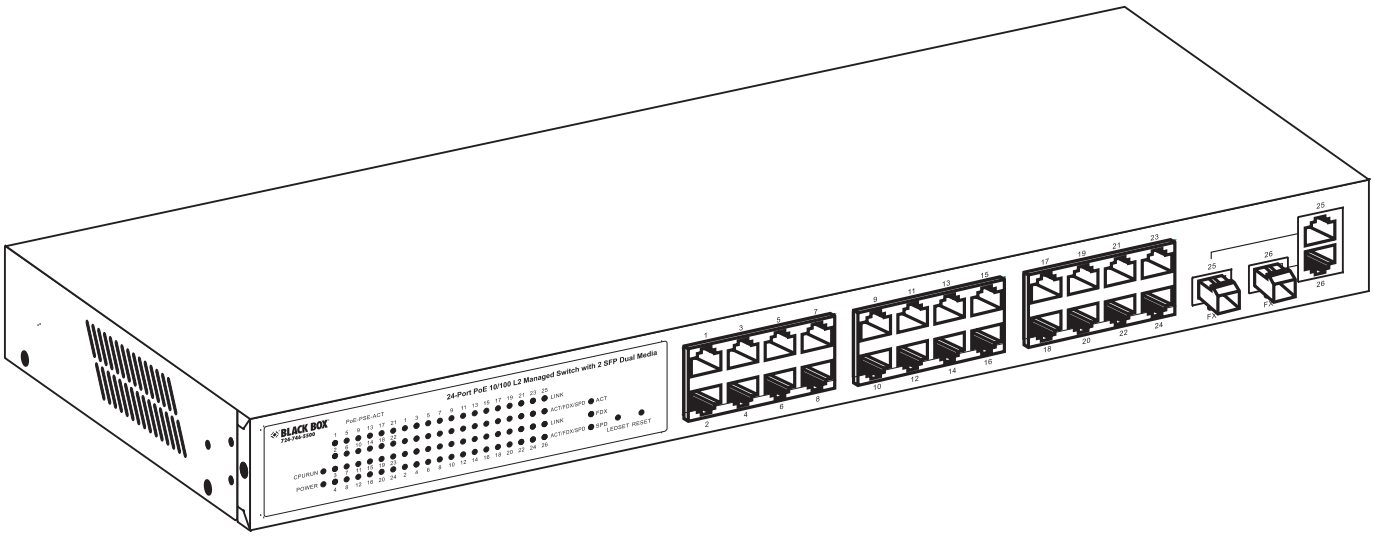
1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

BLACK BOX®
NETWORK SERVICES

JUNE 2006
LPB201A

24-Port 1000BASE-TX L2 Managed PoE Switch With 2 SFP Dual Media Ports



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**

FEDERAL COMMUNICATIONS COMMISSION
AND
INDUSTRY CANADA
RADIO FREQUENCY INTERFEREN CE 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 B 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 radio électriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radio électrique publié par Industrie Canada.

EUROPEANUNION DECLARATIONOF CONFORMITY

This equipment complies with the requirements of the European EMC Directive 89/336/EEC.

CE

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 switch, always:

- **Touch your computer's metal chassis to ground the static electrical charge before you pick up the switch.**
- **Pick up the switch by holding it on the left and right edges only.**

INSTRUCCIONES DE SEGURIDAD (Normas Oficiales Mexicanas Electrical Safety Statement)

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, sótanomojado 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 deoperación. 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 aparatoeléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar enlibreros 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, estufasu 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 deoperación, 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 objetoscolocados 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 deventilación.
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.

TRADEMARKS USED IN THIS MANUAL

ST is a registered trademark of AT&T.

BLACK BOX and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

VT100 is a trademark of Digital Equipment Corporation.

DB2 and IBM are registered trademarks of International Business Machines Corporation.

Linux is a registered trademark of Linus Torvalds.

Internet Explorer, Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation.

Telnet is a trademark of Telnet Communications, Inc.

UNIX is a registered trademark of UNIX System Laboratories, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

NOTE

The 24-Port 10/100BASE-TX L2 Managed PoE Switch with 2 SFP Dual Media Ports is called the LPB201A in the software screens and also in the screens shown in this manual. Both names refer to the LPB201A switch.

Contents

Chapter **Page**

Chapter **Page**

Contents (continued)

Chapter **Page**

1. Specifications

1.1 Hardware

Standards: IEEE802.3, 802.3ab, 802.3z, 802.3u, 802.3af Power over Ethernet, 802.1v protocol-based VLAN classification, 802.3x port-based network access control, 802.1q tag-based VLAN, 802.1d Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, 802.1p Class of Service with 2-level priority queuing, 802.1ad port trunking with flexible load distribution and failover function

Compatible Fiber Transceiver Modules: Ports 25, 26 are TP/SFP fiber dual-media ports with auto detection function; Optional SFP module (LGB200C-MLC, LGB200C-SLC10, LGB200C-SLC30, LGB204C, LGB205C) supports LC or BiDi LC transceiver

Network Interface: 10/100 Mbps Fast Ethernet twisted-pair (ports 1–24), or 1000BASE-LX duplex multimode, duplex single-mode, or single-strand single-mode LC or WDM (BiDi LC) (ports 25, 26)

Transmission Mode: 10-/100-Mbps support for full or half-duplex; 1000-Mbps support for full duplex only

Speed: 10/100 Mbps for twisted pair; 1000 Mbps for fiber

Forwarding/Filtering Packet Rate: 1,488,000 pps at 1000 Mbps; 148,800 pps at 100 Mbps; 14,880 pps at 10 Mbps

MAC Address and Self-Learning: 8K MAC address, 256 VLAN table entries, 256 IP multicast table entries

Buffer Memory: Embedded frame buffer: 256 KB, control memory: 128 KB

Flow Control: IEEE802.3x compliant for full duplex; Backpressure flow control for half-duplex

Cable Type and Maximum Length: Twisted-pair: CAT5 UTP cable, up to 328 feet (100 m) (ports 1–8);
Single-mode single-strand fiber, up to 12.4miles (20 km): 1000BASE-LX single-strand single-mode WDM (BiDi) SFP for LGB204C and LGB205C (slots 7 and 8);
Multimode fiber, up to 1804.4 feet (550 m) for LGB200C-MLC;
Single-mode duplex fiber, up to 6.2 miles (10 km) for LGB200C-SLC10;
Single-mode duplex fiber up to 18.6 miles (30 km)for LGB200C-SLC30

User Controls: (1) Reset button

Connectors: (24) RJ-45, (2) slots for fiber media converter modules;
LGB200C-MLC, LGB200C-SLC10, LGB200C-SLC30: (2) LC;
LGB204C, LGB205C: (1) LC

Indicators: (49) LEDs: All: System LEDs: (1) Power, (1) CPU; (24) 10/100 Mbps TP, (24) Link/Act and (24) Full-duplex for ports 1–24, (2) SFP (1000 Mbps), (2) SFP (Link/Act) and (2) Full-duplex for ports 25, 26

Temperature Tolerance: 32˚ to 104˚F (0˚ to 40˚C)

Relative Humidity: 5% to 90%

Power: 100–240 VAC, 50–60 Hz

Size: 1.7"H x 17.4"W x 8.2"D (4.4 x 44.2 x 20.9 cm)

1.2 Management Software

System Configuration: Auto negotiation support on 10/100BASE-TXports; Web browser or console interface can set transmission speed (10/100 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, RMONMIB

Spanning Tree Algorithm: IEEE 802.1d

VLAN Function: Port-based/802.1q tagged allows up to 256 VLANs in one switch

Trunk Function: Port trunk connections allowed

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 to as Class of Service (CoS)by the IEEE802.1p standard; classification of packet priority can be based on either a VLAN tag on a packet or 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 in the filtering table stay in the filtering table

Internetworking Protocol: Bridging: 802.1d spanning tree; IP Multicast: IGMP snooping; Maximum of 256 active LANs and IP multicast sessions

Network Management: (1) RS-232 port as local control console, Telnet™ remote-control console; SNMP agent: MIB-2 (RFC 1213), Bridge MIB (RFC1493), RMON MIB (RFC1757)-statistics; VLAN MIN (802.1q); Web browser support based on HTTP server and CGI parser TFTP software-upgrade capability

1.3 Null-Modem Cable

Use the included DB9 cable to connect a terminal or terminal emulator to the managed switch's RS-232 port to access the command-line interface. Table 1-1 shows the pin assignments for the DB9 cable.

Table 1-1. Command-line interface DB9 connector pin out.

Function	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

Table 1-2 shows the pin out for the null-modem cable.

Table 1-2. Null-modem cable pin out.

Signal	Pin	Pin	Signal
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	CTS
CTS	8	7	RTS
Not used	9	9	Not used

2. Overview

2.1 Introduction

The 24-Port 10/100BASE-TX L2 Managed PoE Switch with 2 SFP Dual Media Ports is standard switch that meet all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications. Manage the switch via an async console directly connected to the switch's RS-232 port, or through an Ethernet port using CLI or SNMP. In this switch, ports 25, 26 include two types of media — TP and SFP Fiber (LC, BiDi LC, etc); this port supports 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion.

This PoE Switch also complies with IEEE 802.3af, its advanced auto-sensing algorithm enables providing power devices (PD) discovery, classification, current limit, and other necessary functions. It also supports high safety with short circuit protection and power-out auto-detection to PD.

This standalone off-the-shelf switch provides comprehensive hardware features. This switch has 24 RJ-45 twisted-pair ports and 2 STP fiber transceiver module slots (for STP fiber [LC or BiDi LC] modules). The 1000-Mbps SFP fiber transceiver is used for high-speed connection expansion. These two ports auto detect whether the 10/100/1000-Mbps TP or the 1000-Mbps SFP fiber port is used. On this switch, ports 25, 26 can be twisted-pair or Ethernet. Multimode or single-mode fiber transceiver modules plug into these two ports. (See Section 2.4 for more information about the fiber transceiver modules.)

The LPB201A has a 256 KB on-chip frame buffer. The switch features jumbo frame support, programmable classifier for QoS (Layer4/Multimedia), 8K MAC address and 256 VLAN support (IEEE 802.1a), per-port shaping, policing, and Broadcast Storm Control, IEEE 802.1q-in-q nested VLAN support, full-duplex flow control (IEEE 802.3x) and half-duplex backpressure, and extensive front-panel diagnostic LEDs.

Software features include port status and configuration, per-port traffic monitoring counters, system information snapshot upon login, port mirroring, static trunk, and 802.1q VLAN. The switch also supports user management and limits three users to login to enhance security. The maximum packet length can be up to 9208 bytes for a jumbo frame application. More features include DHCP broadcasting suppression to avoid a suspended or crashed network, sending trap event for monitored events, default configuration that can be restored to overwrite the current configuration working on either a Web browser or CLI, online plug/unplug SFP modules, port mirror function with Ingress traffic, rapid spanning tree (802.1w RSTP), 802.1x port security on a VLAN, user management, and only the first login administrator can configure the device.

With the SNMP agent, the network administrator can log in to the switch to monitor, configure, and control each port's activity. The overall network management is enhanced and the network efficiency is also improved to accommodate high-bandwidth applications. In addition, the switch features comprehensive and useful functions such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, and IGMP Snooping capability via the intelligent software. These functions are described below and on the next page. The switch is suitable for both metro-LAN and office applications.

• QoS complies with the IEEE802.1p standard. There are two priority queue and packet transmission schedules.

• Spanning Tree complies with IEEE802.1d and IEEE802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

- The switch also supports port-based VLAN and IEEE 802.1a tag VLAN, with 256 active VLANs and VLAN IDs from 1–4094. It also handles static port trunking and IEEE 802.3ad LACP port trunking.
- Supports Ingress and Egress per port bandwidth control.
- Port Security: Support allowed, denied forwarding, and port security with MAC address.
- SNMP/RMON: SNMP agent and RMON MIB. In the device, the SNMP agent is client software that's operating over the SNMP protocol used to receive the command from an SNMP manager (server site) and echo the corresponding data (MIB object). The SNMP agent actively issues TRAP information.
- RMON is the abbreviation for Remote Network Monitoring and is a branch of the SNMP MIB.
- The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group1, 2, 3, and 9, Ethernet-like MIB (RFC 1643), and Ethernet MIB (RFC 1643).
- IGMP Snooping: Supports IGMP version 2 (RFC 2236): IGMP snooping establishes the multicast groups that forward multicast packets to the member ports. This avoids wasting the bandwidth while IP multicast packets are running over the network.

2.2 What's Included

Your package should contain the following items. If anything is missing or damaged, please contact Black Box at 724-746-5500.

- 24-Port 10/100BASE-TX L2 Managed PoE Switch with 2 SFP Dual Media Ports
- CD-ROM containing this user's manual in PDF format
- A printed Quick Start Guide
- AC power cord
- DB9 female to DB9 female RS-232 cable
- Rackmount kit
- (4) rubber feet

2.3 Hardware Description

Figure 2-1 shows the 24-Port 10/100BASE-TX L2 Managed PoE Switch's front panel. The numbered components in the figure are described in Table 2-1.

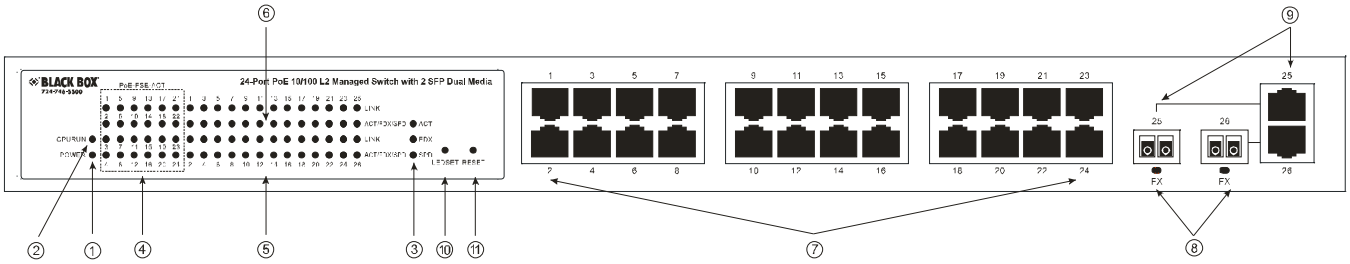


Figure 2-1. Front panel.

Table 2-1. Front-panel components.

Component	Description
① Power LED	Lights when power is on.
② CPU LED	Lights when there is activity on the CPU.
③ ACT/ FDX/ SPD	Lights when LEDSET set on active/ full-duplex/ speed mode.
④ PoE Status LEDs	Lights when PoE Power is active.
⑤ TP ACT/ FDX/ SPD LEDs (ports 1-24)	LEDSET set on ACT (active) mode: Blinks when any traffic is present. LEDSET set on FDX (full-duplex) mode: Lights when full-duplex mode is active. Blinks when any collision is present. LEDSET on SPD (speed) mode: Lights when 100 Mbps speed is active. Off when 10 Mbps speed is active.
⑤ SFP Fiber ACT/ FDX/ SPD LEDs (ports 25, 26)	LEDSET set on ACT (active) mode: Blinks when any traffic is present. LEDSET set on FDX (full-duplex) mode: Lights when full-duplex mode is active. Blinks when any collision is present. LEDSET on SPD (speed) mode: Lights when 100 Mbps speed is active. Off when 10 Mbps speed is active.

Table 2-1 (continued). Front-panel components.

Component	Description
⑥ TP Link LEDs (ports 1-24)	There are 24 TP Link/ACT LEDs. Each lights when the twisted-pair connection to the remote device is good. Blinks when any traffic is present. Off when the cable connection is not good.
⑥ TP Link LEDs (ports 25, 26)	There are 24 TP Link/ACT LEDs. Each lights when the twisted-pair connection to the remote device is good. Blinks when any traffic is present. Off when the cable connection is not good.
⑦ Fast Ethernet ports	24 10/100-Mbps auto sensing ports.
⑧ SFP Fiber FX LEDs	Lights when Fiber port is active. Off when TP port is active.
⑨ SFP Fiber/ Gigabit TP Ports	SFP fiber port module slots/ Gigabit TP ports.
⑩ LEDSET button	Selects the LEDSET mode.
⑪ Reset button	Resets the management system.

The switch's rear panel is shown in Figure 2-2. The numbered components in the figure are described in Table 2-2.

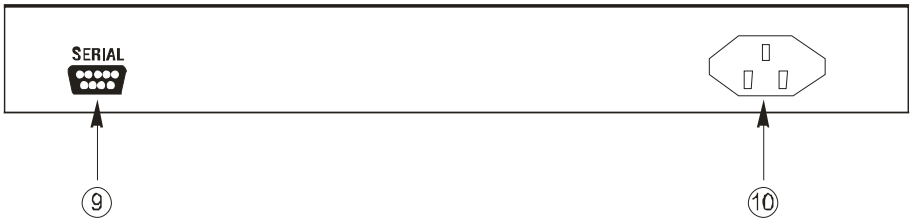


Figure 2-2. Rear panel.

Table 2-2. Rear panel components.

Component	Description
⑨ DB9 connector	RS-232 serial console port for configuration or management.
⑩ Power connector	Connects to a 100–240-VAC, 50/60-Hz AC power line.

2.4 Optional SFP Fiber Transceiver Modules

Ports 25. 26 on the LGB1005A 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 (ports 25, 26). 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 auto 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 2-3 and 2-4.

- 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)

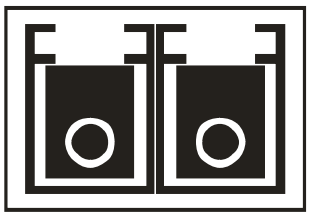


Figure 2-3. LGB200C-MLC, LGB200C-SLC10, or LGB200C-SLC30 module.

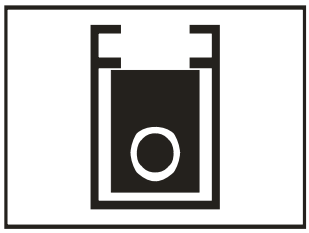


Figure 2-4. LGB204C or LGB205C module.

NOTE

The LGB204C and LGB205C fiber transceivers must be used together.

3. Installation

3.1 Installation Instructions

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.

INSTALLING THE OPTIONAL MODULES

NOTE

If you do not plan to install SFP fiber transceivers in the switch's ports 25, 26, skip this section.

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

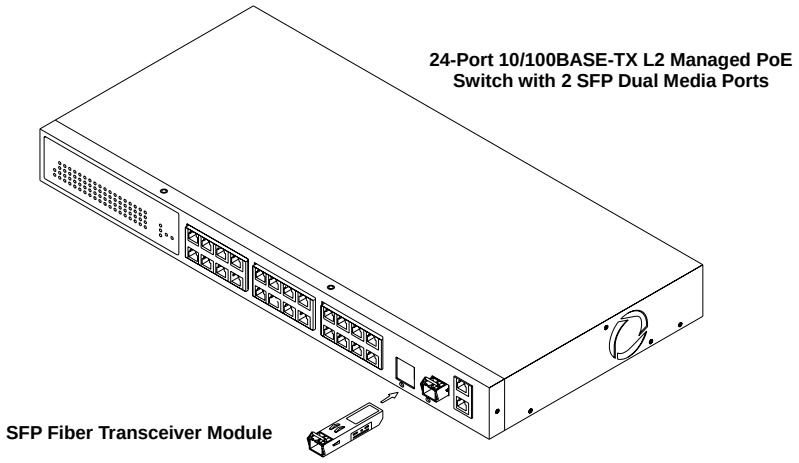


Figure 3-1. Installing the optional SFP fiber transceiver module.

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 LC connector(s) on the module.
4. If you want to install a second module in the switch, repeat steps 1–3.

Installing the Rubber Feet

For this switch, install the rubber feet and place it on a desktop, or install the switch in the rack with mounting hardware (see Section3.2).

TP Port and Cable Installation

1. The switch's twisted-pair (TP) ports support MDI/MDI-X auto-crossover, so either type of cable (straight-through or crossover) can be used for each TP port.
2. Use Category 5 grade RJ-45 TP cable to connect to a switch TP port at one end and a Gigabit device (for example, a workstation or server) at the other end.
3. Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

The switch is now ready to operate.

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. It does not matter whether any network device (such as a workstation or server) or fiber transceiver module is plugged into the switch or not when powered on. After the power is on, all LED indicators will light up immediately and then all LEDs except the power LED go off. This resets the system.

Firmware Loading

After resetting, the boot loader will load the firmware into the memory. This will take about 30 seconds, then all switch LEDs will flash once as the switch automatically performs a self-test.

3.2 Installing the Chassis in a 19-Inch Wiring Closet Rail

CAUTION

Allow proper spacing and air ventilation for the cooling fan on both sides of the chassis.

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.

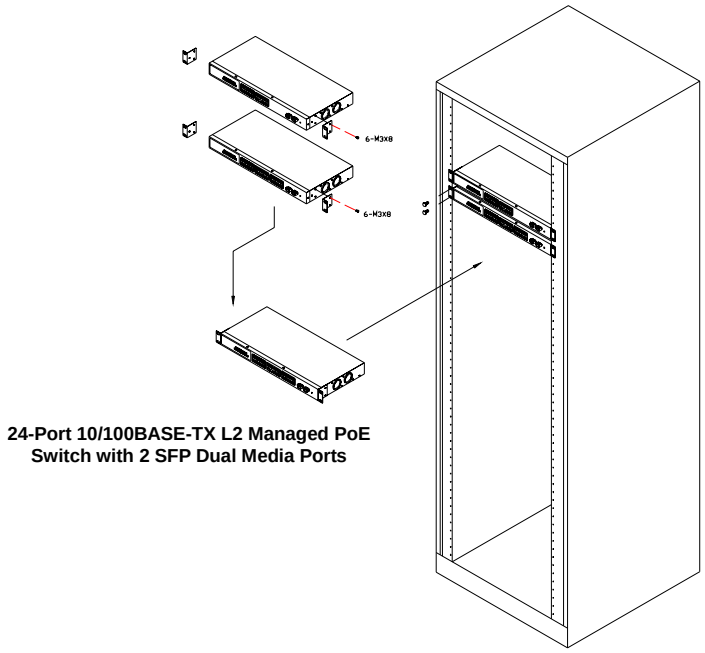


Figure 3-2. Installing the switch chassis in a 19"rack.

3.3 Cabling Requirements

3.3.1 Twisted-Pair Ports

For Fast Ethernet or Gigabit Ethernet twisted-pair (TP) connections, use CAT5 or CAT5e cable up to 328 feet (100 m) long.

3.3.2 Fiber Transceiver Ports

For Gigabit Ethernet fiber transceiver ports, use fiber optic cable as described below.

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

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

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

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

3.3.3 Switch Cascading

Theoretically, the switch partitions the collision domain for each port in switch cascading so that you may up-link 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 timer 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 as described in Table 3-1.

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

1000BASE-X TP, Fiber	100BASE-TX TP	100BASE-FX Fiber
Round-Trip Delay: 4096	***Round-Trip Delay: 512***	
Cat. 5 TP Wire: 11.12/m Fiber Cable: 10.10/m Bit Time Unit: 1 ns (1 sec./1000 Mega bit)	Cat. 5 TP Wire: 1.12/m Fiber Cable: 1.0/m TP to Fiber Converter: 56 kbps Bit Time Unit: 0.01 ms (1 sec./100 Mega bit)	

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

Typical Network Topology in Deployment

A hierarchical network with minimum switch levels may reduce the timing delay between the server and the client station. This approach will minimize the number of switches in any one path. It will also lower the network loop possibility and will improve network efficiency. If more than two switches are connected in the same network, select one switch as the Level 1 switch and connect all other switches to it at Level 2. We recommend that you connect a server/host to the Level 1 switch.

Example 1: Same LAN.

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

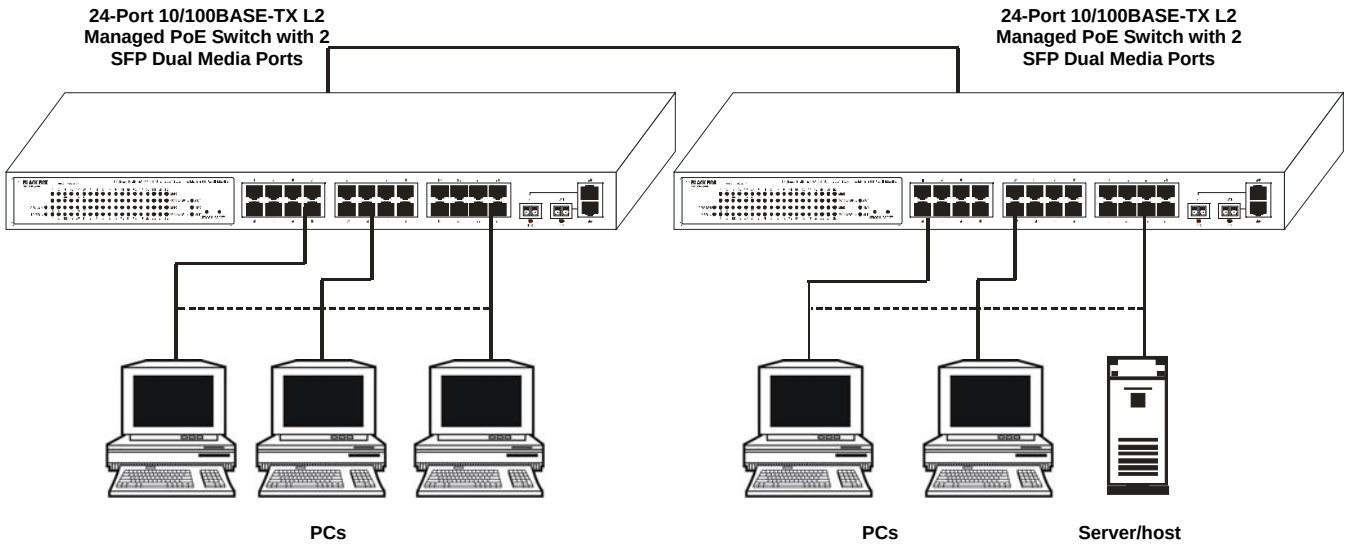


Figure 3-3. No VLAN configuration.

Example 2: Port-based VLAN

If VLAN is enabled and configured, each node in the network that can communicate with each other directly is in the same VLAN.

The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. Figures 3-4 and 3-5 show a port-based VLAN and Figure 3-6 shows an attribute-based VLAN.

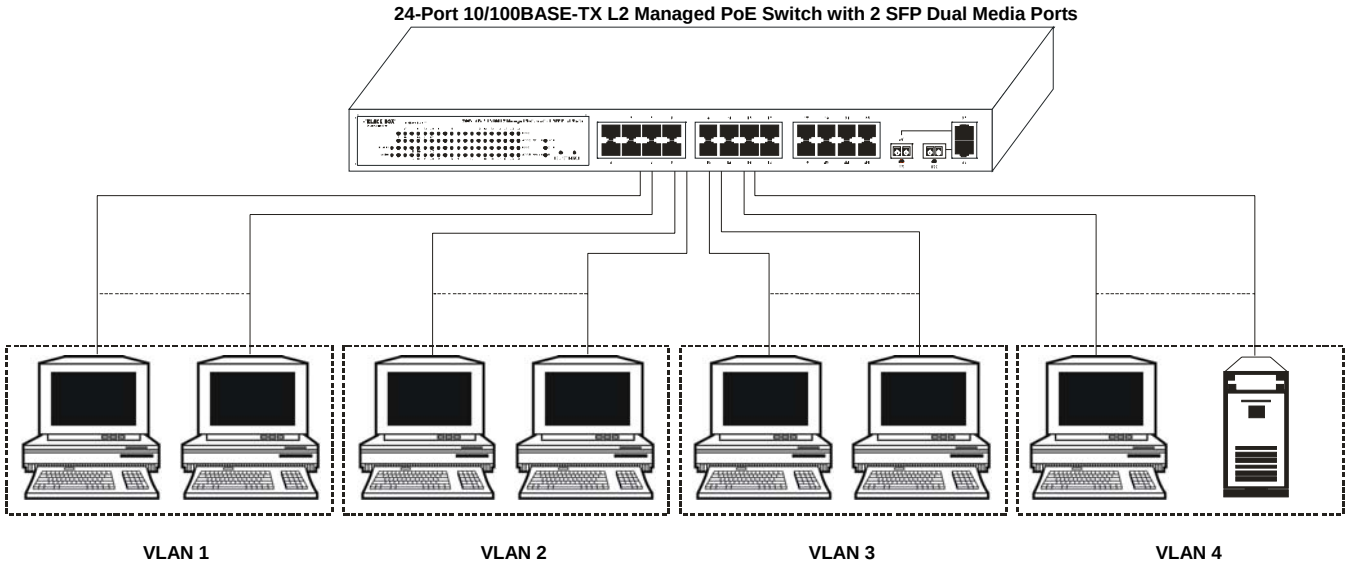


Figure 3-4. One switch connected to four VLANs in a port-based VLAN.

NOTES

The same VLAN members must be connected to the same switch.

VLAN members can't access another VLAN's members.

The switch manager must assign different names for each VLAN group at one switch.

Example 3: Another Port-Based VLAN

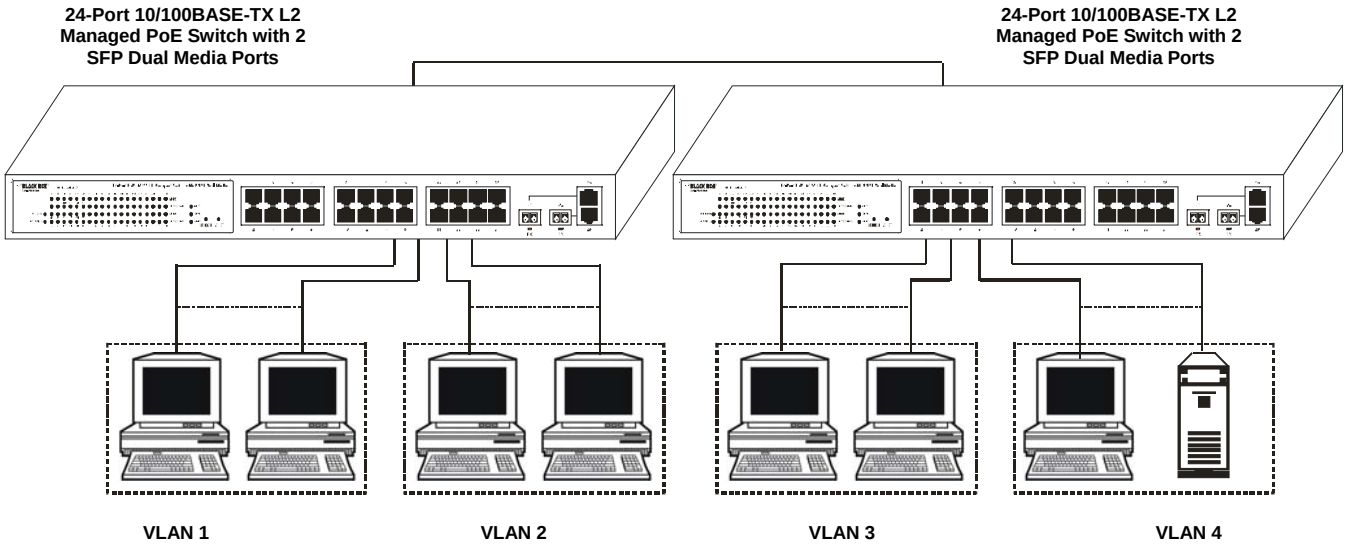


Figure 3-5. Two switches connected to two VLANs, each in a port-based VLAN.

NOTES

VLAN 1 members can't access VLAN 2, VLAN 3, and VLAN 4 members.

VLAN 2 members can't access VLAN 1 and VLAN 3 members, but they can access VLAN 4 members.

VLAN 3 members can't access VLAN 1, VLAN 2, and VLAN 4.

VLAN 4 members can't access VLAN 1 and VLAN 3 members, but they can access VLAN 2 members.

Example 4. The same VLAN members can be at different switches with the same VID

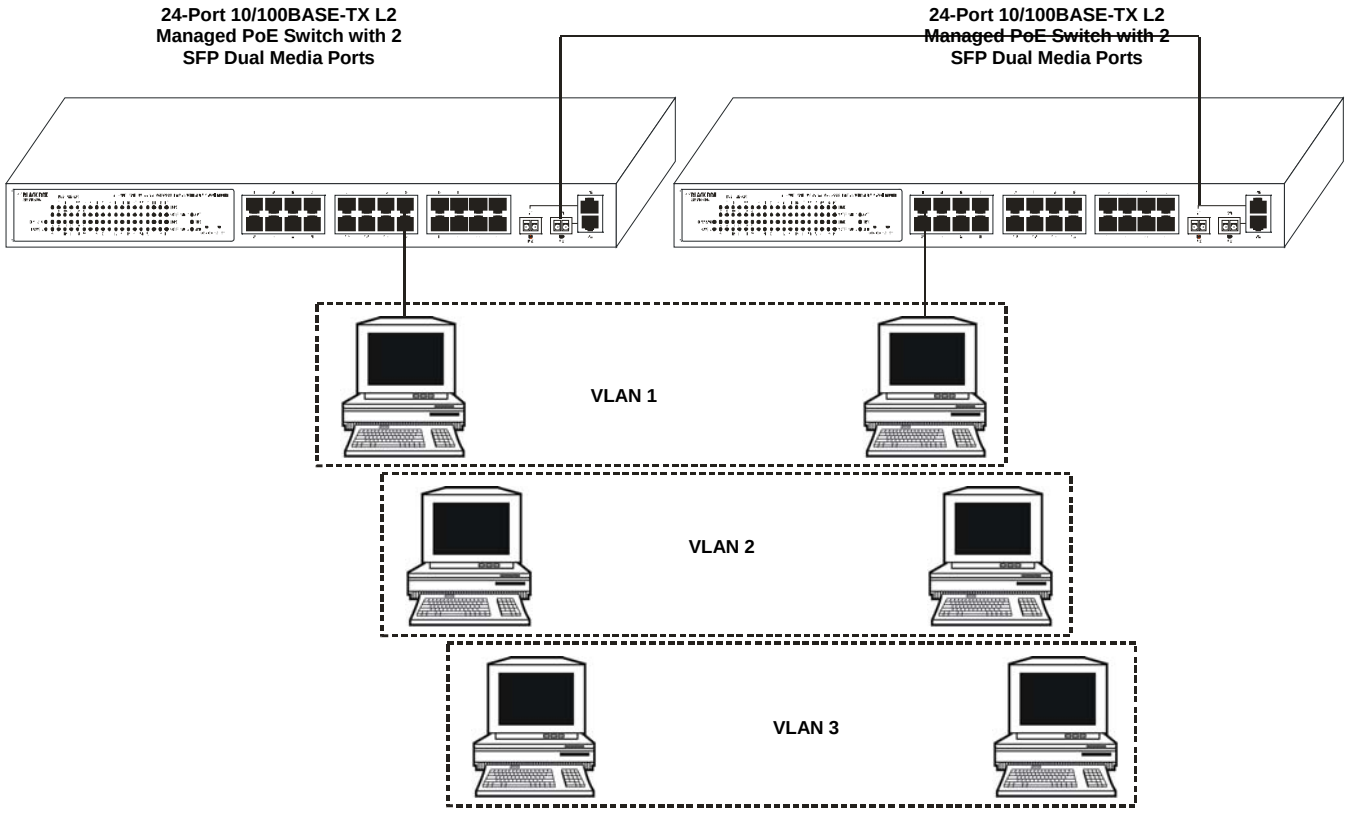


Figure 3-6. Attribute-based VLAN diagram.

3.4 Configuring the Management Agent

There are two ways to start up the switch management function: RS-232 console and Ethernet port. Use one to monitor and configure the switch. Follow the instructions in **Sections 3.4.1** and **3.4.2.**

NOTE

Modify the IP address, subnet mask, default gateway, and DNS through the RS-232 console.

3.4.1 Via The Serial RS-232 Console Port

To configure the switch through its serial RS-232 console port, the port must be directly connected to a DCE device (for example, a PC, through an RS-232 cable with a DB9 connector). See Figure 3-7.

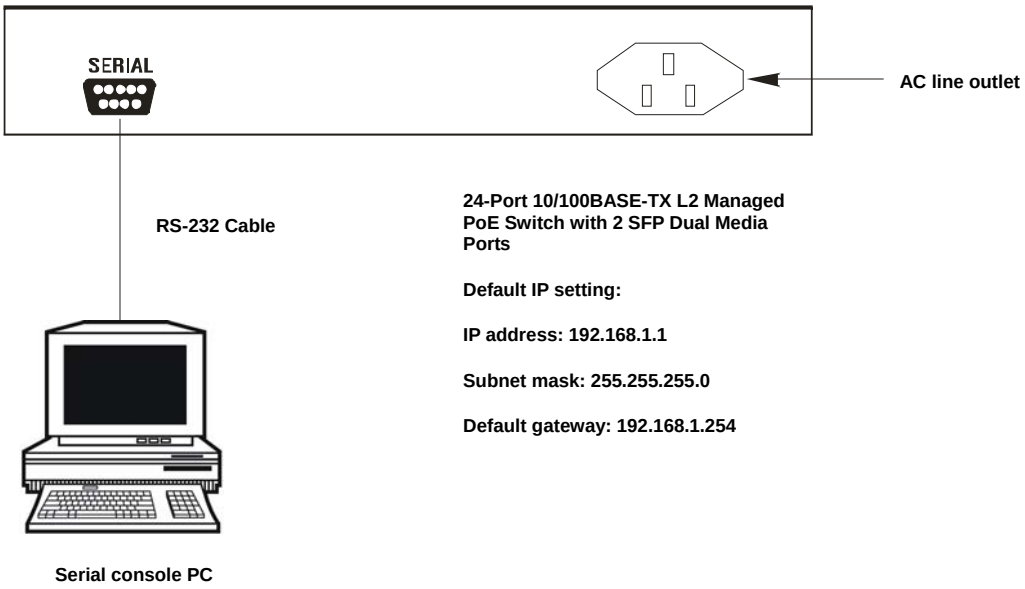


Figure 3-7. Connecting the switch's RS-232 DB9 port to a serial console.

Next, run a terminal emulator with the switch's serial port's default setting. Using this, you can communicate with the switch.

The RS-232 interface only supports a 57.6-kbps baud rate with 8 data bits, 1 stop bit, no parity check, and no flow control.

To configure the switch:

1. Attach the included DB9 female cable's connector to the switch's male serial RS-232 DB9 connector.
2. 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, use the Windows® 98/2000/XP HyperTerminal utility.

NOTE

The switch's serial port default settings are listed below:

Baud rate:	**57600**
Stop bits:	**1**
Data bits:	**8**
Parity:	**N**
Flow control:	**None**

3. Once the cable is connected, press the Enter key. The login prompt appears on the screen. The default username and password are:

Username = admin
Password = admin

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

The switch's default IP address, gateway, and subnet mask are listed in Table 3-2.

Table 3-2. The switch's default and revised network settings.

Parameter	Default Value	Sample 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

NOTE

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

You can first either configure your PC's IP address or change the switch's IP address, then change the default gateway's IP address and subnet mask.

For example, suppose your network address is 10.1.1.0, and the 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 255.255.255.0. Then, choose the default gateway's address (for example 10.1.1.254).

After completing these settings, reboot it so the configuration takes effect. After this step, operate the management through the network, either from a Web browser or Network Management System (NMS). See Figure 3-8.

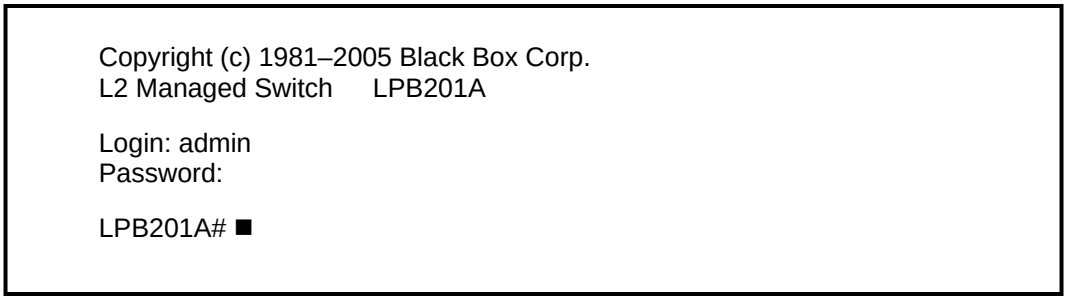


Figure 3-8. The CLI login screen for the LPB201A.

3.4.2 Via The Ethernet Port

There are three ways to configure and monitor the switch through the switch's Ethernet port: CLI, Web browser, and SNMP management. The user interface for SNMP is NMS dependent and is not described here. CLI and Web browser interfaces are described below.

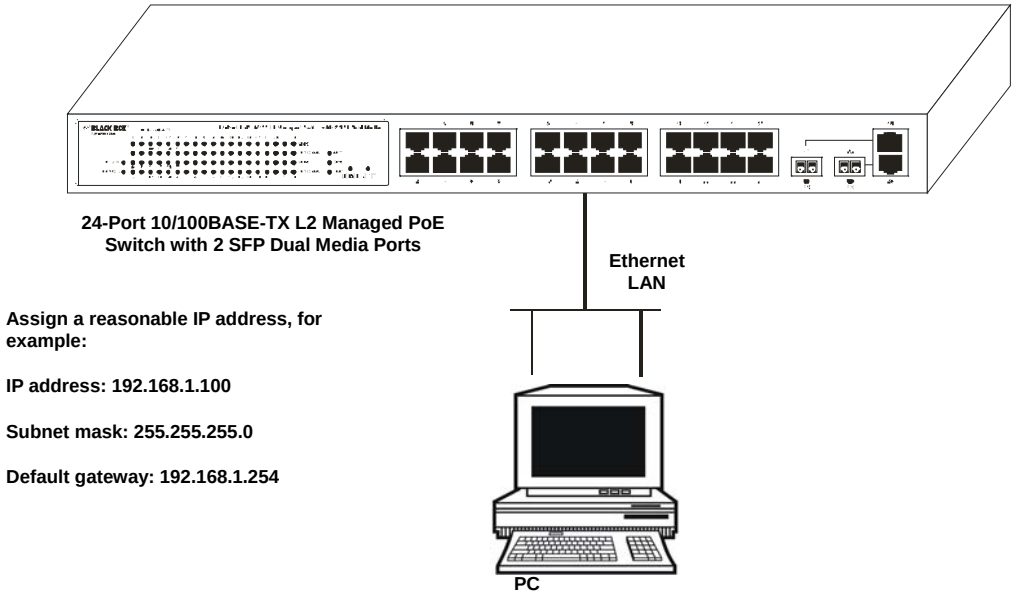


Figure 3-9. Connecting the Ethernet LAN PC to the switch for network management through an Ethernet port.

Managing the Switch via the Ethernet Port

Before you communicate with the switch, you must first configure or identify the switch's IP address. Next, follow the steps listed below.

1. Connect the switch and PC together via UTP CAT5 cable with RJ-45 connectors.

NOTE

If the PC directly connects to the switch, set up the same subnet mask between them.

If the PC connects to the switch through a remote site, the remote PC's subnet mask may be different.

2. Run CLI or a Web browser and follow the menus. For details, refer to **Chapters 4** and **5**.

3. A login screen appears. Type in the switch's username and password in this screen.

3.5 IP Address Assignment

For IP address configuration, you will need the switch's IP address, subnet mask, default gateway, and DNS.

3.5.1 IP Address

The network device's address is used for internetworking communication. The 32-bit address consists of a network identifier and a host identifier. It's 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 has two parts: network identifier (address) and host identifier (address). The network address is the network where the addressed host resides, and the host identifier indicates the individual host in the network that the host address refers to. The host identifier must be unique in the same LAN.

The IP address is divided into three classes: class A, class B, and class C. The rest of the IP addresses are used for multicast and broadcast. The network prefix's bit length is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. The address range for each class is described below.

Class A

The address is less than 126.255.255.255. A total of 126 networks can be defined. (The address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loop back 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 of65534 (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 to 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 24bits, 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 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 3-3. 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 table above, a subnet mask 255.255.255.0 will partition a network with the class C. This means that a maximum of 254 effective nodes exist in this subnetted network and it's considered a physical network in an autonomous network. A sample network IP address is 168.1.2.0.

With the subnet mask, for more than two independent networks in a worknet, the network can be partitioned into smaller networks. A subnet mask must be applied.

For different network applications, a sample subnet mask is 255.255.255.240. This is for a small network with 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 put into the device with the designated IP address, known as the default router. Only the switch uses the gateway setting for Trap Events Host.

When assigning an IP address to the switch, first check to see what an existing switch on the same network uses as a network address. Use the same network address and append your host address to it.

Once you type in the username and password in the login screen, the IP Configuration screen appears. Options in this screen include DHCP Setting, IP Address, Subnet Mask, Default Gateway, DNS Server, and the Apply button.

Type in the IP address in the format 192.168.1.xon your PC.

For the subnet mask, enter 255.255.255.0. Any subnet mask such as 255.255.255.x is allowed.

3.5.4 DNS

The Domain Name Server translates a human-readable machine name to an IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the server's IP. However, a user generally uses the name to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to find the named server's IP address.

3.6 Typical Applications

The LGB201A implements 24 Fast Ethernet TP ports with auto MDIX and 2 Gigabit dual media ports with SFP for removable module supported comprehensive fiber types of connection, including LC, BiDi LC for SFP.

Use the switch for the following applications.

- FTTB (Fiber To The Building)/FTTO (Fiber To The Office) application is used in carrier or ISP (see Figure 3-10).
- FTTH (Fiber To The Home) application is used in carrier or ISP (see Figure 3-11).
- Daisy-Chain Fiber Network Connection (see Figure 3-12).

3.6.1 FTTB/FTTO Connection

Figure 3-10 shows a FTTB/FTTO application is used in carrier or ISP.

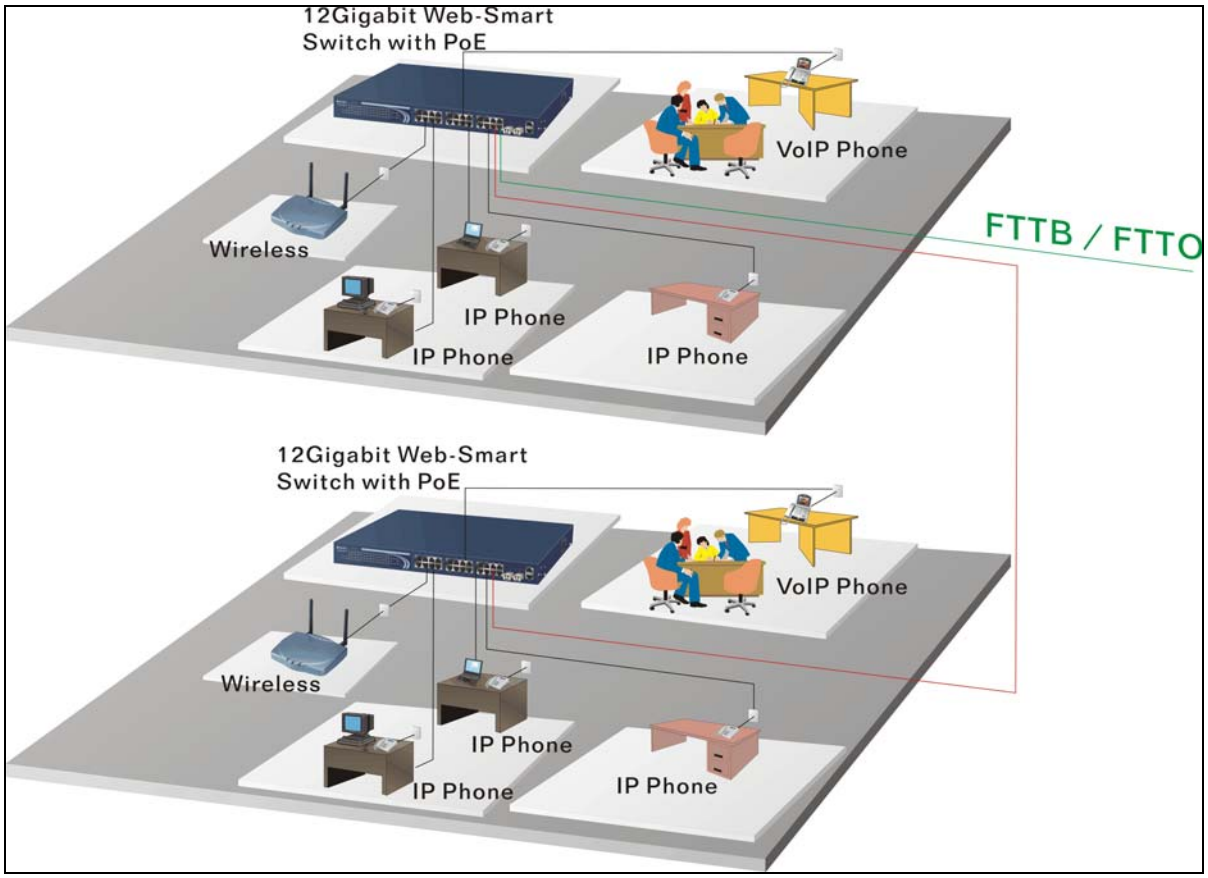


Figure 3-10. Network Connection of FTTB/FTTO.

3.6.2 FTTH Connection

Figure 3-11 shows a FTTH application is used in carrier or ISP.

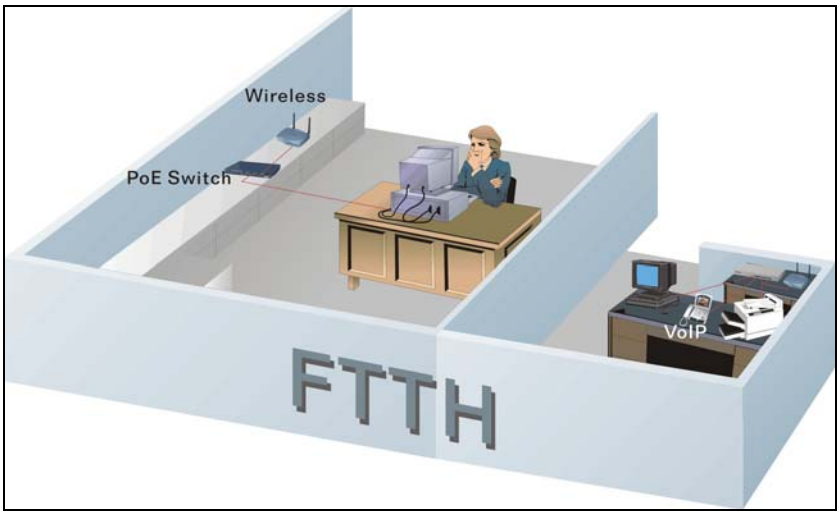


Figure 3-11. Network Connection of FTTH.

3.6.3 Daisy-Chain Fiber Network Connection

Figure 3-12 shows the Daisy-Chain Fiber Network Connection.

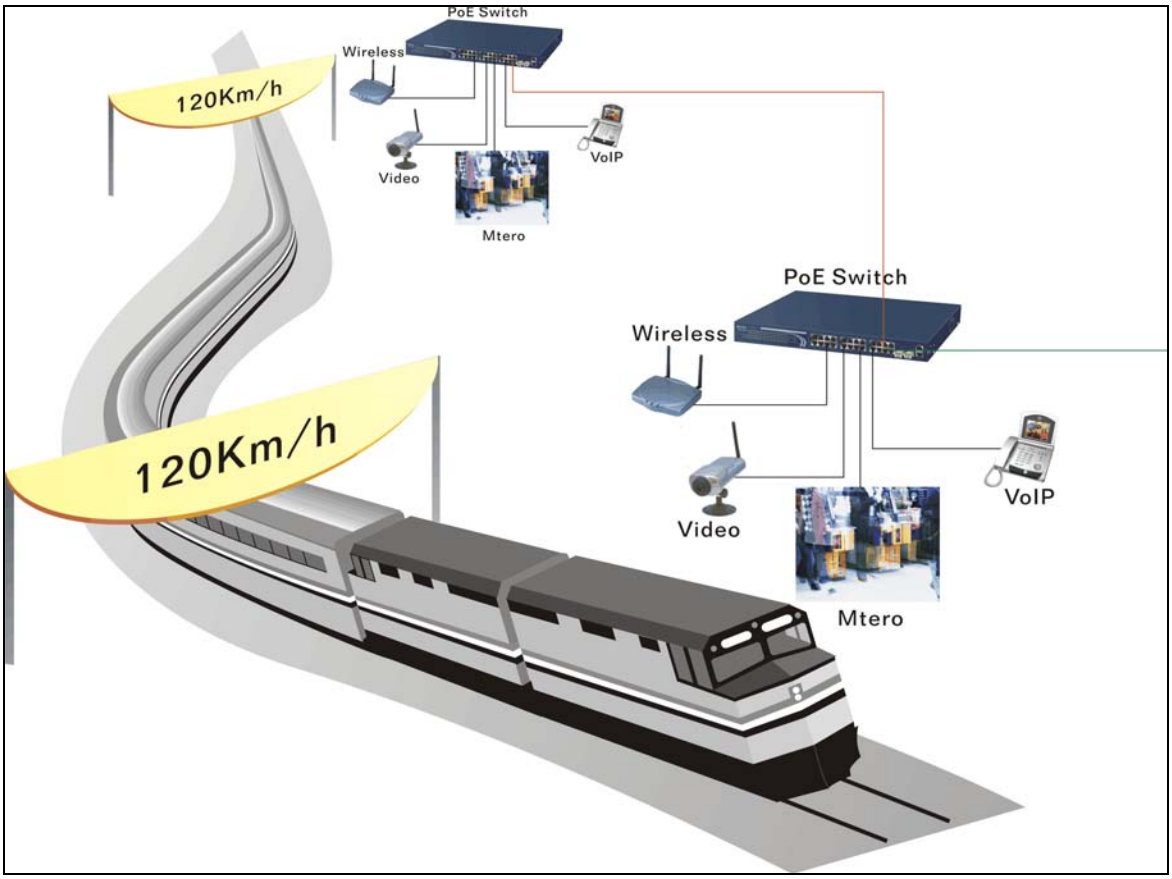


Figure 3-12. Typical office network using three switches.

4. Web-Based Management

This chapter explains how to configure and manage the switch through the Web user interface. Via one switch port, you can easily access and monitor the switch's status, including MIBs, port activity, spanning tree, port aggregation, multicast traffic, VLAN and priority, and even a record of illegal access to the network.

The switch's default values are listed in Table 4-1.

Table 4-1. Default settings.

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

NOTE

Before accessing the managed switch via a network port, you must first configure the switch in its command-line interface (CLI) from the connected a sync serial COM/RS-232 interface. For details, see Chapter 5.

Once you configure the switch, type in the IP address (for example, http://192.168.1.1) in the address row in a browser. The login screen appears. Table 4-2 lists the screen options.

Table 4-2. Login screen parameters.

Parameter	Setting
Username	admin
Password	admin
Login	Click on this button to log in.
Cancel	Click on this button to cancel the log in.
Forget Password	Click on this button to choose a new password.

Type in the username and password. (The default username and password are both admin.) The first time you log in, type in the default username and password, then click on the **Login** button.

If you forget the password, click the link of **Forget Password** in Web UI or press the **Ctrl** button, then type Z in the CLI login screen. The system then displays a serial number. Write down this serial number and contact Black Box—we'll give you a temporary password. Type in this new password as ID and Password, and the system will allow you to temporarily log into the system with manager authority. This password allows you to login to the system only one time, so modify your password immediately after you log into the system successfully.

To modify your password, type in the complete new username and password. The switch will not give you a shortcut to the username automatically. This looks inconvenient, but it provides additional system security.

The switch supports a simple user management function, allowing only one administrator to configure the system at a time. If two or more users use the administrator's identity, the switch will allow only the one who logs in first to configure the system. Other users, even with an 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 log in simultaneously.

To optimize the display effect, we recommend using Microsoft® Internet Explorer® version 6.0 or above, Netscape® V7.1 or above, or FireFox V1.00 or above with a resolution of 1024 x 768. The switch supports a neutral Web browser interface.

4.1 Home Overview

Once you log into the switch, the Home screen appears.

At the top of the screen, the switch's front-panel diagram appears. The linked ports display green, and the unlinked ports appear dark. The slot shows only a coverplate if no module exists, and it shows a module if a module is present. The module image depends on the one that's installed in the switch. If disconnected, the port will appear dark; if linked, it will be green.

Simply click on the ports in the switch diagram to browse the information for a specific port. An information window appears, containing Link, State, Auto Negotiation, Speed/Duplex, Flow Control, Ingress All State, Ingress All Rate, Ingress Storm State, Egress All State, Egress All Rate, Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision, RX Error Packet, and the **Close** button.

In the left top corner of the screen, a pull-down list appears for Auto Logout. This is a security function meant to prevent illegal users from accessing the switch. If you select ON, the system will log out automatically when there is no action on the device for three minutes. If you select OFF, the screen will remain visible to the user. The default setting is ON.

On the left side of the screen, the main menu tree for the Web is listed. Options (in a vertical list on the left side of the screen) include System, Port, Mirror, Bandwidth, QoS, SNMP, IGNP Snooping, Max. Packet Length, DHCP Boot, VLAN, MAC Table, GVRP, STP, Trunk, 802.1x, Alarm, Configuration, Diagnostics, TFTP Server, Log, Firmware Upgrade, Reboot, and Logout. These options are described in **Sections 4.2** through **4.24**.

4.2 System

4.2.1 System Information

Click on **System** in the Home screen, and the System Information screen appears. This screen's settings are described in Table 4-3.

Table 4-3. System Information screen settings.

Parameter	Description
Model Name	LPB201A
System Description	24-Port 10/100BaseT/TX Managed PoE Switch.
Location	The user-defined switch location.
Contact	This is the contact name and phone number for help. Configure this parameter via the switch's user interface or SNMP.
Device Name	The user-defined switch's name. LPB201A is the default.
System Up Time	Time in days, hours, and minutes accumulated since the switch was powered on. Its format is day of week, month, day, hours: minutes: seconds, year. For example, Wed., Apr. 26, 12:10:10, 2006.
Current Time	The switch's system time. Its format is day of week, month, day, hours: minutes: seconds, year. For example, Wed., Apr. 26, 12:10:10, 2006.
BIOS Version	The switch's BIOS version.
Firmware Version	The switch's firmware version.
Hardware-Mechanical Version	The electrical and mechanical switch version. The figure before the hyphen is the electronic hardware version; the one after the hyphen is the mechanical hardware version.
Serial Number	The switch's serial number; assigned by the manufacturer.
Host IP Address	The switch's IP address.
Host MAC Address	The switch's management agent's Ethernet MAC address.
Device Port	Displays all types and numbers of switch ports.
RAM Size	The switch's DRAM size.
Flash Size	The switch's Flash memory size.
Apply button	Click on this button to apply the selections.

4.2.2 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 for the setting to take effect and to use the new IP to browse for Web management and CLI management. To get to the IP Configuration screen, click on **IP** in the System menu. Then, set the switch's IP address, subnet mask, default gateway, and DNS. Table 4-4 describes the IP Configuration screen parameters.

Table 4-4. IP Configuration screen options.

Parameter	Description
DHCP Setting	Dynamic Host Configuration Protocol (DHCP) can be ON or OFF. Select Enable or Disable from the drop-down menu. 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 as requesting, until the DHCP server is up. Before getting an IP address from the DHCP server, the device will not continue booting procedures. If this field is set to Disable, you must type in the IP address manually. For more details about IP address and DHCP, see **Section3.5**. The default setting is Disable.
IP address	If DHCP is set to Disable, you can type in new IP settings. Then click on the **Apply** button. When DHCP is disabled, the default setting is 192.168.1.1. If DHCP is enabled, this field is filled by the DHCP server and will not allow you to manually type it in.
Subnet mask	An IP device in a network must own its IP address, composed of a Network address and a Host address; otherwise, it can't communicate with other devices. Subnet mask is designed to provide more network addresses. The network classes A, B, and C are all too large to fit for almost all networks; subnet mask solves this problem. The subnet mask uses some bits from the host address and makes an IP address look like a network address, subnet mask number, and host address. This reduces the total IP number that a network can support, by the amount of 2 power of the bit number of subnet number ($2^{[\text{bit number of subnet number}]}$).

Table 4-4 (continued). IP Configuration screen options.

Parameter	Description
Subnet mask (continued)	Subnet mask sets the subnet mask value, which should be the same value as that of the other devices residing in the same network that the switch is attached to. For more information, see **Section 3.5**. 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 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 the 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. 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 DNSIP address. Fixed mode manually specifies its IP address, and dynamic mode is assigned by the DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with meaningful words. The default is no DNS address assignment. Default: 0.0.0.0
Apply button	Click on this button to save the changes.

4.2.3 Time Configuration

In the System menu, click on **Time Configuration** (see Table 4-5).The switch provides manual and automatic ways to set the system time via NTP*. The manual setting is simple—just type in the year, month, day, hour, minute, and second within the valid value range indicated in each item. If you type in an invalid value (for example, 61 in minutes), the switch changes the figure to 59.

*NTP is a well-known protocol used to synchronize the switch system time clock over a network. NTP, an Internet draft standard formalized in RFC 1305, has been adopted on the system as version 3 protocol. The switch provides four built-in NTP server IP addresses residing in the Internet and a user-defined NTP server IP address. The time zone is Greenwich-centered (Greenwich Mean Time or GMT), using the form GMT+/- xx hours.

Table 4-5. Time Configuration screen options.

Parameter	Description
Time	Type in the system time or set it by syncing from Time servers. The function also supports daylight savings time for different areas' time adjustment.
Current Time	Shows the current system time.
Manual	Adjust the time manually. Type in the valid figures in the Year, Month, Day, Hour, Minute, and Second fields respectively, then click on the **Apply** button to adjust the time. The valid figures for the parameter Year, Month, Day, Hour, Minute, and Second are >=2000, 1–12, 1–31, 0–23, 0–59, and 0–59 respectively. If you type in 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	NTP is Network Time Protocol and is used to sync the network-time-based 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 as well as Time Zone, the switch will sync the time after you press the **Apply** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user processing. Time Zone is an offset time of GMT. From the drop-down menu, select the time zone first and then perform time sync via NTP. The switch will combine this time zone offset and update NTP time to the local time; otherwise, you will not be able to get the correct time. The switch supports a configurable time zone from -12 to +13 in 1-hour steps. Default time zone: +8 Hrs.
Daylight Saving	If set for daylight savings time, the switch will adjust the time lag or advance in units of hours, according to the starting date and the ending date. From the drop-down menu, set the daylight savings time to 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

Table 4-5 (continued). Time Configuration screen options.

Parameter	Description
Daylight saving (continued)	The switch supports valid configurable daylight savings time of -5 to+5 step one hour. The zero for this parameter means it does not have to adjust current time; it's equivalent to activating daylight saving. In this case, you don't have to set the starting/ending date. If you set daylight saving to be non-zero, you have to set the starting/ending dates; otherwise, the daylight saving function will not be activated. Default for Daylight Saving: 0
Daylight Saving Start	This defines when to start performing the daylight saving time. Mth: Range is 1–12. Default: 1 Day: Range is 1–31. Default: 1 Hour: Range is 0–23. Default: 0
Daylight Saving End	Set this to stop performing the daylight saving time. Mth: Range is 1–12. Default: 1 Day: Range is 1–31. Default: 1 Hour: Range is 0–23. Default: 0
Apply button	Click on this button to apply the settings.

4.2.4 Account Configuration

To get to the Account Configuration screen, click on **Account** in the System menu. Only the user logged in as administrator can create, modify, or delete the username and password. The administrator can modify other guest identities' passwords without confirming the password but must also modify the administrator-equivalent identity. A guest-equivalent identity can modify his own password only. You must confirm administrator/guest identity in the Authorization field in advance before configuring the username and password. Only one administrator is allowed to exist and can't be deleted. Up to four guest user accounts can be created.

Table 4-6. Account configuration screen settings.

Parameter	Description
Account Name	Type in the name.
Authorization	Select administrator or guest user from the drop-down menu.
Create New	Click on this button to create a new guest user account.
Edit	Click on this button to edit a guest user account.
Delete	Click on this button to delete a guest user account.

The default setting for administrator user account is:

Username: `admin`
Password: `admin`

The default setting for guest user account is:

Username: `guest`
Password: `guest`

4.2.5 Management Policy

Limiting User Access to the Switch

Through the management security configuration, the administrator can control the switch and limit the user's access to this switch. To get to this screen, click on **Management Policy** in the System menu.

The following rules apply:

1. When no lists exist, then the switch will accept all connections.
2. When only "accept lists" exist, then the switch will deny all connections, excluding the connection inside the accepting range.
3. When only "deny lists" exist, then the switch will accept all connections, excluding the connection inside the denying range.
4. When both "accept and deny" lists exist, then the switch will deny all connections, excluding the connection inside the accepting range.
5. When both "accept and deny" lists exist, then the switch will deny all connections, excluding the connection inside the accepting range and NOT inside of the denying range at the same time.

Management Security Configuration

With the Management Security Configuration function (see Table 4-7), the manager can easily control the user's mode when connecting 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).Some restrictions also can be placed on the user mode while connecting to the switch. For example, a VLANVID can be accepted or denied by the switch, the user's IP range can be accepted or denied by the switch, the port that the user is allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch can vary (via HTTP, Telnet, or SNMP).

Table 4-7. Management Security Configuration settings.

Parameter	Description
Name	A name is composed of any letter (A–Z, a–z) and digit (0–9) with a maximum of 8 characters.
VID	VID supports two buttons for managed valid VLAN VID: Any and Custom. The default is the **Any** button. When you click on the **Custom** button, you can type in the VID number. The valid VID range is 1–4094.
IP Range	The switch supports two options for the managed valid IP Range: Any and Custom. The default is the **Any** button. When you click on the **Custom** button, you can type in an effective IP range. The valid range is 0.0.0.0–255.255.255.255.
Incoming Port	The switch supports options for managed valid Port Range: Any and Custom. The default is the **Any** button. When you click on the **Custom** button, you can check the box(es) next to the ports that you would like to be restricted in the management security configuration.
Access Type	The switch supports two options for managed valid Access Type: Any and Custom. The default is the **Any** button. When you click on the **Custom** button, you can check the box next to the option you want to use to access and manage the switch. The three options include HTTP, Telnet, and SNMP.
Action	The switch supports two options for managed valid Action Type: Deny and Accept. The default is the **Deny** button. When you choose Deny, you can't manage the switch. If you click on the **Accept** button, you can manage the switch.
Edit/Create	Click on this button to create a new management security entry, or to modify an existing entry.
Delete	Click on this button to remove the selected management security configuration entry from the management security table.

4.2.6 Virtual Stack

Virtual Stack Management (VSM) is the group management function. To get to this option, click on **Virtual Stack** in the System menu. Through the proper configuration of this function, switches in the same LAN will be grouped automatically. Among these switches, one switch will be a master machine, and the others in this group will become the slave devices.

VSM offers a simple centralized management function. You don't have to remember all devices' addresses, since the administrator can manage the network with knowing only the Master machine's address. Instead of

an SNMP or Telnet user interface, VSM is only available in a Web user interface (UI). While one switch is the Master, two rows of buttons for a group device will appear on the top of its Web UI. Press the buttons to connect the group devices' Web UI in the same window without logging in to the corresponding devices.

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

NOTE

If you log into the switch via the console, the grouping will be removed temporarily.

The group device is shown as station address (the last number of IP Address) + device name on the button (for example, 196_LGB1001A); otherwise it will display "—"if no corresponding device exists.

Once the devices join the group successfully, then they can only be managed via the Master device, and a user won't be able to manage them individually via Telnet/console/Web.

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

Table 4-8. Virtual Stack screen options.

Parameter	Description
State	Activates or de-activates VSM. Select Enable or Disable from the drop-down menu. The default is Enable.
Role	The role that the switch plays in the virtual stack. Select Master or Slave from the drop-down menu. The default is Master.
Group ID	Type in the group identifier (GID) to indicate a VSM. Valid letters are A–Z, a–z, 0–9, "-" and "_" characters. The maximum length is 15 characters.
Apply button	Click on this button to apply the settings.

4.3 Port Configuration

To get to the Port Configuration menu, click on Port in the Home screen. This menu contains Status, Configuration, Simple Counter, and Detail Counter for port monitoring and management. They are described in Sections **4.3.1** through **4.3.4**.

4.3.1 Status

The function Port Status gathers the information of all ports' current status and reports it by port number, link status, port state, auto-negotiation status, speed/duplex, and flow control. To get to the Port Status screen, click on Port Status in the Port menu (see Table 4-9). Media type information for the module ports 25—26 is listed in Table 4-10.

Table 4-9. Port Configuration menu options.

Parameter	Description
Port Status	Report the latest updated status of all switch ports. When any one of the ports in the switch changes its parameter displayed in the page, the port status will automatically refresh about every 5 seconds.
Port No.	Display the port number. The number is 1–26. Ports 25, 26 are optional modules.
Media	Show the media type adopted in all ports. The Port 25 and Port 26 are optional modules, which support either fiber or UTP media with either Gigabit Ethernet (1000Mbps) or 10/100Mbps Fast Ethernet port. They may have different media types and speed. Especially, fiber port has comprehensive types of connector, distance, fiber mode and so on. The switch describes the module ports with the following page.
Link	Shows if the link on the port is active or not. If the link is connected to a device that is working properly, the Link will show the link Up; otherwise, it will show Down. Both connected devices determine the link value. No default value.
State	Shows that the port's communication function is Enabled or Disabled. When it's enabled, traffic can be transmitted and received via this port. When it's disabled, no traffic can be transferred through this port. The Port State is configured by the user. Default: Enabled.
Auto Negotiation	Shows the Ethernet MAC's exchange mode. The switch supports two modes: auto-negotiation mode Enabled and forced mode Disabled. When in Enabled mode, this switch automatically negotiates the best speed and duplex values at both ends of the connection. When in Disabled mode, both parties must have the same speed and duplex settings; otherwise, they won't be linked. In this case, the link result is Down. Default: Enabled

Table 4-9 (continued). Port Configuration menu options.

Parameter	Description
Speed/Duplex Mode	Displays all ports' speed and duplex settings. Three speeds (10 Mbps, 100 Mbps, and 1000 Mbps) are supported for TP media, and half-duplex and full duplex are supported. If the media is 1-Gbps fiber, 1000-Mbps is supported. The speed/duplex mode status 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 has to preset its capability. In port 1 – 24, they are supported Fast Ethernet with TP media only, so the result will show 100M/Full or 100M/Half, 10M/Full and 10M/Half duplex. In port 25 and port 26, if the media is 1000Mbps with TP media, it will show the combinations of 10/100M and Full/Half duplex, 1000Mbps and Full duplex only. If the media is 1000Mbps with fiber media, it will show only 1000M/Full duplex. Default: None, depends on the negotiation result.
Rx Pause	The way that the port adopts to process the PAUSE frame. If it shows **on**, the port will care the PAUSE frame; otherwise, the port will ignore the PAUSE frame. Default: None
Tx Pause	It decides that whether the port transmits the PAUSE frame or not. If it shows **on**, the port will send PAUSE frame; otherwise, the port will not send the PAUSE frame. Default: None

Table 4-10. Ports 25–26.

Parameter	Description
Connector Type	Displays the connector type—for example, UTP, SC, ST®, or LC.
Fiber Type	Displays the fiber mode—for example, multimode or single-mode.
Tx Central Wavelength	Displays the fiber optic transmitting central wavelength—for example, 850-nm, 1310-nm, or 1550-nm.
Baud Rate	Displays the fiber module's maximum supported baud rate—for example, 10M, 100M, or 1G.

Table 4-10 (continued). Ports 25–26.

Parameter	Description
Vendor OUI	Displays the Manufacturer's OUI code that's assigned by IEEE.
Vendor Name	Displays the module manufacturer's company name.
Vendor P/N	Displays the manufacturer's switch's part number.
Vendor Rev (Revision)	Displays the module revision.
Vendor SN (Serial Number)	Shows the manufacturer-assigned serial number.
Date Code	Shows the date this SFP module was made.
Temperature	Shows the SFP module's current temperature.
Vcc	Shows the SFP module's working DC voltage.
Mon1 (Bias) mA	Shows the SFP module's bias current.
Mon2 (TX PWR)	Shows the SFP module's transmit power.
Mon3 (RX PWR)	Shows the SFP module's receiver power.
Close button	Click on this button to close the window.

4.3.2 Configuration

Use the Configuration menu to change each port's setting. To get to this screen, click on Config in the Port menu. In this menu, you can set/reset the following functions. All are described in detail in Table 4-11.

Table 4-11. Configuration screen options.

Parameter	Description
State	From the drop-down menu, set the port's communication capability to Enabled or Disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. If you set a port's state to Disable, then that port is prohibited from passing any traffic. Default: Enable.

Table 4-11 (continued). Configuration screen options.

Parameter	Description
Speed/Duplex	Set the speed and duplex of the port. In speed, 10/100Mbps baud rate is available for Fast Ethernet, Gigabit module in port 25, 26. If the media is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports. Media Type NWay Speed Duplex 100M TP ON/OFF 10/100M Full/Half 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	There are two modes to choose in flow control, including Symmetric and Asymmetric. If flow control is set Symmetric, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Asymmetric, this will let the receiving port care the PAUSE frame from transmitting device(s), but it doesn't send PAUSE frame. This is one-way flow control. Default: Symmetric
Apply	Click on this button to save the settings.

4.3.3 Simple Counter

Simple Counter collects any information and provides the port traffic counting, whether the packet is good or bad. To get to this screen, click on Simple Counter in the Port Configuration screen.

The Simple Counter window can show all ports' counter information at the same time. To get to this screen, click on Simple Counter in the Port menu. Each data field is 20 digits long. If the count is more than 20 (overflow), the counter will reset and restart counting. The data is updated every time a user defines an interval. The valid range is 3 to 10 seconds. The Refresh Interval sets the update frequency. The default update time is 3 seconds.

Table 4-12. Simple Counter screen options.

Parameter	Description
Simple Counter	Displays each port's traffic summary counting, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision, and Rx Error Packet.
Refresh Interval	Select a number (in seconds) from the drop-down menu.
Reset button	Click on this button to reset the simple counter.
Port No.	The port number.
Tx Byte	Total transmitted bytes.
Rx Byte	Total received bytes.
Tx Packet	Total transmitted packets.
Rx Packet	Total received packets.
Tx Collision	Total collisions experienced while transmitting frames.
Rx Error Packet	Total bad packets received.

4.3.4 Detail Counter

The Detail Counter collects any information and provides the port traffic counting, whether the packet is good or bad. To get to this screen, click on Detail Counter in the Port Configuration screen.

The Detail Counter window can show only one port counter information at the same time. To get to this screen, click on **Detail Counter** in the Port menu. To see another port's counter, select it from the drop-down menu.

Each data field is 20 digits long. If the counting is longer than 20 digits (overflows), the counter will be reset and restart counting. The data is updated every user-defined time interval. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. The default update time is 3 seconds.

Table 4-13. Detail Counter screen options.

Parameter	Description
Detail Counter	Displays the detailed counting number of each port's traffic. The Detail Counter window can show all counter information of each port at onetime. To get to this screen, click on Detail Counter in the Port menu.
Select	Choose the port number from the drop-down menu.
Refresh Interval	Select the interval from the drop-down menu. The valid range is 3 to 10 seconds, and the default is 3 seconds.
Reset button	Click on this button to reset the choices.
Rx Packets	Total packets received.
Rx Octets	Total received bytes.
Rx Error	Number of bad packets received.
Rx Unicast Packets	Show the counting number of the received unicast packet.
Rx Broadcast Packets	Show the counting number of the received broadcast packets.
Rx Multicast Packets	Show the counting number of the received multicast packets.
Rx Pause Packets	Show the counting number of the received pause packets.
Tx Collisions	Number of collisions transmitting frames experienced.
TX Single Collision	Number of frames transmitted that experienced exactly one collision.
Tx Multiple Collision	Number of frames transmitted that experienced more than one collision.
Tx Drop Packets	Number of frames dropped due to excessive collision, late collision, or frame aging.
Tx Deferred Transmit	Number of frames delayed to transmission due to the medium is busy.
Tx Late Collision	Number of times that a collision is detected later than 512 bit-times into the transmission of a frame.
Tx Excessive Collision	Number of frames that are not transmitted because the frame experienced 16 transmission attempts.

Table 4-13 (continued). Detail Counter screen options.

Parameter	Description
Packets 64 Octets	Number of 64-byte frames in good and bad packets received.
Packets 65-127 Octets	Number of 65–127-byte frames in good and bad packets received.
Packets 128-255 Octets	Number of 128–255-byte frames in good and bad packets received.
Packets 256-511 Octets	Number of 256–511-byte frames in good and bad packets received.
Packets 512-1023 Octets	Number of 512–1023-byte frames in good and bad packets received.
Packets 1024- 1522 Octets	Number of 1024-max_length-byte frames in good and bad packets received.
Tx Packets	The counting number of the packet transmitted.
TX Octets	Total transmitted bytes.
Tx Unicast Packets	Show the counting number of the transmitted unicast packets.
Tx Broadcast Packets	Show the counting number of the transmitted broadcast packets.
Tx Multicast Packets	Show the counting number of the transmitted multicast packets.
Tx Pause Packets	Show the counting number of the transmitted pause packets.
Rx FCS Errors	Number of bad FSC packets received.
Rx Alignment Errors	Number of Alignment errors packets received.
Rx Fragments	Number of short frames (< 64 bytes) with invalid CRC
Rx Jabbers	Number of long frames(according tomax_length register) with invalid CRC.
Rx Drop Packets	Frames dropped due to the lack of receiving buffer
Rx Undersize Packets	Number of short frames (<64 Bytes) with valid CRC
Rx Oversize Packets	Number of long frames(according to max_length register) with valid CRC.

4.4 PoE

4.4.1 POE STATUS

Table 4-14 shows all the parameters of the PoE status.

Table 4-14 PoE screen options.

Parameter	Description
PoE Status	Display the information about the PoE status.
Vmain	The volt is supplied by the PoE.
Imain	The sum of the current that every port supplies.
Pconsume	The sum of the power that every port supplies
Power Limit	The maximal power that the switch can supply (Read Only).
Temperature	The temperature of the chip on PoE
Port No	Port number.
Port On	Show whether the port is supplying the power to the PD or not
AC Disconnect Port Off	Port is turned off due to the AC Disconnect function.
DC Disconnect Port Off	Port is turned off due to the DC Disconnect function.
Overload Port Off	The switch will stop supplying the power to the port due to the power required by the PD that is linked to the port on the switch excesses the Class setting of the PD
Short Circuit Port Off	The switch will stop supplying the power to the port if it detects that the PD linked to the port is short circuit.
Over Temp. Protection	The port of the switch will be disabled due to fast transient rise in temperature to 240^{o}C or slow rise in temperature to 200^{o}C.
Power Management Port Off	Due to total power required by all PDs linked to the switch excesses the power limit, so the switch stops supplying the power to this port after referring to the information of the priority.

4.4.2 POE Configuration

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

Table 4-15. PoE Configuration screen settings

Parameter	Description
Status	Include **Normal** or **Active** two kinds of status. The former means the port is ready to link and supply the power to the PD at any time. The latter means the port is in the condition of supplying the power.
State	**Enable** means the manager allows the power supplied to the PD is legal while the port linked to the PD; **Disable** means the port does not own PoE function.
Priority	Three options are offered for the user to choose, including 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 excesses the power limit. As the ports have the same priority, then the switch will cease the power supplement from the port with the highest port id (12→1).
Power (W)	The power is consumed by the port
Current (mA)	The current is supplied to the PD by the port
Class	The Class of the PD linked to the port of the switch

4.5 SNMP Configuration

Any Network Management System (NMS) running the 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 and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP **Enable**, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set **Disable**, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Table 4-16. SNMP Configuration screen settings.

Parameter	Description
SNMP Configuration	This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name.
SNMP	The term SNMP here is used for the activation or de-activation of SNMP. 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. Hence, the requesting network management unit can not access the device with 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. There is not allowed to put any blank in the community name string. Any printable character is allowable. The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can't be applied to other function 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 :16

Table 4-16 (continued). SNMP Configuration screen options.

Trap	In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address; 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. In other words, 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 the important trap message from losing. 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 corresponded trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. As to the Enterprise (no. 6) trap is classified as private trap, which are listed in the Trap Alarm Configuration function folder. Default for all public traps: Enable.
Apply button	Click on this button to apply the settings.

4.6 DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a bigger time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and many connections predefined when the whole building or block lose the power and then reboot and recover. At this moment, a bunch of switch or other network device on the LAN will try its best to find the server to get the services or try to set up the predefined links, they will issue many broadcast packets in the network.

Table 4-17. DHCP Boot screen options.

Parameter	Description
DHCP Broadcasting Suppression	If DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds, because the exactly delay time is computed by the switch itself. The default is **Disable**.
Delay Time	The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are at booting stage in the same time. The maximum user-defined delay time is 30 sec.
Apply button	Click on this button to apply the settings.

4.7 IGMP Snooping

The function, IGMP Snooping, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, 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 can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

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

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

4.7.1 Status

Table 4-18 shows the IGMP Snooping status screen options.

Table 4-18. Status screen options.

Parameter	Description
IGMP Snooping Status	IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member port.
Snooping mode	The switch supports three kinds of IGMP Snooping status, including Passive, Active and Disable. Disable: Set “Disable” mode to disable IGMP Snooping function. Active: In Active mode, IGMP snooping switch will periodically issue the Membership Query message to all hosts attached to it and gather the Membership report message to update the database of the Multicast table. By the way, this also reduces the unnecessary multicast traffic. Passive: In Passive Snooping mode, the IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router. Default: Disable

Table 4-18 (continued). Status screen options.

IP Address	Show all multicast groups IP addresses that are registered on this device.
VLAN ID	Show VLAN ID for each multicast group
Member Port	Show member ports that join each multicast group. Member port may be only or more than one.

4.7.2 Allowed Group

Table 4-19. Allowed Group screen options.

Parameter	Description
Allowed Group	The Allowed Group function allows the IGMP Snooping to set up the IP multicast table based on user's specific conditions. IGMP report packets that meet the items you set up will be joined or formed the multicast group.
IP Range	The switch supports two kinds of options for managed valid IP range, including **Any** and **Custom**. Default is **Any**. In case that **Custom** had been chosen, you can assigned effective IP range. The valid range is 224.0.0.0~239.255.255.255.
VID	The switch supports two kinds of options for managed valid VLAN VID, including **Any** and **Custom**. Default is **Any**. When you choose **Custom**, you can fill in VID number. The valid VID range is 1~4094.
Port	The switch supports two kinds of options for managed valid port range, including **Any** and **Custom**. Default is **Any**. You can select the ports that you would like them to be worked and restricted in the allowed group configuration if **Custom** had been chosen.
Add	A new entry of allowed group configuration can be created after the parameters as mentioned above had been setup and then press **Add** button.
Edit	The existed entry also can be modified after pressing **Edit** button
Delete	Remove the existed entry of allowed group configuration from the allowed group.

4.8 VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Support 256 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

4.8.1 VLAN MODE

To get to this screen, click on **VLAN Mode** in the VLAN menu. The VLAN Mode Selection function includes five modes: Port-based, Tag- based, Metro Mode, Double-tag, and Disable. Choose one from the drop-down menu. Then, click on the **Apply** button for the settings to take effect immediately.

Table 4-20. VLAN Mode screen settings.

Parameter	Description
VLAN Mode	When you select Disable from the drop-down menu, this stops the switch's VLAN function. In this mode, no VLAN is applied to the switch. This is the default setting. Port-based: Port-based VLAN is defined by port. When you select Port-based from the drop-down menu, 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 namedPVLAN-1 contains port members 1–4. If you are on port 1, you can communicate with ports 2–4. If you are on the port 5, then you can't talk to them. Each port-based VLAN you build must be assigned a group name. This switch can support up to eight port-based VLAN groups. Tag-based: Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. When you select Tag-based from the drop-down menu, if there are any more rules in the Ingress filtering list or Egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports a supplement of 802.1q. Each tag-based VLAN you build must be assigned a VLAN name and VLAN ID. Valid VLAN IDs are 1–4094. User can create a total of up to 64 Tag VLAN groups.

Table 4-20 (continued). VLAN Mode screen options.

Parameter	Description
Symmetric Vlan	This is a Ingress Rule (Rule 1, The Ingress Filtering Rule 1 is "forward only packets with VID matching this port's configured VID".). For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Symmetric-Vlan function is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped. **Note** If Symmetric is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped
SVL	While SVL is enable, all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. While SVL is disable, it means learning mode is IVL. In this mode, different VLAN uses different filtering database storing the membership information of the VLAN to learn or look up the information of a VLAN member.
Double Tag	Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.
SNMP Configuration	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 target device's MIB information. Both parties must have the same community name. After choosing the setting, click on the **Apply** button and the setting will take effect.

4.8.2 Tag-Based Group

It shows the information of existed Tag-based VLAN Groups. You can also easily create, edit and delete a Tag-based VLAN group by pressing **Add**, **Edit** and **Delete** function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID after pressing **Add** button.

Table 4-21. Tag-based Group screen options.

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 maximal length is 15 characters.
VID	VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.
Member	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. Just tick the check box beside the port x to enable it.

Add Group

To create a new tag-based LAN, type in the VLAN name and the VID, configure the SYM-VLAN function, and choose the member by checking the box beside the port number (1–8, 1–16, or 1–24). Click on the **Apply** button for the setting to take effect. Table 4-22 describes the Tag-based VLAN Add Group screen options.

Table 4-22. Add Group screen options.

Parameter	Description
VLAN Name	The administrator-defined VLAN name is associated with a VLAN group. Valid letters are A–Z, a–z, 0–9, "-" and "_" characters. The maximum length is 15 characters.
VID	VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and double-tag mode.
Member	When set to Enable, a port is a VLAN member. Check the box beside the port x to enable it.
Untag	Check the box beside the port x to enable it.

Delete Group

To remove the selected group entry from the Tag-based group table, click on the **Delete** button in the Tag-based Group screen.

Edit a group

Just select a group entry and press the **Edit** button, then you can modify a group's description, member and untag settings.

4.8.3 PVID

In PVID Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rule (Rule 2) to each port. The Ingress Filtering Rule 2 is **drop untagged frame**. While Rule 2 is enabled, the port will discard all Untagged-frames.

Table 4-23. PVID screen options.

Parameter	Description
Port No.	Shows the number of each port.
PVID	This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.
Default Priority	It bases on 802.1p QoS and affects untagged packets. When the packets enter the switch, it would get the priority precedence according to your Default Priority setting and map to 802.1p priority setting in QoS function. For example, while you set Default Priority of port 2 with 2 and transmit untagged packets to port 2, these packets will own priority 2 precedence due to your default 802.1p Priority Mapping setting in QoS function and be put into Queue 1.
Drop Untag	Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then the packets with tagged or untagged will be processed. If the later is the case, only the packets carrying VLAN tag will be processed, the rest packets will be discarded.

4.8.4 PORT-BASED GROUP

It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing **Add**, **Edit** and **Delete** function buttons. User can add a new VLAN group by inputting a new VLAN name.

Table 4-24. Port-based Group screen options.

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 maximal length is 15 characters.
Member	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. Just tick the check box beside the port x to enable it.

Add Group

Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the **Apply** button to have the setting taken effect.

Delete Group

Just press the **Delete** button to remove the selected group entry from the Port-based group table.

Edit a group

Just select a group entry and press the **Edit** button, then you can modify a group's description and member set.

4.9 MAC Table

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

4.9.1 MAC Table Information

To get to this screen, click on **MAC Table Information** in the MAC Table menu. MAC Table Information displays the static or dynamic learning MAC entry and the state for the selected port.

Table 4-25. MAC Table Information screen options.

Parameter	Description
Port	Check box 1–24 or Select/Unselect All to select the port you want to inquire about.
Search	Set up the MAC entry you want to inquire about. The default is blank (no numbers).
MAC	Display the MAC address of one entry you selected from the searched MAC entries table.

Table 4-25 (Continued). MAC Table Information screen options.

Alias	Type in the Alias for the selected MAC entry.
Set Alias	Click on this button to save the alias of the MAC entry you set up.
Search button	Click on this button to find the entry that meets your setup.
Previous Page button	Click on this button to move to the previous page.
Next Page	Click on this button to move to the next page.
Alias	The searched entry's alias.
MAC Address	The searched entry's MAC address.
Port	The port that exists in the searched MAC entry.
VID	The searched MAC entry's VLAN group.
State	Displays the method for building this MAC entry—Dynamic MAC or Static MAC.

4.9.2 MAC Table Maintenance

This function can allow the user to set up the processing mechanism of MAC Table. 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 learning limit of MAC maintenance is able to limit the amount of MAC that each port can learn.

Table 4-26. MAC Table Maintenance screen options.

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.
Learning Limit	To set up the maximum amount of MAC that each port can learn. Valid value of learning limit for port 1~24 ranges from 0-8191. As to port 25~port 26, only the fixed value "8192" is assigned to these two ports and user cannot configure this value.
Apply button	Click on this button to apply the settings.

4.9.3 STATIC

The function of Static is used to configure MAC's real manners inside of the switch. Three kinds of manners including static, static with destination drop and static with source drop are contained in this function.

As **static** is chosen, assign a MAC address to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

As **static with destination drop** is chosen, the packet will be dropped if its DA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.

As **static with source drop** is chosen, the packet will be dropped if its SA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.

Table 4-27. Static screen settings.

Parameter	Description
MAC	It 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
VID	VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.
Queue (Priority)	Set up the priority (0~3) for the MAC.
Forwarding Rule(Drop Policy)	Static: A MAC address is assigned to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port. Static with Destination Drop: While the DA of the incoming packets meets the value you set up, these packets will be dropped. Static with Source Drop: While the SA of the incoming packets meets the value you set up, these packets will be dropped.
Port	Select the port No. you would like to do setup in the switch. It is 1 ~26.

4.9.4 MAC ALIAS

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 existed 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. You can click **Create/Edit** button to add/modify a new or an existed alias name for a specified MAC address, or mark an existed entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.

Table 4-28. MAC Alias screen options.

Parameter	Description
MAC Alias Create/Edit or Delete	In the MAC Alias function, MAC Alias Add/Edit function is used to let you add or modify an association between MAC address and a plain English name. User can click **Create/Edit** button to add a new record with name. As to MAC Alias Delete function is used to let you remove an alias name to a MAC address. You can select an existed MAC address or alias name to remove.
MAC Address	It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 - 02
Alias	MAC alias name you assign. **Note** If there are too many MAC addresses learned in the table, we recommend you inputting the MAC address and alias name directly.

Delete Group

To remove the selected group entry from the Tag-based group table, click on the **Delete** button in the Tag-based Group screen.

4.10 GVRP Configuration

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 offers the function providing the VLAN registration service through a GARP application. It makes use of 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 machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these 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, including GVRP Config, GVRP Counter and GVRP Group explained below.

4.10.1 GVRP Config

Table 4-29. GVRP Configuration screen options.

Parameter	Description
GVRP Config	In the function of GVRP Config, it is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.
GVRP State Setting	This function is simply to let you enable or disable GVRP function. You can pull down the list and click the **Downward** arrow key to choose **Enable** or **Disable**. Then, click the **Apply** button, 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 for announcement that all registered device is 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 mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user's choice. Normal: It is Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal. Non-Participant: It is Non-Participant. In this mode, the switch does not send or reply any GARP messages. It just listens messages and reacts for the received GVRP BPDU.

Table 4-29 (continued). GVRP Configuration screen options.

Parameter	Description
Default Registrar Mode	The mode here means the type of Registrar. There are three types of parameters for registrar administrative control value, normal registrar, fixed registrar and forbidden registrar, provided for the user's choice. Normal: It is Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal. Fixed: It is Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state. Forbidden: It is Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.
Restricted Mode	This function is used to restrict dynamic VLAN be created when this port received GVRP PDU. There are two modes, disable and enable, provided for the user's choice. Disabled: In this mode, the switch 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 dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch, this port will be added into the static VLAN members dynamically.

4.10.2 GVRP Counter

All GVRP counters are mainly divided into Received and Transmitted two categories to let you monitor the GVRP actions. Actually, they are GARP packets.

Table 4-30. GVRP Counter screen options.

Parameter	Description
Total GVRP Packets	Total GVRP BPDU is received/ transmitted by the GVRP application.
Invalid GVRP Packets	Number of invalid GARP BPDU is received/ transmitted by the GARP application.
LeaveAll Message Packets	Number of GARP BPDU with Leave All message is received/ transmitted by the GARP application.
JoinEmpty Message Packets	Number of GARP BPDU with Join Empty message is received/ transmitted by the GARP application.
JoinIn Message Packets	Number of GARP BPDU with Join In message is received/ transmitted by the GARP application.
LeaveEmpty Message Packets	Number of GARP BPDU with Leave Empty message is received/ transmitted by the GARP application.
Empty Message Packets	Number of GARP BPDU with Empty message is received/ transmitted by the GARP application.

4.10.3 GVRP Group Information

Table 4-31. GVRP Group Information screen options.

Parameter	Description
Current Dynamic Group Number	The number of GVRP group that are created currently.
VID	VLAN identifier. When GVRP group creates, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.
Member Port	Those are the members belonging to the same dynamic VLAN group.
Edit Administrative Control	When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.
Refresh	Refresh function can help you to see current GVRP group status.

4.11 STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on 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.

4.11.1 STP Status

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

Table 4-32. STP Status screen options.

Parameter	Description
STP State	Show the current STP Enabled / Disabled status. Default is Disabled.
Bridge ID	Show switch's bridge ID which stands for the MAC address of this switch.
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 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 root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-learn and determine which the root bridge is. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.

Table 4-32 (Continued). STP Status screen options.

Parameter	Description
Current Forward Delay	Show 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 port in bridge.
Hello Time	Show 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 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 be reset to 0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.
Time Since Last Topology Change	Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.

4.11.2 STP Configuration

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

Table 4-33. STP Configuration screen options.

Parameter	Description
STP Configuration	User 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.
Spanning Tree Protocol	Set 802.1W Rapid STP function Enable / Disable. 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 PSES-2126Cas 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.

Table 4-33 (Continued). STP Configuration screen options.

Parameter	Description
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 PSES-2126Cis 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 unit of second. Default is 2 seconds.
Max. Age	When the PSES-2126Cis the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received 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 malfunctioned 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. Default is 20 seconds.
Forward Delay	You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors. The valid value is 4 ~ 30 seconds, 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 STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

4.11.3 STP Port Configuration

In the STP Port Setting, one item selection and five parameters settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set **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.

Table 4- 34. STP Port setting screen options.

Parameter	Description
Port Status	It 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 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 cannot forward packets still. ▪ FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.
Path Cost Status	It is the contribution 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 become the Root Port more possibly.
Configured Path Cost	The range is 0 – 200,000,000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status. 802.1w RSTP 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. Default is 128.

Table 4-34 (continued). STP Port setting screen options.

Parameter	Description
Admin Edge Port	If 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 transit to 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 keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU. Default: No.
Admin Point To Point	We say a port is a point-to-point link, from RSTP’s view, if it is in full-duplex mode but is 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 have the port fast transited to forwarding state. There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configure this parameter to be Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today’s switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited 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 **M Check** button to send a RSTP BPDU from the port you specified.

4.12 Trunking Configuration

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means 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 three times as high as a single Fast Ethernet port has.

The switch supports two kinds of port trunking methods:

LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~3) to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready 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 followings:

- Link Aggregation across switches

- Aggregation with non-IEEE 802.3 MAC link

- Operating in half-duplex mode

- Aggregate the ports with different data rates

Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~3, this Static groupID can be the same with another LACP groupID) to form a logic trunked port. The benefit of using 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 be aggregate together to form a logic trunked port. Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

As to system restrictions about the port aggregation function on the switch, in the management point of view, the switch supports maximum 3 trunk groups for LACP and additional 3 trunk groups for Static Trunk. But in the system capability view, only 3 real trunked groups are supported. An LACP trunk group with more than one ready member-ports is 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. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Trunk Setting Rules are listed below.

Rule1: Maximum 3 groups are allowed

Rule 2: The members of each group cannot exceed more than 4 ports

Rule 3: Group 1 and 2 can not exist member 25 and 26 port

Rule 4: Group 3 cannot exist member from 1 to 24 ports

4.12.1 Port Setting/ Status

Port setting/status is used to configure the trunk property of each and every port in the switch system.

Table 4-35. Port Setting/ Status screen options.

Parameter	Description
Method	This determines the method a port uses to aggregate with other ports. None: A port does not want to aggregate with any other port should choose this default setting. LACP: A port use LACP as its trunk method to get aggregated with other ports also using LACP. Static: A port use Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.
Group	Ports choosing the same trunking method other than **None** must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 8) in order to declare that they wish 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 which uses a trunking method other than **None**. It also represents the management link status of a port which uses the "None" trunking method. --- means not ready.

4.12.2 Aggregator View

To display the current port trunking information from the aggregator point of view.

Table 4-36. Aggregator View screen options.

Parameter	Description
Aggregator	It shows the aggregator ID (from 1 to 26) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No.
Method	Show 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).

This page shows the detailed information of the LACP trunking group.

Table 4-37. LACP Detail screen options.

Parameter	Description
Actor	The switch you are watching on.
Partner	The peer system from this aggregator's view.
System Priority	Show the System Priority part of a system ID.
MAC Address	Show the MAC Address part of a system ID.
Port	Show the port number part of an LACP port ID.
Key	Show the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through management.
Trunk Status	Show the trunk status of a single member port. --- means not ready.

4.12.3 LACP System Config

It is used to set 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 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.

Table 4-38. LACP System Configuration screen options.

Parameter	Description
System Priority	The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768.
Hash Method	DA+SA, DA and SA are three Hash methods offered for the Link Aggregation of the switch. Packets will decide the path to transmit according to the mode of Hash you choose. Default: DA and SA

4.13 802.1x Configuration

802.1x port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1x-enabled port without authentication. If a user wishes to touch the network through a port under 802.1x control, he (she) must firstly input his (her) account name for authentication and waits for gaining 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 pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in Fig. 4-1.

Supplicant:

It is 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 request to 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 authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, 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 MAC bridge, at any time.

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.

The overview of operation flow for the Fig. 4-1 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges 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 to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

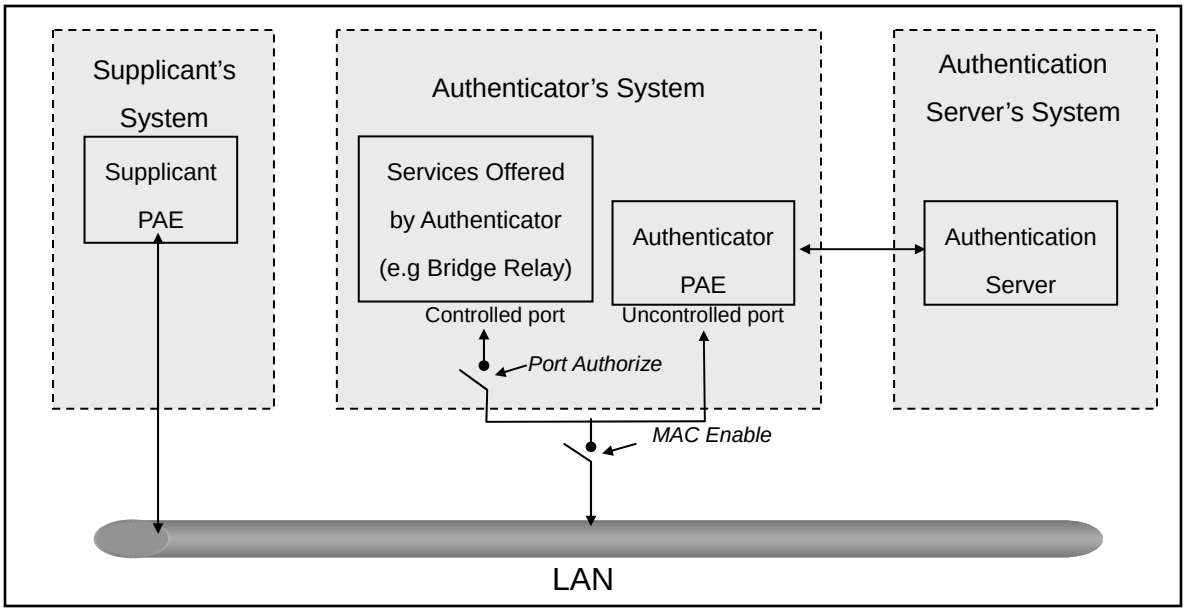


Figure 4-1.

In the Fig. 4-2, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and 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, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is 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 to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

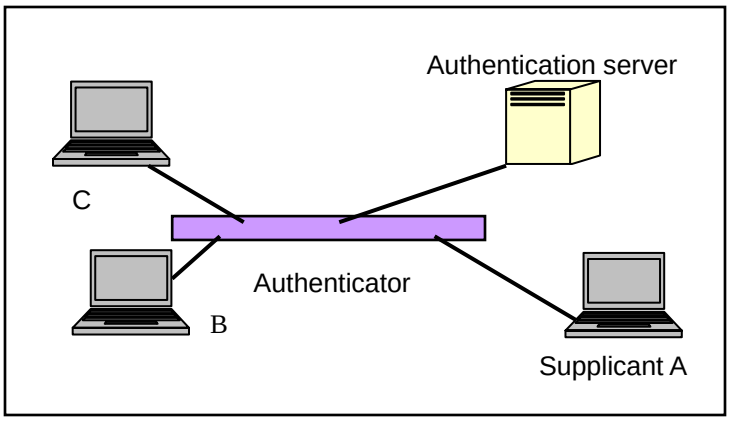


Figure 4-2.

The Fig. 4-3 shows the procedure of 802.1x authentication. There are steps for the login based on 802.1x port access control management. The protocol used in 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. So the access is blocked in this stage.

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

3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.

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

5. And next, the Supplicant replies 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 for confirming its identity.

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

7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, 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 other else algorithm.

8. If user ID and password is 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. At this time, the supplicant is 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 is failed to authenticate. The port it connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.

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

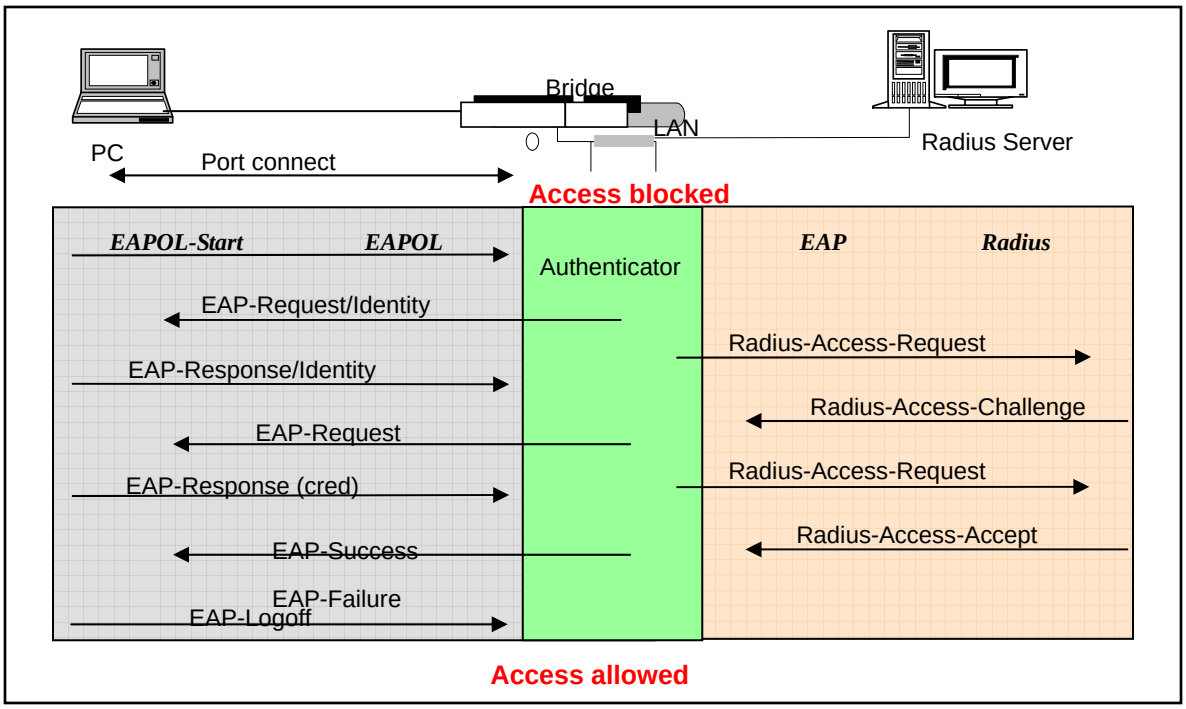


Figure 4-3.

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

802.1x Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic Multihost mode, which can distinguish the device's MAC address and its VID. The following table is the summary of the combination of 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. Here Entry Authorized means MAC entry is authorized.

Table 4-39.

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

4.13.1 802.1x State Setting

Table 4-40. 802.1x Configuration screen options.

Parameter	Description
802.1x State Setting	This function is used to configure the global parameters for RADIUS authentication in 802.1x port security application.
Radius Server	RADIUS server IP address for authentication. Default: 192.168.1.1
Port Number	The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535. Default port number is 1812.
Secret Key	The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters. Default: Radius

4.13.2 802.1x Mode Setting

Set the operation mode of 802.1X for each port. In this device, it supports only Multi-host operation mode.

Table 4-41. 802.1x Mode Setting screen options.

Parameter	Description
Port Number	Indicate which port is selected to configure the 802.1x operation mode.
802.1x Mode	802.1x operation mode. There are two options, including Disable and Multi-host mode. Default is Disable. Disable: It will have the chosen port acting as a plain port, that is no 802.1x port access control works on the port. 802.1x with Multi-host: In Multi-host mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

4.13.3 Port Security Management

This page shows each port status. In Multihost mode, it shows the port number and its status, authorized or unauthorized.

Table 4-42. Port Security Management screen options.

Parameter	Description
Disable Mode	When selecting Disable mode for a port in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply 802.1X authenticator on it. Any node attached on this port can access the network without the admittance of 802.1X authenticator. The Port Status will show the following screen.
Port Number	The port number to be chosen to show its 802.1X Port Status. The valid number is Port 1 – 26.
Port Status	The current 802.1X status of the port. In Disable mode, this field is Disabled.
802.1x with Multihost mode	When selecting 802.1x with Multihost mode for a port in the function 802.1X Port Mode Configuration, Devices can access the network through this port once the authenticator is authorized. The Port Status will show the following screen. If the port is granted to access the network, the port status is authorized, otherwise, unauthorized.

4.13.4 Parameter Setting

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.

Table 4-43. Parameter Setting screen options.

Parameter	Description
Port	It is the port number to be selected for configuring its associated 802.1x parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.
Port Control	This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto. ForceUnauthorized: The controlled port is forced to hold in the unauthorized state. ForceAuthorized: The controlled port is forced to hold in the authorized state. Auto: 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. Default: Auto
reAuthMax (1-10)	The number of authentication attempt that is permitted before the port becomes unauthorized. Default: 2
txPeriod (1-65535 s)	A time period to transmitted 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 in this port. Default: ON
reAuthPeriod (1-65535 s)	A non-zero number seconds between the periodic re-authentication of the supplicant

Table 4-43 (continued). Parameter Setting screen options.

Parameter	Description
max. Request (1-10)	The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10. Default: 2 times
suppTimeout (1-65535 s)	A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 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: 1 –65535. Default: 30 seconds

4.14 Alarm Configuration

4.14.1 Events Configuration

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 22 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (☑) the trap event individually on the web page shown as below.

Table 4-44. Events Configuration screen options.

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	Port-based VLAN Enabled, Tag-based VLAN Enabled
Module Swap	Module Inserted, Module Removed, Dual Media Swapped
PoE	PoE Failure

4.14.2 Email/ Sms Configuration

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both. 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. 3-51). Then, user can read the trap information from the email or the mobile phone. This function provides 6 email addresses and 6 mobile phone numbers at most. The 22 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses and mobile phone numbers. Then, please click **Apply** button to complete the alarm configuration. It will take effect in a few seconds.

NOTE

SMS may not work in your mobile phone system. It is customized for different systems.

Table 4-45 Email/ SMS Configuration screen options.

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 would like to receive the alarm message
SMS	SMS Server: the IP address of the server transferring your SMS. Username: your username in ISP. Password: your username in ISP. Mobile Phone 1-6: the mobile phone number that would like to receive the alarm message

4-15 Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

Default Configuration

This is the manufacturer's setting and cannot be altered. In the Web user interface (UI) two restore default functions are offered for the user to restore to the switch's default setting. The first function is Restore Default Configuration for the included default IP address. This will restore the IP address to the default 192.168.1.1. The other function is Restore Default Configuration without changing the current IP address. This will keep the same IP address that you saved before.

Working Configuration

This is the configuration you are currently using. It can be changed any time. The configurations you are using are saved into this configuration file. It's updated each time you press the **Apply** button.

User Configuration

This is the configuration file for the specified or backup purposes. It can be updated while confirming the configuration. Retrieve it by performing Restore User Configuration

4.15.1 Save/Restore

To get to this screen, click on **Save/Restore** in the Configuration menu.

Table 4-46. Save/Restore Configuration screen options.

Parameter	Description
Save As Start Configuration	Save the current configuration as a start configuration file in Flash memory.
Save As User Configuration	Save the current configuration as a user configuration file in Flash memory.
Restore Default Configuration (includes default IP address)	The Restore Default Configuration function can retrieve the manufacturer's setting to replace the start configuration. The switch's IP address is also restored to 192.168.1.1.
Restore Default Configuration (excludes current IP address)	The Restore Default Configuration function can retrieve the manufacturer's setting to replace the start configuration. However, the switch's current IP address that the user set up will not be changed and will not be restored to 192.168.1.1.
Restore User Configuration	The Restore User Configuration function can retrieve the previous confirmed working configuration stored in the Flash memory to update the start configuration. When restoring the configuration, the system's start configuration is updated and will change its system settings after rebooting the system.

4.15.2 Config File

To get to this screen, click on **Config File** in the Configuration menu. With this function, you can back up or reload the Save As Start or Save As User via TFTP configuration files.

Table 4-47. Config File screen options.

Parameter	Description
TFTP Server IP	The TFTP server's IP address.
Export File Path	Export Start button: Export Save As Start's config file stored in the Flash. Export User-Conf button: Export Save As User's config file stored in the Flash.

Table 4-47 (Continued). Config File screen options.

Parameter	Description
Import File Path	Import Start button: Import Save As Start's config file stored in the Flash. Import User-Conf button: Import Save As User's config file stored in the Flash.

4.16 Security

4.16.1 Mirror

Table 4-48. Mirror screen options.

Parameter	Description
Mirror Configuration	Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.
Mode	Used for the activation or de-activation of Port Mirror function. Default is disable.
Monitoring Port	Set up the port for monitoring. Valid port is Port 1~26 and default is Port 1.
Monitored Ingress Port	Set up the port for being monitored. It only monitor the packets received by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~26.
Monitored Egress Port	Set up the port for being monitored. It only monitor the packets transmitted by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~26.

4.16.2 Isolated Group

Isolated Group function can let the port be independent of other ports in the Isolated group, and the communication is also forbidden between these ports. But, the ports of the Isolated group are still able to communicate with the ports of the non-Isolated group. With this design, it will be helpful to the administrator to immediately find and solve the port that results in the occurrence of looping problems in the network.

Table 4-49. Isolated Group screen options.

Parameter	Description
Mode	Used for the activation or de-activation of Isolated Group function. Default is disable
Isolated Group	User can choose any port to be the member of this group. Just tick the check box (☑) beside the port x and valid port is Port 1~26. In this group, all of these member ports cannot forward packets with each other. Thus, the switch will not be capable of forwarding any packets in case its all ports become the members of the Isolated group.

4.16.3 RESTRICTED GROUP

The function of the Restricted Group can decide the direction of transmitting packets for the specific port. The packets received by the port with the **Ingress** mode of Restricted Group will be sent to the ports with the **Egress** mode of Restricted Group.

Table 4-50. Restricted Group screen options.

Parameter	Description
Mode	Used for the activation or de-activation of Restricted Group function. Default is disable.
Ingress	Select the ports that you would like their Restricted Group to set into Ingress mode. Just tick the check box beside the port x and valid port is Port 1~26.
Egress	Select the ports that you would like their Restricted Group to set into Egress mode. Just tick the check box beside the port x and valid port is Port 1~26.

4.17 Bandwidth Management

4.17.1 Ingress Bandwidth Setting

Ingress Bandwidth Setting function is used to set up the limit of Ingress bandwidth for each port.

Table 4-51. Ingress Bandwidth Setting screen options.

Parameter	Description
Port No.	Choose the port that you would like this function to work on it. Valid range of the port is 1~26.
Rate	Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

4.17.2 Egress Bandwidth Setting

Egress Bandwidth Setting function is used to set up the limit of Egress bandwidth for each port.

Table 4-52. Egress Bandwidth Setting screen options.

Parameter	Description
Port No.	Choose the port that you would like this function to work on it. Valid range of the port is 1~26.
Rate	Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

4.17.3 Storm Setting

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.

Table 4-53. Storm Setting screen options.

Parameter	Description
Storm Type	Disable: Disable the function of the bandwidth storm control. Broadcast Storm Control: Enable the function of bandwidth storm control for broadcast packets. Multicast Storm Control: Enable the function of bandwidth storm control for multicast packets. Unknown Unicast Storm Control: Enable the function of bandwidth storm control for unknown unicast packets. These packets are the MAC address that had not completed the learning process yet. Broadcast, Multicast, Unknown Unicast Storm Control: Enable the function of bandwidth storm control for all packets in transmission.
Storm Rate	Set up the limit of bandwidth for storm type you choose. Valid value of the storm rate ranges from 1-100 with the minimum unit of 1. And only integer is acceptable. Default is 100.

4.18 QoS Configuration

The switch supports 5 kinds of QoS, are as follows, MAC Priority, 802.1p Priority, IP TOS Priority, and DiffServ DSCP Priority. Port Based Priority has a special name called VIP Port in the switch. Any packets enter VIP Port will have highest transmitting priority. MAC Priority act on the destination address of MAC in packets. VLAN tagged Priority field is effected by 802.1p Priority setting. IP TOS Priority affects TOS fields of IP header, and you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED (1bit).

User can randomly control these fields to achieve some special QoS goals. When bits D, T, R, or M set, the D bit requests low delay, the T bit requests high throughput, the R bit requests high reliability, and the M bit requests low cost.

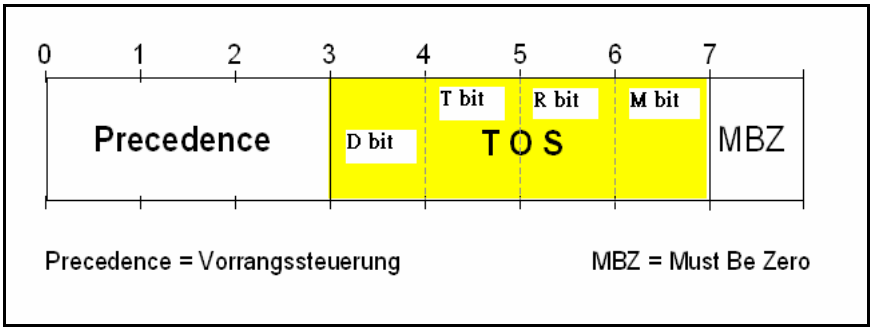


Figure 4-4.

DiffServ DSCP Priority act on DSCP field of IP Header. In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

High Priority Packet streams will experience less delay into the switch. For handing different priority packets, each egress port has designed up to 4 queues. Each QoS is influenced by two scheduling, WRR (Weighted Round Robin) and Strict Priority as well. When you finish to set the priority mapping to the queue, WRR scheduling will distribute the bandwidth according to the weight you set for 4 queues (queue 0 to queue 3). Another scheduling is Strict Priority dedicated for the function named VIP Port of QoS. While we select some ports as the VIP Port, these ports will own the highest transmitting priority in egress queue of the switch.

The QoS functions as we mentioned above are able to enabled at the same time. But, the following precedence will decide whether these functions work or not.

1. enable both VIP and TOS
   Choose priorities of VIP and TOS.

2. enable both VIP and DSCP
   Choose priorities of VIP and DSCP.

3. enable both TOS and DSCP
   Choose DSCP.

4. enable both VIP and DSCP
   Choose priorities of VIP and DSCP.

5. enable both 802.1p and TOS
   Choose "TOS".

6. enable both 802.1p and DSCP
   Choose DSCP.

7. enable both 802.1p and DSCP and TOS
   Choose DSCP.

8. enable both 802.1p and DSCP and TOS and VIP
   Choose priorities of VIP and DSCP.
   ** VIP/DSCP > TOS > 802.1p (Final result).

4.18.1 QoS Global Setting

When you want to use QoS function, please enable QoS Mode in advance. Then you can use MAC Priority, 802.1p Priority, IP TOS Priority, DiffServ DSCP Priority, or VIP Port functions and take effect. In this function, you can Enable QoS Mode. Choose any of Priority Control, such as 802.1p, TOS, DSCP. Moreover, you can select Scheduling Method of WRR (Weighted Round Robin) or Strict Priority. Next, you can arrange Weight values for queue 0 to queue 3.

Table 4-54. QoS Global Setting screen options.

Parameter	Description
QoS Mode	You can Enable QoS Mode and let QoS function become effective. Default is Disable.
Priority Control	Just tick the check box (☑) of 802.1P, TOS, or DSCP Qos and click Apply button to be in operation.
Scheduling Method	There are two Scheduling Method, WRR and Strict Priority. Default is WRR. After you choose any of Scheduling Method, please click Apply button to be in operation.
Weight (1~55)	Over here, you can make an arrangement to Weight values of Queue 0 to Queue 3. The range of Weight you can set is 1~55. In default, the weight of Queue 0 is 1, the weight of Queue 1 is 2, the weight of Queue 2 is 4, and the weight of Queue 3 is 8.

4.18.2 VIP Port Setting

When the port is set as VIP Port, the packets enter this port and will have highest transmitting priority. For example, as you choose port 2 is VIP Port, simultaneously transmit packets from port 2 and port 3 to port 1 at speed of 100MB and let congestion happen. The packets for port 3 will be dropped because the packets from port 2 owns highest precedence. For the sake of this function taking effect, you must choose Scheduling Method of Strict Priority ahead.

Table 4-55. VIP Port Setting screen options.

Parameter	Description
VIP Port	Just tick the check box (☑) to select any port(port 1~26) as the VIP Port. Then, click the **Apply** button to have the setting taken effect.

4.18.3 802.1p Setting

This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~8 priorities, priorities can map to 4 queues of the switch (queue 0~3) and possess different bandwidth distribution according to your weight setting.

Table 4-56. 802.1p Setting screen options.

Parameter	Description
802.1p Priority Mapping	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

4.18.4 D-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Delay Priority Mapping works while D-TYPE in TOS field of IP header of the packets received by the switch is configured.

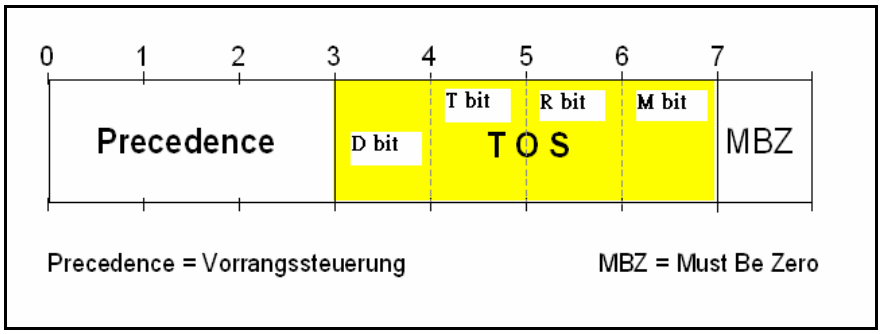


Figure 4-5.

Table 4-57. D-Type TOS screen options.

Parameter	Description
TOS Delay Priority Mapping	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

4.18.5 T-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Throughput Priority Mapping works while T-TYPE in TOS field of IP header of the packets received by the switch is configured.

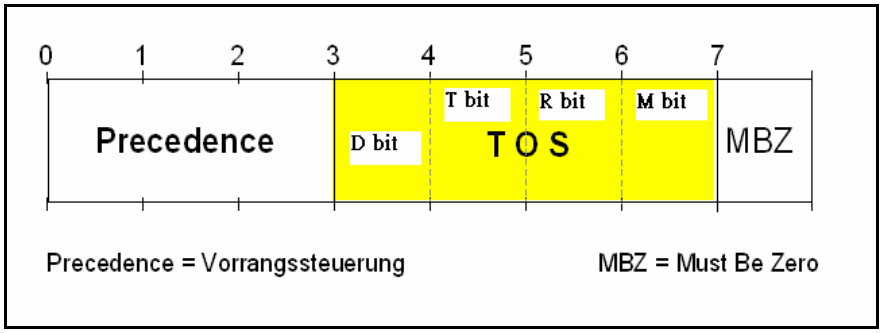


Figure 4-6.

Table 4-58. T-Type TOS screen options.

Parameter	Description
TOS Throughput Priority Mapping	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

4.18.6 R-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Reliability Priority Mapping works while R-TYPE in TOS field of IP header of the packets received by the switch is configured.

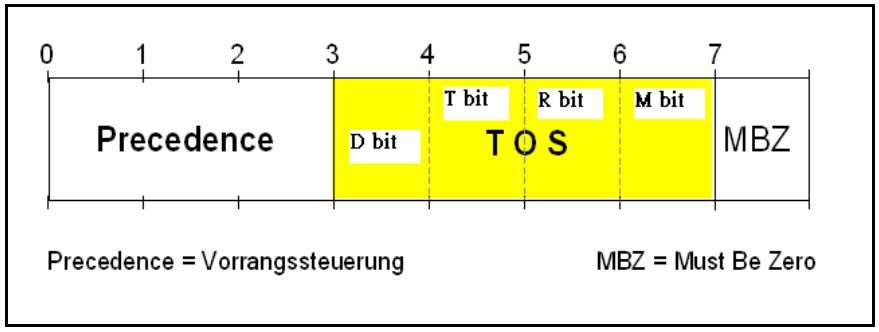


Figure 4-7.

Table 4-59. R-Type TOS screen options.

Option	Description
TOS Reliability Priority Mapping	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

4.18.7 M-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Monetary Cost Priority Mapping works while M-TYPE in TOS field of IP header of the packets received by the switch is configured.

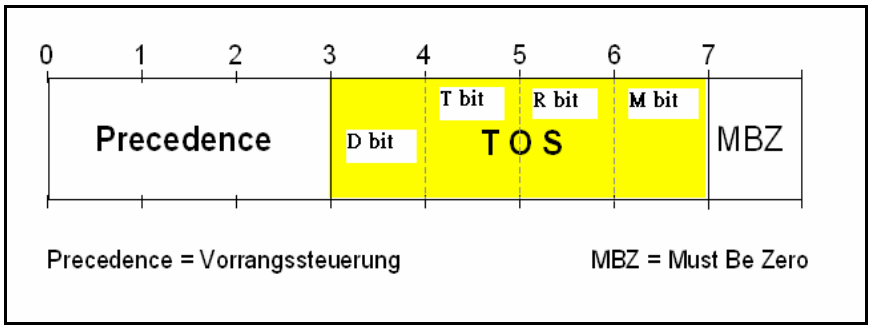


Figure 4-8.

Table 4-60. M-Type TOS screen options.

Parameter	Description
TOS Monetary Cost Priority Mapping	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

4.18.8 DSCP Setting

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a code point, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue 0~3.

Table 4-61. DSCP Setting screen options.

Parameter	Description
DSCP Priority Mapping	64 kinds of priority traffic as mentioned above, user can set up any of Queue 0~3. In default, Priority 0~15 are mapping to Queue 0, Priority 16~31 are mapping to Queue 1, Priority 32~47 are mapping to Queue 0, Priority 48~63 are mapping to Queue 0.

4.19 Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics. Each of them will be described in detail orderly in the following sections.

4.19.1 Diagnostics

Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.

4.19.2 Loopback Test

In the Loopback Test function, there are two different loopback tests. One is Internal Loopback Test and the other is External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch box. As to the latter test function, it will send the test signal to its link partner. If you do not have them connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are ok, it just shows OK.

NOTE

Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with the normal system working, and all packets in sending and receiving also will stop temporarily.

4.19.3 Ping Test

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device is available or not. You can simply fill in a known IP address and then click **Ping** button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.

Table 4-62. Ping Test screen options.

Parameter	Description
IP Address	An IP address with the version of v4, e.g. 192.168.1.1.
Default Gateway	IP address of the default gateway.

4.20 TFTP Server

You can set up IP address of TFTP server in this page.

Table 4-63. TFTP Server screen options.

Parameter	Description
Server	Specify the IP address where the TFTP server locates. Fill in the IP address of your TFTP server, then press **Apply** button to have the setting taken effect.

4.21 Log

This function shows the log data. The switch provides system log data for users. There are 17 private trap logs, 5 public trap logs. The switch supports total 120 log entries. For more details on log items, please refer to the section of Trap/Alarm Configuration and SNMP Configuration.

Table 4-64. Log screen options.

Parameter	Description
Log Data	The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.
No.	Display the order number that the trap happened.
Time	Display the time that the trap happened.
Events	Display the trap event name.
Auto Upload Enable	Switch the enabled or disabled status of the auto upload function.
Upload Log	Upload log data through tftp.
Clear Log	Clear log data.

4.22 Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. The switch provides a TFTP client for software upgrade. This can be done through Ethernet.

The switch supports TFTP upgrade tool for upgrading software. If you assure to upgrade software to a newer version one, you must follow two procedures:

1. Specifying the IP address where TFTP server locates. In this field, the IP address of your TFTP server should be filled in.

2. Specifying what the filename and where the file is. You must specify full path and filename.

Then, press **Upgrade** button if your download is not successful, the switch will also be back to "Software Upgrade", and it will not upgrade the software as well.

When download is completed, the switch starts upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the switch to have new software worked.

NOTE

Software upgrade is hazardous if power is off. You must do it carefully.

Table 4-65. Firmware Upgrade screen options.

Parameter	Description
TFTP Server	A TFTP server stored the image file you want to upgrade.
Path and Filename	File path and filename stored the image file you want to upgrade.

4.23 Reboot

We offer you many ways to reboot the switch, including power up, hardware reset and software reset. You can 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 taken effect. Here we are discussing is software reset for the reboot in the main menu.

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.

Table 4-66. Reboot screen options.

Parameter	Description
Save and Reboot	Save the current settings as start configuration before rebooting the switch.
Reboot	Reboot the system directly.

4.24 Logout

You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

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. Besides this manually logout and implicit logout, you can pull down the **Auto Logout** list at the left-top corner to explicitly ON/OFF this logout function.

Table 4-67. Logout screen options.

Parameter	Description
Auto Logout	Default is ON. If it is ON, and no action and no key is stroke as well in any function screen more than 3 minutes, the switch will have you logout automatically.

5. CLI Management

Locate the included RS-232 null-modem cable. Refer to Section 1.3for the null-modem cable's configuration.

Attach the DB9 female connector to the male DB9 serial port connector on the switch.

Attach the other end of the DB9 cable to an ASCII terminal emulator. Or, connect the cable to a PC COM1 or COM2 port on a PC running a utility such as Microsoft Windows HyperTerminal.

At the COM Port Properties Menu, configure the parameters as follows:

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	None

5.1 Login

The command-line interface (CLI) is a text-based interface. Access the CLI through either a direct serial connection to the device or a Telnet session. The switch's default values are listed below.

Username: `admin`

Password: `admin`

After you login successfully, the prompt appears as "#" if you are the first login person and your authorization is administrator; otherwise, it appears as "$." The former means you act as an administrator and have all system access rights. The latter means you act as a guest and are only allowed to view the system without permission to apply configuration settings to the switch.

5.2 Commands

To see the CLI mode commands, type in a "?" after the prompt, then all commands will be listed. All command scan be divided into two categories, global and local commands. Global commands (end, exit, help, history, logout, restore default, restore user, save start, and save user) can be used in either administrator or user mode. For details, refer to **Section 5.2.1**.

Command instructions residing in user mode are local commands. A local command can have the same name as a remote command, but it performs a totally different function. 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 5.2.2**.

Once you log into the switch as described in **Section 5.1**, the screen shown in Figure 5-1 appears.

```
Managed Switch – PSES-2126C

Login: admin
Password:

PSES-2126C# ?
802.1x              Enter into 802.1x mode
account             Enter into account mode
alarm               Enter into alarm mode
autologout          Change autologout time
bandwidth           Enter into bandwidth mode
config-file         Enter into config file moded
dhcp-boot           Enter into dhcp-boot mode
diag                Enter into diag mode
firmware            Enter into firmware mode
gvrp                Enter into gvrp mode
hostname            Change hostname
Igmp-snooping       Enter into igmp mode
ip                  Enter into ip mode
log                 Enter into log mode
mac-table           Enter into mac table mode
management          Enter into management mode
poe                 Enter into poe function
port                Enter into port mode
```

Figure 5-1. Login screen.

5.2.1 Global CLI Commands

end

Syntax: end

Description: Return to the top mode.

When you enter this command, your current position moves to the top mode.

Argument: None

Possible value: None

Example:

```
Giga Switch alarm
Giga Switch (alarm)# events
Giga Switch (alarm-events)# end

Giga Switch#
```

exit

Syntax: exit

Description: Return to the previous mode.

When you enter this command, your current position moves back to the previous mode.

Argument: None

Possible value: None

Example:

Giga Switch# trunk
Giga Switch(trunk)# exit

Giga Switch#

help

Syntax: help

Description: Shows available commands.

Some commands are the combination of more than two words. When you enter this command, the CLI shows the complete commands. This command also helps you classify the commands as either local or global commands.

Argument: None

Possible value: None

Example:

```
Giga Switch# ip
Giga Switch (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

 ------------<< Local 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 were run.

When you enter this command, the CLI shows a list of commands that you typed previously. The CLI supports up to 256 records. If you don't type in anything, the CLI lists up to 256 total records. If you do type in a number, the CLI only shows the records' last numbers.

Argument: [#]: show last number of history records. (optional)

Possible value: [#]: 1, 2, 3, …., 256

Example:

```
Giga Switch(ip)# history
Command history:
  0. trunk
  1. exit
  2. Giga Switch# trunk
  3. Giga Switch(trunk)# exit
  4. Giga Switch#
  5. ?
  6. trunk
  7. exit
  8. alarm
  9. events
  10. end
  11. ip
  12. help
  13. ip
  14. history
```

```
Giga Switch(ip)# history 3
  Command history:
  13. ip
  14. history
  15. history 3

Giga Switch(ip)#
```

logout

Syntax: logout

Description: When you enter this command via a Telnet connection, you will log out of the system and disconnect. If you connect the system through a direct serial port with an RS-232 cable, you will log out of the system and return to the initial login prompt when you run this command.

Argument: None

Possible value: None

Example:

```
Giga Switch# logout
```

restore default

Syntax: restore default

Description: When you use this function in CLI, the system will prompt "Do you want to restore the default IP address?(y/n)". If you choose Y or y, the IP address will restore to the default 192.168.1.1. If you choose N or n, the IP address will keep the same one that you saved before.

If restoring the default is successful, the CLI asks if it will reboot immediately or not. Pressing Y or y reboots the system immediately; otherwise, it goes back to the CLI system. After restoring the default configuration, all the changes in the startup configuration are lost. After rebooting, the entire startup configuration resets to the factory default.

Argument: None

Possible value: None

Example:

```
Giga Switch# restore default
Restoring ...
Restore Default Configuration Successfully
Press any key to reboot system.
```

restore user

Syntax: restore user

Description: Restores the startup configuration as a user-defined configuration. If restoring default is successful, the CLI asks if you want to reboot immediately or not. Pressing Y or y reboots the system immediately; if you press N or n, the software returns to the CLI system. After restoring a user-defined configuration, all the changes in the startup configuration are lost. After rebooting, the entire startup configuration replaces the user-defined one.

Argument: None

Possible value: None

Example:

```
Giga Switch# restore user
Restoring ...
Restore User Configuration Successfully
Press any key to reboot system.
```

save start

Syntax: save start

Description: Saves the current configuration as the startup one. When you enter this command, the CLI saves your current configuration to the nonvolatile Flash. If you want the configuration to work after rebooting, save the configuration using the command save start.

Argument: None

Possible value: None

Example:

```
Giga Switch# save start
Saving start...
Save Successfully

Giga Switch#
```

save user

Syntax: save user

Description: Saves the current configuration as the user-defined configuration. When you enter this command, the CLI saves your current configuration in the nonvolatile Flash as a user-defined configuration.

Argument: None

Possible value: None

Example:

Giga Switch# save user
Saving user...
Save Successfully

Giga Switch#

5.2.2 Local CLI Commands

NOTE

For local CLI commands, syntax 1, 5–7 represents a range of ports. For example, if the port range is shown as 1, 5–7, available from 1 to 8, the range of ports available is 1–8.

802.1X

set max-request

Syntax: set max-request <port-range> <times>

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
<times> : max-times, range 1–10

Possible value:
<port range> : 1 to 8
<times>: 1–10, default is 2

Example:

```
Giga Switch(802.1X)# set max-request 2 2
```

set mode

Syntax: set mode <port-range> <mode>

Description: Sets up each port's 802.1x authentication mode.

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:

```
Giga Switch(802.1X)# set mode 2 1
```

set port-control

Syntax: set port-control <port-range> <authorized>

Description: Sets up each port's 802.1x status.

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:

```
Giga Switch(802.1X)# set port-control 2 2
```

set quiet-period

Syntax: set quiet-period <port-range> <sec>

Description: A timer that the Authenticator state machine uses to define time periods when it won't attempt to acquire a Supplicant. (A state machine is a service within the switch that monitors connections and times them out when the time reaches a set maximum time.)

Argument:

<port range>: syntax 1, 5–7, available from 1 to 8
<sec>: timer, range 0–65535

Possible value:

<port range> : 1 to 8
<sec> : 0–65535, default is 60

Example:

```
Giga Switch(802.1X)# set quiet-period 2 30
```

set reAuthEnabled

Syntax: set reAuthEnabled <port-range> <ebl>

Description: A constant that defines whether regular reauthentication will occur on this port.

Argument:

<port range> : syntax 1, 5–7, available from 1 to 8
<ebl> :
0: OFF Disable reauthentication
1: ON Enable reauthentication

Possible value:

<port range> : 1 to 8
<ebl> : 0 or 1, default is 1

Example:

```
Giga Switch(802.1X)# set reAuthEnabled 2 1
```

set reAuthMax

Syntax: set reAuthMax <port-range> <max>

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
<max> : max. value, range 1–10

Possible value:

<port range> : 1 to 8
<max> : 1–10, default is 2

Example:

```
Giga Switch(802.1X)# set reAuthMax 2 2
```

set reAuthPeriod

Syntax: set reAuthPeriod <port-range> <sec>

Description: A constant that defines a nonzero number of seconds between the Supplicant's periodic reauthentication.

Argument:

<port range> : syntax 1, 5–7, available from 1 to 8
<sec> : timer, range 1–65535

Possible value:

<port range> : 1 to 8
<sec> : 1–65535, default is 3600

Example:

```
Giga Switch(802.1X)# set reAuthPeriod 2 3600
```

set serverTimeout

Syntax: set serverTimeout <port-range> <sec>

Description: A timer used by the backend authentication state machine determines timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. (A state machine is a service within the switch that monitors connections and times them out when the time reaches a set maximum time.) The initial value of this timer is either suppTimeout or serverTimeout, as determined by the backend Authentication state machine's operation.

Argument:

<port range> : syntax 1, 5–7, available from 1 to 8
<sec> : timer, range 1–65535

Possible value:

<port range> : 1 to 8
<sec> : 1–65535, default is 30

Example:

```
Giga Switch(802.1X)# set serverTimeout 2 30
```

set state

Syntax: set state <ip> <port-number> <secret-key>

Description: Configures the settings related to the 802.1x Radius Server.

Argument:

<ip> : the IP address of Radius Server
<port-number> : 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:

<port-number> : 1–65535, default is 1812

Example:

```
Giga Switch(802.1X)# set state 192.168.1.115 1812 WinRadius
```

set suppTimeout

Syntax: set suppTimeout <port-range> <sec>

Description: A timer used by the Backend Authentication state machine that determines timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. (A state machine is a service within the switch that monitors connections and times them out when the time reaches a set maximum time.) The timer's initial value is either suppTimeout or serverTimeout, as determined by the Backend Authentication state machine's operation.

Argument:

<port range> : syntax 1, 5–7, available from 1 to 8
<sec> : timer, range 1–65535

Possible value:

<port range> : 1 to 8
<sec> : 1–65535, default is 30

Example:

```
Giga Switch(802.1X)# set suppTimeout 2 30
```

set txPeriod

Syntax: set txPeriod <port-range> <sec>

Description: A timer used by the Authenticator state machine to determine when a packet will be transmitted.

Argument:

<port range> : syntax 1, 5–7, available from 1 to 8
<sec> : timer, range 1–65535

Possible value:

<port range> : 1 to 8
<sec> : 1–65535, default is 30

Example:

```
Giga Switch(802.1X)# set txPeriod 2 30
```

show mode

Syntax: show mode

Description: Displays each port's mode.

Argument: None

Possible value: None

Example:

```
Giga Switch(802.1X)# show mode

  Port      Mode
  ======    ============
  1         Disable
  2         Multi-host
  3         Disable
  4         Disable
  5         Disable
  6         Disable
            :
            :
            :
```

show parameter

Syntax: show parameter

Description: Displays each port's parameter settings.

Argument: None

Possible value: None

Example:

```
Giga Switch(802.1X)# show parameter
port 1)   port control     : Auto
          reAuthMax        : 2
          txPeriod         : 30
          Quiet Period     : 60
          reAuthEnabled    : ON
          reAuthPeriod     : 3600
          max. Request     : 2
          suppTimeout      : 30
          serverTimeout    : 30

port 2)   port control     : Auto
          reAuthMax        : 2
          txPeriod         : 30
          Quiet Period     : 60
          reAuthEnabled    : ON
          reAuthPeriod     : 3600
          max. Request     : 2
          suppTimeout      : 30
          serverTimeout    : 30
                           :
                           :
                           :
```

show security

Syntax: show security

Description: Displays each port's authentication status.

Argument: None

Possible value: None

Example:

```
Giga Switch(802.1X)# show security
Port     Mode            Status
======   ============    ==============
  1       Disable
  2       Multi-host     Unauthorized
  3       Disable
  4       Disable
  5       Disable
  6       Disable
          :
          :
```

show state

Syntax: show state

Description: Shows the Radius server's configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(802.1X)# show state
Radius Server: 192.168.1.115
Port Number : 1812
Secret Key : WinRadius
```

account

add

Syntax: add <name>

Description: Creates a new guest user. Type in a password and confirm it when prompted.

Argument: <name> : new account name

Possible value: A string must be at least 5 characters.

Example:

```
Giga Switch(account)# add aaaaa
Password:
Confirm Password:
Save Successfully
Giga Switch(account)#
```

Del

Syntax: del <name>

Description: Deletes an existing account.

Argument: <name> : existing user account

Possible value: None

Example:

```
Giga Switch(account)# del aaaaa
Account aaaaa deleted
```

Modify

Syntax: modify <name>

Description: Changes an existing account's username and password.

Argument: <name> : existing user account

Possible value: None

Example:

```
Giga Switch(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 a system account, including account name and identity.

Argument: None

Possible value: None

Example:

```
Giga Switch(account)# show
Account Name       Identity
--------------------------------
  admin             Administrator
  guest             guest
```

alarm

<<email>>

del mail-address

Syntax: del mail-address <#>

Description: Removes the email address configuration.

Argument: <#>: email address number, range of 1 to 6

Possible value: <#>: 1 to 6

Example:

```
Giga Switch(alarm-email)# del mail-address 2
```

del server-user

yntax: del server-user

Description: Removes the server, user account, and password configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(alarm-email)# del server-user
```

set mail-address

Syntax: set mail-address <#> <mail address>

Description: Sets up the email address.

Argument:

<#> :email address number, range of 1 to 6
<mail address>:email address

Possible value:

<#>: 1 to 6

Example:

```
Giga Switch(alarm-email)# set mail-address 1 abc@mail.abc.com
```

set server

Syntax: set server <ip>

Description: Sets up the email server's IP address.

Argument: <ip>:email server ip address or domain name

Possible value: None

Example:

```
Giga Switch(alarm-email)# set server 192.168.1.6
```

set user

Syntax: set user <username>

Description: Sets up the email server's account and password.

Argument: <username>: email server account and password

Possible value: None

Example:

```
Giga Switch(alarm-email)# set user admin
```

show

Syntax: show

Description: Displays the e-mail configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(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:
```

<<events>>

del all

Syntax: del all <range>

Description: Disables email, sms, and events trap.

Argument: <range>:del the range of events, syntax 1, 5–7

Possible value: <range>: 1–24

Example:

```
Giga Switch(alarm-events)# del all 1-3
```

del email

Syntax: del email <range>

Description: Disables the events' email.

Argument: <range>:del the range of email, syntax 1, 5–7

Possible value: <range>: 1–24

Example:

```
Giga Switch(alarm-events)# del email 1-3
```

del sms

Syntax: del sms <range>

Description: Disables the events' sms.

Argument: <range>: del the range of sms, syntax 1, 5–7

Possible value: <range>: 1–26

Example:

```
Giga Switch(alarm-events)# del sms 1-3
```

del trap

Syntax: del trap <range>

Description: Disables the events' trap.

Argument: <range>:del the range of trap, syntax 1, 5–7

Possible value: <range>: 1–26

Example:

```
Giga Switch(alarm-events)# del trap 1-3
```

set all

Syntax: set all <range>

Description: Enables email, sms, and events' trap.

Argument: <range>:set the range of events, syntax 1, 5–7

Possible value: <range>: 1–26

Example:

```
Giga Switch(alarm-events)# set all 1-3
```

set email

Syntax: set email <range>

Description: Enables the events' email.

Argument: <range>:set the range of email, syntax 1, 5–7

Possible value: <range>: 1–26

Example:

```
Giga Switch(alarm-events)# set email 1-3
```

set sms

Syntax: set sms <range>

Description: Enables the events'sms.

Argument: <range>:set the range of sms, syntax 1, 5–7

Possible value: <range>: 1–26

Example:

```
Giga Switch(alarm-events)# set sms 1-3
```

set trap

Syntax: set trap <range>

Description: Enables the events' trap.

Argument: <range>:set the range of trap, syntax 1, 5–7

Possible value: <range>: 1–26

Example:

```
Giga Switch(alarm-events)# set trap 1-3
```

show

Syntax: show

Description: Displays the alarm event's configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(alarm-events)# show
Events                                  Email SMS Trap

----------------------------------------
1  Cold Start                           v
2  Warm Start                           v
3  Link Down                            v
4  Link Up                               v
5  Authentication Failure                v
6  User Login
7  User Logout
8  STP Topology Changed
9  STP Disabled
10 STP Enabled
11 LACP Disabled
12 LACP Enabled
13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 VLAN Disabled
18 Port-based Vlan Enabled
19 Tag-based Vlan Enabled
20 Metro-mode Vlan Enabled
21 Double-tag Vlan Enabled
22 Module Inserte
23 Module Removed
24 Module Media Swapped
```

show (alarm)

Syntax: show

Description: Displays the trap, SMS, or e-mail configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(alarm)# show events
Giga Switch(alarm)# show email
Giga Switch(alarm)# show sms
```

<<sms>>

del phone-number

Syntax: del phone-number <#>

Description: Deletes the sms' phone number.

Argument: <#>: mobile phone number, range of 1 to 6

Possible value: <#>: 1 to 6

Example:

```
Giga Switch(alarm-sms)# del phone-number 3
```

del server-user

Syntax: del server-user

Description: Deletes sms server, user account, and password.

Argument: None

Possible value: None

Example:

```
Giga Switch(alarm-sms)# del server-user
```

set phone-number

Syntax: set phone-number <#> <phone-number>

Description: Adds sms phone number.

Argument:

<#>: mobile phone number, range of 1 to 6
<phone-number>: phone number

Possible value:

<#>: 1 to 6

Example:

```
Giga Switch(alarm-sms)# set phone-number 1 0968777777
```

set server

Syntax: set server <ip>

Description: Sets up the sms server's IP address.

Argument: <ip>: SMS server ip address or domain name

Possible value: None

Example:

```
Giga Switch(alarm-sms)# set server 192.168.1.7
```

set user

Syntax: set user <username>

Description: Sets up the sms server's user account and password.

Argument: <username>: SMS server account

Possible value: None

Example:

```
Giga Switch(alarm-sms)# set user ABC
```

show

Syntax: show

Description: Displays the SMS trap event's configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(alarm-sms)# show
SMS Server: 192.168.1.7
Username       : ABC
Password       : ****************
Mobile Phone  1: 0968777777
Mobile Phone  2:
Mobile Phone  3:
Mobile Phone  4:
Mobile Phone  5:
Mobile Phone  6:
```

autologout

autologout

Syntax: autologout <time>

Description: Sets 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:

```
Giga Switch# autologout 3600
Set autologout time to 3600 seconds
```

bandwidth

disable egress-rate

Syntax: disable egress-rate <range>

Description: Cancels the port's Egress rate.

Argument: <range>:syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

```
Giga Switch(bandwidth)# disable egress-rate 1-8
```

disable ingress-rate

Syntax: disable ingress-rate <range>

Description: Cancels the port's Ingress rate.

Argument: <range>:syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

```
Giga Switch(bandwidth)# disable ingress-rate 1-8
```

disable storm-rate

Syntax: disable storm-rate <range>

Description: Cancels the port's storm rate.

Argument: <range>:syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

```
Giga Switch(bandwidth)# disable storm-rate 1-8
```

enable egress-rate

Syntax: enable egress-rate <range> <data_rate>

Description: Sets up the port's Egress rate.

Argument:

<range>:syntax 1, 5–7, available from 1 to 8
<data_rate>: 0–1000

Possible value:

<range>: 1 to 8

<data_rate>: 0–1000

Example:

```
Giga Switch(bandwidth)# enable egress-rate 1-8 200
```

enable ingress-rate

Syntax: enable ingress-rate <range> <data_rate>

Description: Sets up the port's Ingress rate.

Argument:

<range>:syntax 1, 5–7, available from 1 to 8
<data_rate>: 0–1000

Possible value:

<range>: 1 to 8
<data_rate>: 0–1000

```
Example:
```

```
Giga Switch(bandwidth)# enable ingress-rate 1-8 100
```

enable storm-rate

Syntax: enable storm-rate <range> <data_rate>

Description: Sets up the port's storm rate.

Argument:

<range>:syntax 1, 5–7, available from 1 to 8
<data_rate>: 0–1000

Possible value:

<range>: 1 to 8
<data_rate>: 0–1000

Example:

```
Giga Switch(bandwidth)# enable storm-rate 1-8 150
```

show

Syntax: show

Description: Displays all current bandwidth settings.

Argument: None

Possible value: None

Example:

```
Giga Switch(bandwidth)# show
                    Ingress       Egress
  Port============================================== ======================
  All State         All Rate    Storm State   Storm Rate    All state   All Rate
====== =========== ========== ============= ============ ====================
  1      Disabled    0           Disabled     0            Disabled    0
  2      Disabled    0           Disabled     0            Disabled    0
  3      Disabled    0           Disabled     0            Disabled    0
  4      Disabled    0           Disabled     0            Disabled    0
  5      Disabled    0           Disabled     0            Disabled    0
  6      Disabled    0           Disabled     0            Disabled    0
  7      Disabled    0           Disabled     0            Disabled    0
  8      Disabled    0           Disabled     0            Disabled    0
```

config-file

export start

Syntax: export start

Description: Runs the export start function.

Argument: None

Possible value: None

Example:

```
Giga Switch(config-file)# export start
Export successful.
```

export user-conf

Syntax: export user-conf

Description: Runs the export user-conf function.

Argument: None

Possible value: None

Example:

```
Giga Switch(config-file)# export user-conf
Export successful.
```

import start

Syntax: import start

Description: Runs the import start function.

Argument: None

Possible value: None

Example:

```
Giga Switch(config-file)# import start
Import successful.
```

import user-conf

Syntax: import user-conf

Description: Runs the import user-conf function.

Argument: None

Possible value: None

Example:

```
Giga Switch(config-file)# import user-conf
Import successful.
```

set export-path

Syntax: set export-path <filepath>

Description: Sets up the filepath and filename that will be exported.

Argument: <filepath>:filepath and filename

Possible value:<filepath>:filepath and filename

Example:

```
Giga Switch(config-file)# set export-path log/21511.txt
```

set import-path

Syntax: set import-path <filepath>

Description: Sets up the filepath and filename that will be imported.

Argument: <filepath>:filepath and filename

Possible value: <filepath>:filepath and filename

Example:

```
Giga Switch(config-file)# set import-path log/21511.txt
```

show

Syntax: show

Description: Displays the config-file information.

Argument: None

Possible value: None

Example:

```
Giga Switch(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: nmap/123.ts
Import Path and Filename: user123.txt
```

dhcp-boot

set dhcp-boot

Syntax: set dhcp-boot <sec>

Description: Sets up the DHCPBoot delay time.

Argument: <sec>:range syntax: 0, 1–30; 0 disables dhcp-boot delay

Possible value: <sec>:0–30

Example:

```
Giga Switch(dhcp-boot)# set dhcp-boot 30
```

show

Syntax: show

Description: Displays the DHCP Boot's status.

Argument: None

Possible value: None

Example:

```
Giga Switch(dhcp-boot)#show
dhcp boot: Enable
Second: 10
```

diag

diag

Syntax: diag

Description: Tests whether UART, DRAM, Flash, and EEPROM are normal or not.

Argument: None

Possible value: None

Example:

```
Giga Switch(diag)# diag
EEPROM Test: OK
UART Test: OK
DRAM Test: OK
Flash Test: OK
```

loopback

Syntax: Loopback

Description: Starts Internal/External Loopback Test.

Argument: None

Possible value: None

Example:

```
Giga Switch(diag)# loopback
Internal Loopback Test: OK
External Loopback Test: Port 1 2 3 4 5 6 7 8 Fail
```

ping

Syntax: ping <ip>

Description: Confirms whether the remote end-station or not the switch itself is available.

Argument: <ip> : ip address or domain name

Possible value: IP address (for example, 192.168.2.65 or tw.yahoo.com)

Example:

```
Giga Switch(diag)# ping 192.168.1.115
Gateway: 192.168.1.253
192.168.1.115 is alive.
```

firmware

set upgrade-path

Syntax: set upgrade-path <filepath>

Description: Sets up the image file that will be upgraded.

Argument: <filepath>: upgrade file path

Possible value: <filepath>: upgrade file path

Example:

```
Giga Switch(firmware)# set upgrade-path gs2108c_Giga Switch_v2.03.img
```

show

Syntax: show

Description: Displays the tftp server and upgrade-path information.

Argument: None

Possible value: None

Example:

```
Giga Switch(firmware)# show
TFTP Server IP Address: 192.168.3.111
Path and Filename: gs2108c_Giga Switch_v2.03.img
```

upgrade

Syntax: upgrade

Description: Runs the upgrade function.

Argument: None

Possible value: None

Example:

```
Giga Switch(firmware)# upgrade
Upgrading firmware ...
```

gvrp

disable

Syntax: disable

Description: Disables the gvrp function.

Argument: None

Possible value: None

Example:

```
Giga Switch(gvrp)# disable
```

enable

Syntax: enable

Description: Enables the gvrp function.

Argument: None

Possible value: None

Example:

```
Giga Switch(gvrp)# enable
```

group

Syntax: group <group number>

Description: Enter any gvrp group for which you want to change the gvrp group setting. You can change the applicant or registrar mode of an existing gvrp group per port.

Argument: <group number>: enter which gvrp group you had created, using value is vid; available range is 1 to 4094

Possible value: <group number>: 1–4094

Example:

```
Giga Switch(gvrp)# show group
GVRP group information
Current Dynamic Group Number: 1
VID     Member Port
----    ------------------------------------------------
2       5

Giga Switch(gvrp)# group 2
Giga Switch(gvrp-group-2)# set applicant 1-6 non-participant

Giga Switch(gvrp-group-2)# show
GVRP group VID: 2
Port    Applicant          Registrar
----    ---------------    ---------
1       Non-Participant    Normal
2       Non-Participant    Normal
3       Non-Participant    Normal
4       Non-Participant    Normal
5       Non-Participant    Normal
6       Non-Participant    Normal
7       Normal             Normal
8       Normal             Normal

Giga Switch(gvrp-group-2)# set registrar 1-8 fixed
Giga Switch(gvrp-group-2)# show
GVRP group VID: 2
Port    Applicant          Registrar
----    ---------------    ---------
1       Non-Participant    Fixed
2       Non-Participant    Fixed
3       Non-Participant    Fixed
4       Non-Participant    Fixed
5       Non-Participant    Fixed
6       Non-Participant    Fixed
7       Normal             Fixed
8       Normal             Fixed
```

set applicant

Syntax: set applicant <range> <normal|non-participant>

Description: Sets each port's default applicant mode.

Argument:

<range>: port range, syntax 1, 5–7, available from 1 to 8
<normal>: set applicant as normal mode
<non-participant>: set applicant as non-participant mode

Possible value:

<range>: 1 to 8
<normal|non-participant>: normal or non-participant

Example:

```
Giga Switch(gvrp)# set applicant 1-8 non-participant
```

set registrar

Syntax: set registrar <range> <normal|fixed|forbidden>

Description: Sets each port's default registrar mode.

Argument:

<range>: port range, syntax 1, 5–7, available from 1 to 8
<normal>: set registrar as normal mode
<fixed>: set registrar as fixed mode
<forbidden>: set registrar as forbidden mode

Possible value:

<range>: 1 to 8
<normal|fixed|forbidden>: normal, fixed, or forbidden

Example:

```
Giga Switch(gvrp)# set registrar 1-5 fixed
```

set restricted

Syntax: set restricted <range> <enable|disable>

Description: Sets each port's restricted mode.

Argument:
<range>: port range, syntax 1, 5–7, available from 1 to 8
<enable>: set restricted enabled
<disable>: set restricted disabled

Possible value:

<range>: 1 to 8
<enable|disable>: enable or disable

Example:

```
Giga Switch(gvrp)# set restricted 1-8 enable
Giga Switch(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 <range> <join> <leave> <leaveall>

Description: Sets each port's gvrp join time, leave time, and leave all time.

Argument:

<range> : port range, syntax 1, 5–7, available from 1 to 8
<join>: join timer, available from 20 to 100
<leave>: leave timer, available from 60 to 300
<leaveall>: leaveall timer, available from 1000 to 5000
Leave Time must equal double Join Time at least.

Possible value:

<range> : 1 to 8
<join>: 20 to 100
<leave>: 60 to 300
<leaveall>: 1000 to 5000

Example:

```
Giga Switch(gvrp)# set timer 2-8 25 80 2000
```

show config

Syntax: show config

Description: Displays the gvrp configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(gvrp)# show config
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
```

show counter

Syntax: show counter <port>

Description: Displays the port's counter number.

Argument: <port>: port number

Possible value: <port>: available from 1 to 8

Example:

```
Giga Switch(gvrp)# show counter 2
GVRP Counter port: 2
Counter Name           Received      Transmitted
------------           --------      ------------
Total GVRP Packets     0             0
Invalid GVRP Packets    0             ----
LeaveAll message       0              0
JoinEmpty message      0              0
JoinIn message          0             0
LeaveEmpty message     0             0
Empty message          0             0
```

show group

Syntax: show group

Description: Shows the gvrp group.

Argument: None

Possible value: None

Example:

```
Giga Switch(gvrp)# show group
GVRP group information
VID   Member Port
----  ------------------------------------------------
```

hostname

hostname

Syntax: hostname <name>

Description: Sets up the switch's hostname.

Argument: <name>: hostname, maximum of 40 characters

Possible value: <name>: hostname, maximum of 40 characters

Example:

```
Giga Switch# hostname Company
Company#
```

Igmp-snooping

set igmp_snooping

Syntax: set igmp_snooping <status>

Description: Sets up the IGMP Snooping mode.

Argument: <status>: 0: disable, 1: active, 2: passive

Possible value: <status>: 0, 1, or 2

Example:

```
Giga Switch(igmp)# set igmp-snooping 2
```

show

Syntax: show

Description: Displays the IGMP snooping mode and IP Multicast Table.

Argument: None

Possible value: None

Example:

Giga Switch(igmp)# show
Snoop Mode: Active

```
IP Multicast:
1)  IP Address:   224.1.1.1
    VLAN ID:    0
    Member Port: 22
```

ip

disable dhcp

Syntax: disable dhcp

Description: Disables the system's DHCP function.

Argument: None

Possible value: None

```
Example:

Giga Switch(ip)# disable dhcp
```

enable dhcp

Syntax: enable dhcp <manuallauto>

Description: Enables the system DHCP function and sets the DNS server via manual or auto mode.

Argument: <manuallauto> : set dhcp by using manual or auto mode

Possible value: <manuallauto> : manual or auto

Example:

```
Giga Switch(ip)# enable dhcp manual
```

set dns

Syntax: set dns <ip>

Description: Sets the DNS server's IPaddress.

Argument: <ip> : dns ip address

Possible value: 168.95.1.1

Example:

```
Giga Switch (ip)# set dns 168.95.1.1
```

set ip

Syntax: set ip <ip> <mask> <gateway>

Description: Sets 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:
```

```
Giga Switch(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253
```

show

Syntax: show

Description: Displays 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:

```
Giga Switch(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
```

log

clear

Syntax: clear

Description: Clears the log data.

Argument: None

Possible value: None

Example:

```
Giga Switch(log)# clear
```

disable auto-upload

Syntax: disable auto-upload

Description: Disables the auto-upload function.

Argument: None

Possible value: None

Example:

```
Giga Switch(log)# disable auto-upload
```

enable auto-upload

Syntax: enable auto-upload

Description: Enables the auto-upload function.

Argument: None

Possible value: None

Example:

```
Giga Switch(log)# enable auto-upload
```

show

Syntax: show

Description: Shows a list of trap log events. When any log event happens, it will be recorded and it will use show command in the log function to query. Up to 120 log records are supported.

Argument: None

Possible value: None

Example:

```
Giga Switch(log)# show

Tftp Server: 0.0.0.0
Auto Upload: Disable

1)   Wed Apr 13 12:13:27 2005   Link Up [Port 1]
2)   Wed Apr 13 12:13:26 2005   Link Down [Port 1]
3)   Wed Apr 13 11:58:31 2005   Login [admin]
4)   Wed Apr 13 11:19:45 2005   Login [admin]
5)   Wed Apr 13 11:19:37 2005   Logout [admin]
```

upload

Syntax: upload

Description: Uploads log data through TFTP.

Argument: None

Possible value: None

Example:

```
Giga Switch(log)# upload
```

mac-table

<<alias>>

del

Syntax: del <mac>

Description: Deletes the MAC alias entry.

Argument: <mac> : MAC address, format: 00-02-03-04-05-06

Possible value: <mac> : MAC address

Example:

```
Giga Switch(mac-table-alias)# del 00-44-33-44-55-44
```

set

Syntax: set <mac> <alias>

Description: Sets up the MAC alias entry.

Argument:

<mac> : MAC address, format: 00-02-03-04-05-06
<alias> : MAC alias name, maximum of 15 characters

Possible value: None

Example:

```
Giga Switch(mac-table-alias)# set 00-44-33-44-55-44 www
```

show

Syntax: show

Description: Displays the MAC alias entry.

Argument: None

Possible value: None

Example:

```
Giga Switch(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
```

<<information>>

search

Syntax: search <port> <mac> <vid>

Description: Looks for the relative MAC information in the MAC table.

Argument:

<port> : set up the range of the ports to search for, syntax 1, 5–7, available from 1 to 8
<mac> : mac address, format: 01-02-03-04-05-06, "?" can be used

<vid> : vlan id, from 1 to 4094; '?' represents "don't care", 0 as untagged

Possible value:

<port> :1 to 8
<vid> : 0, 1–4094

Example:

```
Giga Switch(mac-table-information)# search 1-8 ??-??-??-??-??-?? ?
MAC Table List
Alias               MAC Address         Port    VID State
-----               -----------         -----   ----------
                    00-40-c7-88-00-06   10       Dynamic
```

show

Syntax: show

Description: Displays all MAC table information.

Argument: None

Possible value: None

Example:

```
Giga Switch (mac-table-information)# show
MAC Table List
  Alias                  MAC Address        Port    VID    State
  -----------           ------------------  -----   ----   ---------------
                        00-10-db-1d-c5-a0   8       0      Dynamic
                        00-40-f4-89-c9-7f   8       0      Dynamic
                        00-e0-18-2b-9d-e2   8       0      Dynamic
                        00-40-c7-d8-00-02   8       0      Dynamic
```

<<maintain>>

set aging

Syntax: set aging <#>

Description: Sets up the dynamic learning MAC's age out time.

Argument: <#>: age-timer in seconds, 0, 10 to 65535; 0 disables aging.

Possible value: <#>: 0, 10 to 65535.

Example:

```
Giga Switch(mac-table-maintain)# set aging 300
```

set flush

Syntax: set flush

Description: Deletes all dynamically-learned MACs.

Argument: None

Possible value: None

Example:

```
Giga Switch(mac-table-maintain)# set flush
```

show

Syntax: show

Description: Displays the age-timer settings.

Argument: None

Possible value: None

Example:

```
Giga Switch(mac-table-maintain)# show
age-timer : 300 seconds
Giga Switch(mac-table-maintain)#
```

<<static-mac>>

add

Syntax: add <mac> <port> <vid> [alias]

Description: Adds the static MAC entry.

Argument:

<mac> : MAC address, format: 00-02-03-04-05-06
<port> : 0–8; 0 means this entry is filtering entry
<vid> : vlan id. 0, 1–4094; VID must be zero if vlan mode is not tag-based
[alias] : MAC alias name, maximum of 15 characters

Possible value:

<mac> : mac address
<port> : 0–8
<vid> : 0, 1–4094
[alias] : MAC alias name

Example:

```
Giga Switch(mac-table-static-mac)# add 00-02-03-04-05-06 3 0 aaa
```

del

Syntax: del <mac> <vid>

Description: Removes 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:

```
Giga Switch(mac-table-static-mac)# del 00-02-03-04-05-06 0
```

show filter

Syntax: show filter

Description: Displays the static filter table.

Argument: None

Possible value: None

Example:

```
Giga Switch(mac-table-static-mac)# show filter
Static Filtering Entry: (Total 1 item(s))
1) mac: 00-33-03-04-05-06, vid: -, alias: ccc
```

show forward

Syntax: show forward

Description: Displays the static forward table.

Argument: None

Possible value: None

Example:

```
Giga Switch(mac-table-static-mac)# show forward
Static Forwarding Entry: (Total 1 item(s))
1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa
```

management

add

Syntax:

Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]
[<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2–5, 8
type h, s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

Description:

Saves the adding management policy records.
When you don't know how to set the management policy records, you can use this command as follows:

`Giga Switch`(management-add)# set

This command shows an operating explanation for setting the management policy records.

Argument:

[<name> <value>]	ACL entry name
[<vid> <value>]	VLAN ID
[<ip> <value>]	IP range
[<port> <value>]	Incoming port
[<type> <value>]	Access type
<action> <value>	a(ccept) or d(eny)

Possible value:

[<name> <value>]	No default and it must be set
[<vid> <value>]	The range is 1–4095 and can be set to any
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any
[<port> <value>]	For example, 1 or 1–8 or 1, 3–5 or any
[<type> <value>]	For example, h(ttp), s(nmp), t(elnet) or any
<action> <value>	No default and it must be set

Example:

```
Giga Switch(management-add)# set name Mary vid 20 ip 192.168.1.1-192.168.1.90
port2-5,8 type h,s action a
```

```
Giga Switch(management-add)# show

#: 1
Name:       Mary       VlanID: 20       IP: 192.168.1.1-192.168.1.90
Type:       Http,SNMP  Action: Accept   Port : 2,3,4,5,8
```

delete

Syntax: delete #

Description: Deletes a specific record or range.

Argument: <#>: a specific or range management security entry(s)

Possible value: None

Example:

```
Giga Switch(management)# show
#: 1
Name:       Tom       VlanID : 2       IP : 192.168.1.30-192.168.1.80
Type:       SNMP      Action : Deny    Port : 1,2

Giga Switch(management)# delete 1
Giga Switch(management)# show

Security rule list is empty now
```

edit [#]: the specific management policy entry. Available range of 1 to 65536.

Syntax:

Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]
[<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2–5, 8
type h, s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

Description: Edits a management policy record.

Argument:

[<name> <value>]	ACL entry name
[<vid> <value>]	VLAN ID
[<ip> <value>]	IP Range
[<port> <value>]	Incoming port
[<type> <value>]	Access type
<action> <value>	a(ccept) or d(eny)

Possible value:

[<name> <value>]	No default and it must be set
[<vid> <value>]	The range is 1–4095 and can be set to any
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any
[<port> <value>]	For example, 1 or 1–8 or 1, 3–5 or any
[<type> <value>]	For example, h(ttp), s(nmp), t(elnet) or any
<action> <value>	No default and it must be set

Example:

```
Giga Switch(management)# edit 1

Giga Switch(management-edit-1)# set name Tom vid 2 ip 192.168.1.30-192.168.1.80
port 1-2 type s action d

Giga Switch(management-edit-1)# show

#: 1
Name: TomVlanID : 2IP : 192.168.1.30-192.168.1.80
Type: SNMPAction : DenyPort : 1, 2
```

show

Syntax: show

Description: Shows the specific management policy record.

Argument: None

Possible value: None

Example:

```
Giga Switch(management)# show

#: 1
Name:Tom   VlanID: 2      IP: 192.168.1.30-192.168.1.80
Type: SNMP   Action: Deny    Port: 1,2
```

poe

set priority

Syntax: set priority <port-range> <priority >

Description: To set the PoE priority on ports.

Argument:

<port-range>：which port(s) you want to set, syntax 1,5-7, available from 1 to 24
<priority>: set priority as 0:Low, 1:Normal, 2:High

Possible value:

<range> : 1 to 24
<priority>: 0, 1 or 2
Example:

```
PSES-2126C(poe)# set priority 1-12 2
```

set state

Syntax: set state <port-range> <state>

Description: To set the PoE state on ports.

Argument:

<port-range>：which port(s) you want to set, syntax 1,5-7, available from 1 to 24

<state>: enable or disable PoE function. 0:Disable 1:Enable

Possible value:

<port-range>：1 to 24

<state>: 0 or 1

Example:

```
PSES-2126C(poe)# set state 11 0
```

show

Syntax: show

Description: To display the PoE status.

Argument: None

Possible value: None

Example:

```
PSES-2126C(poe)# show
Vmain       : 48.3 V
Imain       : 0.0 A
Pconsume    : 0.0 W
Power Limit  : 185 W
Temperature  : 37 'C / 98 'F

Port No                   | 1  2  3  4  5  6  7  8  9  10  11  12
------------------------- | -  -  -  -  -  -  -  -  -  --  --  --
Port On                   | X  X  X  X  X  X  X  X  X  X   X   X
AC Disconnect Port Off    | X  X  X  X  X  X  X  X  X  X   X   X
DC Disconnect Port Off    | X  X  X  X  X  X  X  X  X  X   X   X
Overload Port Off         | X  X  X  X  X  X  X  X  X  X   X   X
Short Circuit Port Off    | X  X  X  X  X  X  X  X  X  X   X   X
Over Temp. Protection     | X  X  X  X  X  X  X  X  X  X   X   X
Power Management Port Off | X  X  X  X  X  X  X  X  X  X   X   X

Port No                   | 13 14 15 16 17 18 19 20 21 22  23  24
------------------------- | -- -- -- -- -- -- -- -- -- --  --  --
Port On                   | X  X  X  X  X  X  X  X  X  X   X   X
AC Disconnect Port Off    | X  X  X  X  X  X  X  X  X  X   X   X
DC Disconnect Port Off    | X  X  X  X  X  X  X  X  X  X   X   X
Overload Port Off         | X  X  X  X  X  X  X  X  X  X   X   X
Short Circuit Port Off    | X  X  X  X  X  X  X  X  X  X   X   X
Over Temp. Protection     | X  X  X  X  X  X  X  X  X  X   X   X
Power Management Port Off | X  X  X  X  X  X  X  X  X  X   X   X
```

```
Port Status  State  Priority Power(W) Current(mA) Class
---- ------ ------- -------- -------- ----------- -----
  1  Normal Enable   Normal    0.0      0         0
  2  Normal Enable   Normal    0.0      0         0
  3  Normal Enable   Normal    0.0      0         0
  4  Normal Enable   Normal    0.0      0         0
  5  Normal Enable   Normal    0.0      0         0
  6  Normal Enable   Normal    0.0      0         0
  7  Normal Enable   Normal    0.0      0         0
  8  Normal Enable   Normal    0.0      0         0
  9  Normal Enable   Normal    0.0      0         0
 10  Normal Enable   Normal    0.0      0         0
 11  Normal Enable   Normal    0.0      0         0
 12  Normal Enable   Normal    0.0      0         0
 13  Normal Enable   Normal    0.0      0         0
 14  Normal Enable   Normal    0.0      0         0
 15  Normal Enable   Normal    0.0      0         0
 16  Normal Enable   Normal    0.0      0         0
 17  Normal Enable   Normal    0.0      0         0
 18  Normal Enable   Normal    0.0      0         0
 19  Normal Enable   Normal    0.0      0         0
 20  Normal Enable   Normal    0.0      0         0
 21  Normal Enable   Normal    0.0      0         0
 22  Normal Enable   Normal    0.0      0         0
 23  Normal Enable   Normal    0.0      0         0
 24  Normal Enable   Normal    0.0      0         0
```

port

clear counter

Syntax: clear counter

Description: Clears all ports' counter (include simple and detail port counter) information.

Argument: None

Possible value: None

Example:

```
Giga Switch (port)# clear counter
```

disable flow-control

Syntax: disable flow-control <range>

Description: Disables the port's flow control function.

Argument: <range>: syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1–8, 1–16, or 1–24

Example:

```
Giga Switch (port)# disable flow-control 6
```

disable state

Syntax: disable state <range>

Description: Disables the port's the communication capability.

Argument: <range>: syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1–8

Example:

```
Giga Switch (port)# disable state 1-2
```

enable flow-control

Syntax: enable flow-control <range>

Description: Enables the port's flow control function.

Argument: <range>: syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1–8

Example:

```
Giga Switch (port)# enable flow-control 3-8
```

enable state

Syntax: enable state <range>

Description: Enables the port's communication capability.

Argument: <range>: syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1–8

Example:

```
Giga Switch (port)# enable state 3-7
```

set speed-duplex

Syntax: set speed-duplex <range> <auto|10half|10full|100half|100full|1Gfull>

Description: Sets up all ports' speed and duplex.

Argument:

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:

<range>: 1 to 8
<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull

Example:

```
Giga Switch(port)# set speed-duplex 5 auto
```

show conf

Syntax: show conf

Description: Display each port's state, speed-duplex, and flow control configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch (port)# show conf
```

show detail-counter

Syntax: show detail-counter <#>

Description: Displays each port's traffic detailed counting number.

Argument: <#>: port, available from 1 to 8

Possible value: <#>:1–8

Example:

```
Giga Switch (port)# show detail-counter 5
```

show sfp

Syntax: show sfp <port>

Description: Displays the SFP module information.

Argument: <port>: The switch's SFP port, available from 7, 8

Possible value: <port>: 7, 8

Example:

```
Giga Switch (port)# show sfp 7

Port 7 SFP information
-------------------------------------------------------------------------
Connector Type:          SFP – LC
Fiber Type:              Multi-mode (MM)
Tx Central Wavelength:   850
Baud Rate:               1G
Vendor OUI:              00:40:c7
Vendor Name:             APAC Opto
Vendor PN:               KM28-C3S-TC-N
Vendor Rev:              0000
Vendor SN:               5425010708
Date Code:               050530
Temperature:             none
Vcc:                     none
Mon1 (Bias) mA:          none
Mon2 (TX PWR):           none
Mon3 (RX PWR):           none
```

show simple-counter

Syntax: show simple-counter

Description: Displays each port's traffic summary counting.

Argument: None

Possible value: None

Example:

```
Giga Switch (port)# show simple-counter
```

show status

Syntax: show status

Description: Displays the port's current status.

Argument: None

Possible value: None

Example:

```
Giga Switch (port)# show status
```

qos

set advance-layer4

Syntax: set advance-layer4 <port-range> <#> <tcp/udp port> <default> <match>

Description: Sets the ports class in Layer 4 qos advanced mode.

Argument:

<port-range>: port range, syntax 1, 5–7, available from 1 to 8
<#>: special UDP/TCP port selection, range: 1–10
<tcp/udp port range>: 0–65535.
<default>: default class (all other TCP/UDP ports). 1: high, 0: low
<match>: special TCP/UDP class. 1: high, 0: low

Possible value:

<port-range>: 1 to 8
<#>: 1–10
<tcp/udp port range>: 0–65535
<default>: 1 or 0
<match>: 1 or 0

Example:

```
Giga Switch(qos)# set advance-layer4 5 2 80 1 0
```

set default

Syntax: set default <class>

Description: Sets the packets' priority class that qos won't affect.

Argument: <class>: class of service setting. 1: high, 0: low

Possible value: <class>: 1 or 0

Example:

```
Giga Switch(qos)# set default 1
```

set diffserv

Syntax: set diffserv <ds-range> <class>

Description: Sets ports' class on IP DiffServe qos.

Argument:

<ds-range>: dscp field, syntax 1, 5–7, available from 0 to 63
<class>: class of service setting. 1: high, 0: low

Possible value:

<ds-range>: 0 to 63
<class>: 1 or 0

Example:

```
Giga Switch(qos)# set diffserv 0-20 1
```

set mode

Syntax: set mode <port/pri_tag/tos/layer4/diffserv>

Description: Sets the switch's qos priority mode.

Argument:

<port>: per port priority
<pri_tag>: vlan tag priority
<tos>: ip tos classification
<layer4>: ip tcp/udp port classification

<diffserv>: ip diffserv classification

Possible value: port/pri_tag/tos/layer4/diffserv

Example:

```
Giga Switch(qos)# set mode port
```

set port

Syntax: set port <range> <class>

Description: Set ports' class on port-based qos.

Argument:

<range> : port range, syntax 1, 5–7, available from 1 to 8
<class> : class of service setting. 1: high, 0: low

Possible value:

<range>: 1 to 8
<class>: 1 or 0

Example:

```
Giga Switch(qos)# set port 1-8 1
```

set pri-tag

Syntax: set pri_tag <port-range> <tag-range> <class>

Description: Sets ports' class on vlan tag-based qos.

Argument:

<port-range>: port range, syntax 1, 5–7, available from 1 to 8
<tag-range>: tag priority level, syntax: 1, 5–7, available from 0 to 7
<class>: class of service setting. 1: high, 0: low

Possible value:

<port-range>: 1 to 8
<tag-range>: 0 to 7
<class>: 1 or 0

Example:

```
Giga Switch(qos)# set pri-tag 1-7 1-2 1
```

set simple-layer4

Syntax: set simple-layer4 <#>

Description: Sets ports class on simple Layer 4 qos mode.

Argument:

<#>: layer-4 configuration mode, valid values are as follows:
0: disable ip tcp/udp port classification
1: down prioritize web browsing, e-mail, FTP, and news
2: prioritize ip telephony (VoIP)
3: prioritize iSCSI
4: prioritize web browsing, e-mail, FTP transfers, and news
5: prioritize streaming Audio/Video
6: prioritize databases (Oracle, IBM DB2, SQL, Microsoft)

Possible value:

<#>:0–6

Example:

```
Giga Switch(qos)# set simple-layer4 2
```

set tos

Syntax: set tos <port-range> <tos-range> <class>

Description: Sets ports class on IP TOS qos.

Argument:

<port-range>: port range, syntax: 1, 5–7, available from 1 to 8
<tos-range>: tos precedence field, syntax 1, 5–7, available from 0 to 7
<class>: class of service setting. 1: high, 0: low

Possible value:

<port-range>: 1 to 8
<tos-range>: 0 to 7
<class>: 1 or 0

Example:

```
Giga Switch(qos)# set tos 1-5 0-3 0
```

show

Syntax: show

Description: Displays the chosen mode's information.

Argument: None

Possible value: None

Example:

```
Giga Switch (qos)# show
IP Diffserv Classification

Default Class:high

DiffServ  Class  DiffServ  Class  DiffServ  Class  DiffServ  Class
--------  -----  --------  -----  --------  -----  --------  ------
   0     high       1     high      2      high      3     high
   4     high       5     high      6      high      7     high
   8     high       9     high     10      high     11     high
   12    high      13     high     14      high     15     high
   16    high      17     high     18      high     19     high
   20    high      21     high     22      high     23     high
   24    high      25     high     26      high     27     high
   28    high      29     high     30      high     31     high
   32    high      33     high     34      high     35     high
   36    high      37     high     38      high     39     high
   40    high      41     high     42      high     43     high
   44    high      45     high     46      high     47     high
   48    high      49     high     50      high     51     high
   2     high      53     high     54      high     55     high
   56    high      57     high     58      high     59     high
   60    high      61     high     62      high     63     high
```

reboot

reboot

Syntax: reboot

Description: Reboots the system.

Argument: None

Possible value: None

Example:

```
Giga Switch# reboot
```

snmp

disable

Syntax:

disable set-ability
disable snmp

Description:

Disable de-activates snmp or set-community.

Argument: None

Possible value: None

Example:

```
Giga Switch(snmp)# disable snmp
Giga Switch(snmp)# disable set-ability
```

enable

Syntax:

enable set-ability
enable snmp

Description: Enable activates snmp or set-community.

Argument: None

Possible value: None

Example:

Giga Switch(snmp)# enable snmp
Giga Switch(snmp)# enable set-ability

set

Syntax:

set get-community <community>
set set-community <community>
set trap <#> <ip> [port] [community]

Description:

Sets 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:

```
Giga Switch(snmp)# set get-community public
Giga Switch(snmp)# set set-community private
Giga Switch(snmp)# set trap 1 192.168.1.1 162 public
```

show

Syntax: show

Description: Displays the SNMP configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(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
```

stp

disable

Syntax: disable

Description: Disables the STP function.

Argument: None

Possible value: None

Example:

```
Giga Switch(stp)# disable
```

enable

Syntax: enable

Description: Enables the STP function.

Argument: None

Possible value: None

Example:

```
Giga Switch(stp)# enable
```

MCheck

Syntax: MCheck <range>

Description: Forces the port to transmit RST BPDUs. (RST is the Rapid Spanning Tree IEEE802.1d standard. BPDU is an abbreviation for Bridge Protocol Data Unit. This is a message type used by bridges to exchange management and control information.)

Argument: <range>: syntax 1, 5–7, available from 1 to 8

Possible value: <range>: 1 to 8

Example:

```
Giga Switch(stp)# Mcheck 1-8
```

set config

Syntax: set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

Description: Sets 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:

```
Giga Switch(stp)# set config 61440 2 20 15
```

set port

Syntax: set port <range> <path cost> <priority> <edge_port> <admin p2p>

Description: Sets 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:

```
Giga Switch(stp)# set port 1-8 0 128 yes auto
```

set version

Syntax: set version <stp|rstp>

Description: Sets up the STP version.

Argument: <stp|rstp>: stp/rstp

Possible value: <stp|rstp>: stp/rstp

Example:

```
Giga Switch(stp)# set version rstp
```

show config

Syntax: show config

Description: Displays the STP configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(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: Displays the STP port information.

Argument: None

Possible value: None

Example:

```
Giga Switch# stp
Giga Switch(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
  4   DISCARDING   2000000    128       No               Auto
  5   DISCARDING   2000000    128       No               Auto
  6   DISCARDING   2000000    128       No               Auto
  7   DISCARDING   2000000    128       No               Auto
  8   DISCARDING   2000000    128       No               Auto
```

show status

Syntax: show status

Description: Displays the STP status.

Argument: None

Possible value: None

Example:

```
Giga Switch(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
```

system

set contact

Syntax: set contact <contact string>

Description: Sets 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:

```
Giga Switch(system)# set contact Taipei
```

set device-name

Syntax: set device-name <device-name string>

Description: Sets 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:

```
Giga Switch(system)# set device-name CR-2600
```

set location

Syntax: set location <location string>

Description: Sets 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:

```
Giga Switch(system)# set location Taipei
```

show

Syntax: show

Description: Displays the switch's basic information.

Argument: None

Possible value: None

Example:

```
Giga Switch(system)# show
Model Name                   : Giga Switch
System Description           : L2 Managed Switch
Location                     :
Contact                      :
Device Name                  : Giga Switch
System Up Time               : 0 Days 3 Hours 28 Mins 17 Secs
Current Time                 : Fri Jan 20 21:37:19 2006
BIOS Version                 : v1.01
Firmware Version             : v2.14
Hardware-Mechanical Version  : v1.01-v1.01
Serial Number                : 030F03000003
Host IP Address              : 192.168.1.1
Host MAC Address             : 00-40-c7-de-00-e7
Device Port                  : UART * 1, TP * 6, Dual-Media Port(RJ45/SFP) * 2
RAM Size                     : 16 M
Flash Size                   : 2 M
```

tftp

set server

Syntax: set server <ip>

Description: Sets the tftp server's IP address.

Argument: <ip>: the IP address of tftp server

Possible value: <ip>: tftp server ip

Example:

```
Giga Switch(tftp)# set server 192.168.3.111
```

show

Syntax: show

Description: Displays the tftp server's information.

Argument: None

Possible value: None

Example:

```
Giga Switch(tftp)# show
Tftp Server : 192.168.3.111
```

time

set daylightsaving

Syntax: set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>

Description: Sets up the daylight saving.

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:

```
Giga Switch(time)# set daylightsaving 3 10/12/01 11/12/01
Save Successfully
```

set manual

Syntax: set manual <YYYY/MM/DD> <hh:mm:ss>

Description: Sets 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:

```
Giga Switch(time)# set manual 2004/12/23 16:18:00
```

set ntp

Syntax: set ntp <ip> <timezone>

Description: Sets up the current time via Network Time Protocol (NTP) server. This is used to synchronize a computer client or server's time to another 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:

```
Giga Switch(time)# set ntp clock.via.net 8
Synchronizing...(1)
Synchronization success
```

show

Syntax: show

Description: Shows the time configuration, including Current Time, NTP Server, Timezone, Daylight Saving, Daylight Saving Start, and Daylight Saving End.

Argument: None

Possible value: None

Example:

```
Giga Switch(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
```

trunk

del trunk

Syntax: del trunk <port-range>

Description: Deletes 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:

```
Giga Switch(trunk)# del trunk 1
```

set priority

Syntax: set priority <range>

Description: Sets up the LACP system priority.

Argument: <range>: available from 1 to 65535

Possible value: <range>: 1 to 65535, default: 32768

Example:

```
Giga Switch(trunk)# set priority 33333
```

set trunk

Syntax: set trunk <port-range> <method> <group> <active LACP>

Description: Sets up the trunk status, including the group number and trunk mode as well as 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 : set the LACP to active mode
  passive : set the LACP to passive mode<active LACP>:

Possible value:

<port-range> : 1 to 8
<method>: static / lacp
<group>: 1–8
<active LACP>: active/passive

Example:

```
Giga Switch(trunk)# set trunk 1-4 lacp 1 active
```

show aggtr-view

Syntax: show aggtr-view

Description: Displays the aggregator list.

Argument: None

Possible value: None

Example:

```
Giga Switch(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: Displays the LACP trunk group's detailed information.

Argument: <aggtr>: aggregator, available from 1 to 8

Possible value: <aggtr>: 1 to 8

Example:

```
Giga Switch(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: Displays the LACP Priority's value.

Argument: None

Possible value: None

Example:

```
Giga Switch(trunk)# show lacp-priority
LACP System Priority : 32768
```

show status

Syntax: show status

Description: Displays each port's aggregator status and settings.

Argument: None

Possible value: None

Example:

```
Giga Switch(trunk)# show status
  Trunk Port Setting                Trunk Port Status
--------------------------          -------------------------
  port    Method    Group           Active LACP   Aggregator   Status
  ====    ======    =====           ===========   ==========   ============
  1       None      0               Active        1            ---
  2       None      0               Active        2            ---
  3       None      0               Active        3            ---
  4       None      0               Active        4            ---
  5       None      0               Active        5            ---
  6       None      0               Active        6            ---
  7       None      0               Active        7            ---
  8       None      0               Active        8            ---
```

vlan

del port-group

Syntax: del port-group <name>

Description: Deletes the port-based vlan group.

Argument: <name>: which vlan group you want to delete

Possible value: <name>: port-vlan name

Example:

```
Giga Switch(vlan)# del port-group VLAN-2
```

del tag-group

Syntax: del tag-group <vid>

Description: Deletes 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:

```
Giga Switch(vlan)# del tag-group 2
```

disable drop-untag

Syntax: disable drop-untag <range>

Description: Does not 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:

```
Giga Switch(vlan)# disable drop-untag 5-8
```

disable sym-vlan

Syntax: disable sym-vlan <range>

Description: Drops 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:

```
Giga Switch(vlan)# disable sym-vlan 5-8
```

enable drop-untag

Syntax: enable drop-untag <range>

Description: Drops 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:

```
Giga Switch(vlan)# enable drop-untag 5-8
```

enable sym-vlan

Syntax: enable sym-vlan <range>

Description: Drops 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:

```
Giga Switch(vlan)# enable sym-vlan 5-8
```

set mode

Syntax: set mode <disable|port|tag|metro|double-tag> [up-link]

Description: Switches VLAN mode, including disable, port-based, tag-based, metro, and double-tag modes.

Argument:

<disable>: vlan disable
<tag>: set tag-based vlan
<port>: set port-based vlan
<metro>: set metro mode vlan
<double-tag>: enable Q-in-Q function
<up-link>: syntax 1, 5–7, available from 7 to 8, only for metro mode vlan

Possible value:

<disable|port|tag|metro|double-tag>: disable,port,tag,metro,double-tag
[up-link]: 25 or 26 or "25,26"

Example:

```
Giga Switch(vlan)# set mode port
```

set port-group

Syntax: set port-group <name> <range>

Description: Adds or edits 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:

```
Giga Switch(vlan)# set port-group VLAN-1 2-5,6,8
```

set port-role

Syntax: set port-role <range> <access|trunk|hybrid> [vid]

Description: Sets Egress rule: configures 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:

```
Giga Switch(vlan)# set port-role 5 hybrid 6
```

set pvid

Syntax: set pvid <range> <pvid>

Description: Sets the vlan pvid.

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:

```
Giga Switch(vlan)# set pvid 3,5,6-8 5
```

set tag-group

Syntax: set tag-group <vid> <name> <range> <#>

Description: Adds or edits 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:

```
Giga Switch(vlan)# set tag-group 2 VLAN-2 2-5,6,8 0
```

show group

Syntax: show group

Description: Displays the vlan mode and vlan group.

Argument: None

Possible value: None

Example:

Giga Switch(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

2)    Vlan Name   : VLAN-2
      Vlan ID     :  2
      Sym-vlan    : Disable
      Member      : 2 3 4 5 6
```

show pvid

Syntax: show pvid

Description: Displays pvid, Ingress/Egress rule.

Argument: None

Possible value: None

Example:

```
Giga Switch(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         -
```

vs

disable

Syntax: disable

Description: Disables the virtual stack.

Argument: None

Possible value: None

Example:

```
Giga Switch(vs)# disable
```

enable

Syntax: enable

Description: Enables the virtual stack.

Argument: None

Possible value: None

Example:

```
Giga Switch(vs)# enable
```

set gid

Syntax: set gid <gid>

Description: Sets the group id.

Argument: <gid>:Group ID

Possible value: <gid>:a–z, A–Z, 0–9

Example:

```
Giga Switch(vs)# set gid group1
```

set role

Syntax: set role <master|slave>

Description: Sets the role.

Argument:

<master|slave>:
master: act as master, slave: act as slave

Possible value:

<master|slave>: master or slave

Example:

```
Giga Switch(vs)# set role master
```

show

Syntax: show

Description: Displays the virtual stack's configuration.

Argument: None

Possible value: None

Example:

```
Giga Switch(vs)# show
Virtual Stack Config:
State    : Enable
Role     : Master
Group ID : group1
```

6. Troubleshooting

6.1 Resolving a No Link Condition

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.

6.2 Problems/Solutions

Problem: Computer A can connect to Computer B but cannot connect to Computer C through the switch.

Solution #1: The network device connected to Computer C may fail to work. Check Computer C's Link/Act LED status. Try another network device on this connection.

Solution #2: Computer C's network configuration may be incorrect. Verify the computer's network configuration.

Problem: The uplink connection function fails to work.

Solution #1: The connection ports on another switch must be connection ports. Make sure connection ports are used on that switch.

Solution #2: Verify that the uplink function is enabled.

Problem: The console interface doesn't appear on the console port connection.

Solution#1: The COM port default parameters are: baud rate: 57600; Data bits: 8; Parity bits: None; Stop bit: 1; Flow control: None. Check the COM port values in the terminal program. If the parameters are changed, set the COM configuration to the default settings.

Solution #2: Make sure that the RS-232 cable is securely connected to the switch's console port and the PC's COM port.

Solution #3: Make sure the PC's COM port is enabled.

Problem: How do I configure the switch?

Solution: "Hyperterm" is the terminal program in Windows 95, 98, or Windows NT®. You can also use any other terminal programs in Linux® or UNIX® to configure the switch. Refer to terminal program's user guide. The COM port parameters (baud rate, data bits, parity bits, flow control) must be the same as the switch's console port setting.

6.3 Calling Black Box

If you determine that your switch is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

6.4 Shipping and Packaging

If you need to transport or ship your 24-Port 10/100BASE-TX L2 Managed PoE Switch with 2 SFP Dual Media Ports:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the 24-Port 10/100BASE-TX L2 Managed PoE Switch with 2 SFP Dual Media Ports for repair, make sure you include everything that came in the original package. Before you ship, contact Black Box to get a Return Authorization (RA) number.