LGB2118A
LGB2124A

BLACK BOX®

Gigabit Smart Switch Eco Fanless

Supports http and SNMP interface for switch management.

- The LGB2118A has (16) 10-/100-/1000-Mbps TP ports and (2) Gigabit SFP ports.
- The LGB2124A has (20) 10-/100-/1000-Mbps TP ports and (4) Gigabit TP/SFP dual-media ports.

Contact Information

Order toll-free in the U.S. or for FREE 24/7 technical support: Call 877-877-BBOX
(outside U.S. call 724-746-5500)
www.blackbox.com • info@blackbox.com

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Intel is a registered trademark of Intel Corporation.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation.

Novell and NetWare are registered trademarks of Novell, Inc.

Xerox is a registered trademark of Xerox Corporation.

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

We're here to help! If you have any questions about your application
or our products, contact Black Box Tech Support at **877-877-2269**
or go to **blackbox.com** and click on "Talk to Black Box."
You'll be live with one of our technical experts in less than 60 seconds.

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart 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 radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

CAUTION:

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

To protect your device, always: Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device. Pick up the device by holding it on the left and right edges only.

If you need to connect an outdoor device to this switch with cable, add an arrestor on the cable between the outdoor device and this switch.

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

Table of Contents

1. Specifications 7
   - 1.1 General 7
   - 1.2 Management Software Specifications 8

2. Overview 9
   - 2.1 Introduction 9
   - 2.2 Features 9
   - 2.3 What's Included 10
   - 2.4 Hardware Description 11
     - 2.4.1 18-Port Gigabit Smart Switch Eco Fanless (LGB2118A) 11
     - 2.4.2 24-Port Gigabit Smart Switch Eco Fanless (LGB2124A) 12

3. Installation 15
   - 3.1 Starting Up the Switch 15
     - 3.1.1 Hardware and Cable Installation 15
     - 3.1.2 Cabling Requirements 16
     - 3.1.3 Configuring the Management Agent of the Gigabit Smart Switch Eco Fanless 20
     - 3.1.4 Address Assignment 21
   - 3.2 Typical Applications 24

4. Basic Concepts and Management 27
   - 4.1 Ethernet 27
   - 4.2 Logical Link Control (LLC) 28
   - 4.3 Media Access Control (MAC) 30
     - 4.3.1 MAC Addressing 30
     - 4.3.2 Ethernet Frame Format 30
   - 4.4 Flow Control 33
   - 4.5 How Does a Switch Work? 37
   - 4.6 Virtual LAN 38
   - 4.7 Link Aggregation (LGB2118A Only) 43

5. Operation of Web-Based Management 45
   - 5.1 Web Management Home Overview 45
   - 5.2 Configuration 47
     - 5.2.1 System Information 48
     - 5.2.2 Port Configuration 49
     - 5.2.3 VLAN Mode Configuration 51
     - 5.2.4 VLAN Group Configuration 51
     - 5.2.5 VLAN Port Isolation Configuration 54
     - 5.2.6 Aggregation (LGB2118A Only) 55
     - 5.2.7 IGMP Snooping 56
     - 5.2.8 Mirroring Configuration 56
     - 5.2.9 SNMP 57
     - 5.2.10 Loop Detection 59
     - 5.2.11 Broadcast Storm Protection 60
     - 5.2.12 Quality of Service (QoS) Configuration 62
   - 5.3 Monitoring 64
     - 5.3.1 Statistics Overview 64
     - 5.3.2 Detailed Statistics 65
     - 5.3.3 IGMP Status 67

5.3.4 Ping Status 68
5.4 Maintenance 69
5.4.1 Warm Restart 69
5.4.2 Factory Default 70
5.4.3 Software Upgrade 70
5.4.4 Configuration File Transfer 70
5.4.5 Logout 71
6. Troubleshooting 72
6.1 Resolving Line Condition 72
6.2 Questions and Answers 72
6.3 Contacting Black Box 72
6.4 Shipping and Packaging 72
Appendix. MIB 73

1. Specifications

1.1 General

Aging — Auto-aging with programmable inter-age time

Auto-Negotiation — Supports auto-negotiation for configuring speed and duplex mode

Blocking Prevention — Supports Head of Line (HOL) blocking prevention

Buffer Memory — Embedded 512 KB frame buffer

Cable Type and Maximum Length — Twisted-Pair (TP): CAT5 UTP cable, up to 328 ft. (100 m);
Fiber: 1000BASE-SX: up to 721.7/902.2/1640.4/1804.5 ft. (220/275/500/550 m), depending on multimode fiber type,
1000BASE-LX: Single-mode fiber, up to 6.2/18.6/31.1 mi. (10/30/50 km)

Filtering — Supports broadcast storm filtering

Flow Control — IEEE 802.3x flow control for full-duplex ports; collision-based backpressure for half-duplex ports

Forwarding/Filtering Rate (Packets per Second [PPS]) — 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

Management — Web-based management provides the ability to completely manage the switch from any Web browser

Network Interface —

Table 1-1. Network interface.

Configuraton	Mode	Connector/Port Number
10/100/1000 Mbps Gigabit TP	Auto-negotiation	LGB2118A: TP (RJ-45) 1–16 LGB2124A: TP (RJ-45) 1–24
1000BASE-SX Gigabit fiber	1000 FX	LGB2118A: *SFP 9, 10 LGB2124A: **SFP 21–24
1000BASE-LX Gigabit fiber	1000 FX	LGB2118A: *SFP 9, 10 LGB2124A: **SFP 21–24

*NOTE: *Ports 9 and 10 on the LGB2118A SFP fiber ports and **Ports 21–24 on the LGB2124A are TP/SFP fiber dual media ports with auto detection function. Optional SFP modules support LC transceivers.*

Priority Queueing — 802.1p Class of Service with 2-level priority queueing

Programmable Maximum Ethernet Frame Length — 1518 to 9600 bytes jumbo frames

Self-Learning and Address Recognition Mechanism — Enables forwarding rate at wire speed

Sniffer Function — Supported

Standards Compliance — IEEE 802.3/802.3ab/802.3z/802.3u/802.3x, IEEE 802.1ad QinQ;
LGB2118A also has: 802.3ad LACP

Store-and-Forward — Non-blocking store-and-forward shared memory Web Smart switched

Transmission Mode — 10-/100-Mbps support full- or half-duplex, 1000-Mbps support full-duplex only

Transmission Speed — 10-/100/1000-Mbps for TP, 100-/1000-Mbps for Fiber

Trunking — LGB2118A Only: Supports port trunking with flexible load distribution and failover function

VLAN — Supports Port-based VLAN and Tag-based (IEEE 802.1Q) VLAN

Connectors — LGB2118A: (16) 10-/100-/1000-Mbps Gigabit Ethernet (TP) switching ports, (2) Gigabit SFP fiber module ports;
LGB2124A: (20) 10-/100-/1000-Mbps Gigabit Ethernet (TP) switching ports, (4) Gigabit TP/SFP fiber dual media ports with auto detection function

Indicators — LGB2118A: (33) LEDs: (1) System Power, (16) LINK/ACT and (16) SPD LEDs for 10/100/1000 M TP Ports 1 to 16, (2) LINK/ACT and (2) SPD LEDs for 1000 M SFP fiber Ports 19 to 20;
LGB2124A: (49) LEDs: (1) System Power, (24) LINK/ACT and (24) SPD LEDs for 10/100/1000 M TP Ports 1 to 24, (4) LINK/ACT and (4) SPD LEDs for 1000 M SFP fiber Ports 21 to 24

Power — Input: 100–240 VAC, 50-60 Hz;
Consumption: 20 W

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

Humidity Tolerance — 10 to 90%

Size — LGB2118A: 1.45"H x 8.57"W x 5.86"D (3.7 x 21.8 x 14.9 cm);
LGB2124A: 1.7"H x 17.4"W x 6.7"D (4.4 x 44.2 x 17 cm)

Weight — LGB2118A: 4.63 lb. (2.1 kg);
LGB2124A: 5.51 lb. (2.5 kg)

1.2 Management Software Specifications

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

Quality of Service (QoS) — Referred to as Class of Service (CoS) by the IEEE 802.1P standard

System Configuration — Auto-negotiation support on 10/100/1000BASE-TX ports, Web browser can set transmission speed (10-/100-/1000-Mbps) and operation mode (Full-/Half-duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection

Trunk Function — Port trunk connections allowed

VLAN Function — Port-Base/802.1Q-Tagged, allows up to 10 active VLANs in one switch

Web Browser Support — Based on HTTP Server

2. Overview

2.1 Introduction

The Gigabit Smart Switch Eco Fanless is a standard switch that meets all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications. The LGB2118A switch has (16) 10-/100-/1000-Mbps TP ports and (2) Gigabit SFP fiber transceiver slots. The LGB2124A switch has (20) 10/100/1000Mbps TP ports and (4) Gigabit dual media TP/SFP transceiver slots. Both switches support http and SNMP interfaces for switch management. The network administrator can logon to the switch to monitor, configure, and control each port's activity. In addition, the switch implements Quality of Service (QoS), VLAN, and Trunking.

Increase power saving support or reduce power consumption with power management.

The LGB2118A switch's Ports 17–18 support SFP fiber modules (with LC connectors). The LGB2124A switch's Ports 21, 22, 23, and 24 include two types of media—TP and SFP Fiber (with LC connectors). The four combo ports on the LGB2124A support 10-/100-/1000-Mbps TP or 1000-Mbps SFP Fiber with auto-detection. A 1000-Mbps SFP Fiber transceiver is used for high-speed connection expansion.

Table 2-1. 1000-Mbps SFP fiber transceivers.

Product Code	Description
LFP411	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 850-nm Multimode, LC, 300 m
LFP412	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 1310-nm Multimode, LC, 2 km
LFP413	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 1310-nm Single-Mode, LC, 10 km
LFP414	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 1310-nm Single-Mode, LC, 30 km

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

2.2 Features

The 18- or 24-Port Gigabit Smart Switch Eco Fanless, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

- Quality of Service (QoS): The switch supports 802.1p VLAN tag priority and DSCP on Layer 3 of the network framework.
- VLAN: Supports Port-based VLAN, IEEE 802.1Q Tag VLAN. LGB2118A supports 18 active VLANs and LGB2124A supports 24 active VLANs and VLAN IDs 1–4094.
- Port Trunking (LGB2118A Only): Allows one or more links to be aggregated together to form a link aggregation group by the static setting.
- Power Saving: The switch uses two proprietary power management techniques that detect when the client is idle and also detect the cable length automatically. This saves the switch power and reduces the power consumption.
- The LGB2118A has (16) and the LGB2124A has (20) 10-/100-/1000-Mbps Auto-negotiation Gigabit Ethernet TP ports.
- The LGB2118A has (2) SFP fiber module ports and the LGB2124A has (4) 10-/100-/1000-Mbps TP or 1000-Mbps SFP Fiber dual media autosensing ports.
- Includes 512-KB on-chip frame buffer.
- Supports 9-KB jumbo frames.
- Programmable classifier for QoS (Layer 2/Layer 3).
- Provides 8K MAC address and supports VLAN ID (1–4094).
- Features per-port shaping, policing, and Broadcast Storm Control.

- Saves power using two proprietary power management techniques.
- Includes IEEE 802.1Q-in-Q nested VLAN support.
- Uses full-duplex flow control (IEEE 802.3x) and half-duplex backpressure.
- Features extensive front-panel diagnostic LEDs: For LGB2118A: System: Power, TP Port 1–16: LINK/ACT, 10-/100-/1000-Mbps, SFP Port 17 and 18: SFP (LINK/ACT); For LGB2124A: System: Power, TP Port 1–24: LINK/ACT, 10-/100-/1000-Mbps, SFP Port 21, 22, 23, and 24: SFP (LINK/ACT)
- Includes these management features:

- Port status and easy port configuration.
- Per port traffic monitoring counters.
- Provides a snapshot of the system information when you login.
- Port mirror function.
- Static trunk function.
- Supports 802.1Q VLAN.
- Supports user management and limits login to one user.
- Maximum packet length can be up to 9600 bytes for jumbo frame applications.
- Broadcasting Suppression prevents a suspended or crashed network.
- Sends the trap event while monitored events are happening.
- Supports default configuration, which can be restored to overwrite the current configuration via Web UI and/or by pressing the switch's Reset button.
- Hot-pluggable SFP modules.
- Supports Quality of Service (QoS) for real-time applications based on the information taken from Layer 2 to Layer 3.
- Use the built-in Web-based management instead of the CLI interface, providing a more convenient GUI for the user.

2.3 What's Included

Before you install the switch, verify that the package contains the following:

- 18- or 24-Port Gigabit Smart Switch Eco Fanless
- Mounting Accessory (for 19" Rack Shelf)
- AC Power Cord

To access this user manual PDF file, go to ftp://ftp.blackbox.com/anonymous/manuals/L/LGB2118A_rev1.pdf

If anything is missing or damaged, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

You might also need:

- SFP Modules (optional, LFP411, LPF412, LFB413, or LFP414, described in Table 2-1)

2.4 Hardware Description

2.4.1 18-Port Gigabit Smart Switch Eco Fanless (LGB2118A)

Figures 2-1 ad 2-2 show the front and back panels of the switch. Table 2-2 describes its components. Table 2-3 describes the LEDs in detail.

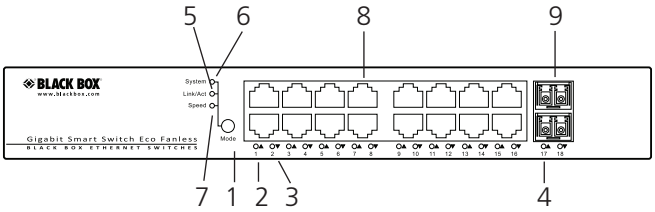


Figure 2-1. LGB2118A front panel.

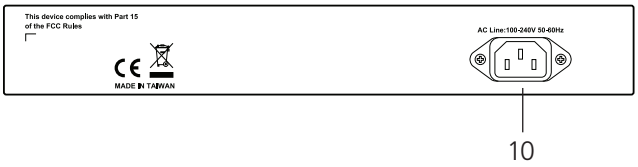


Figure 2-2. LGB2118A back panel.

Table 2-2. LGB2118A components.

Number	Component	Description
1	(1) Mode button	Switches between what is being displayed by LEDs.
2	(16) TP port status LEDs	For details, see Table 2-3.
3	(16) TP port speed LEDs	For details, see Table 2-3.
4	(2) SFP port status LEDs	For details, see Table 2-3.
5	Link/Act LED	Lit to show switch is in Link/Act mode.
6	System LED	Lit to show switch is in System mode.
7	Speed LED	Lit to show switch is in Speed mode.
8	(16) 10/100/1000BASE-T RJ-45 ports	10-/100-/1000-Mbps Ethernet ports
9	(2) 100/1G SFP ports	Connect up to two SFP links.
10	(1) AC power socket (on back of unit)	IEC-320 power connection.
11	(1) Power LED* (on left side of unit)	Lights when power is on.

*Not shown in Figure 2-1 or 2-2.

Table 2-3. LGB2118A LED functions.

LED	Color	Function
(1) System Power LED	Green	Lit when power is on.
(16) LINK/ACT LEDs	Steady green Blinking green	Lit when connection with remote device is good. Blinks when any traffic is present.
(16) SPD LEDs	Green Yellow Off	Green when TP link is on 1000 Mbps speed. Yellow when TP link is on 10/100 Mbps speed. Off when no link is present.
1000SX/LX Gigabit fiber port 17, 18 (2) LINK/ACT LEDs	Green Yellow Off	Green when SFP link is on 1000 Mbps speed. Yellow when SFP link is on 100 Mbps speed. Off when no link is present.

2.4.2 24-Port Gigabit Smart Switch Eco Fanless (LGB2124A)

Figures 2-3 and 2-4 show the front and back panels of the switch. Table 2-4 describes its components. Table 2-5 describes the LEDs in detail.

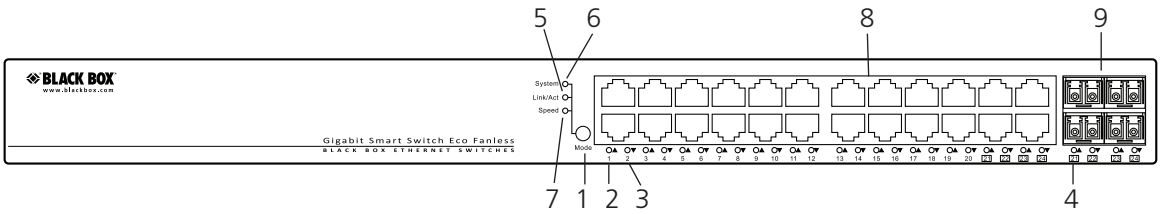


Figure 2-3. LGB2124A front panel.

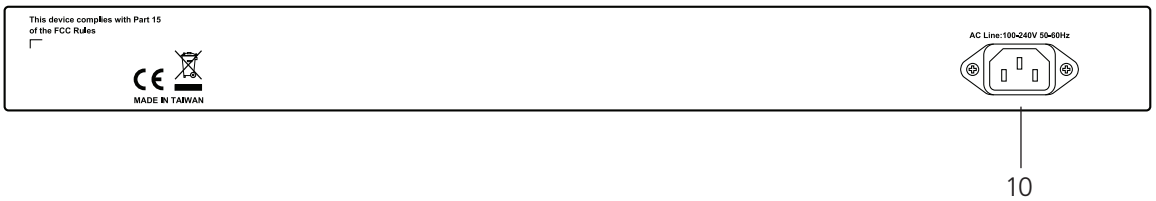


Figure 2-4. LGB2124A back panel.

Table 2-4. LGB2124A components.

Number	Component	Description
1	(1) Mode button	Switches between what is being displayed by LEDs.
2	(24) TP port status LEDs	For details, see Table 2-5.
3	(24) TP port speed LEDs	For details, see Table 2-5.
4	(4) SFP port status LEDs	For details, see Table 2-5.
5	Link/Act LED	Lit to show switch is in Link/Act mode.
6	System LED	Lit to show switch is in System mode.
7	Speed LED	Lit to show switch is in Speed mode.
8	(24) 10/100/1000BASE-T RJ-45 ports	10-/100-/1000-Mbps Ethernet ports
9	(4) 100/1G SFP ports	Connect up to two SFP links.
10	(1) AC power socket (on back of unit)	IEC-320 power connection.
11	(1) Power LED* (on left side of unit)	Lights when power is on.

*Not shown in Figure 2-3 or 2-4.

Table 2-5. LGB2124A LED functions.

LED	Color	Function
(1) System Power LED	Green	Lit when +3.3 V power is on.
(20) LINK/ACT LEDs	Steady green Blinking green	Lit when connection with remote device is good. Blinks when any traffic is present.
(20) SPD LEDs	Green Yellow Off	Green when TP link is on 1000 Mbps speed Yellow when T link is on 10/100 Mbps speed. Off when no link is present.
1000SX/LX Gigabit fiber port 21, 22, 23, 24 (2) LINK/ACT LEDs	Green Yellow Off	Green when SFP link is on 1000 Mbps speed Yellow when SFP link is on 100 Mbps speed. Off when no link is present.

Optional Modules for LGB2118A and LGB2124A

On the LGB2118A switch, Ports 17–18 are SFP fiber module ports. On the LGB2124A, Ports 21–24 include two types of media—TP and SFP Fiber (with LC connectors); they support 10-/100-/1000-Mbps TP or 1000-Mbps SFP Fiber with auto-detect function. Use a 1000-Mbps SFP Fiber transceiver for high-speed connection expansion; choose from four optional SFP types listed in Table 2-6.

Table 2-6. 1000-Mbps SFP fiber transceivers.

Product Code	Description
LFP411	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 850-nm Multimode, LC, 300 m
LFP412	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 1310-nm Multimode, LC, 2 km
LFP413	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 1310-nm Single-Mode, LC, 10 km
LFP414	SFP, 1.25-Gbps Fiber with Extended Diagnostics, 1310-nm Single-Mode, LC, 30 km

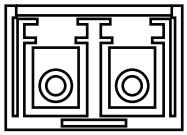


Figure 2-5. Front view of 1000BASE-SX/LX LC, SFP Fiber Transceiver.

3. Installation

3.1 Starting Up the Switch

This section will give users a quick start for:

- Hardware and cable installation.
- Management station installation.
- Software booting and configuration.

3.1.1 Hardware and Cable Installation

CAUTION:

Wear a grounding device to avoid damage from electrostatic discharge.

Make sure that power switch is OFF before you insert the power cord into the power source.

Installing Optional SFP Fiber Transceivers to the Gigabit Smart Switch Eco Fanless

NOTE: If you have no modules, please skip this section.

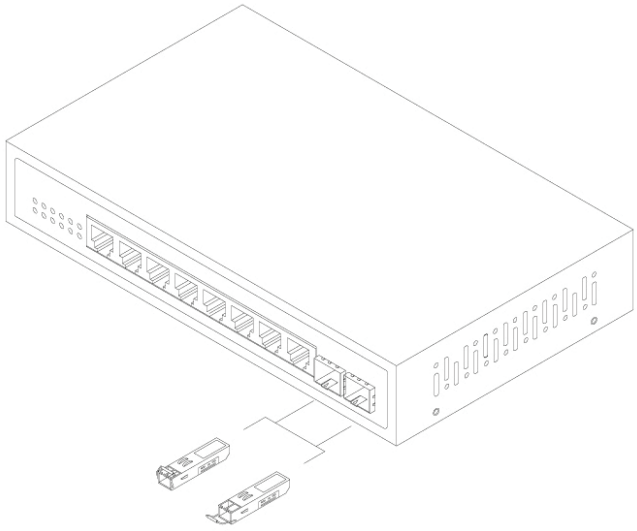


Figure 3-1. Installing an optional SFP fiber transceiver.

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.

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. Install the media cable for network connection.
4. Repeat the above steps, as needed, for each module to be installed into slot(s).
5. Power ON the switch after the above procedures are done.

TP Port and Cable Installation

The switch's TP ports support MDI/MDI-X auto-crossover, so you can use straight-through or crossover cable.

Connect CAT5 grade RJ-45 TP cable to a TP port of the switch and connect the other end to a network-aware device such as a workstation or a server.

Repeat the above steps, as needed, to connect each RJ-45 port to a Gigabit 10/100/1000 TP device.

The switch is 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. The switch's ports are hot-swappable, so you can plug in devices or SFPs while the switch is powered on. After the power is on, all LED indicators will light on and then all will go off except for the power LED, which remains on. This resets the system.

Firmware Loading

After resetting, the bootloader will load the firmware into the memory. It will take about 30 seconds; after that, all the LEDs on the switch will flash once while the switch performs a self-test and is ready to use.

3.1.2 Cabling Requirements

For successful installation and good network performance, follow these cabling requirements. Low-quality cables can cause the switch to malfunction.

Cabling Requirements for TP Ports

For Fast Ethernet TP network connections, use CAT5 or CAT5e cable that's up to 328 feet (100 m) long.

For Gigabit Ethernet TP network connections, use CAT5 or CAT5e cable that's up to 328 feet (100 m) long.

We recommend using CAT5e cable.

Cabling Requirements for 1000SX/LX SFP Modules

There are two categories of fiber: multimode (MM) and single-mode (SM). Single-mode cable is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX.

The following table lists the types of fiber that the switch supports. If you don't see the cable type you need, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

Table 3-1. Fiber supported by the switch.

Fiber cable type	Multimode Fiber Cable and Modal Bandwidth			
IEEE 802.3z Gigabit Ethernet 1000BASE-SX, 850 nm	Multimode 62.5-/125-µm		Multimode 50-/125-µm	
	Modal Bandwidth	Distance	Modal Bandwidth	Distance
	160 MHz-km	721.7 ft. (220 m)	400 MHz-km	1640.4 ft. (500 m)
	200 MHz-km	902.2 ft. (275 m)	500 MHz-km	1804.5 ft. (550 m)
1000BASE-LX/LHX/ZX	Single-mode fiber 9/125 m			
	Single-mode transceiver 1310 nm, 6.2 mi. (10 km), or 18.6 mi. (30 km)			
	Single-mode transceiver 1550 nm, 31.1 mi. (50 km)			
1000BASE-LX single fiber (BiDi SC)	Single-mode 12.4 mi. (20 km)		TX (Transmit) 1310 nm	
			RX (Receive) 1550 nm	
	Single-mode 12.4 mi. (20 km)		TX (Transmit) 1550 nm	
			RX (Receive) 1310 nm	

Switch Cascading Topology

The switch cascading topology takes the delay time into account.

Theoretically, the switch partitions the collision domain for each port in switch cascading so that you can uplink an unlimited number of switches. In practice, the network extension (cascading levels and overall diameter) must follow the constraints of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications. The limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and the timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP (for LGB2118A only), and so on.

The fiber, TP cables, and devices' bit-time delay (round trip) are as follows:

Table 3-2. Fiber, TP cables, and devices' bit-time delay (round trip).

1000BASE-X TP Fiber		100BASE-TX TP		100BASE-FX Fiber	
Round-trip delay: 4096		Round-trip delay: 512			
CAT5 TP wire	11.12/m	CAT5 TP wire	1.12 m	Fiber cable	1.0/m
Fiber cable	10.10/m	TP to fiber converter: 56			
Bit time unit	1 ns (1 sec/1000M)	Bit time unit: 0.01 s (1 sec/.100 Megabit			

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

Typical Network Topology in Deployment

A hierarchical network with minimum levels of switches may reduce the timing delay between the server and the client station. This approach will minimize the number of switches in any one path, lower the possibility of network loops, and 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 connecting the Server/Host to the Level 1 switch. This is general advice if no VLAN or other special requirements apply.

Case 1: All switch ports are in the same local area network. Every port can access each other (see Figure 3-2).

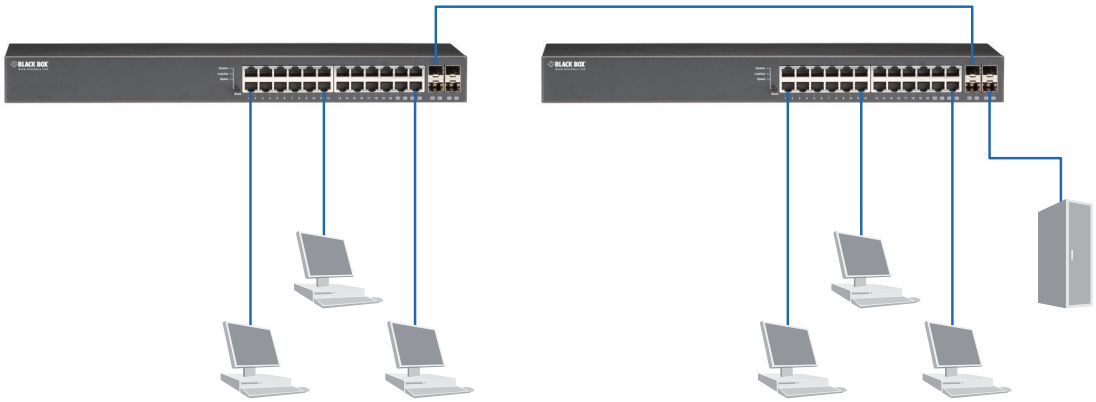


Figure 3-2. No VLAN configuration diagram.

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

Here, VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. See Figure 3-3.

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

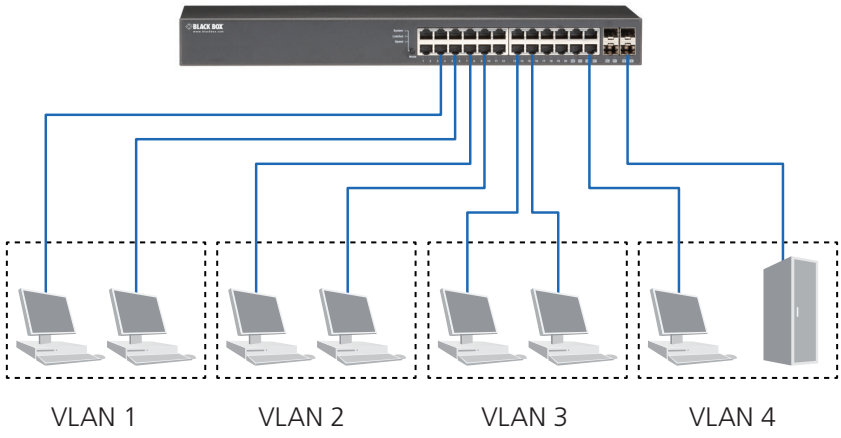


Figure 3-3. Port-based VLAN diagram.

1. The same VLAN members cannot be in different switches.

2. Every VLAN member cannot access each other's VLAN members.

3. The switch manager has to assign different names for each VLAN group at one switch.

Case 2b: Port-based VLAN (See Figure 3-4).

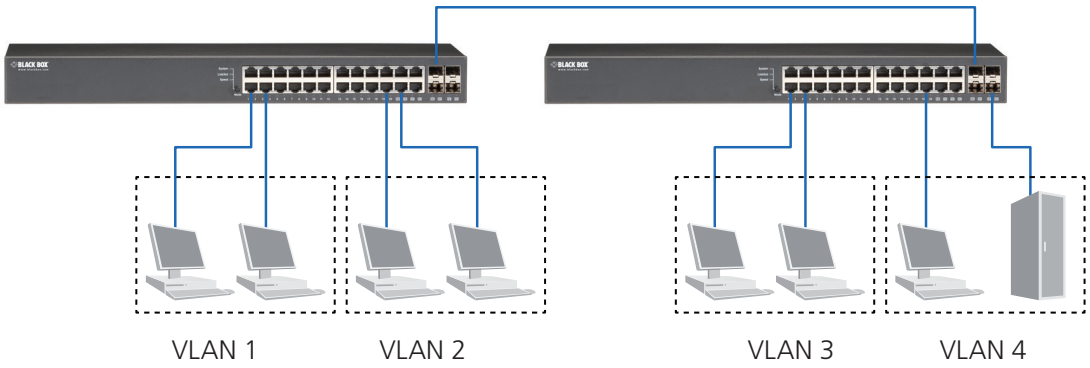


Figure 3-4. Port-based VLAN diagram.

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

Case 3a: The same VLAN members can be at different switches with the same VID. (See Figure 3-5).

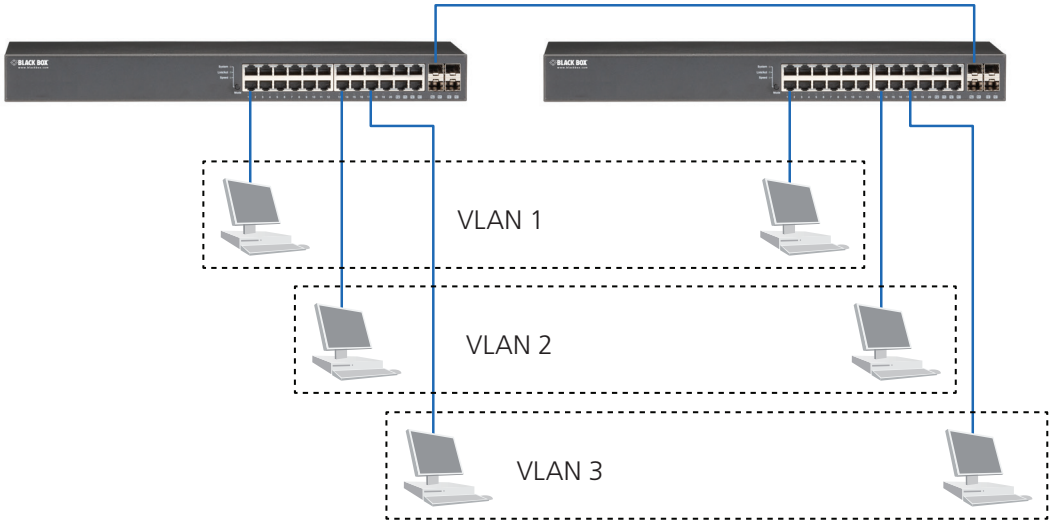


Figure 3-5. Attribute-based VLAN diagram.

3.1.3 Configuring the Management Agent of the Gigabit Smart Switch Eco Fanless

Via the Web, the switch can set up the management function. Use any one of them to monitor and configure the switch.

Configuring the Management Agent of the Gigabit Smart Switch Eco Fanless through the Ethernet Port

There are two ways to configure and monitor the switch through the switch's Ethernet port. They are Web browser and SNMP manager. The user interface for the SNMP manager is management software-dependent and is not described in this manual. Using the Web-based UI for the switch is described here.

24-Port Gigabit Smart Switch Eco Fanless

Default IP setting:

IP = 192.168.1.1

Subnet Mask = 255.255.255.0

Default Gateway = 192.168.1.254

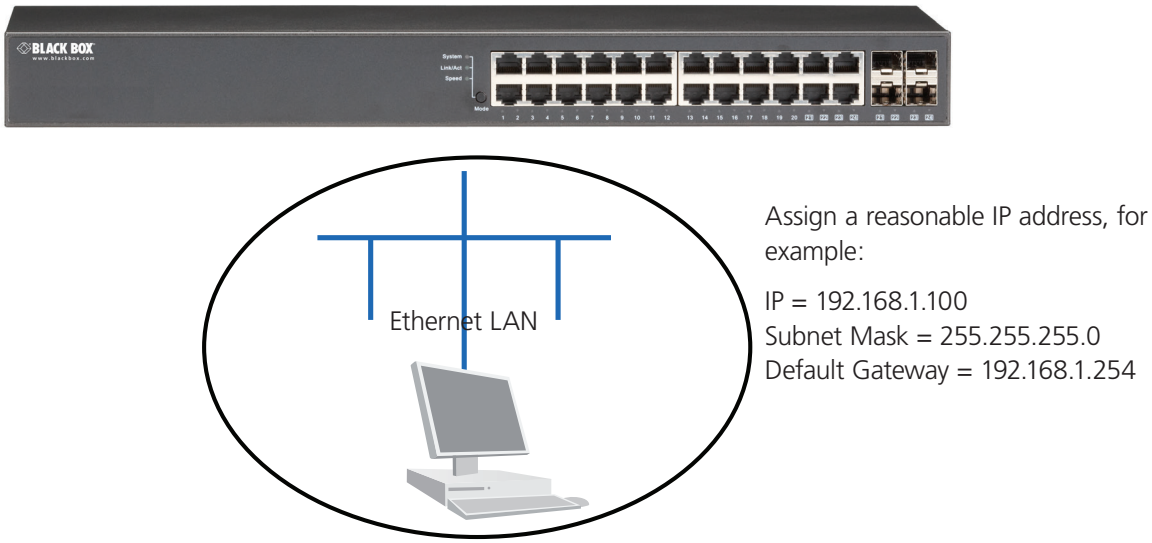


Figure 3-6. Gigabit Smart Switch Eco Fanless.

Managing the Gigabit Smart Switch Eco Fanless through the Ethernet Port

Before you communicate with the switch, you must first configure its IP address or know the IP address of the switch. Then, follow the procedures described next.

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

NOTE: If a PC directly connects to the switch, you have to set up the same subnet mask between them. However, the subnet mask may be different for the PC in the remote site. See Figure 3-6 for default IP address information of the 24-Port Gigabit Smart Switch Eco Fanless.

2. Run a Web browser and follow the menu. The default username is "admin" and the default password is blank (just press Enter)..

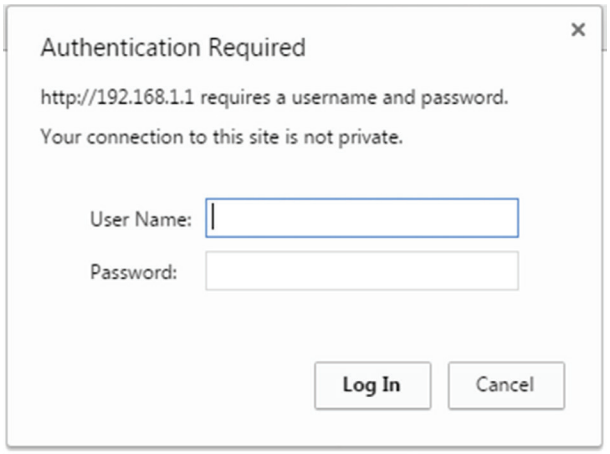


Figure 3-7. The Login screen for the Web.

3.1.4 Address Assignment

For IP address configuration, there are four parameters that need to be filled in. They are IP address, Subnet Mask, Default Gateway, and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure is shown in Figure 3-8. It is split into predefined address classes or categories.

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

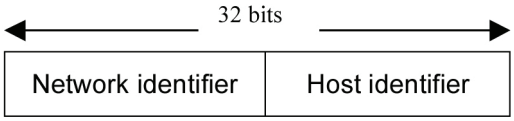


Figure 3-8. IP address structure.

The switch divides the IP address into three classes, class A, class B, and class C. The rest of the IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/10. Each class has its address range (described next).

Class A:

A Class A address is less than 126.255.255.255. The switch can define a total of 126 networks because the address 0.0.0.0 is reserved for a default route and 127.0.0.0/8 is reserved for a loopback function.

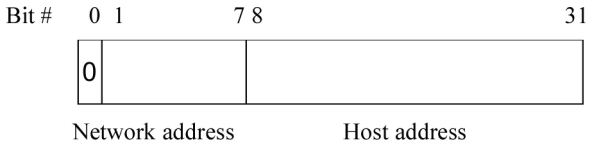


Figure 3-9. Class A IP address.

Class B:

A Class B 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 (2^{14})/16 networks able to be defined with a maximum of 65534 (2^{16} –2) hosts per network.

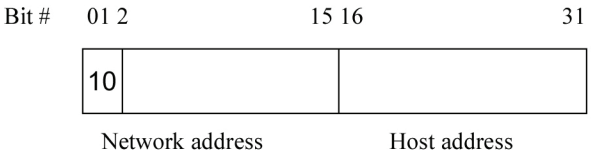


Figure 3-10. Class B IP address.

Class C:

A Class C 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. There are 2,097,152 (2^{21})/24 networks able to be defined with a maximum of 254 (2^{8} –2) hosts per network.

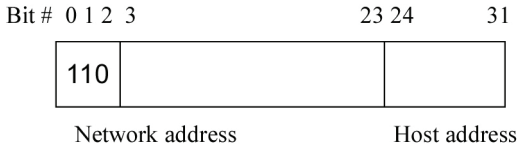


Figure 3-11. Class C IP address.

Class D and E:

Class D is a class with first 4 MSB (most significant bit) set to 1-1-1-0 and is used for IP multicast. See also RFC 1112.

Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to the Internet Assigned Numbers Authority (IANA), there are three specific IP address blocks reserved that can be used for extending an internal network. We call it a private IP address (described 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

Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

A 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 in the network prefix and the host address is based on bits. It uses IP addresses more efficiently and makes it easy to manage an IP network.

For a class B network, 128.1.2.3, the default subnet mask may be 255.255.0.0, with the first two bytes all 1s. This means more

than 60,000 nodes with a flat IP address will be in the same network. It's too large to manage practically. If we divide it into smaller networks by extending the network prefix from 16 bits to, say 24 bits, the switch uses its third byte to subnet this class B network. The subnet mask is 255.255.255.0, in which each bit of the first three bytes is 1. The first two bytes identify the class B network, the third byte identifies 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 that have the host number as all zeros and all ones. For example, for an IP address 128.1.2.128, the reserved IP will have all 0s for the network itself, and all 1s for IP broadcast.

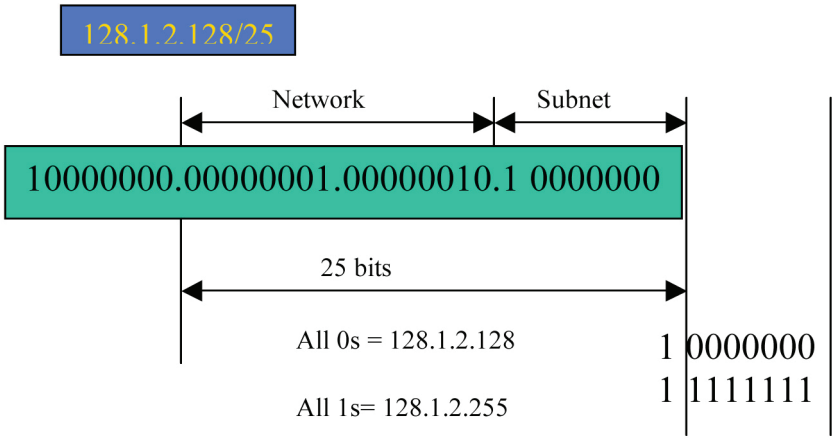


Figure 3-12. Subnet mask.

In this diagram, the subnet mask is 25 bits long, 255.255.255.128, and contains 126 members in the subnetted network. The length of the network prefix equals the number of the bit with 1s in that subnet mask. This enables the switch to count the number of IP addresses matched. The following table shows the results.

Table 3-3. Number of IP addresses matched.

Prefix Length	No. of IP matched	No. of Addessable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

According to the scheme above, a subnet mask 255.255.255.0 will partition a network as class C. A maximum of 254 effective nodes will exist in this sub-netted network, and it is considered a physical network in an autonomous network. The network IP address might be 168.1.2.0.

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

For different network applications, the subnet mask may be 255.255.255.240. It is a small network that accommodates a maximum of 15 nodes in the network.

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. Basically, it is a routing policy.

To assign an IP address to the switch, check what the IP address is for the network that will be connected to the switch. Use the same network address and append your host address to it.

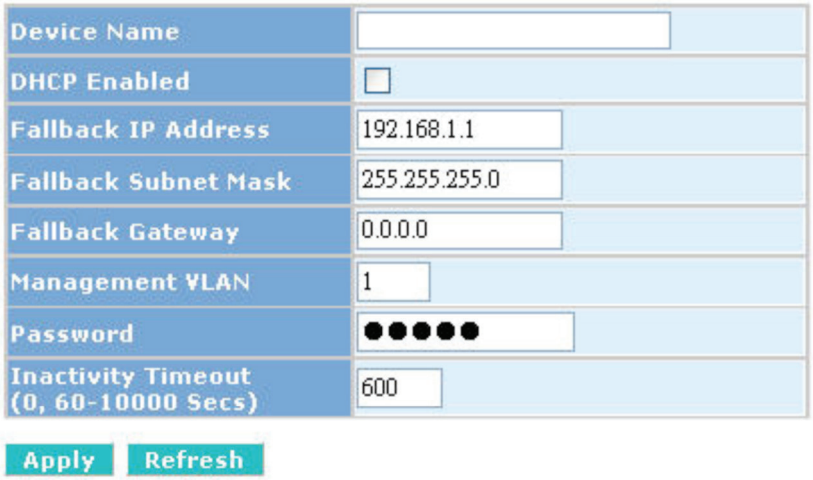


Figure 3-13. Default gateway.

For example, you can enter the IP address, "192.168.1.1," as shown in Figure 3-13. An IP address such as 192.168.1.x must be set on your PC.

Next, type in the Subnet Mask, for example, "255.255.255.0." Any subnet mask such as 255.255.255.x is allowable in this case.

3.2 Typical Applications

The LGB2118A implements (16) Gigabit Ethernet TP ports with auto MDI-X and (2) slots for the removable module supporting LC fiber SFP modules. The LGB2124A has (20) Gigabit Ethernet TP ports with auto MDI-X and (4) slots for the removable combo module supporting twisted-pair and LC fiber SFP modules. For more details about the switch's specifications, refer to Chapter 1.

The switch is suitable for the following applications.

• Central site/remote site application is used in carrier or ISP (see Figure 3-14).

- Peer-to-peer application is used in two remote offices (see Figure 3-15).
- Office network (see Figure 3-16).

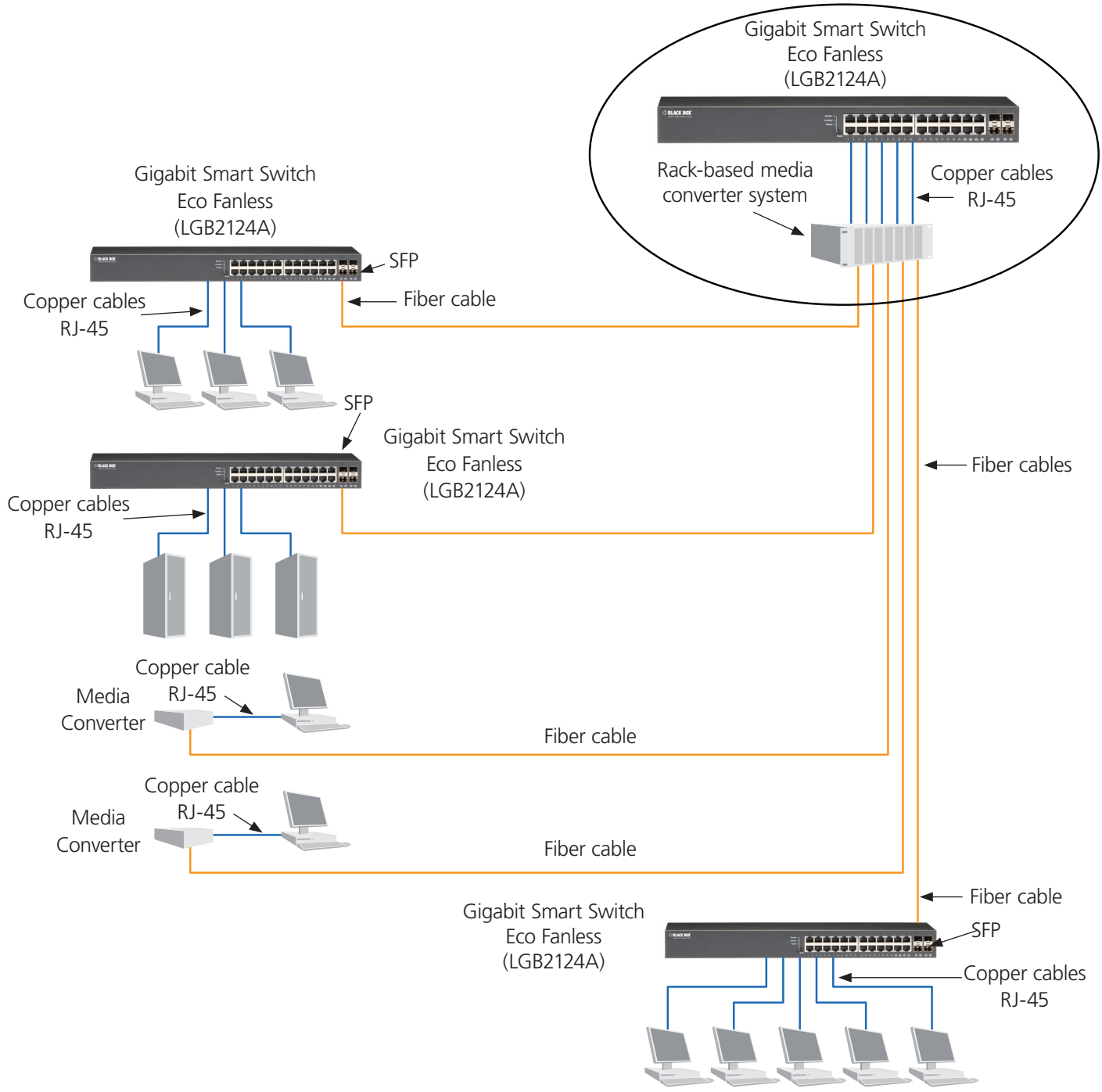


Figure 3-14. Network connection between remote site and central site.

Fig. 3-14 is a system-wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

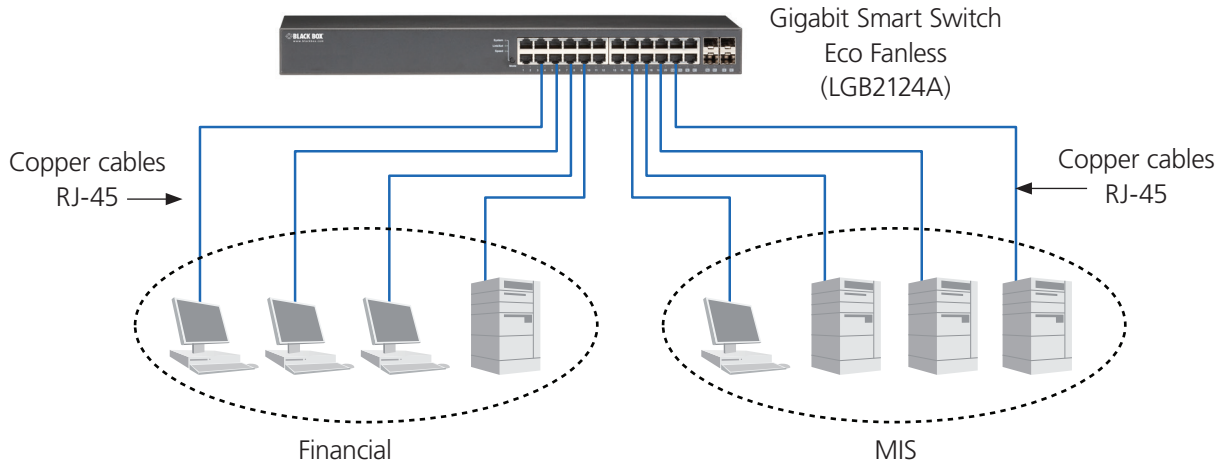


Figure 3-15. Peer-to-peer network connection.

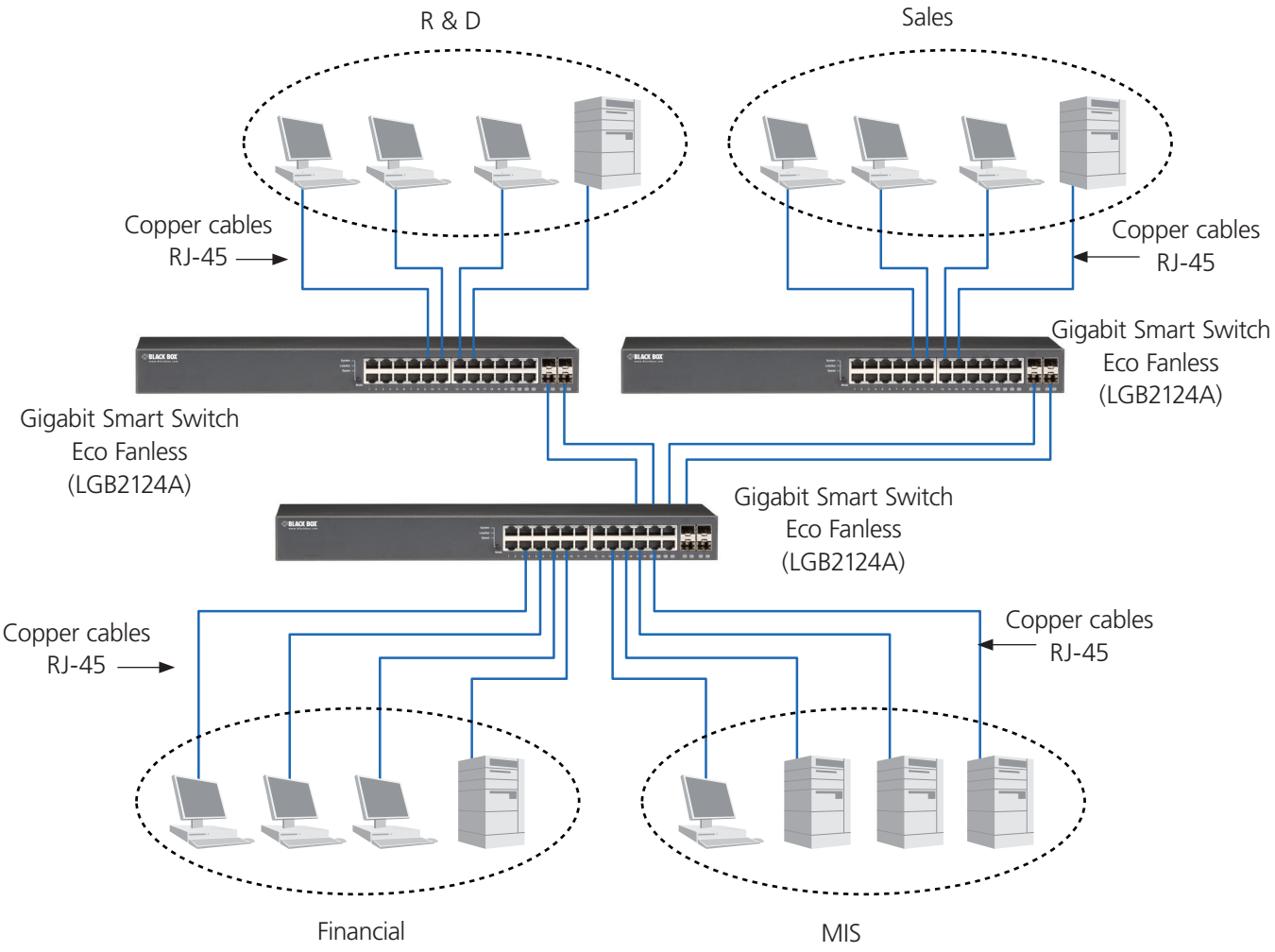


Figure 3-16. Office network connection.

4. Basic Concepts and Management

This chapter describes the features used to manage this switch and how they work.

4.1 Ethernet

Ethernet originated and was implemented at Xerox® in Palo Alto, CA in 1973 and was successfully commercialized by Digital Equipment Corporation (DEC), Intel® and Xerox (DIX) in 1980. In 1992, Grand Junction Networks unveiled a new high-speed Ethernet with the same characteristic of the original Ethernet but operating at 100 Mbps, now called Fast Ethernet. This means Fast Ethernet inherits the same frame format, CSMA/CD, software interface. In 1998, Gigabit Ethernet was rolled out and provided 1000 Mbps. The 10 Gbps Ethernet standard was released in 2002. Although these types of Ethernet have different speeds, they still use the same basic functions. They are software compatible and can connect to each other almost without limitation, based on the transmission media used.

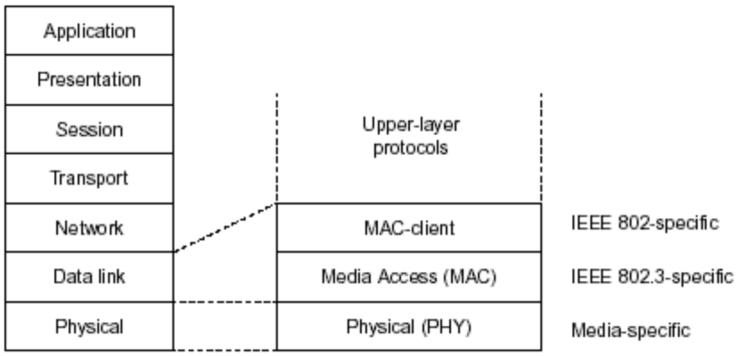


Figure 4-1. IEEE 802.3 reference model vs. OSI reference mode.

In Figure 4-1, Ethernet uses the Data Link layer and Physical layer and consists of three portions, including logical link control (LLC), media access control (MAC), and physical layer. The first two portions work at the Data link layer, which splits data into frames for transmitting, receiving acknowledge frames, error checking, and re-transmitting when not received correctly, and also provides an error-free channel upward to the network layer.

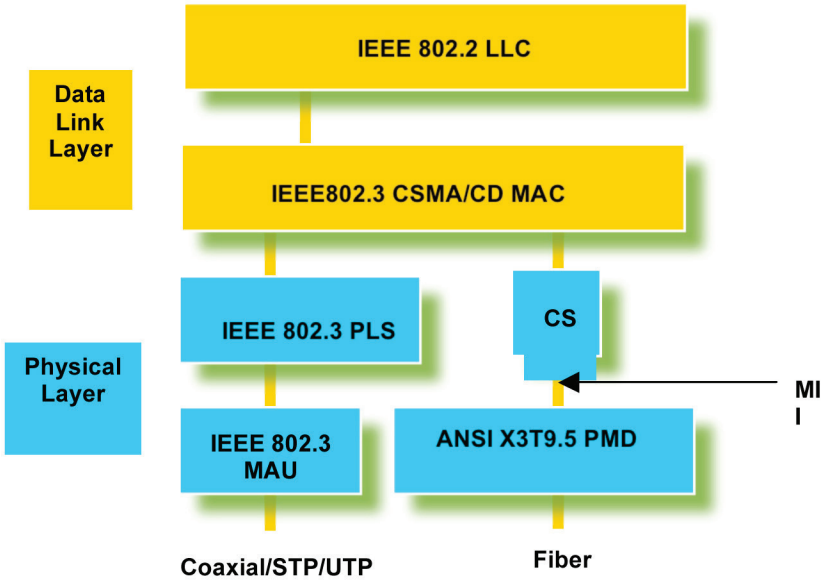


Figure 4-2. MAC sub layer in physical layer in OSI model.

This diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which operate at the Data Link layer, and transceivers, which work at the Physical layer in the OSI model. In this section, we describe the MAC sub-layer.

4.2 Logical Link Control (LLC)

The data link layer consists of both the sub-layers of MAC and MAC-client. The MAC client may be logical link control or the bridge relay entity.

Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, such as Network layer. It can operate over different LAN technologies, such as Token Ring, FDDI, and so on. For the interface to the MAC layer, LLC defines the services with the interface, independent of the medium access technology.

Table 4-1. LLC PDU format.

Parameter	Value	Description
DSAP address	8 bits	Destination service access point address field
SSAP address	8 bits	Source service access point address field
Control	8 or 16 bits	Control field (16 bits for formats that include seqeuence numbering, and 8 bits for formats that do not)
Information	M*8 bits	Information

* = Multiplication

M = An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

Table 4-1 shows the format of LLC PDU. It consists of four fields: DSAP, SSAP, Control, and Information. The DSAP address field identifies one or more service access points that have an I/G bit for an individual or group address. If all bits of DSAP are 1s, it's a global address. The SSAP address field identifies the specific services indicated by the C/R bit (command or response). The DSAP and SSAP pair with some reserved values indicate some well-known services listed in Table 4-2.

Table 4-2. SSAP address field options.

OxAAAA	SNAP
0xE0E0	Novell® IPX
0x F0F0	NetBios
0xFEFE	IOS network layer PDU
0xFFFF	Novell IPX 802.3 RAW packet
0x4242	STP BPDU
0x0606	IP
0x9898	ARP

LLC type 1 is a connectionless service, LLC type 2 is a connection-oriented service, and LLC type 3 acknowledges a connectionless service and has three types of LLC frames for all classes of service. Figure 4-3 shows the format of the Service Access Point (SAP).

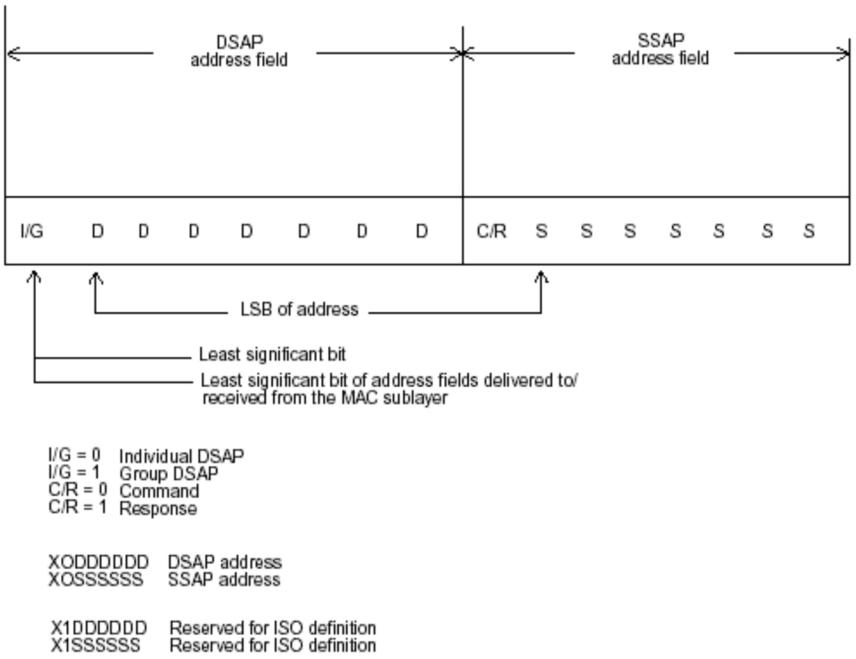


Figure 4-3. SAP format.

For more information about SAP, refer to the IEEE 802.2 standard.

4.3 Media Access Control (MAC)

4.3.1 MAC Addressing

A LAN is composed of many nodes. To exchange data among these nodes, each node must have its own unique address to identify who should send the data or should receive the data. In the OSI model, each layer provides its own way to identify the unique address in some form, for example, IP address in network layer.

The MAC belongs to Data Link Layer (Layer 2). The address is a 48-bit long and locally unique address. Since this type of address applies only to the Ethernet LAN media access control (MAC), it is referred to as a MAC address.

The first three bytes are Organizational Unique Identifier (OUI) codes assigned by IEEE. The last three bytes are the serial number assigned by the vendor of the network device. All six bytes are stored in non-volatile memory in the device. Their format is shown in Table 4-3. It is normally written as aa-bb-cc-dd-ee-ff, 12 hexadecimal digits separated by hyphens, in which the aa-bb-cc is the OUI code and the dd-ee-ff is the serial number assigned by manufacturer.

Table 4-3. Ethernet MAC address.

Bit 47					bit 0
1st byte	2nd byte	3rd byte	4th byte	5th byte	6th byte
OUI code			Serial number		

The first bit of the first byte in the Destination address (DA) determines the address to be a Unicast (0) or Multicast frame (1), known as I/G bit indicating individual (0) or group (1). So the 48-bit address space is divided into two portions, Unicast and Multicast. The second bit is for a globally-unique (0) or locally-unique address. The globally-unique address is assigned by the device manufacturer, and the locally-unique address is usually assigned by the administrator. In practice, globally-unique addresses are always applied.

A unicast address works with a single network interface. With a MAC address, a frame transmitted can be received exactly by the target interface that the destination MAC points to.

A multicast address works with a group of network devices or network interfaces. In Ethernet, many-to-many connectivity in the LANs is supported. It provides a way to send a frame to many network devices at a time. When all bits of DA are 1s, it is a broadcast, which means all network devices except the sender itself can receive the frame and response.

4.3.2 Ethernet Frame Format

There are two major forms of Ethernet frame, type encapsulation and length encapsulation, and both are categorized as four-frame formats 802.3/802.2 SNAP, 802.3/802.2, Ethernet II, and Netware 802.3 RAW. The basic Ethernet frame format defined by the IEEE 802.3 standard required for all MAC implementations is explained next.

Table 4-4. Ethernet frame structure.

PRE	SFD	DA	SA	Type/Length	Data	Pad bit if any	F CS
7	7	6	6	2	46–1500		4

- Preamble (PRE) — The PRE is 7-bytes long with an alternating pattern of ones and zeros used to tell the receiving node that a frame is coming, and to synchronize the physical receiver with the incoming bit stream. The preamble pattern is:

  10101010 10101010 10101010 10101010 10101010 10101010 10101010

- Start-of-frame delimiter (SFD) — The SFD is one-byte long with alternating patterns of ones and zeros, ending with two consecutive 1-bits. It immediately follows the preamble and uses the last two consecutive 1s bits to indicate that the next bit is the start of the data packet and the left-most bit in the left-most byte of the destination address. The SFD pattern is 10101011.
- Destination address (DA) — The DA field is used to identify which network device(s) should receive the packet. It is a unique address. See Section 4.3.1.
- Source addresses (SA) — The SA field indicates the source node. The SA is always an individual address and the left-most bit in the SA field is always 0.

- Length/Type — This field indicates either the number of the data bytes contained in the data field of the frame, or the Ethernet type of data. If the value of first two bytes is less than or equal to 1500 in decimal notation, the number of bytes in the data field is equal to the Length/Type value, that is, this field acts as a Length indicator at this moment. When this field acts as Length, the frame has optional fields for 802.3/802.2 SNAP encapsulation, 802.3/802.2 encapsulation, and NetWare® 802.3 RAW encapsulation. Each of them has different fields following the Length field.
- If the Length/Type value is greater than 1500, the Length/Type acts as Type. Different type values are the frames with different protocols running over Ethernet being sent or received.

For example,

0x0800	IP datagram
0x0806	ARP
0x0835	RARP
0x8137	IPX datagram
0x86DD	IPv6

- Data — Less than or equal to 1500 bytes and greater or equal to 46 bytes. If data is less than 46 bytes, the MAC will automatically extend the padding bits and the payload will be equal to 46 bytes. The length of the data field must equal the value of the Length field when the Length/Type acts as Length.
- Frame check sequence (FCS) — This field contains a 32-bit cyclic redundancy check (CRC) value, and is a check sum computed with DA, SA, through the end of the data field with the following polynomial.

  $G(x) = x32 + x26 + x24 + x22 + x16 + x12 + x11 + x10 + x8 + x7 + x5 + x4 + x2 + x + 1$

  It is created by the sending MAC and recalculated by the receiving MAC to check if the packet is damaged or not.

How does a MAC work?

The MAC sub-layer has two primary jobs to do:

1. Receiving and transmitting data. When receiving data, it parses frames to detect errors; when transmitting data, it performs frame assembly.
2. Performing Media access control. It prepares the initiation jobs for a frame transmission and enables recovery from transmission failure.

Frame transmission

Ethernet uses Carrier Sense Multiple Access with Collision Detect (CSMA/CD), so it detects if there is any carrier signal from another network device running over the physical medium when a frame is ready for transmission. This is referred to as sensing carrier, also "Listen." If there is a signal on the medium, the MAC defers the traffic to avoid a transmission collision and waits for a random period of time, called backoff time, then sends the traffic again.

After the frame is assembled, when transmitting the frame, the preamble (PRE) bytes are inserted and sent first, then, the Start-of-Frame Delimiter (SFD), DA, SA and through the data field and FCS field in turn. The following summarizes what a MAC does before transmitting a frame.

1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed by DA, SA, tag ID if tagged VLAN is applied, Ethertype or the value of the data length, and payload data field, and finally the FCS data will be put in order into the responding fields.
2. Listen if there is any traffic running over the medium. If yes, wait.
3. If the medium is quiet, and no longer senses any carrier, the MAC waits for a period of time, called the inter-frame gap time, to have the MAC ready with enough time and then start transmitting the frame.

4. During the transmission, the MAC keeps monitoring the status of the medium. If no collision happens until the end of the frame, it transmits successfully. If there is a collision, the MAC will send the patterned jamming bit to guarantee the collision event is propagated to all involved network devices, then wait for a random period of time, called back off time. When backoff time expires, the MAC goes back to the beginning state and attempts to transmit again. After a collision happens, MAC increases the transmission attempts. If the count of the transmission attempts reaches 16 times, the frame in the MAC's queue will be discarded.

Ethernet MAC transmits frames in half-duplex and full-duplex modes. In half-duplex operation mode, the MAC can either transmit or receive frames at a moment, but cannot transmit and receive at the same time.

Because the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For the two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the frame just before the frame from the first device arrives. The collision happens and will be detected by the second device immediately. Because of the medium delay, this corrupted signal needs to spend some time to propagate back to the first device. The maximum time to detect a collision is approximately twice the signal propagation time between the two most-distant devices. This maximum time is traded-off by the collision recovery time and the diameter of the LAN.

In the original 802.3 specification, Ethernet operates in half duplex only. Under this condition, when in 10-Mbps LAN, it's 2500 meters, in 100-Mbps LAN, it's approximately 200 meters and in 1000-Mbps, 200 meters. According to the theory, it should be 20 meters. But it's not practical, so the LAN diameter is kept by increasing the minimum frame size with a variable-length non-data extension bit field that is removed at the receiving MAC. The following diagrams show the frame format suitable for 10M, 100M, and 1000M Ethernet, and some parameter values that apply to all these three types of Ethernet.

Gigabit Ethernet chips in practice are supported in full-duplex mode only, as well as all network vendors' devices. The switch's Gigabit module supports only full-duplex mode.

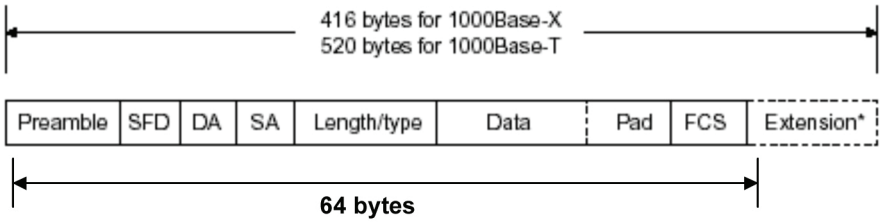


Figure 4-4. Gigabit Ethernet Frame.

Table 4-5. Ethernet parameters for half-duplex mode.

Parameter Value/LAN	10BASE	100BASE	1000BASE
Max. collision domain DTE to DTE	328 feet (100 m)	328 feet (100 m) for UTP 1351.7 feet (412 m) for fiber	328 feet (100 m) for UTP 1043.3 feet (316 m) for fiber
Max. collision domain with repeater	8202.1 feet (2500 m)	672.6 feet (205 m)	646.1 feet (200 m)
Slot time	512 bit times	512 bit times	512 bit times
Interframe gap	9.6 µs	0.96 µs	0.096 µs
Attempt Limit	16	16	16
Backoff Limit	10	10	10
Jam size	32 bits	32 bits	32 bits
Max. frame size	1518	1518	1518
Min. frame size	64	64	64
Burst limit	Not applicable	Not applicable	65536 bits

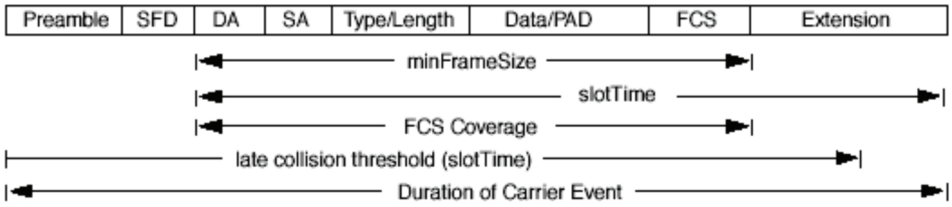


Figure 4-5. Full-duplex mode.

In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles the total bandwidth. Full-duplex is much easier than half-duplex because it does not involve media contention, collision, retransmission schedule, and padding bits for short frames. It functions according to the IEEE 802.3 specification. The minimum inter-frame gap requirement between successive frames and frame formats is the same as that in the half-duplex operation.

No collision will happen in full-duplex operation. What happens if the receiving device is busy and a frame is coming at the same time? Can it use "backpressure" to tell the source device? A flow control function is introduced in full-duplex operation.

4.4 Flow Control

Flow control is a mechanism that tells the source device to stop sending frames for a specified period of time designated by a target device until the PAUSE time expires. It does this by sending a PAUSE frame from the target device to the source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to the source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. The PAUSE frame is identical in the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. As per the specification, PAUSE operation can not be used to inhibit the transmission of a MAC control frame.

Normally, in 10-Mbps and 100-Mbps Ethernet, only symmetric flow control is supported. However, the Gigabit Smart Switch Eco Fanless supports not only symmetric, but also asymmetric flow control for the special application. In Gigabit Ethernet, both symmetric flow control and asymmetric flow control are supported. Asymmetric flow control only allows transmitting a PAUSE frame in one way from one side; the other side is not transmitted. Instead the switch receives and discards the flow control information. Symmetric flow control allows both two ports to transmit PAUSE frames to each other simultaneously.

Inter-frame Gap time

After the end of a transmission, if a network node is ready to transmit data out and if there is no carrier signal on the medium at that time, the device will wait for a period of time known as an inter-frame gap time to clear and stabilize the medium, as well as to have the jobs ready, such as adjusting buffer counter, updating counter, and so on, in the receiver site. Once the inter-frame gap time expires after the de-assertion of carrier sense, the MAC transmits data. In the IEEE 802.3 specification, this is 96-bits time or more.

Collision

Collision happens only in half-duplex operation. When two or more network nodes transmit frames at approximately the same time, a collision always occurs and interferes with each other. As a result, the carrier signal is distorted and un-discriminated. The MAC can detect, through the physical layer, the distortion of the carrier signal. When a collision is detected during a frame transmission, the transmission will not stop immediately but, instead, continues transmitting until the rest of the bits specified by jamSize are completely transmitted. This guarantees that the duration of the collision is long enough for all involved devices to detect the collision. This is referred to as jamming. After a jamming pattern is sent, MAC stops transmitting the rest of the data queued in the buffer and waits for a random period of time, known as backoff time with the following formula. When backoff time expires, the device goes back to attempting to transmit the frame. The backoff time is determined by the formula below. When the time of collision is increased, the backoff time increases up to the collision times plus 16. If this happens, the frame will be discarded and the backoff time will also be reset.

$$0 <= r < 2k$$

where

$$k = \min(n, 10)$$

Frame Reception

Frame reception is the same for both half-duplex and full-duplex operation, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always "listens" if there is traffic running over the medium when it is not receiving a frame. When a frame destined for the target device comes, the receiver of the target device begins receiving the bit stream, and looks for the Preamble (PRE) pattern and Start-of-Frame Delimiter (SFD) that indicates the next bit is the starting point of the MAC frame, until all bits of the frame are received.

For a received frame, the MAC will check:

1. Is it less than one slotTime in length, that is, a short packet? If yes, the frame will be discarded by MAC because, by definition, the valid frame must be longer than the slotTime. If the length of the frame is less than one slotTime, a collision may have happened somewhere or the interface might have malfunctioned in the LAN. When detecting the case, the MAC drops the packet and goes back to the ready state.
2. Does the DA of the received frame exactly match the physical address that the receiving MAC owns or the multicast address is designated to recognize? If not, the MAC discards it and passes the frame to its client and goes back to the ready state.
3. Is the frame is too long? If yes, the MAC throws it away and reports "Frame Too Long."
4. Is the FCS of the received frame valid? If not, for 10M and 100M Ethernet, the MAC discards the frame. For Gigabit Ethernet or higher speed Ethernet, the MAC has to check one more field, that is, the extra bit field, if FCS is invalid. If any extra bits exist, they must meet the IEEE 802.3 specification to be considered valid. When both FCS and extra bits are valid, the received frame will be accepted; otherwise, the switch discards the received frame and reports frameCheckError if no extra bits are appended, or alignmentError if extra bits are appended.
5. Is the length/type valid? If not, the switch discards the packet and reports lengthError.
6. If all five procedures above are ok, then the MAC treats the frame as good and disassembles the frame.

What if VLAN tagging is applied?

VLAN tagging is a 4-byte long data immediately following the MAC source address. When tagged VLAN is applied, the Ethernet frame structure will change slightly.

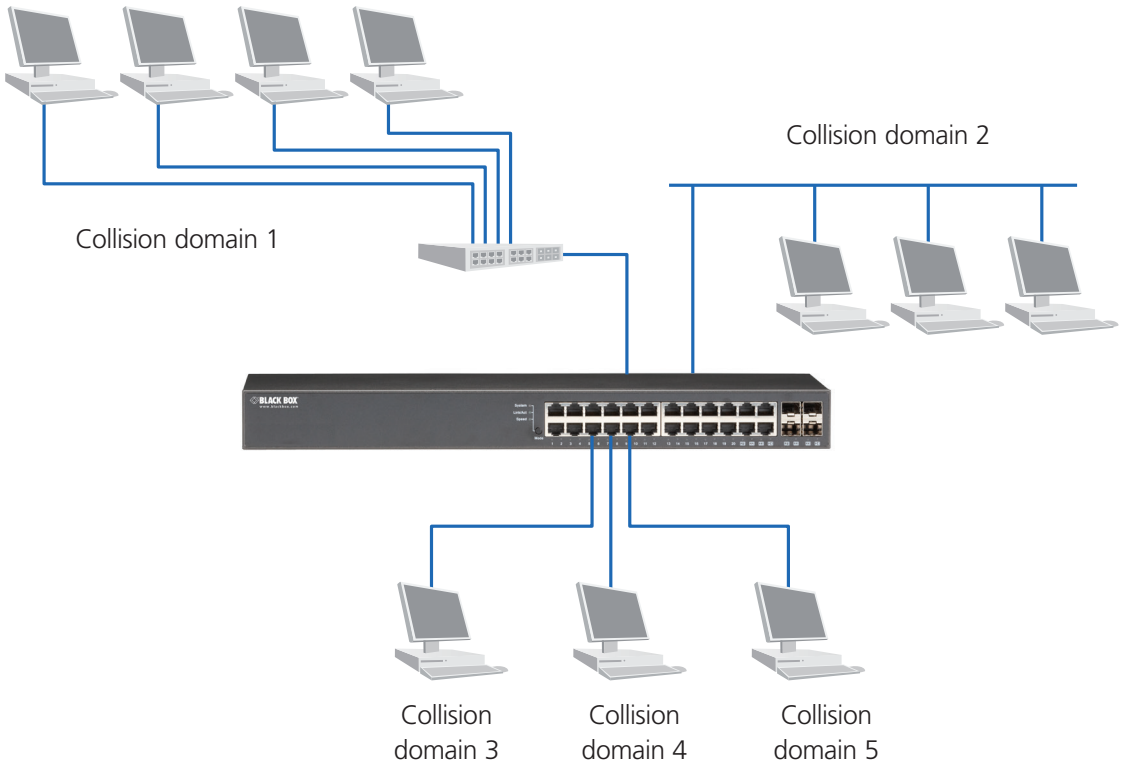


Figure 4-6.

Only two fields, VLAN ID and Tag control information, are different when compared to the basic Ethernet frame. The rest of the fields are the same.

The first two bytes are the VLAN type ID, with the value of 0x8100 indicating the received frame is a tagged VLAN. The next two bytes are Tag Control Information (TCI). They provide user priority and VLAN ID, explained next.

Table 4-6. User priority and VLAN ID.

Bits 15–13	User priority 7–0, 0 is lowest priority
Bit 12	CFI (Canonical Format Indicator) 1: RIF field is present in the tag header. 0: No RIF field is present.
Bits 11–0	VID (VLAN identifier) 0x000: Null VID. No VID is present and only user priority is present. 0x001: Default VID 0xFFF: Reserved

NOTE: RIF is used in Token Ring networks to provide source routing and consists of two fields: Routing Control and Route Descriptor.

When MAC parses the received frame and finds a reserved special value 0x8100 at the location of the Length/Type field of the normal non-VLAN frame, it will interpret the received frame as a tagged VLAN frame. If this happens in a switch, the MAC will forward it, according to its priority and egress rule, to all the ports associated with that VID. If it happens in a network interface card, MAC will deprive the tag header and process it in the same way as a basic normal frame. For a VLAN-enabled LAN, all involved devices must be equipped with the optional VLAN function.

At operating speeds above 100 Mbps, the slotTime employed at slower speeds is inadequate to accommodate network topologies of the desired physical extent. Carrier Extension provides a means by which the slotTime can be increased to a sufficient value for the desired topologies, without increasing the minFrameSize parameter, because this would have deleterious effects. Non-data bits, referred to as extension bits, are appended to frames that are less than slotTime bits in length so that the resulting transmission is at least one slotTime in duration. Carrier Extension can be performed only if the underlying physical layer is capable of sending and receiving symbols that are readily distinguished from data symbols, as is the case in most physical layers that use a block encoding/decoding scheme.

The maximum length of the extension is equal to the quantity (slotTime - minFrameSize). The MAC continues to monitor the medium for collisions while it is transmitting extension bits, and it will treat any collision that occurs after the threshold (slotTime) as a late collision.

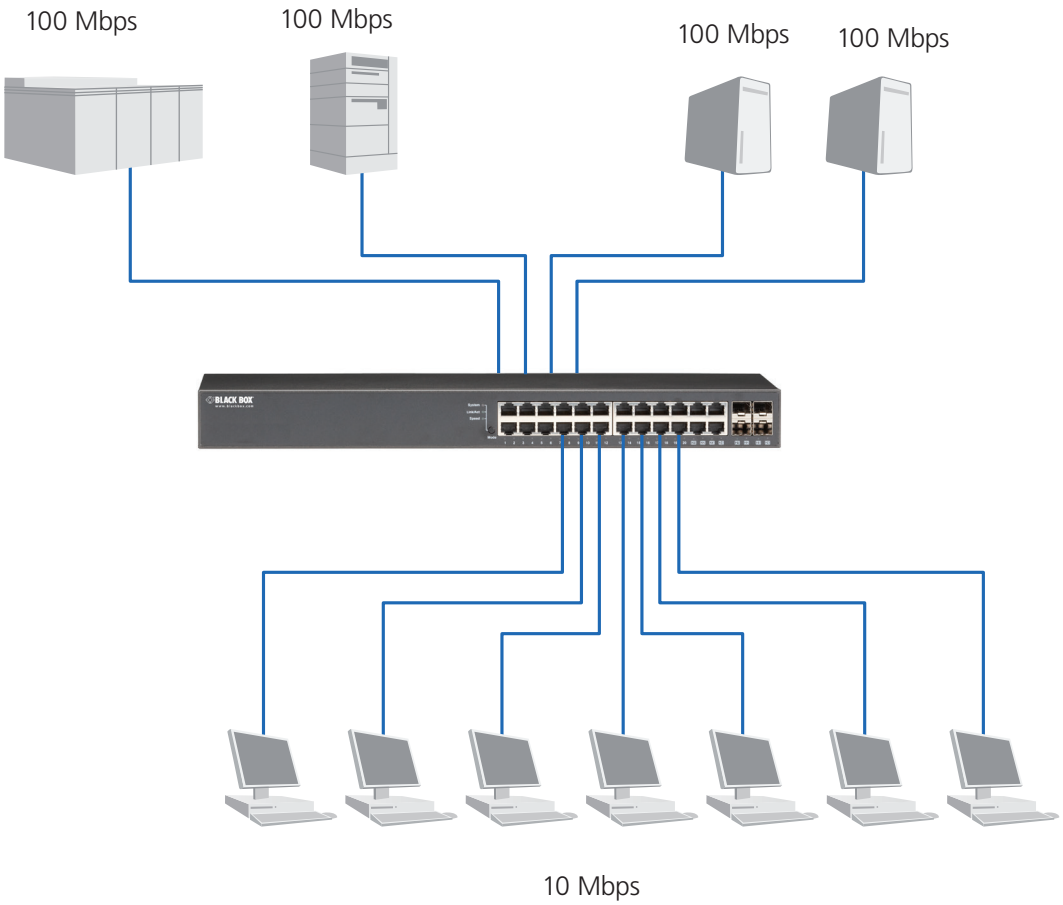


Figure 4-7. Collision domain.

4.5 How Does a Switch Work?

The LGB2118A switch is a layer 2 Ethernet Switch equipped with (16) TP Gigabit Ethernet ports and (2) slots for optional SFP fiber modules. The LGB2124A switch has (20) TP ports and (4) slots for optional TP/SFP combo modules. Each port on the switch is an independent LAN segment and thus has 26 LAN segments and 26 collision domains, in contrast to the traditional shared Ethernet hub, in which all ports share the same media and use the same collision domain and thus limit the bandwidth use. A switch's separated collision domain extends the LAN diameter farther than the shared hub does and greatly improves the efficiency of the traffic transmission.

Because of the architecture, the switch can provide full-duplex operation to double the bandwidth per port and many other features, such as VLAN, bandwidth aggregation (LGB2118A only), and so on, which are not able to be supported in a shared hub.

Terminology

Separate Access Domains:

Ethernet uses CSMA/CD to arbitrate who can transmit data to the station(s) attached in the LAN. When more than one station transmits data within the same slot time, the signals will collide, referred to as a collision. The arbitrator will arbitrate who should gain the media. The arbitrator is a distributed mechanism in which all stations contend to gain the media. Please refer to Section 4.1 for more details.

In Figure 4-7, running in half-duplex mode, you will see that some ports of the switch are linked to a shared hub, which connects many hosts, and some ports just are individually linked to a single host. The hosts attached to a shared hub will be in the same collision domain, separated by the switch, and use the CSMA/CD rule. The host directly attached to the switch, because no other host(s) joins the traffic contention, will not be affected by CSMA/CD. These LAN segments are separated in different access domains by the switch.

Micro-segmentation:

When a port of the switch is connected to a single host, this is referred to as micro-segmentation. It has the following characteristics.

- There is no need for access contention (for example, Collision). They have their own access domain. But, collision still could happen between the host and the switch port.
- When operating in full-duplex mode, the collision vanishes.
- The host owns a dedicated bandwidth of the port.

The switch port can run at different speeds, such as 10 Mbps, 100 Mbps, or 1000 Mbps. A shared hub cannot do this.

Extended Distance Limitations:

The diameter of a half-duplex LAN segment is determined by its maximum propagation delay time. For example, in a 10M LAN, the maximum distance of a LAN segment using TP cable is 2500 meters and 185 meters when using coaxial cable. The switch with its per port per collision domain can extend the distance in the same way as a bridge does. When operating in full-duplex mode, the distance can reach farther than half-duplex because it is not limited by the maximum propagation delay time (512 bits time). If fiber media is used, the distance can be up to tens of kilometers.

Traffic Aggregation:

Traffic aggregation combines the bandwidth of more than one port and treats it as a single port in the LAN. This single port has the features of a normal port, plus loading balance. You can use this when you need more bandwidth but cannot afford to pay the high cost of a high-bandwidth port.

How does a switch operate?

A Layer 2 switch uses some features of the Data Link layer in the OSI model to forward the packet to the destination port(s). Here we introduce some important features of switches and how they work.

- MAC address table: When a packet is received on a switch port, the switch first checks if the packet is good or bad and extracts the source MAC address (SA) and destination MAC address (DA) to find if SA exists in the MAC address table: if no, it puts it in the MAC address table; if yes, it looks up the DA and its associated port to which the traffic is forwarded. If the DA does not exist, the packet is broadcasted.

  Because the number of MAC addresses is limited, the switch applies the MAC address aging function. When the MAC address has resided and keeps no update in the table for a long time, the traffic using that entry has been inactive. If this time period is more than the aging time, the entry will be marked invalid. The vacancy is now available for other new MACs.

  Both learning and forwarding are the most important functions in a switch. VLAN can be one of the rules to forward the packet. Ingress rules and egress rules apply. The ingress rule is used to filter the incoming packet by VLAN ID and to decide whether the packet is allowed to enter the switch or not. The egress rule is used to forward the packet to the proper port.

- Mac address aging: There is a field in the MAC address table used to put the entry's Age time, which determines how long a MAC entry can reside in a switch. The age time is refreshed when a packet with source MAC address (SA) is sent. Usually, the age time is programmable.

- Transmission schedule: In most layer 2 switches, QoS is supported. QoS in a switch must associate a transmission schedule to transmit the packet. This function depends on the priority level that a packet has. With the given priority, the scheduler will perform the proper action. The scheduler has many ways to implement, and different chips may support different schedule algorithms. Most common schedulers are:

  FCFS: First Come First Service.

  Strictly Priority: All High before Low.

  Weighted Round Robin:

Set a weight figure to the packet with a priority level, say 5–7, and next, set another weight to the packet with a priority level, say 2–4, and so on. The WRR will transmit the packet with the weight. So the packet of each priority level can be allocated a fixed bandwidth.

Bandwidth rating

Bandwidth rating is the limitation set by administrator, and it can be applied to those with SLA. Bandwidth rating can be total bandwidth, types of service of a port with many steps. The switch supports by-port Ingress and Egress total bandwidth rate control capacity. The bandwidth rate resolution is 0.1 Mbps (100 Kbps) and ranges from 0 to 100 Mbps.

4.6 Virtual LAN

What is a VLAN?

It is a subset of a LAN. Before we discuss VLAN, we must understand what LAN is. In general, a LAN is composed of different physical network segments bridged by switches or bridges that attach to end stations in the same broadcast domain. The traffic can reach any station on the same LAN. Beyond this domain, the traffic cannot go without a router's help. This also implies that a LAN is limited. If you need to communicate with the station outside the LAN, a router is needed and always is located on the edge of the LAN.

A layer 2 VLAN, uses a logical subset of a physical LAN separated by specific rules such as tag, port, MAC address, and so on. In other words, they can communicate with each other between separated small physical LANs within a LAN, but cannot between any two separated logical LANs.

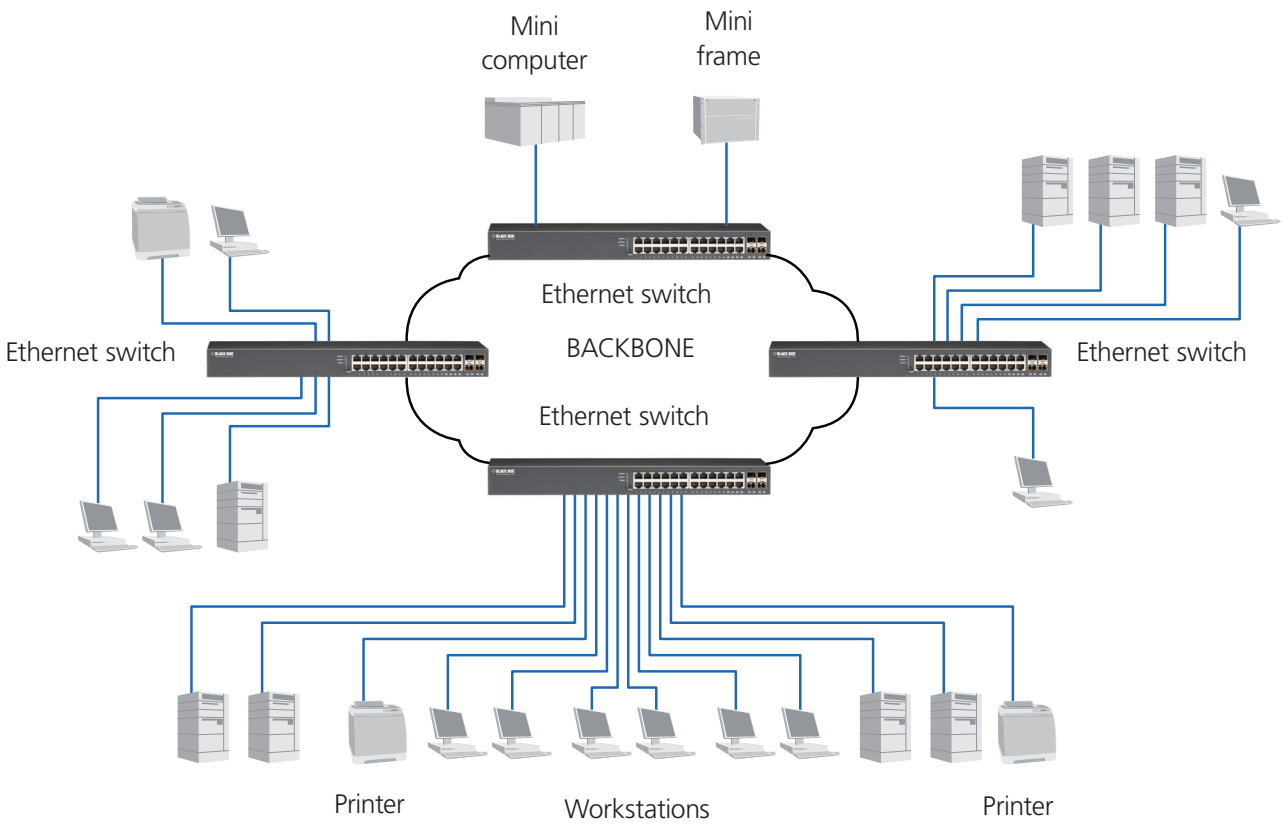


Figure 4-8.

In the figure above, all stations are within the same broadcast domain. For these stations, the traffic is getting congested when adding more stations to the broadcast domain. With more and more users joining the LAN, broadcast traffic will rapidly decrease the performance of the network. In this case, the network may fail.

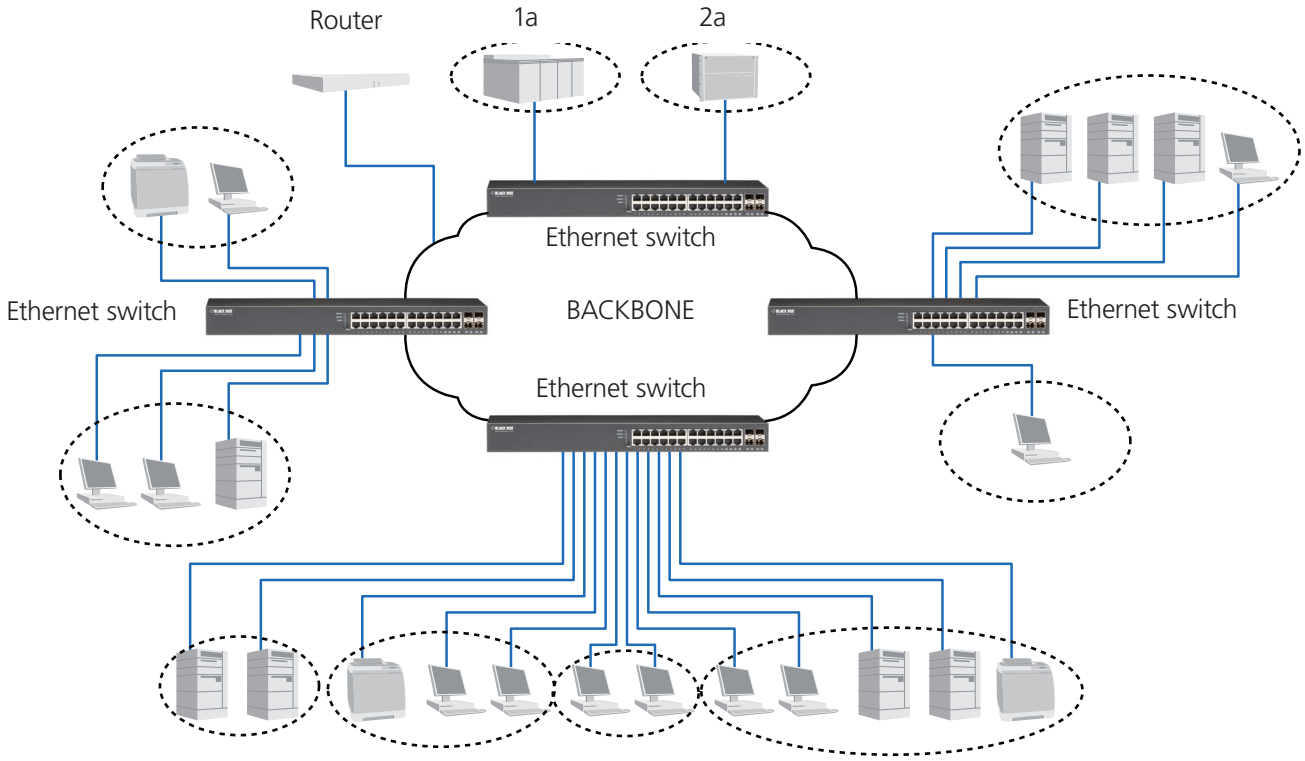


Figure 4-9. Virtual LAN.

By applying VLAN technology, you can configure the system shown in Figure 4-9. You can partition the users into the different logical networks that have their own broadcast domain. The traffic will not disturb these logical networks. The users 1x (x denotes a – d) are members of VLAN 1. Any traffic within VLAN 1 does not flow to VLAN 2 and others. This helps configure the network easily according to the criteria needed, for example, financial, accounting, R&D, and whatever you think is necessary. You can also easily move a user to a different location or join a new user somewhere in the building to VLAN. Without VLAN, it is very hard to do. Basically, VLAN can be used to move and change users, reduce broadcast traffic, and increase performance.

VLANs can greatly reduce the traffic congestion and increase total performance, because there are no longer too many users in the same broadcast domain.

There are many types of VLAN. Most popular are port-based VLAN, tag-based VLAN, and protocol-based VLAN.

- Port-based VLAN: Some physical ports are configured as members of a VLAN. All stations attached on these ports can communicate with each other.
- Tag-based VLAN identifies the membership by VLAN ID, no matter where the packet comes from. It is also referred to as 802.1Q VLAN.
- Protocol-based VLAN identifies the VLAN membership by layer 3 protocol types, for example IPX, Appletalk, IP, etc.

Other VLAN technologies not mentioned above are MAC-based VLAN, and IP-based VLAN.

Terminology

Tagged Frame:

A frame carrying a tag field with the source MAC address is four bytes long and contains VLAN protocol ID and tag control information composed of user priority, Canonical Format Indicator (CFI), and optional VLAN identifier (VID). Normally, the maximum length of a tagged frame is 1522 bytes.

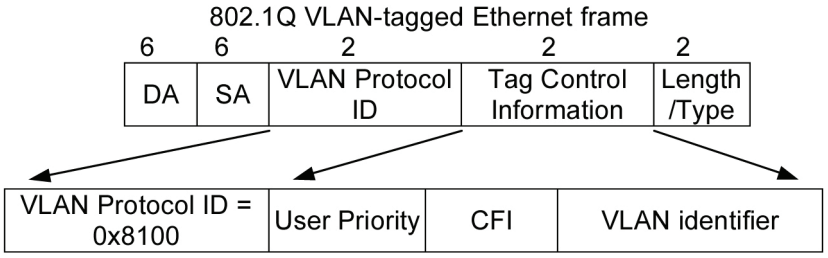


Figure 4-10. Tag format.

VLAN Protocol ID: 8100 is reserved for VLAN-tagged frame.

User Priority: 3 bits long. User priority is defined from 7–0. 0 is the lowest priority.

CFI: Canonical Format Indicator is 1 bit long. It encapsulates a token ring packet so it can travel across the Ethernet. Usually, it is set to 0.

VLAN ID: 12 bits long. 0 means no VLAN ID is present. 1 means default VLAN, 4095 is reserved.

VLAN-tagged frame: An Ethernet frame, carrying a VLAN tag field, contains VLAN identification without the value of 0 and 4095, and priority information.

Priority-tagged frame: An Ethernet frame, carrying a VLAN tag field, contains VLAN identification with the value of 0 and priority information.

Untagged frame: An Ethernet frame carries no VLAN tag information.

VLAN Identifier: Also referred to as VID. It is used to identify whether a member belongs to the VLAN group with the VID. The assignable number is 1–4094. If VID=0, the tagged frame is a priority packet. Values of 0 and 4095 also cannot be assigned in VLAN management.

Port VLAN Identifier: VLAN identifier of a port. It also can be referred to as PVID. When an untagged frame or a priority-tagged frame is received, the frame will be inserted into the PVID of that port in the VLAN tag field. The frame with VID assigned by a port is called PVID. Each port can only be assigned a PVID. The default value for PVID is 1, the same as VID.

Ingress filtering: The process to check a received packet and compare its VID to the VLAN membership of the ingress port. The ingress filtering can be set per port. When receiving a packet, a VLAN bridge examines if the VID in the frame's header presents.

If the VID of the received packet presents, the VID of the packet is used. And VLAN bridge will check its MAC address table to see if the destination ports are members of the same VLAN. If both are members of the tagged VLAN, then the packet will be forwarded.

If the packet is an untagged or a null tag packet, the ingress port's PVID is applied to the packet. A VLAN bridge will then look up the MAC address table and determine to which ports the packet should be forwarded. Next, it will check to see if the destination ports belong to the same VLAN with that PVID. If the destination ports are members of the VLAN used by the ingress port, the packet will be forwarded.

NOTE: VID cannot be 0 or 4095.

Ingress Rule: Each packet received by a VLAN-aware bridge will be classified to a VLAN. The classification rule is described as follows.

1. If the VID of the packet is null VID (VID=0) or this packet is an untagged packet:

a. If there are still some other ways (for example, protocol, MAC address, application, IP-subnet, etc.) to classify the incoming packets besides port-based classification, use the value of VID offered by other classifications for a VLAN's classification.

b. If there is only port-based classification implemented, other classification approaches cannot offer non-zero VID for the incoming packets, and then assign the PVID to the incoming packets as VID for the classification of the VLAN group.

2. If the VID is not a null VID (VID is not equal to 0), then use the value to classify the VLAN group.

Egress Rule: An egress list is used to make the tagging and forwarding decision on an outgoing port. It specifies the VLANs whose packets can be transmitted out and specifies if the packet should be tagged or not. It can be configured for the port's VLAN membership, and tagged or untagged for a transmitted packet. When a packet is transmitted out, the VLAN bridge checks the port's egress list. If the VLAN of the packet is on the egress list of the port that the packet transmits out on, the packet will be transmitted with the priority accordingly. If enabled, an egress port will transmit out a tagged packet if the port is connected to a 802.1Q-compliant device. If an egress port is connected to a non-802.1Q device or an end station, the VLAN bridge must transmit out an untagged packet. The tag has been stripped off in an egress port. Egress rule can be set by per port.

Independent VLAN Learning (IVL) specifies the mode chosen to learn a MAC address. For a specified VLAN, it will use an independent filtering database (FID) to learn or look up the membership information of the VLAN and decide where to go.

Shared VLAN Learning (SVL) specifies the mode chosen to learn a MAC address. In this mode, some VLANs or 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. For the Gigabit Smart Switch Eco Fanless, you can choose a VID for sharing a filtering database in a Shared VID field if you want to use the existing filtering database. For a specified VLAN, when a MAC address is learned by a switch, the VLAN will use this formation to make forwarding decisions.

Filtering Database (FID) tells you where the packet will be sent. The filtering database will supply the outgoing port according to the request from the forwarding process with VID and DA. When a packet is received, if it has a non-zero VID, then FID will offer the associated outgoing ports information to the packet.

In SVL, VLANs use the same Filtering Database. In IVL, VLANs use different FIDs. Any VID can be assigned to the same FID by the administrator.

How does a Tagged VLAN work?

If the ingress filtering is enabled, when a packet is received, the VLAN bridge will first check if the VID of the packet presents.

1. If the packet has a non-zero VID, the VLAN bridge will apply this VID as the VLAN ID of the packet in the network.
2. For a packet with null tag or no VLAN tag, the VLAN bridge provides rules to decide its VID, then applies this VID to the packet.

If a VLAN bridge does not support any rule for VID, then it applies the PVID of the port to the packet that came from that port. A LAN bridge checks to see if the ingress port and the received packet are on the same VLAN. If not, it drops the packet. If yes, it forwards the packet to the associated ports. Meanwhile, this VLAN must be applied to the egress port, or the packet will be dropped.

If ingress filtering is disabled, a VLAN bridge will only check the MAC address table to see if the destination VLAN exists. If the VLAN does not exist, then the packet is dropped, and if both DA and VLAN do not exist, the packet is forwarded. If it just knows a VLAN existed, it then floods the packet to all the ports the VLAN covers.

If you plan to deploy four VLANs in an office and use a switch to partition them, check which ports belong to which VLAN first.

Table 4-7. Ports assigned to each VLAN.

Name	VID	Port Members
Marketing	2	1, 2, 3, 4, 5
Service	3	6, 7, 20, 21, 22
Sales	4	8, 9, 10, 11, 12, 13, 14, 15, 16
Administration	1	17, 18, 19, 23, 24

Next, the switch assigns an IP address to each VLAN. Usually, we use 10.x.x.x as the internal IP block. Because there are a total of four VLANs in the network, we must assign four IP blocks to each of them.

Table 4-8. Network address assigned to each VLAN.

Name	VID	Network Address
Marketing	2	10.1.2.0/24
Service	3	10.1.3.0/24
Sales	4	10.1.4.0/24
Administration	1	10.1.1.0/24

Here we apply the subnet mask 255.255.255, and each VLAN can support 254 nodes.

4.7 Link Aggregation (LGB2118A Only)

Link Aggregation combines the bandwidth of more than one port to an assigned logical link. This increases total bandwidth to the targeted device. There is more than one Link Aggregation technology in many vendors' switch products already, which may cause an interoperability problem. 802.3ad Link Aggregation Control Protocol (LACP) can solve this problem.

Why 802.3ad (LACP)?

Networks vary. For example, if a port malfunctioned or is unplugged accidentally in a static trunk port, the administrator has to reconfigure it, or the network will have problems. The administrator needs a tool with automatic recovery capability. LACP is a protocol that allows a switch to know whether its partner has the capability to setup a trunk between them.

Usually, if the administrator wishes to increase the bandwidth of a specific link, he may:

1. Buy new network equipment with higher throughput, or

2. Aggregate the bandwidth of more than one port to a logical link.

In case 1, you will pay much more money, and hardware performance may limit the solution's scalability.

In case 2, you save money, because all equipment is there already. You can also the solve the interoperability issue. Applying LACP in your network, you will not only gain the benefits listed below to improve the performance of your network but also have these investments to use for future new products.

1. Public standardized specification.

2. No interoperability issues.

3. No change to IEEE 802.3 frame format; no change in software and management.

4. Increased bandwidth and availability.

5. Load sharing and redundancy.

6. Automatic configuration.

7. Rapid configuration and reconfiguration.

8. Deterministic behavior.

9. Low risk of duplication or mis-ordering.

10. Support existing IEEE 802.3 MAC Clients.

11. Backward compatibility with aggregation-unaware devices.

There are also some constraints when applying LACP:

1. LACP does not support inter-switch bandwidth aggregation.
2. The ports aggregated must operate in full-duplex mode.
3. The ports in the same Link Aggregation Group must operate at the same speed, for example, all 100 Mbps or all 1000 Mbps. You cannot aggregate a 1000 Mbps port and two 100 Mbps ports for a 1.2 Gbps trunk port.

Terminology

Link Aggregation enables multiple physical links with the same media and speed to be bundled as a logical link forming a Link Aggregation Group with a group ID. From the viewpoint of MAC clients, each Link Aggregation Group is an independent link.

Links in a network can be switch-to-switch, switch-to-station, and station-to-station. The station may be a host or a router.

Link Aggregation, sometimes called port trunking, uses two types of link configuration: static port trunk and dynamic port trunk.

- Static Port Trunk: When physical links are changed, the administrator needs to manually configure the switches one by one.
- Dynamic Port Trunk: When physical links are changed, LACP takes over and automatically reconfigure. The administrator does not have to do anything and will see the trap message of LACP changed in NMS.

5. Operation of Web-based Management

This chapter explains how to manage your Gigabit Smart Switch Eco Fanless and how to configure the 10-/100-/1000-Mbps TP Ports and Gigabit SFP Fiber ports on the switch via Web user interfaces. The LGB2118A provides (16) fixed Gigabit Ethernet TP ports and (2) optional SFP ports. The LGB2124A provides (20) fixed Gigabit Ethernet ports and (4) TP/SFP dual-media ports. This enables you to easily access and monitor the status such as MIBs, port activity, and multicast traffic through any ports on the switch.

The default values of the Gigabit Smart Switch Eco Fanless (LGB2118A and LGB2124A) are listed in the table below:

Table 5-1. Default values.

Parameter	Default Value
IP address	192.168.1.1
Subnet mask	255.255.255.0
Default Gateway	192.168.1.254
Password	admin

When the configuration of your Gigabit Smart Switch Eco Fanless is finished, you can browse it using the IP address you set up. For instance, type "http://192.168.1.1" in the address row in a browser, then the following screen (see Figure 5-1) will appear and ask for your username and password input for login and access authentication. The default password is "admin." For first-time access, enter the default password and click on the "Apply" button. This completes the login process.

The Gigabit Smart Switch supports a simplified user management function that allows only one administrator to configure the switch at one time.

To optimize the display effect, we recommend that you use Microsoft® Internet Explorer (IE) and 1024 x 768 display resolution.

The default username is "admin" and the default password is blank (just press Enter), then click on the Log In button.

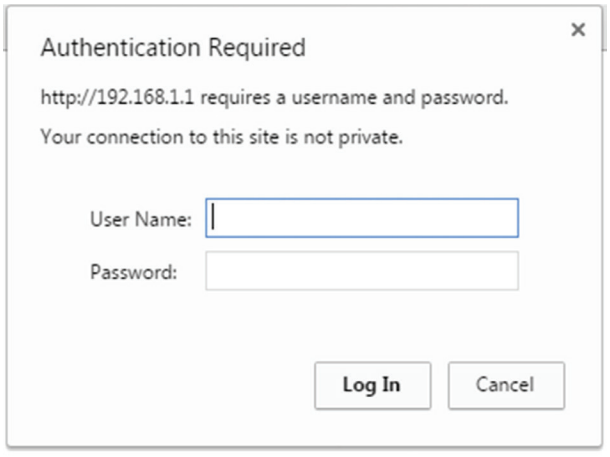


Figure 5-1. Enter password to login screen.

5.1 Web Management Home Overview

After login, System Information is displayed (not shown in this manual). This page lists default values and shows you the basic information of the switch, including Switch Status, TP Port Status, Fiber Port Status, Aggregation, VLAN, Mirror, SNMP, and Maximum Packet Length. With this information, you will know the software version, MAC address, ports available, and so on. This will be helpful if a malfunction occurs. For more details, refer to the Page Layout Information section on the next page.

Page Layout Information

The top part of the information page, shows the front panel of the switch. Linked ports will be displayed in green, and linked-off ports will be in black. For the optional modules, the slots with no module will only show covered plates, the other slots with installed modules would show modules. The images of modules depend on the ones you insert. Vice versa, if ports are disconnected, they will show in black.

The left side of the page shows the Main Menu tree for the Web. According to the function name, all functions can be divided into three parts: Configuration, Monitoring, and Maintenance. To perform a function, click on it. The main function tree for the Web user interface is shown next.

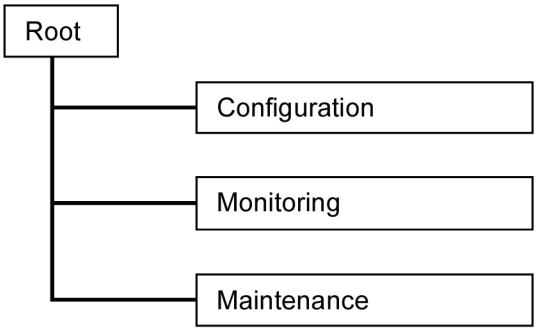


Figure 5-2. Main menu function tree for Web interface.

5.2 Configuration

Configuration includes the following functions: System Configuration, Ports Configuration, VLAN Mode Configuration, VLAN Group Configuration, VLAN Isolation, Aggregation, IGMP Snooping, Mirroring, Loop Detection, Broadcast Storm Protection, and QoS.

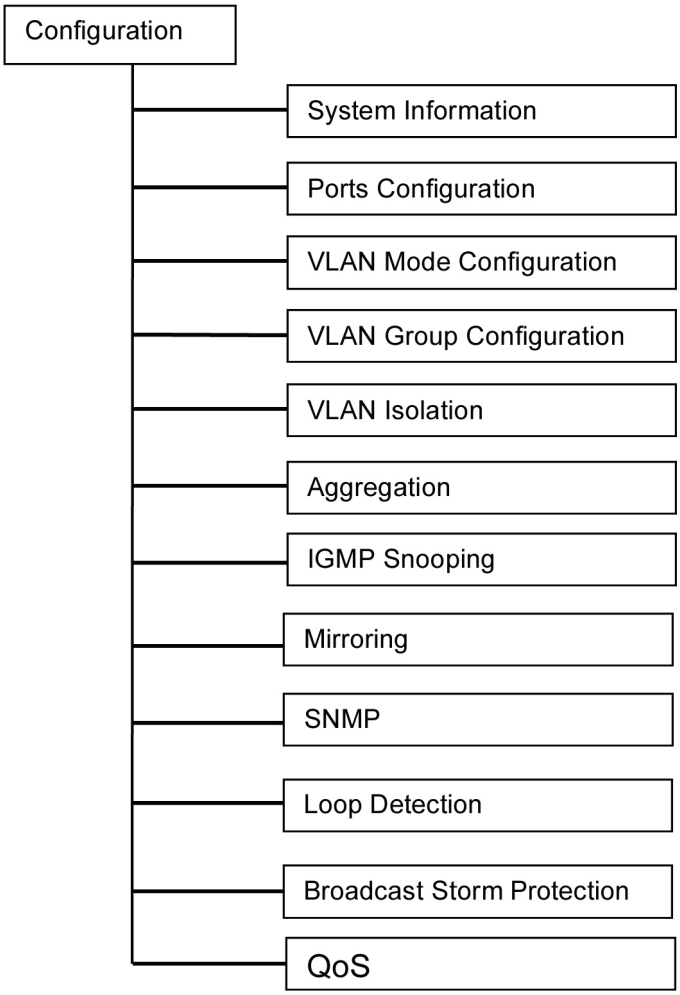


Figure 5-3. Configuration menu function tree.

5.2.1 System Information

System configuration is one of the most important functions. Without a proper setting, the network administrator cannot manage the device. The switch supports manual IP address setting.

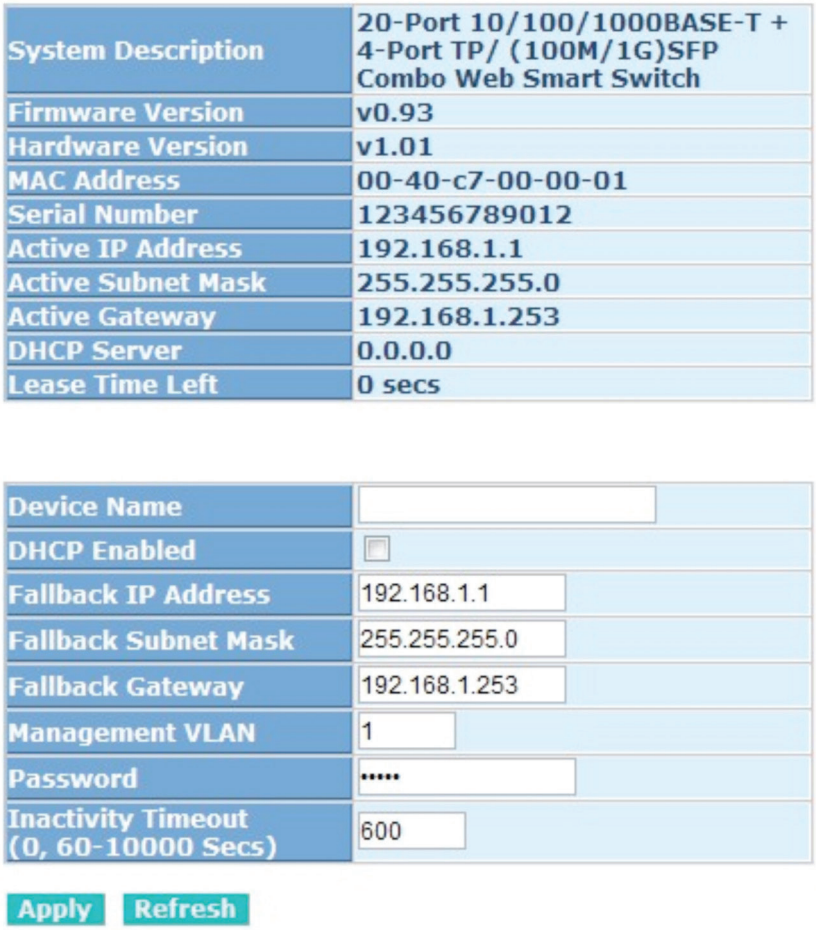


Figure 5-4. System Configuration menu.

Function name: System Configuration

Function description: Show system description, firmware version, hardware version, MAC address, serial number, active IP address, active subnet mask, active gateway, DHCP server, and lease time left.

Set device name, DHCP enabled, fallback IP address, fallback subnet mask, fallback gateway, management VLAN, password, and inactivity timeout.

Parameter description:

System Description: The simple description of this switch.

Firmware Version: The firmware version of this switch.

Hardware Version: The hardware version of this switch.

MAC Address: The Ethernet MAC address of the management agent in this switch.

Serial Number: The serial number assigned by the manufacturer.

Active IP Address: Shows the active IP address of this switch.

Active Subnet Mask: Shows the active subnet mask of this switch.

Active Gateway: Shows the active gateway of this switch.

DHCP Server: Shows the IP address of the DHCP server. The default is 0.0.0.0.

Lease Time Left: Shows the lease time left for the DHCP client.

Device Name: Set a special name for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric characters and the null character are acceptable.

Default: Giga Switch

DHCP Enabled: Enable DHCP snooping, Just tick the check box √ to enable it. The default is disable.

Fallback IP Address: Users can configure the IP settings and fill in new values. Then, click on the "Apply" button to update. The default is 192.168.1.1.

Fallback Subnet Mask: Subnet mask is used to create more network addresses, because any IP device in a network must own its IP address, which is composed of a network address and a host address. Otherwise, the device can't communicate with other devices. Unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, so subnet mask is used to solve this problem. Subnet mask uses some bits from the host address and makes an IP address resemble a network address, subnet mask number, and host address. This reduces the total IP number that a network can support, exponentially, by a power of 2 of the bit number of subnet number ($2^{[\text{bit number of subnet number}]}$).

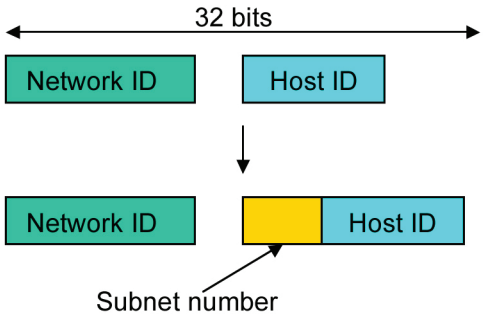


Figure 5-5. IP address.

Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices residing in the same network it attaches to. For more information, see Section 3.1.4, "Address Assignment" in this manual. The default is 255.255.255.0.

Fallback 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. The default is 192.168.1.254.

Management VLAN: Show the management VLAN number.

Password: Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable. The default password is "admin."

Inactivity Timeout (secs): Set the auto-logout timer. The valid value is 0–60 in minutes and a decimal point is not allowed. The value 0 means auto-logout timer is disabled. The default is 0.

5.2.2 Port Configuration

Function name: Port Configuration

Function description: Port Configuration sets the ports on the switch. You can set or reset the values for Mode and Flow Control. You can also set the power-saving mode for switch power consumption.

Figure 5-6. Port Configuration menu.

Parameter description:

Enable Jumbo Frames: This function supports jumbo frames of up to 9600 bytes. Just tick the check box to enable it. The default is disable.

Power Saving Mode: This function supports power saving. Select Full/ Link-up/Link-down/Disable using the drop-down menu. Default: disable

Link: Show link status of this port.

Mode: Set the speed and duplex of the port. If the media is 1-Gbps fiber, there are three modes to choose from: Auto Speed, 1000 Full, and Disable. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10-/100-/1000-Mbps, and duplex mode, full-duplex and half-duplex. The table on the next page summarizes the function the media supports.

Table 5-2. Media supported.

Media Type	Auto-negotiation	Speed	Duplex
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

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

Flow Control: You can tick the check box to enable flow control. If flow control is set to Enable, both parties can send PAUSE frames to the transmitting device(s) if the receiving port is too busy to handle the traffic. When it is set to Disable, there will be no flow control in the port. It drops the packet if it is too much to handle. The default is disable.

5.2.3 VLAN Mode Configuration

The switch supports Port-based VLAN and Tag-based VLAN (802.1q). Its VLAN mode supports 10 active VLANs and the available VLAN ID range is from 1–4094. VLAN configuration is used to divide a LAN into smaller ones. With proper configuration, you can gain not only improved security and increased performance, but also save a lot of VLAN management effort.

Function name: VLAN Mode Setting

Function description: The VLAN Mode Selection function includes four modes: Port-based, Tag-based, Metro mode, or Disable. Choose one of them via the drop-down menu. Then, click on the "Apply" button, and the settings will take effect immediately.

Figure 5-7. Select VLAN Mode

Parameter description:

VLAN Mode:

Port-based: Port-based VLAN is defined by port. Any packet coming in or going out from any one port of a port-based VLAN will be accepted. A no-filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, a port-based VLAN named PVLAN-1 contains port members Port 1, 2, 3, and 4. If you are on Port 1, you can communicate with Port 2, 3, or 4. If you are on Port 5, then you cannot talk to them. Each port-based VLAN you build must be assigned a group name. This switch can support up to 12 groups.

Tag-based: Tag-based VLAN identifies its members by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports a supplement of 802.1q. For more details, see VLAN in Section 4.6.

Each tag-based VLAN you built must be assigned a VLAN name and a VLAN ID. A valid VLAN ID is 1–4094. Users can create up to 16 VLANs simultaneously.

5.2.4 VLAN Group Configuration

Function name: Tag-Based VLAN Configuration (Tag based VLAN mode)

Function description: The VLAN membership configuration for the selected switch can be monitored and modified here. Up to 4094 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

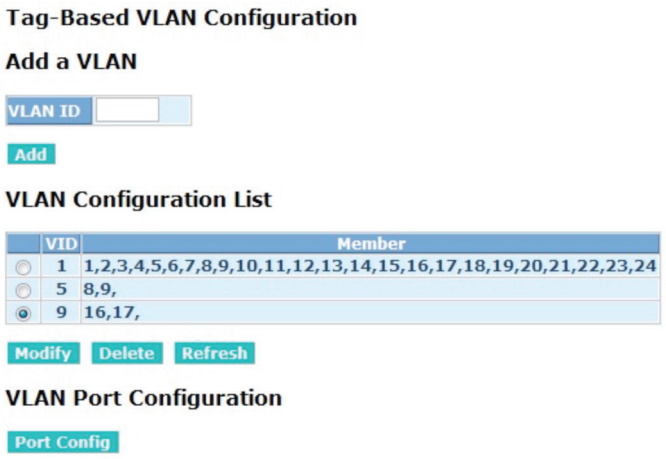


Figure 5-8. tag-VLAN Mode.

Figure 5-9. Per port configuration.

Parameter description:

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

Member: In the modify function, 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 Port x to enable it.

Port: Port number.

VLAN aware Enabled: Discard other VLAN group packets, and only forward this port to joined VLAN group packets.

Packet Type:

All: Forward all tagged and untagged packets.

Tagged Only: Forward tagged packets only and discard untagged packets.

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.

Function name: Port-Based VLAN Configuration (Port-based VLAN mode)

Function description shows the VLAN Groups' information, and allows administrators to maintain them by modifying and deleting each VLAN group. Users also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in a port-based VLAN, it will just show the ID member of the existing port-based VLAN group. If you are in a tag-based VLAN, it will show the ID, VID, and member of the existing tag-based VLAN group. The switch can store the port-based VLAN and tag-based VLAN configurations separately. When you choose one of VLAN modes, the switch shows the VLAN configuration, which keeps the default data. You can easily create and delete a VLAN group by pressing the "Add" and "Delete" function buttons, or click the Group ID directly to edit it.

Figure 5-10. Port-Based VLAN Configuration.

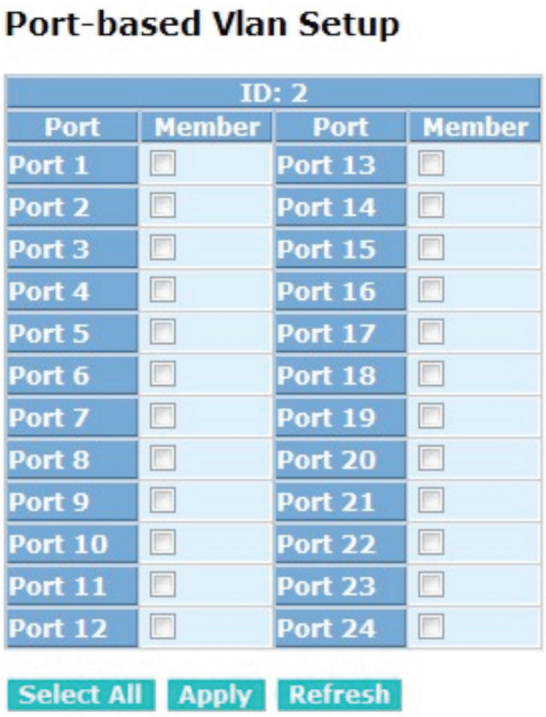


Figure 5-11. Add or Remove VLAN Member.

Parameter description:

ID (Group ID): When you want to edit a VLAN group, you must select the Group ID field. Then, you will enter the Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, depending on which VLAN mode you select.

Member: In modify function, this is used to enable or disable if a port is a member of the newly 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 or tag-based VLAN, which depends on the VLAN mode you choose in the VLAN mode function.

Delete Group: Just tick the check box beside the ID, then press the "Delete" button to delete the group.

5.2.5 VLAN Port Isolation Configuration

Function name: Port Isolation Configuration

Function description: Port Isolation provides a method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. It applies to a switch that has more than one port, and each port is configured as a protected port or a non-protected port. An address table memory stores an address table with a destination address and port number pair. A forwarding map generator generates a forwarding map that responds to a data packet's destination address. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on a data packet is matched with a physical address on the layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to all the ports indicated by the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

Use this page for enabling or disabling port isolation on ports in a private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and private VLAN.

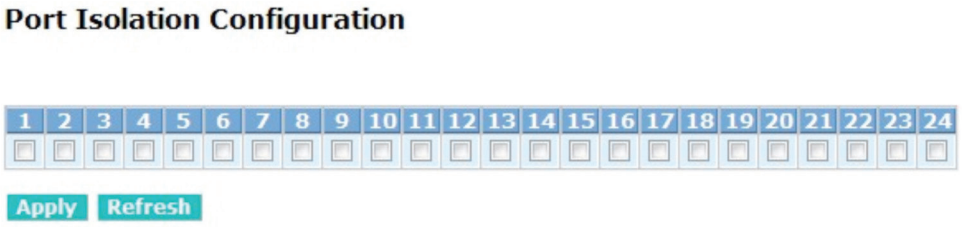


Figure 5-12. Port Isolation configuration.

Parameter description:

Port Members: A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

5.2.6 Aggregation (LGB2118A Only)

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle ports by the same speed, MAC, and full duplex to be a single logical port, so the logical port can aggregate the bandwidth of these ports. This means you can use your current Ethernet equipment to build the bandwidth aggregation. For example, if three Fast Ethernet ports are aggregated into a logical port, then this logical port's bandwidth would be three times as high as a single Fast Ethernet port's.

Function name: Aggregation Configuration

Function description: Display the current setup of Aggregation Trunking. With this function, the user is allowed to add a new trunking group or modify the members of an existing trunking group.

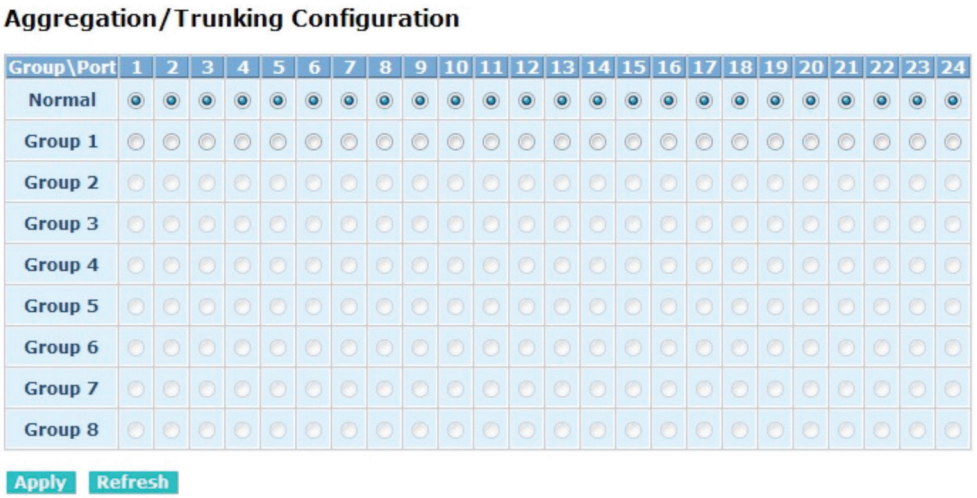


Figure 5-13. Aggregation/Trunking Configuration.

Parameter description:

Normal: Set up the ports that do not join any aggregation trunking group.

Group 1–8: Group the ports you choose together. Up to 12 ports can be selected for each group.

5.2.7 IGMP Snooping

Function name: IGMP Snooping Configuration

Function description: IGMP Snooping lets administrators configure a switch to constrain multicast traffic by listening to Internet Group Management Protocol (IGMP). After finishing the settings, click on the "Apply" button to start up the function.

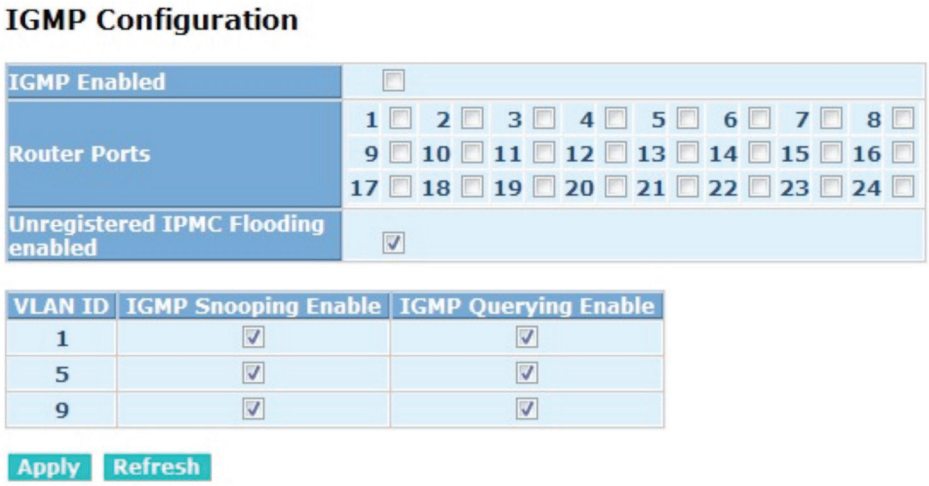


Figure 5-14. IGMP Configuration.

Parameter description:

IGMP Enabled: Just tick the check box to enable this function. The default is disable.

Router Ports: Just tick the check box beside Port x to enable router ports, then press the "Apply" button to start up. The default is none.

Unregistered IGMP Flooding enabled: Just tick the check box to enable this function. The default is enable.

VLAN ID: When IGMP Enable mode is selected, it will list the VLAN ID number.

IGMP Snooping Enabled: After the IGMP Enabled function starts up, tick the check box to enable this function. The default is enable.

IGMP Querying Enabled: After IGMP Enabled function starts up, tick the check box to enable this function. The default is enable.

5.2.8 Mirroring Configuration

Function name: Mirror Configuration

Function description: Mirror Configuration enables the switch to monitor the traffic in the network. This switch supports one-port mirroring multi-ports. For example, if Port A and Port B are Source Ports, and Port C is Mirror Port, the traffic passing through Port A and Port B will be copied to Port C for monitoring.

Parameter description:

Source Port: Set up the port you want to monitor. Just tick the check box beside Port x. Valid ports are Port 1–10.

Mirror Port: Use the drop-down menu to select a mirror port.

Figure 5-15. Mirror ports configuration.

5.2.9 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the managed devices equipped with an SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. This protocol governs 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. An SNMP agent is running on the switch in response the request issued by the SNMP manager.

SNMP is passive except for issuing the trap information. The switch can turn on or off the SNMP agent. If you set the field SNMP to "Enable," the SNMP agent will start. If the field SNMP is set to "Disable," the SNMP agent will be deactivated, and the related Community Name, Trap Host IP Address, Trap, and all MIB counters will be ignored.

Function name: SNMP Configuration

Function description: This function is used to configure SNMP settings, community name, trap host, and public traps, 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. Both parties must have the same community name. Once completing the setting, click on the "Apply" button, and the setting takes effect.

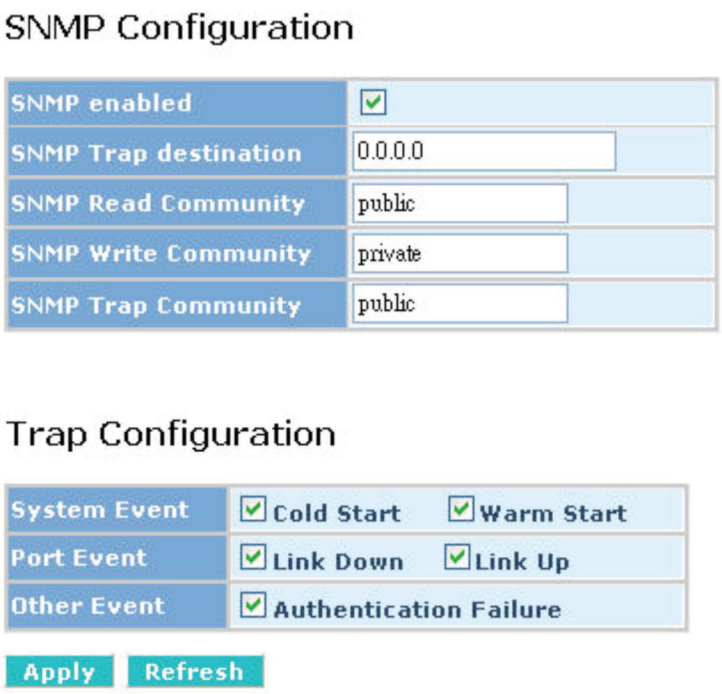


Figure 5-16. SNMP Configuration.

Parameters description:

SNMP enable: The term SNMP enable here is used for the activation or deactivation of SNMP. The default is "Disable."

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. So, the requesting network management unit cannot access the device with a different community name via SNMP protocol; if they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case-sensitive, with no blanks in the community name string. Any printable character is allowed.

The community name for each function works independently. For example, the community name for Read-only works for the Read function and can't be applied to other function, such as Write and Trap.

Default SNMP function: Disable

Default community name for Get: Public

Default community name for Set: Private

Default community name for Trap: Public

System Event: The System Event trap enable here is used for the "cold boot" or "warm boot" of System Event. The default is "Disable."

TP and Fiber Port Event: The TP and Fiber Port Event trap enabled here is used for the "link up" or "link down" of a System Event. The default is "Disable."

Other Event: Authentication fails.

5.2.10 Loop Detection

Function name: Loop Detection Configuration

Function description: The loop detection is used to detect the presence of traffic. When a packet's looping detection frame is received by the switch and has a MAC address the same as its own from a port, loop detection occurs. The port will be locked when it receives the looping detection frames. To resume the locked port, delete the looping path, then select "Unlock port" and click on "Apply" to turn on the locked ports.

Figure 5-17. Loop Detection Configuration.

Parameter description:

Mode: Controls whether Loop Detection is enabled (as a whole).

Unlock Time: The period (in seconds) for which a port will be kept disabled if a loop is detected (and the port shuts down).

State: Show the status on the port.

Protocol Enabled: Controls whether Loop Detection is enabled on this switch port.

When a port number is chosen and Loop detection is enabled, the port detects the loop and the port will be locked. If no Loop occurred, the port remains unlocked.

Unlock port: When ticking the port, the locked port will be opened and become unlocked. If the port is not checked √, it remains locked.

5.2.11 Broadcast Storm Protection

Function name: Broadcast Storm Protection configuration

Function description: When the broadcast packets received by the switch exceed the threshold configured, the port will be blocked for a period of time that can be set. After a configured time, the switch will detect whether the broadcast packets received on the port still exceed the threshold. If the broadcast traffic is still higher than the configured threshold, the port will be closed for a period of time again. If the broadcast traffic is under the threshold, the port will re-open and forward the packets normally.

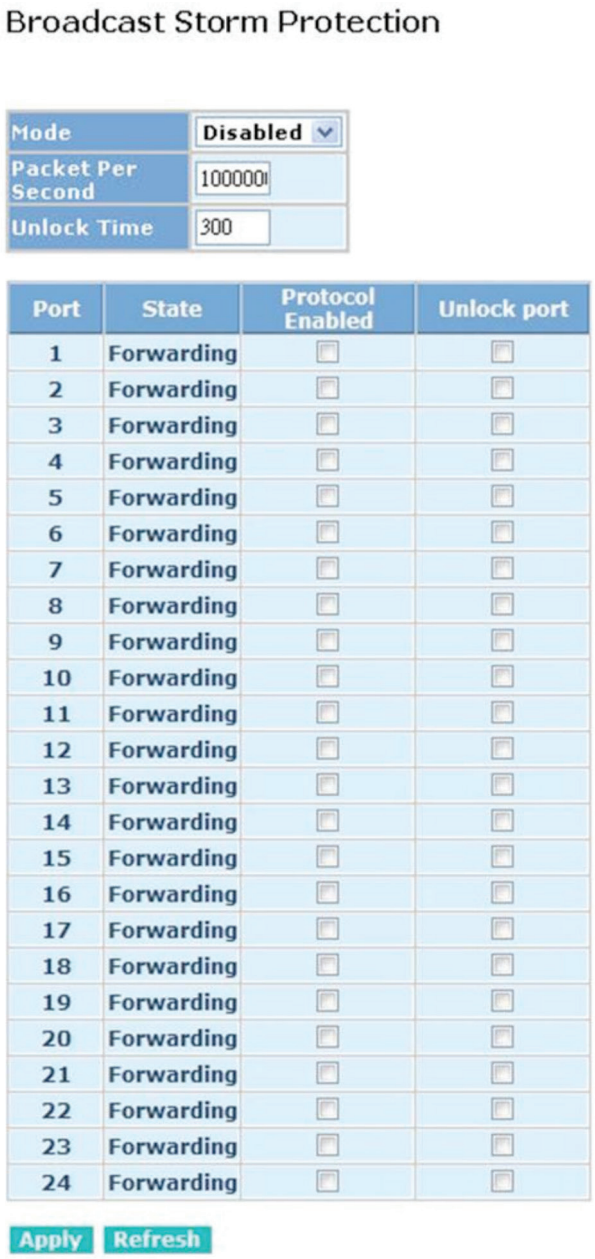


Figure 5-18. Rate Limit Configuration.

Parameter description:

Mode: Controls whether Broadcast Strom Protection is enabled (as a whole).

Packet Per Second: When the broadcast packet traffic in a second is higher than the threshold configured, Broadcast Storm Protection is enabled.

Unlock Time: The period (in seconds) for which a port will be kept disabled if a loop is detected (and the port action is to shut down the port).

Port: Port number.

State: Show the status on the port.

Protocol Enabled: Controls whether Broadcast Strom Protection is enabled on this switch port.

Unlock port: Tick the checkbox next to the locked port and it will be opened and changed to unlocked. If you don't tick the port checkbox, it remains locked.

5.2.12 Quality of Service (QoS) Configuration

The QoS function supports VLAN-tagged priority that can set eight priorities, and DSCP (Differentiated Services Code Point) on Layer 3 of the network framework.

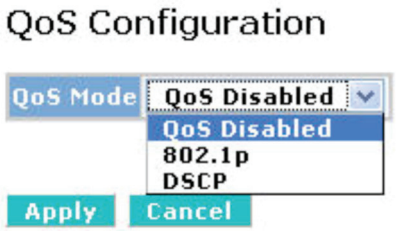


Figure 5-19. QoS Configuration.

Function name: QoS Configuration

Function description: When setting the QoS function, first select QoS Mode in the drop-down menu. Then you can use 802.1p Priority and DSCP Priority functions. You can enable/disable QoS Mode and set Priority Control, such as 802.1p and DSCP. The switch only supports Strict Priority. High priority queue is always passed first.

Function name: 802.1p QoS Mode

Function description: This function will affect the priority of VLAN tag. Based on the priority of the VLAN tag, it can arrange 0–7 priorities that can map to 4 queues of the switch (low, normal, medium, high) and possess different bandwidth distribution according to your weight setting.

Parameter description:

Prioritize Traffic: Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting applies to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

Port Number: When Custom is selected for Prioritize Traffic, you may assign a specific Port Number for 802.1p Configuration.

802.1p Configuration: Each Priority can select any Queue. In Default, Priority 0 is mapping to Queue normal, Priority 1 is mapping to Queue low, Priority 2 is mapping to Queue low, Priority 3 is mapping to Queue normal, Priority 4 is mapping to Queue medium, Priority 5 is mapping to Queue medium, Priority 6 is mapping to Queue high, and Priority 0 is mapping to Queue high.

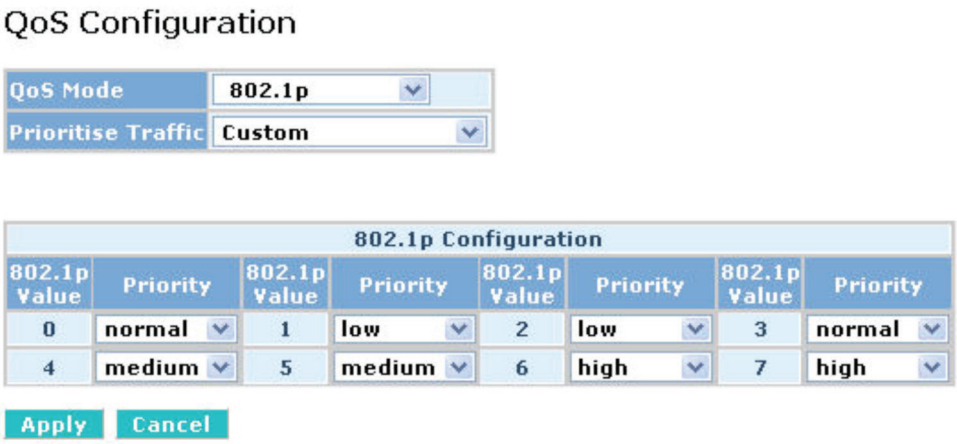


Figure 5-20. 802.1p Setting.

Function name: DSCP QoS Mode

Function description: 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 are a codepoint, 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, the user is allowed to set up these 64 kinds of Class that belong to any queue (low, normal, medium, high).

Parameter description:

Prioritize Traffic: Five Prioritize Traffic values are provided: Custom, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.

Port Number: When Custom is selected for Prioritize Traffic, you may assign a specific Port Number for DSCP Configuration.

DSCP Configuration: Can be 64 kinds of priority traffic as mentioned above. The user can set up any Queue (low, normal, medium, high). In default, Priorities 0–63 map to Queue high.

Figure 5-21. DSCP Setting.

5.3 Monitoring

There are four functions contained in the monitoring function.

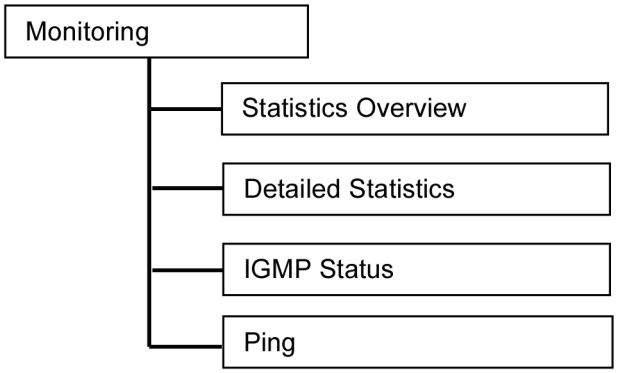
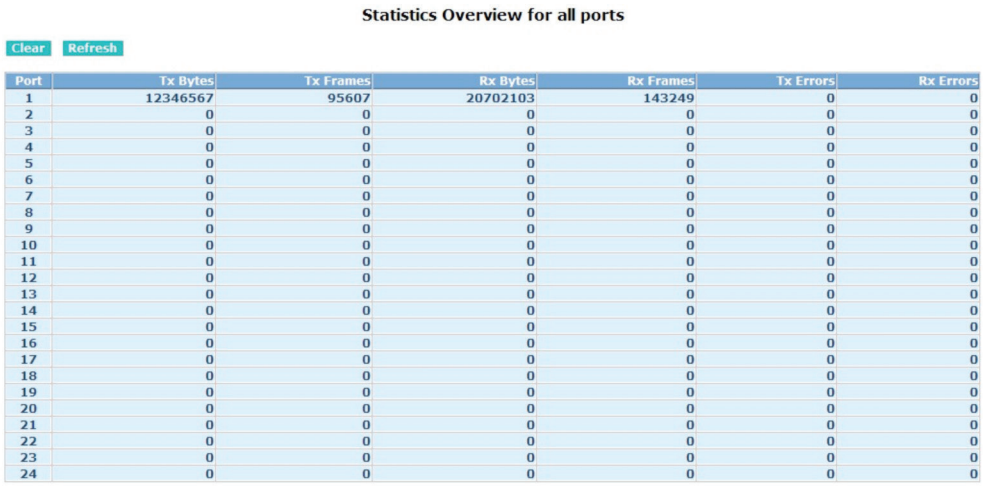


Figure 5-22. Monitoring menu tree.

5.3.1 Statistics Overview

Function name: Statistics Overview for all ports

Function description: The section describes the Port statistics information and provides an overview of general traffic statistics for all switch ports.



Statistics Overview for all ports

Clear Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	12346567	95607	20702103	143249	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	0	0	0	0

Figure 5-23. Statistics Overview for all ports.

Parameter description:

Tx/Rx Bytes: The number of received and transmitted bytes per port.

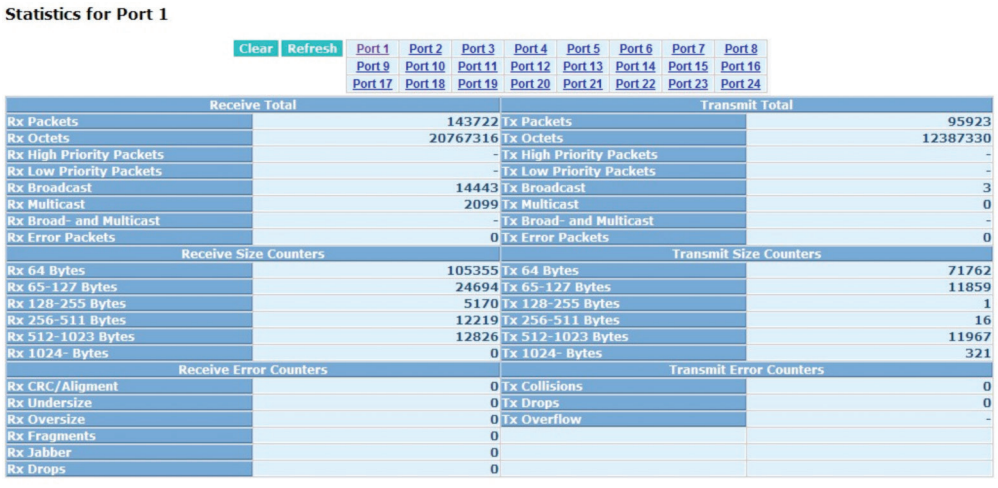
Tx/Rx Frames: The number of received and transmitted frames per port.

Tx/Rx Errors: The number of frames received in error and the number of incomplete transmissions per port.

5.3.2 Detailed Statistics

Function name: Detailed Statistics

Function description: Display the detailed counting number of each port's traffic. This window can show all counter information for each port at one time.



Statistics for Port 1

Clear Refresh Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8 Port 9 Port 10 Port 11 Port 12 Port 13 Port 14 Port 15 Port 16 Port 17 Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24

Receive Total		Transmit Total	
Rx Packets	143722	Tx Packets	95923
Rx Octets	20767316	Tx Octets	12387330
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	14443	Tx Broadcast	3
Rx Multicast	2099	Tx Multicast	0
Rx Broad- and Multicast	-	Tx Broad- and Multicast	-
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	105355	Tx 64 Bytes	71762
Rx 65-127 Bytes	24694	Tx 65-127 Bytes	11859
Rx 128-255 Bytes	5170	Tx 128-255 Bytes	1
Rx 256-511 Bytes	12219	Tx 256-511 Bytes	16
Rx 512-1023 Bytes	12826	Tx 512-1023 Bytes	11967
Rx 1024- Bytes	0	Tx 1024- Bytes	321
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Aligment	0	Tx Collisions	0
Rx Undersize	0	Tx Drops	0
Rx Oversize	0	Tx Overflow	-
Rx Fragments	0		
Rx Jabber	0		
Rx Drops	0		

Figure 5-24. Detailed Statistics for each port.

Parameter description:

Rx Packets: The counting number of the packet received.

RX Octets: Total received bytes.

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

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

Rx Broadcast: Show the counting number of the received broadcast packet.

Rx Multicast: Show the counting number of the received multicast packet.

Rx Broadcast and Multicast: Show the counting number of the received broadcast with multicast packet.

Rx Error Packets: Show the counting number of the received error packets.

Tx Packets: The counting number of the packet transmitted.

TX Octets: Total transmitted bytes.

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

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

Tx Broadcast: Show the counting number of the transmitted broadcast packet.

Tx Multicast: Show the counting number of the transmitted multicast packet.

Tx Broadcast and Multicast: Show the counting number of the transmitted broadcast with multicast packet.

Tx Error Packets: Show the counting number of the received error packets.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tx Collisions: Number of collisions transmitting frames experienced.

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

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

5.3.3 IGMP Status

Function name: IGMP Status

Function description: Display IGMP status. In Fig. 5-26, the window shows the VLAN ID for each multicast group.

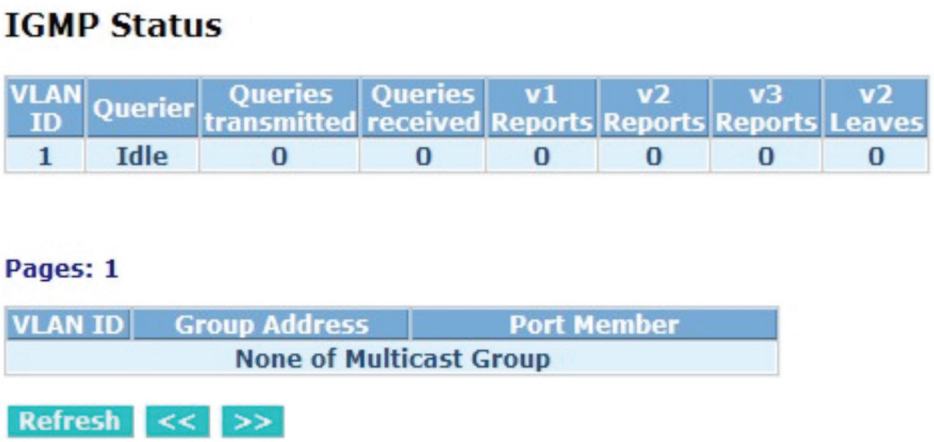


Figure 5-25. IGMP Status.

Parameter description:

VLAN ID: Show VLAN ID for each multicast group.

Querier: Show the group membership queries status.

Queries transmitted: Count the group membership queries transmitted.

Queries received: Count the group membership queries received.

V1 Reports: When a host receives a group membership query, it identifies the groups associated with the query and determines which groups it belongs to. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It calculates the number of times IGMPV1 reports.

V2 Reports: When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It calculates the number of times IGMPV2 reports.

V3 Reports: When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It calculates the number of times IGMPV3 reports.

V2 Leaves: When a host leaves a group, it sends a leave group membership message to multicast routers on the network, it shows the leaves number.

5.3.4 Ping Status

Function name: Ping Status

Function description: Set up a target IP address for ping function and display ping status. In Fig. 5-27, the window shows the ping information.

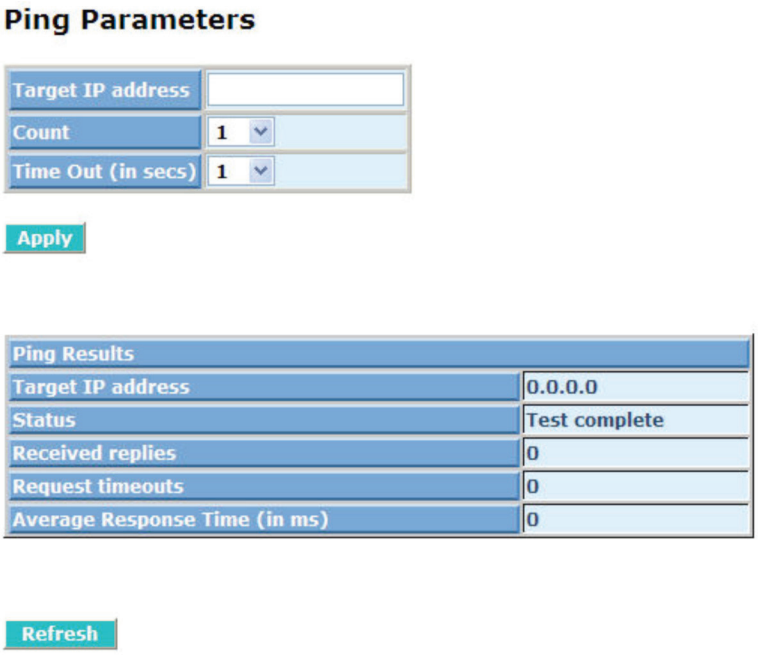


Figure 5-26. Ping.

Parameter description:

Ping Parameters:

Target IP address: Set up a Target IP address to ping.

Count: Use the drop-down menu to set number of echo requests to send. Choose from four numbers: 1, 5, 10, and 20. Default: 1

Time Out (in secs): Use the drop-down menu to set number of echo requests time out in seconds. Choose from four numbers: 1, 5, 10, and 20. Default: 1.

NOTE: Press the "Apply" button to start up after you set up the parameters.

Ping Results:

Target IP address: Show the active target IP address.

Status: Show the result of the ping status.

Received replies: Show the received replies number of times.

Request timeouts: Show the timeout of request.

Average Response times (In ms): Show the average response time in milliseconds.

5.4 Maintenance

There are five functions contained in the maintenance function.

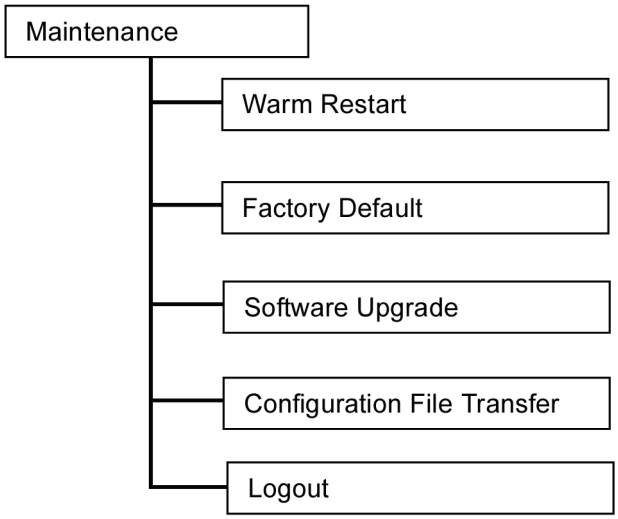


Figure 5-27. Maintenance menu tree.

5.4.1 Warm Restart

You can reboot the switch in three ways: power up, hardware reset, and software reset. Press the "Reset" button on the front panel of your switch to reset the device and to retrieve default settings. After upgrading software, you have to reboot the device to have the new configuration take effect. This is a software reset.

Function name: Warm Restart

Function description: Reboot the switch. Reboot has the same effect as pressing the Reset button on the front panel of the switch. Press the "Yes" button to confirm the warm restart function, and it will take around thirty (30) seconds to complete the system boot.

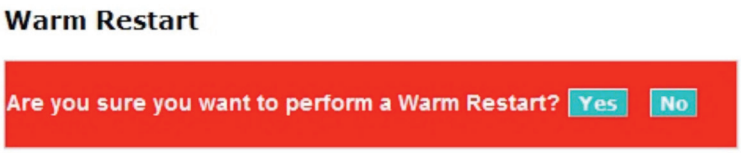


Figure 5-28. Warm Restart.

5.4.2 Factory Default

Function name: Factory Default

Function description: Factory Default provides the function to retrieve default settings and replace the current configuration. Except for the IP address setting, all settings will be restored to the factory default values when the "Factory Default" function is performed. If you want to restore all configurations including the IP address setting to the factory default, please press the "Reset" button on the front panel.

Note for "Reset" button: You must press the "Reset" button for more than 3 seconds to restore the factory default setting.

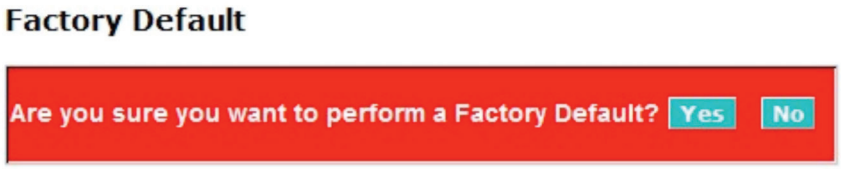


Figure 5-29. Factory Default.

5.4.3 Software Upgrade

Function name: Software Upgrade

Function description: You can just click the "Browse" button to retrieve the file you want in your system to upgrade your switch.

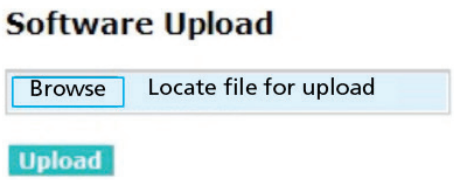


Figure 5-30. Software Upgrade.

5.4.4 Configuration File Transfer

Function name: Configuration File Transfer

Function description: You can backup your switch's configuration file into your computer folder in case an accident happens. Uploading a backup configuration file into a new or a crashed switch also saves time and avoids mistakes.

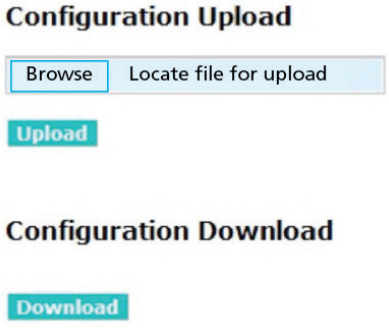


Figure 5-31. Configuration Upload/Download.

5.4.5 Logout

In addition to the auto logout function we just mentioned in the system configuration section, the switch also allows administrators to logout manually using the Logout function.

Function name: Logout

Function description: The switch allows you to logout from the system to prevent other users from accessing the system without permission. If you do not logout and exit the browser, the switch will automatically log you out. Besides this manual logout and implicit logout, you can set up the Auto Logout Timer parameter in the system configuration function to turn ON/OFF the logout function.

Figure 5-32. Manual logout.

Parameter description:

Auto/Manual Logout: If there is no activity in the user interface set up in the time you allotted for the Auto Logout Timer, the switch will log you out automatically. Or, press the "Logout" button to exit the system manually.

6. Troubleshooting

6.1 Resolving a No Link Condition

There are four possible causes for a no-link LED status:

- 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 Questions and Answers

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Gigabit Smart Switch Eco Fanless.

- The network device of Computer C may fail to work. Check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
- The network configuration of Computer C may have something wrong. Verify the network configuration on Computer C.

2. The uplink connection function fails to work.

- Check if connection ports are used on the Gigabit Smart Switch Eco Fanless.
- Check the uplink setup of the Gigabit Smart Switch Eco Fanless to verify the uplink function is enabled.

3. The console interface doesn't appear on the console port connection.

- The Gigabit Smart Switch Eco Fanless has no console port, so you cannot use the console interface to connect with the Gigabit Smart Switch Eco Fanless.

4. How do I configure the Gigabit Smart Switch Eco Fanless?

- You can configure the switch via an Internet Explorer® (IE) Web browser interface. First, choose any port in the Gigabit Smart Switch Eco Fanless. Then, use IE and type default IP address, 192.168.1.1, to connect to a Gigabit Ethernet with a RJ-45 network line. The login screen will appear.

4.3 Contacting Black Box

If you determine that your Gigabit Smart Switch Eco Fanless is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

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.

4.4 Shipping and Packaging

If you need to transport or ship your Gigabit Smart Switch Eco Fanless:

- Package it carefully. We recommend that you use the original container.
- If you are returning the unit, make sure you include everything you received with it. Before you ship for return or repair, contact Black Box to get a Return Authorization (RA) number.

Appendix: MIB Specifications

A brief description of the MIB II Enterprise MIB brief appears next. For technical support or the latest version of MIB download, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

```
PRIVATE-GESM-SW10-MIB DEFINITIONS ::= BEGIN

IMPORTS
        mib-2, DisplayString,ifIndex                    FROM RFC1213-M
        enterprises,Counter, TimeTicks, Gauge,IpAddress  FROM RFC1155-SMI
        OBJECT-TYPE                                     FROM RFC-1212
        TRAP-TYPE                                       FROM RFC-1215;

privatetech         OBJECT IDENTIFIER ::= { enterprises 5205 }

switch               OBJECT IDENTIFIER ::= { privatetech 2 }

gesmsw24LProductId       OBJECT IDENTIFIER ::= { switch 7 }

gesmsw24LProduces        OBJECT IDENTIFIER ::= gesmsw24LProductId 1 }

gesmsw24LIllegalLogin  TRAP-TYPE
        ENTERPRISE gesmsw24LProductId
        DESCRIPTION
        "Send this trap when the illegal user try to login the Web management UI. " ::= 1

gesmsw24LRxErrorThreshold  TRAP-TYPE
        ENTERPRISE gesmsw24LProductId
        VARIABLES   { ifIndex }
        DESCRIPTION
        "Send this trap when the number of the Rx bad packet over the Rx Error
        Threshold. The OID value means the port number. "::= 2

gesmsw24LTxErrorThreshold  TRAP-TYPE
        ENTERPRISE gesmsw24LProductId
        VARIABLES   { ifIndex }
        DESCRIPTION
        "Send this trap when the number of the Tx bad packet over the Tx Error Threshold.
        The OID value means the port number. " ::= 3


END
```

Black Box Tech Support: FREE! Live. 24/7.

Great tech support is just 60 seconds away at 724-746-5500 or blackbox.com.

About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 60 seconds or less.

© Copyright 2016. Black Box Corporation. All rights reserved. Black Box® and the Double Diamond logo are registered trademarks of BB Technologies, Inc. Any third-party trademarks appearing in this manual are acknowledged to be the property of their respective owners.

lgb2118a_user_rev3