



GE-DS-242-PoE Managed Ethernet Switch User Manual



Copyright	<p>© 2010 GE Security, Inc.</p> <p>This document may not be copied in whole or in part or otherwise reproduced without prior written consent from GE Security, Inc., except where specifically permitted under US and international copyright law.</p>
Disclaimer	<p>The information in this document is subject to change without notice. GE Security, Inc. ("GE Security") assumes no responsibility for inaccuracies or omissions and specifically disclaims any liabilities, losses, or risks, personal or otherwise, incurred as a consequence, directly or indirectly, of the use or application of any of the contents of this document. For the latest documentation, contact your local supplier or visit us online at www.gesecurity.com.</p> <p>This publication may contain examples of screen captures and reports used in daily operations. Examples may include fictitious names of individuals and companies. Any similarity to names and addresses of actual businesses or persons is entirely coincidental.</p>
Trademarks and patents	<p>GE and the GE monogram are trademarks of General Electric Company.</p> <p>Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.</p>
Intended use	<p>Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.gesecurity.com.</p>
FCC compliance	<p>This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.</p> <p>You are cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.</p>
Regulatory information	
Manufacturer	<p>GE Security, Inc.</p> <p>HQ and regulatory responsibility: GE Security, Inc., 8985 Town Center Parkway, Bradenton, FL 34202, USA</p> <p>EU authorized manufacturing representative: GE Security B.V., Kelvinstraat 7, 6003 DH Weert, The Netherlands</p>
European Union directives	 <p>2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.</p>
Contact information	<p>For contact information see our Web site: www.gesecurity.com.</p> <p>For contact information see our Web site: www.gesecurity.eu.</p>

Content

Chapter 1 Introduction 1

- Package Contents 2
- Product Description 2
- How to Use this Manual 3
- Product Features 4
- Product Specifications 7

Chapter 2 Installation 11

- Hardware Description 12
- Switch Installation 15

Chapter 3 Switch Management 21

- Requirements 22
- Management Access Overview 22
- Web Management 23
- SNMP-Based Network Management 25
- Administration Console 25
- Protocols 27
- Management Architecture 28

Chapter 4 Web-Based Management 29

- About Web-based Management 29
- System 34
- VLAN Configuration 54
- Rapid Spanning Tree 69
- Trunking 81
- Forwarding and Filtering 88
- IGMP Snooping 91
- QoS Configuration 96
- Access Control List 102
- MAC Limit 107
- 802.1X Configuration 109
- Power Over Ethernet 117

Chapter 5 Console Management 123

- Login in the Console Interface 123
- Configure IP address 125
- Commands Level 127

Chapter 6 Command Line Interface 129

- Operation Notice 129
- System Commands 130
- Switch Static Configuration 131
- Trunk Configuration 137
- VLAN Configuration 140
- Misc Configuration 149
- Administration Configuration 151
- MAC limit 156
- Port Mirroring Configuration 157
- Quality of Service 158
- MAC Address Configuration 161
- STP/RSTP Commands 164
- SNMP 169
- IGMP 173
- 802.1x Protocol 175
- Access Control List 179
- Binding 184
- Power over Ethernet Commands 186

Chapter 7 Switch Operation 193

Chapter 8 Power Over Ethernet Overview 197

- What is PoE? 197

Chapter 9 Troubleshooting 205

Appendix A RJ-45 Pin Assignment 207

- Switch's RJ-45 Pin Assignments 207
- 10/100Mbps, 10/100Base-TX 208

Chapter 1

Introduction



The GE Security **GE-DS-242-PoE** offers 24 10/100Mbps Fast Ethernet ports with 2 Gigabit TP/SFP combo ports (Port-25, 26). The two Gigabit TP/SFP combo ports can be either 1000Base-T for 10/100/1000Mbps or 1000Base-SX/LX through SFP (Small Form-Factor Pluggable) interface. The GE-DS-242-PoE has a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 8.8Gbps. Its two built-in GbE uplink ports also offer incredible extensibility, flexibility and connectivity to the Core switch or Server.

The PoE in-line power following the standard **IEEE 802.3af** makes the **GE-DS-242-PoE** able to power on 24 PoE devices at the distance up to 100 meters through the 4-pair Cat 5/5e UTP wire.

Package Contents

What's in the box

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

The Managed Switch	x1
User's manual CD	x1
Installation Sheet	x1
19" Rack mount accessory kit	x1
Power cord	x1
Rubber feet	X4
RS-232 cable	x1

If any of these are missing or damaged, please contact your dealer immediately. If possible, retain the carton including the original packing material, and use them to repack the product in case there is a need to return it.

Product Description

High Performance Wire-Speed Switching

The GE Security GE-DS-242-PoE Managed Switch offers 24 Ethernet ports with 2 Gigabit TP / SFP combo ports (Port-25, 26). The type 24 Fast Ethernet ports of GE-DS-242-PoE are 10 / 100Base-TX copper (RJ-45). These two Gigabit TP / SFP combo ports of all models can be either 1000Base-T for 10/100/1000Mbps or 1000Base-SX/LX through SFP (Small Form-factor Pluggable) interface. The distance can be extended from 200 meters (TP), 550 meters (Multi-mode fiber), up to above 10/20/30/70 kilometers (Single-mode fiber).

The series Managed Switch boasts a high performance switch's architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 8.8Gbps. Its two built-in GbE uplink ports also offer incredible extensibility, flexibility and connectivity to the Core switches or Servers.

Power Over Ethernet

The PoE in-line power following the standard IEEE 802.3af makes the GE-DS-242-PoE able to power on 24 PoE devices at a distance of up to 100 meters through the 4-pair Cat 5/5e UTP wire.

Cost-effective solution with SNMP monitor for Network deployment

GE Security releases the cost-effective Managed Switch not only for catering to the need of easy WEB-based management, but also the centralized SNMP application to monitor the status of Switch and traffic per port. The key features are:

- WEB / SSL / Telnet
- 802.1Q / Q-in-Q VLAN
- Rapid Spanning Tree
- IGMP Snooping
- 802.1X Authentication / RADIUS
- Access Control List
- SNMP and 4 RMON groups

How to Use this Manual

This User Manual is structured as follows:

Section	Section Content
INTRODUCTION	Product description with features and specifications
INSTALLATION	Explains the functions of the Managed Switch, and how to physically install the Managed Switch
SWITCH MANAGEMENT	Contains information about the software function of the Managed Switch
WEB CONFIGURATION	Explains how to manage the Managed Switch by Web interface
CONSOLE MANAGEMENT	Describes how to use the Console management interface
COMMAND LINE INTERFACE	Explains how to manage the Managed Switch by Command Line interface
SWITCH OPERATION	Explains how to operate the Managed Switch
POWER OVER ETHERNET OVERVIEW	Introduces the IEEE 802.3af PoE standard and PoE provision of the Managed Switch.
TROUBLESHOOTING	Explains how to troubleshoot the Managed Switch
APPENDIX A	Contains cable information for the Managed Switch

Product Features

- Physical Port
 - 24-Port 10/100Base-TX RJ-45 with PoE Injector
 - 2-Port Gigabit TP/SFP combo interfaces
 - Reset button for system management
 - 1 RS-232 male DB9 console interface for Switch basic management and setup
- Layer 2 Features
 - Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
 - High performance Store and Forward architecture, broadcast storm control, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
 - 8K MAC Address Table, automatic source address learning and ageing
 - Support VLANs:
 - IEEE 802.1Q Tag-Based VLAN
 - Up to 255 VLANs groups, out of 4096 VLAN IDs
 - Port-Based VLAN
 - Q-in-Q tunneling (Double Tag VLAN)
 - Supports Link Aggregation
 - Up to 13 Trunk groups
 - Up to 8 ports per trunk group with 1.6Gbps bandwidth (Full Duplex mode)
 - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
 - Cisco ether-Channel (Static Trunk)
 - Support Spanning Tree Protocol:
 - STP, IEEE 802.1D (Classic Spanning Tree Protocol)
 - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
- Quality of Service
 - 4 priority queues on all switch ports
 - Traffic classification:

- IEEE 802.1p Class of Service
 - IP TOS / DSCP code priority
 - Port Base priority
 - Strict priority and weighted round robin (WRR) CoS policies
 - Ingress/Egress Bandwidth control on each port
- Multicast
 - IGMP Snooping v1 and v2
 - IGMP Query mode for Multicast Media application
 - 256 multicast groups
- Security
 - Layer 2 / 3 / 4 Access Control List (ACL)
 - IEEE 802.1x Port-Based Authentication
 - MAC address Filtering and MAC address Binding
 - IP address security management to prevent unauthorized intruder
 - Port Mirroring to monitor incoming or outgoing traffic on a particular port
- Management
 - Switch Management Interface
 - Web switch management
 - Telnet Command Line Interface
 - SNMP v1, v2c switch management
 - Console local management
 - SNMP Trap for alarm notification of events
 - Four RMON groups 1, 2, 3, 9 (history, statistics, alarms, and events)
 - Built-in Trivial File Transfer Protocol (TFTP) client
 - Firmware upload / download via TFTP or HTTP
 - Configuration upload / download via TFTP or HTTP
 - Supports Ping function
- Power over Ethernet
 - Complies with IEEE 802.3af Power over Ethernet End-Span PSE
 - Up to 24 IEEE 802.3af devices powered
 - Support PoE Power up to 15.4 watts for each PoE ports

- Auto detect powered device (PD)
- Circuit protection prevent power interference between ports
- Remote power feeding up to 100m
- PoE Management
 - Total PoE power budget control
 - Per port PoE function enable/disable
 - PoE Port Power feeding priority
 - Per PoE port power limit
 - PD classification detection
 - PoE Power Supply Over temperature Protection

Product Specifications

GE-DS-242-PoE	
HARDWARE SPECIFICATIONS	
10/100Mbps Copper Ports	24 10/100Base-TX RJ-45 Auto-MDI/MDI-X ports
1000Mbps Copper Ports	2 10/100/1000Base-T RJ-45 port
SFP/mini-GBIC Slots	2 SFP interfaces, shared with Port-25 and Port-26
Switch Architecture	Store-and-Forward
Switch Fabric	8.8Gbps / non-blocking
Switch Throughput	6.547Mpps@64Bytes
Address Table	8K entries
Share Data Buffer	512Kbytes
Flash	4Mbytes
DRAM	16Mbytes
Maximum Frame Size	9K Bytes
Flow Control	Back pressure (for Half-Duplex) IEEE 802.3x Pause Frame (for Full-Duplex)
LED	Power, FAN Alarm Link/Activity (Green) PoE In-Use (Amber) 1000 LNK/ACT (Green) 10/100 LNK/ACT (Green)
Dimensions (W x D x H)	440 x 300 x 44 mm, 1U height
Weight	4.3kg
Power Requirement	100~240V AC, 50-60 Hz
Power Consumption	400 Watts (Full PoE Load)
Operating Temperature	Standard: 0 to 50°C
Operating Humidity	10% to 90% (Non-condensing)
Storage Temperature	-20 to +70°C
Layer 2 Functions	
Management Interface	Console, Telnet, Web Browser, SNMP v1, v2c

Port Configuration	Port disable/enable Auto-negotiation 10/100Mbps full and half duplex mode selection Flow Control disable / enable Bandwidth control and broadcast storm filter on each port
Port Status	Display each port's speed duplex mode, link status, flow control status, auto-negotiation status
VLAN	Port-Based VLAN, up to 26 VLAN groups IEEE 802.1q Tagged Based VLAN , 4K VLAN ID, up to 256 VLAN groups
Spanning Tree	IEEE 802.1d Spanning Tree IEEE 802.1w Rapid Spanning Tree
Link Aggregation	Static Port Trunk IEEE 802.3ad LACP (Link Aggregation Control Protocol) Supports 13 groups of 8-Port trunk support
Quality of Service	Traffic classification based on: <ul style="list-style-type: none"> • Port-Based priority • 802.1p priority • IP DSCP/TOS field in IP Packet
IGMP Snooping	v1 and v2 256 multicast groups and IGMP query
Bandwidth Control	Per port ingress/egress bandwidth control in steps of 128Kbps
Port Mirror	RX / TX / Both
Security	802.1x Port-Based Network access control MAC Limit Static MAC MAC Filtering
Access Control List	Supports up to 220 rule entries
SNMP MIBs	RFC-1157 SNMP MIB RFC-1213 MIB-II RFC-1215 Trap RFC-2863 Interface MIB RFC-1493 Bridge MIB RFC-2674 Extended Bridge MIB (Q-Bridge) RFC-1643
Power over Ethernet	
PoE Standard	IEEE 802.3af Power over Ethernet / PSE

PoE Power Supply Type	End-Span
PoE Power Output	Per Port 48V DC, 350mA . Max. 15.4 watts
Power Pin Assignment	1/2(+), 3/6(-)
PoE Power Budget	380 Watts
Max. number of Class 2 PD	24
Max. number of Class 3 PD	24
Standards Conformance	
Safety	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000Base-T IEEE 802.3x Flow Control and Back pressure IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.3af Power over Ethernet
Cable-Fiber-optic cable	<ul style="list-style-type: none"> • 50 / 125µm or 62.5 / 125µm multi-mode fiber cable: <ul style="list-style-type: none"> - 100Base-FX: up to 2km - 1000Base-SX: up to 220/550m • 9 / 125µm single-mode cable, provides long distance for: <ul style="list-style-type: none"> - 100Base-FX: up to 10/40/60km (vary on fiber transceiver or SFP module) - 1000Base-LX / ZX: 10 / 15 / 20 / 30 / 40 / 50 / 60 / 70 / 120km (vary on fiber transceiver or SFP module)

Chapter 2

Installation

This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount.

For easier management and control of the Managed Switch, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit's LED indicators.

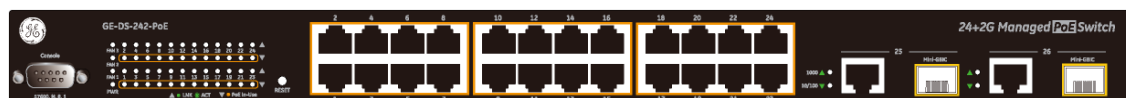
Read this chapter completely before connecting any network device to the Managed Switch.

Hardware Description

Switch Front Panel

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

Figure 2-1: GE-DS-242-PoE Switch front panel



10/100Mbps TP Interface

Port-1~Port-24: 10/100Base-TX Copper, RJ-45 Twist-Pair: Up to 100 meters.

Gigabit TP Interface

Port-25, Port-26: 10/100/1000Base-T Copper, RJ-45 Twist-Pair: Up to 100 meters.

Gigabit SFP Slots

Port-25, Port-26: 1000Base-SX/LX mini-GBIC slot, SFP (Small Form-Factor Pluggable) transceiver module: from 550 meters (Multi-mode fiber), up to 10/30/70 kilometers (Single-mode fiber).

Console Port

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

Reset button

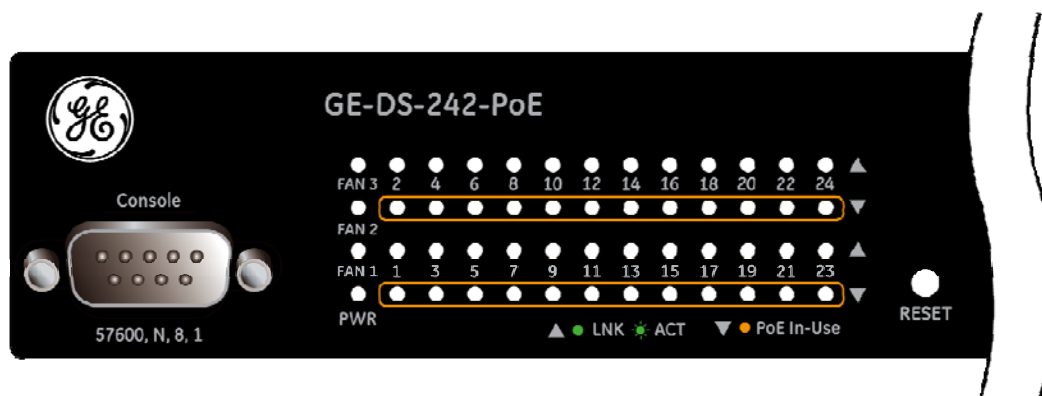
At the left of front panel, the Reset button is designed to reboot the Managed Switch without turning the power off. The following table summarizes the Reset button functions:

Reset Button Pressed and Released	Function
About 1~3 seconds	Reboots the Managed Switch
Until the PWR LED goes out	<p>Resets the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as below:</p> <ul style="list-style-type: none"> • Default Password: admin • Default IP address: 192.168.0.100 • Subnet mask: 255.255.255.0 • Default Gateway: 192.168.0.254

LED Indicators

The front panels LEDs indicate instant status of port links, data activity and system power. They help monitor the system and aid in troubleshooting when necessary. The front panel LEDs are shown in Figure 2-2.

Figure 2-2: GE-DS-242-PoE LED panel



- **System**

LED	Color	Function
PWR	Green	Lit: indicates there is power to the Switch

- **Per 10/100Base-TX, PoE interfaces (Port-1 to Port-24)**

LED	Color	Function
LNK/ACT	Green	Lit: indicates the link through that port is successfully established Blink: indicates the Switch is actively sending or receiving data over that port
PoE In Use	Orange	Lit: indicates the port is providing 48VDC in-line power Off: indicates the connected device is not a PoE Powered Device (PD)

- **Per 10/100/1000Base-T port/SFP interfaces**

LED	Color	Function
LNK/ACT 1000	Green	Lit: indicates the port is operating at 1000Mbps Off: indicates the port is operating at 10Mbps or 100Mbps Blink: indicates the Switch is actively sending or receiving data over that port
LNK/ACT 100	Green	Lit: indicates the port is operating at 100Mbps Off: indicates the port is operating at 10Mbps or 1000Mbps Blink: indicates the Switch is actively sending or receiving data over that port

NOTE:

1. Press the RESET button once. The Switch will reboot automatically.
2. Press the RESET button for about 10 seconds. The Switch will revert to the factory default mode; the entire configuration will be erased.
3. The 2 Gigabit TP/SFP combo ports are shared with port 25/26 of GE-DS-242-PoE. Both of them can operate at the same time.

Switch Rear Panel

The rear panel of the Managed Switch includes an AC inlet power socket, which accepts input power from 100 to 240VAC, 50-60 Hz. Figure 2-3 shows the rear panel of the Managed Switch.

Figure 2-3: GE-DS-242-PoE Rear panel

POWER NOTICE:

1. The Managed Switch is a power-required device: it will not work unless it is receiving power. If your networks must be active at all times, it is recommended that the Switch be connected to a UPS (Uninterruptable Power Supply) to prevent data loss or downtime.
2. In some areas, installing a surge suppression device may also help protect your Managed Switch from being damaged by unregulated power surges or current to either the Switch or the power adapter.

Switch Installation

This text describes how to install the Managed Switch and connect it as necessary. Please read the following instructions, and perform the procedures in the listed order.

Desktop/Shelf Installation

NOTE: Refer to the environmental restrictions listed in the Product Specifications when selecting a location for the Managed Switch.

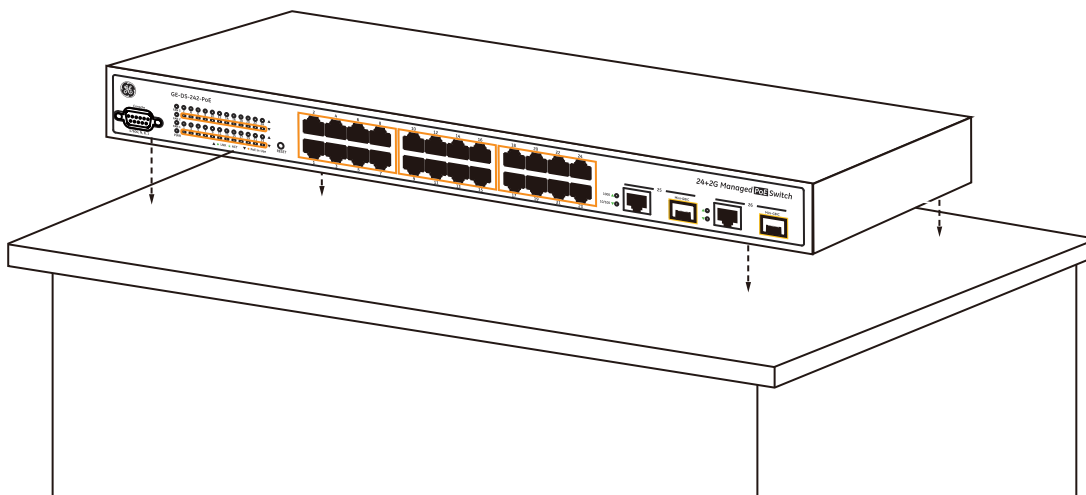


Step 1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step 2: Place the Managed Switch on a desktop or shelf near an AC power source, as shown in Figure 2-4.

Step 3: Ensure there is enough ventilation space between the Managed Switch and surrounding objects.

Figure 2-4: Typical placement of GE-DS-242-PoE on desktop



NOTE: Connection to the Managed Switch requires UTP Category 5 network cabling with RJ-45 tips. Refer to the Cabling Specification in Appendix A for further information.

Step 4: Connect the Managed Switch to network devices.

- A. Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Managed Switch.
- B. Connect the other end of the cable to the network devices (printer servers, workstations, routers etc).

Step 5: Connect the Managed Switch to supply power.

- A. Connect socket end of the power cable to the socket on the Managed Switch rear panel.
- B. Connect the power cable plug to a standard wall outlet.
- C. Switch the power switch on the rear panel to ON.

When the Managed Switch receives power, the Power LED should light and remain solid Green.

Rack-mount Installation

Use the following instructions to install the Managed Switch in a 19-inch standard rack.

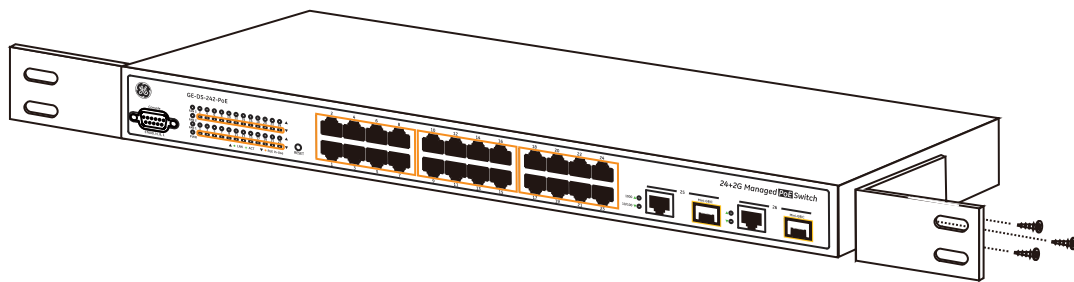
Step 1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front.

CAUTION: Use only the screws supplied with the mounting brackets. Damage caused by using incorrect screws will invalidate the warranty.

Step 2: Attach the rack-mount bracket to each side of the Managed Switch. Use the supplied screws attached to the package.

Figure 2-5 shows how to attach brackets to one side of the Managed Switch.

Figure 2-5: Attaching rack-mount brackets to the GE-DS-242-PoE

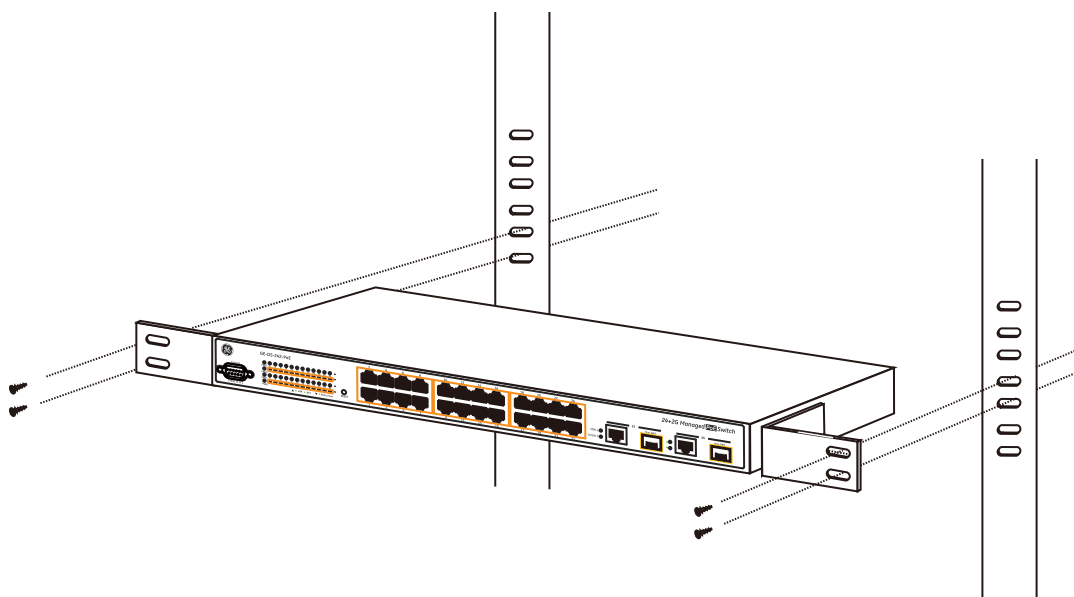


Step 3: Secure the brackets tightly, but do not overtighten screws.

Step 4: Follow the same steps to attach the second bracket to the opposite side.

Step 5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-6.

Figure 2-6: Mounting the GE-DS-242-PoE in a rack



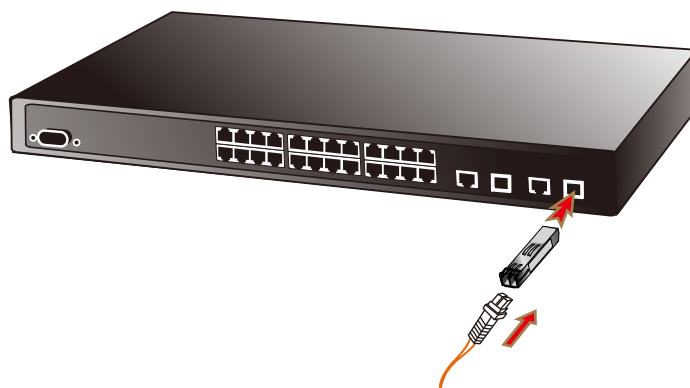
Step 6: Follow steps 4 and 5 of the Desktop Installation section to connect the network cabling and supply power to the Managed Switch.

SFP Transceiver Installation

This section describes how to insert an SFP transceiver into an SFP slot.

SFP transceivers are hot pluggable and hot swappable. You can insert and remove a transceiver to and from any SFP port without powering down the Managed Switch, as shown in Figure 2-7.

Figure 2-7: Plugging-in the SFP transceiver



Approved GE Security SFP Transceivers

GE Security Managed Switches support both Single mode and Multi-mode SFP transceivers. The following list of approved GE Security SFP transceivers is correct at the time of publication:

- SFP1000SX-220 SFP (1000BASE-SX SFP transceiver / Multi-mode / 850nm / 220m~550m)
- SFP1000LX-10Km SFP (1000BASE-LX SFP transceiver / Single mode / 1310nm / 10km)
- SFP100FX1310-TSC-2Km SFP (100BASE-FX SFP transceiver / Multi-mode / 850nm / 2km)
- SFP100FX1310-TSC-20Km SFP (100BASE-FX SFP transceiver / Single mode / 1310nm / 20km)
- SFP1000LX-30KM SFP (1000Base-LX SFP transceiver / Singlemode / 1310nm / 30 km)
- SFP1000LX-70KM SFP1000Base-LX SFP transceiver / Singlemode / 1550nm / 70 km)

NOTE: It is recommended that only approved GE Security SFP transceivers be used on the Managed Switch. If you insert an SFP transceiver that is not supported, the Switch will not recognize it.

Before connecting the other switches, workstations or Media Converter:

1. Make sure both sides of the SFP transceiver are the same media type (for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX).
2. Verify that the fiber-optic cable type matches the SFP transceiver model.
 - To connect to the 1000Base-SX SFP transceiver, use multi-mode fiber cable (one side must be male duplex LC connector type).
 - To connect to the 1000Base-LX SFP transceiver, use single-mode fiber cable (one side must be male duplex LC connector type).

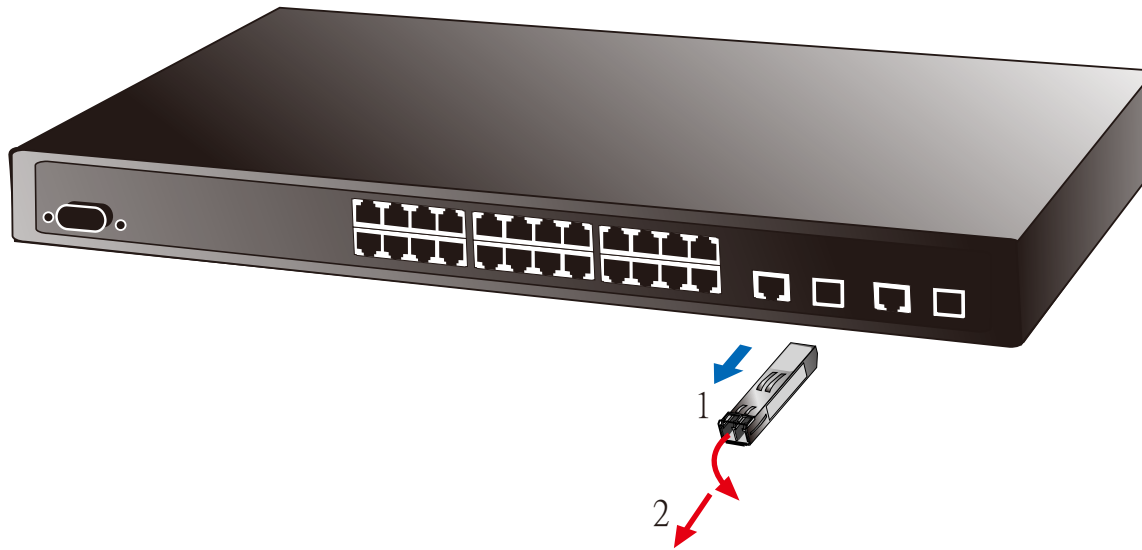
Connect the fiber cable:

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

Remove the transceiver module

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

Figure 2-8: Pulling out the SFP transceiver



CAUTION: Never pull out the module without pulling the handle or the push bolts on the module. Pulling out the module with too much force could damage the module and SFP module slot of the Managed Industrial Switch.

Chapter 3

Switch Management

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

This chapter covers the following topics:

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

Requirements

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

NOTE: We recommended Internet Explore 6.0 or above to access the Managed Switch.

Management Access Overview

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

- Web browser interface
- An external SNMP-based network management application
- The Administration Console

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

Table 3-1: Management Methods Comparison

Method	Advantages	Disadvantages
Web Browser	<ul style="list-style-type: none"> • Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing 	<ul style="list-style-type: none"> • Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	<ul style="list-style-type: none"> • Communicates with switch functions at the MIB level • Based on open standards 	<ul style="list-style-type: none"> • Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)
Console	<ul style="list-style-type: none"> • No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure 	<ul style="list-style-type: none"> • Must be near switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow

Web Management

The Managed Switch offers management features that allow users to manage the Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the switch, you can access the Managed Switch's Web interface applications directly in your Web browser by entering the IP address of the Managed Switch.

You can then use your Web browser to list and manage the Managed Switch configuration parameters from one central location, just as if you were directly connected to the Managed Switch's console port. Web Management requires either Microsoft Internet Explorer 6.0 or later, Safari or Mozilla Firefox 2.0 or later.

Figure 3-1: Web management setup

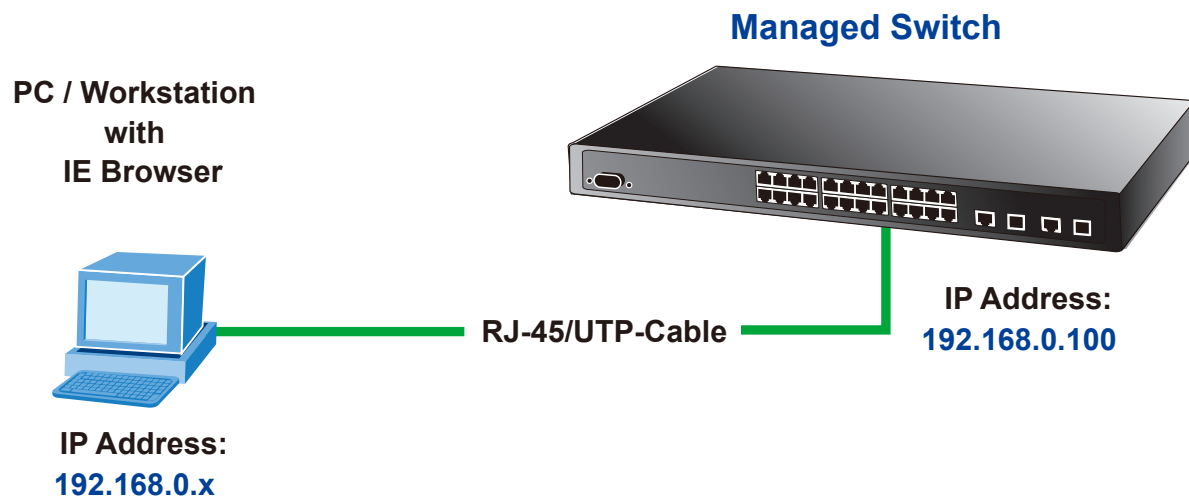


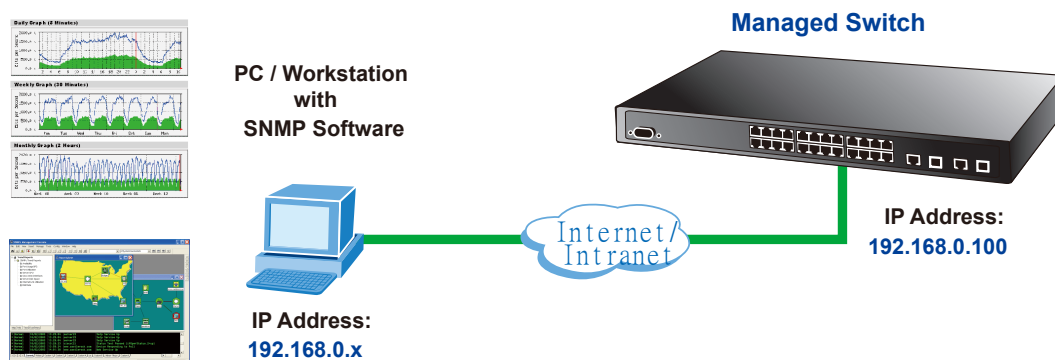
Figure 3-2: Web main screen of Managed Switch



SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the Managed Switch, such as SNMPc Network Manager, HP Openview Network Node Management (NNM) or What'sup Gold. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method, in fact, uses two community strings: the get community string and the set community string. If the SNMP Network management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default gets and sets community strings for the Managed Switch are public.

Figure 3-3: SNMP management



Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the switch's console (serial) port.

There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to Chapter 5: Console Management.

Figure 3-4: Console management setup



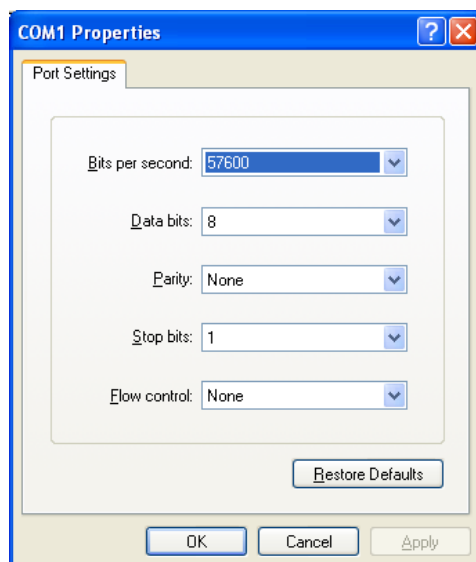
Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the Managed Switch console (serial) port.

When using this management method, a straight DB9 RS-232 cable is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

- 57600 bps
- 8 data bits
- No parity
- 1 stop bit

Figure 3-5: Terminal parameter settings



You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

Protocols

The Managed Switch supports the following protocols:

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

Virtual Terminal Protocols (Telnet)

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

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

NOTE: See the Installation Sheet that came with this product for a Telnet step-by-step procedure using Hyper Terminal.

To access the Managed Switch through a Telnet session:

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

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

SNMP Protocol

Simple Network Management Protocol (SNMP) is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting

devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

Management Architecture

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

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

Chapter 4

Web-Based Management

Summary

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

About Web-based Management

The Managed Switch offers management features that allow users to manage the Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

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

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

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

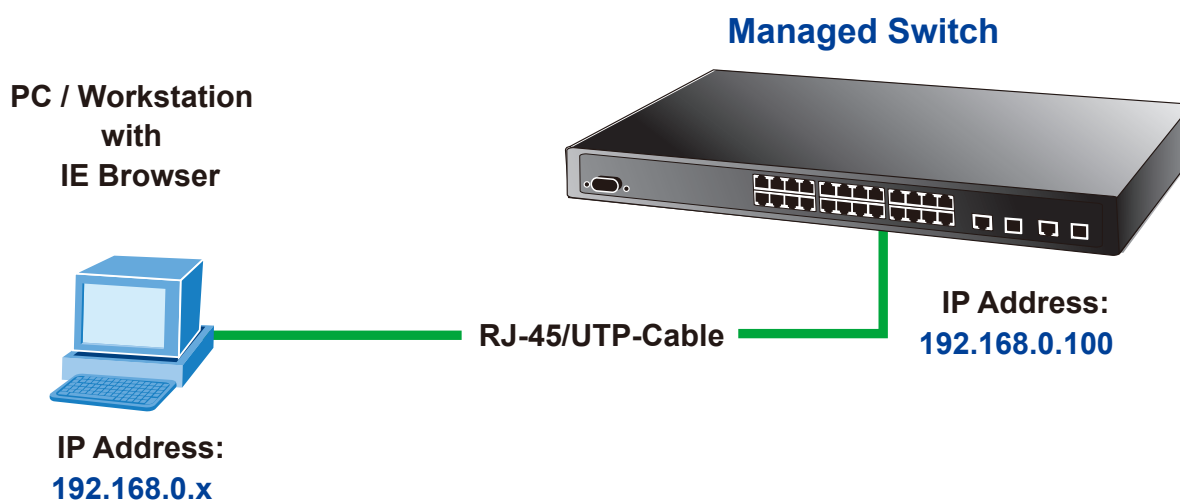
If you have changed the default IP address of the Managed Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

Requirements

- ☐ Workstations of subscribers running Windows 98/ME, NT4.0, 2000/2003/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with TCP/IP protocols.
- ☐ Workstation installed with Ethernet NIC (Network Card).
- ☐ Ethernet Port connect
- ☐ Network cables - Use standard network (UTP) cables with RJ45 connectors.
- ☐ Above PC installed with WEB Browser and JAVA runtime environment Plug-in.

It is recommended to use Internet Explorer 6.0 or above to access the GE-DS-242-PoE Managed Switch.

Figure 4-1: Web management setup



Logging on to the Switch

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

http://192.168.0.100

2. When the following login screen appears, please enter the default username "admin" with password "admin" (or the username/password you have changed via console) to login the main screen of Managed Switch. The login screen in Figure 4-2 appears.

Default User name: **admin**

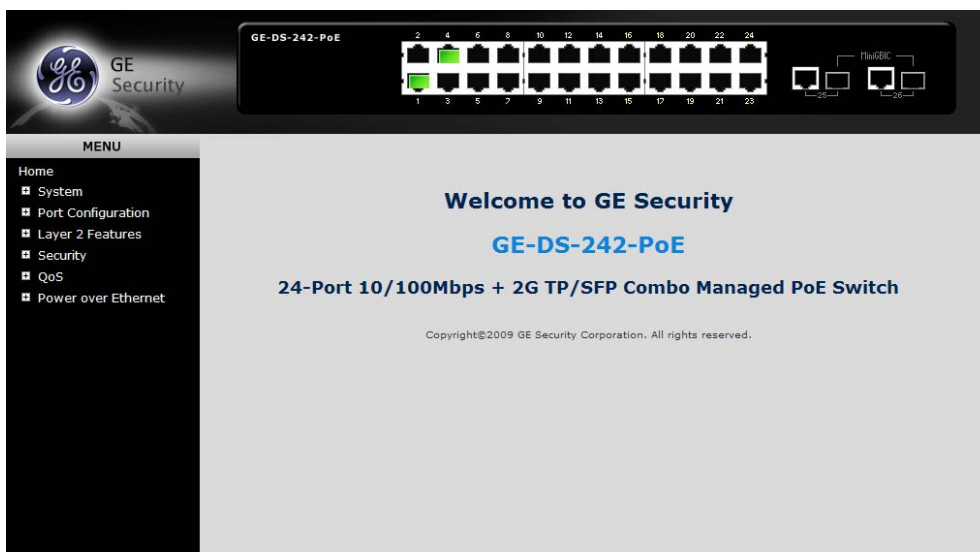
Default Password: **admin**

Figure 4-2: Login screen



1. After entering the username and password, the main screen appears as Figure 4-3.

Figure 4-3: Web main page



2. The Switch Menu on the left of the Web page let you access all the commands and statistics the Switch provides.

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

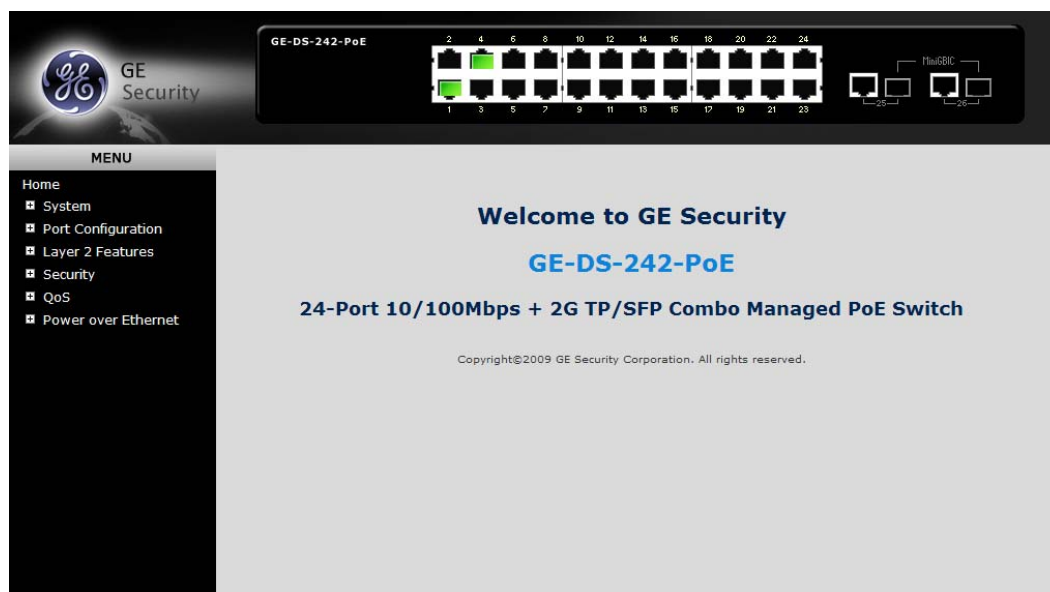
NOTE:

- We recommend using Internet Explorer 6.0 or above to access Managed Switch.
- A changed IP address take effect immediately after click on the Save button, you need to use the new IP address to access the Web interface.
- For security reason, please change and memorize the new password after this first setup.
- Only enter commands in lowercase letters in the web interface.

Main Web Page

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










Figure 4-4: Main page



Panel Display

The web agent displays an image of the Managed Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the Port Statistics page.

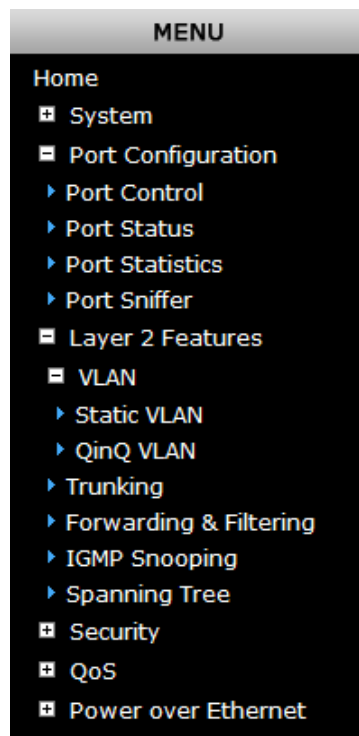
The port states are illustrated as follows:

State	Disabled	Down	Link
RJ-45 Ports			
SFP Ports			
PoE Ports			

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can setup the Managed Switch by select the functions those listed in the Main Function. The screen in Figure 4-5 appears.

Figure 4-5: GE-DS-242-PoE Managed Switch Main Functions Menu



System

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

System Information	Provides basic system description, including contact information
IP Configuration	Sets the IP address for management access
SNMP Configuration	Configure SNMP agent and SNMP Trap
Firmware Upgrade	Upgrade the firmware via TFTP server or Web Browser file transfer
Configuration Backup	Save/view the Managed Switch configuration to remote host. Upload the switch configuration from remote host.
Factory Default	Reset the configuration of the Managed Switch
System Reboot	Restarts the Managed Switch

System Information

The System information page has two parts - Basic and Misc Config.

Basic

The Basic System Info page provides information for the current device information. Basic System Info page helps a switch administrator to identify the model name, firmware / hardware version and MAC address. The screen in Figure 4-6 appears.

Figure 4-6: Basic System Information screenshot

System Information	
Basic	Misc Config
Model Name	GE-DS-242-PoE
Description	24-Port 10/100Mbps + 2G TP/SFP Combo Managed PoE Switch
MAC Address	00:30:4F:75:F2:AA
Firmware Version	1.10
Hardware Version	1.0

This page includes the following fields:

OBJECT	DESCRIPTION
MODEL NAME	Displays the system name of the Managed Switch
DESCRIPTION	Describes the Managed Switch
MAC ADDRESS	Displays the unique hardware address assigned by manufacturer (default)
FIRMWARE VERSION	Displays the Managed Switch's firmware version
HARDWARE VERSION	Displays the current hardware version

Misc Config

Choose Misc Config from System Information of Managed Switch, the screen in Figure 4-7 appears.

Figure 4-7: Switch Misc Config screenshot

System Information

Basic **Misc Config**

☒ MAC Table Address Entry
 Age-Out Time: 300 seconds (6~1572858, must multiple of 6, default is 300s)

Turn On Port Interval: 0 seconds (0~3600 seconds, interval time between turning off and turning on port for flooding CPU port, 0:disable)

Broadcast Storm Filter Mode: OFF

Broadcast Storm Filter Packet select

☐ Broadcast Packets

☐ IP Multicast

☐ Control Packets

☐ Flooded Unicast/Multicast Packets

Collisions Retry Forever : 16

Hash Algorithm : CRC-Hash

IP/MAC Binding : Disable

802.1x Protocol : Disable

Apply Default Help

This page includes the following fields:

OBJECT	DESCRIPTION
MAC Address Age-out Time	Type the number of seconds that an inactive MAC address remains in the switch's address table. The value is a multiple of 6. Default is 300 seconds.
Broadcast Storm Filter Mode	To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold values are 1/2, 1/4, 1/8, 1/16 and OFF. Default is "OFF".
Broadcast Storm Filter Packets Select	To select broadcast storm Filter Packets type. If no packets type by selected, mean can not filter any packets .The Broadcast Storm Filter Mode will show OFF. The selectable items as below: <ul style="list-style-type: none"> • Broadcast Packets • IP Multicast • Control Packets • Flooded Unicast / Multicast Packets
Collision Retry Forever	Provide Collision Retry Forever function "Disable" or 16, 32, 48 collision numbers on Managed Switch. If this function is disabled, when a packet meet a collision, the Managed Switch will retry 6 times before discard the packets. Otherwise, the Managed Switch will retry until the packet is successfully sent. Default value is 16.
Hash Algorithm	Provide MAC address table Hashing setting on Managed Switch; available options are CRC Hash and Direct Map. Default mode is CRC-Hash.
802.1x protocol	Enable / disable 802.1x protocol
Apply button	Press the button to complete the configuration.

IP Configuration

The Managed Switch is a network device, which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the Managed Switch.

IP address overview

What is an IP address?

Each device (such as a computer) which participates in an IP network needs a unique "address" on the network. It's similar to having a US mail address so other people have a know way to send you messages. An IP address is a four byte number, which is usually written in "dot notation" - each of the bytes' decimal value is written as a number, and the numbers are separated by "dots" (aka periods). An example:
199.25.123.1

How do I get one for this box?

The IP addresses on most modern corporate nets are assigned by an employee called a "Network Administrator", or "Sys. Admin". This person assigns IP addresses and is responsible for making sure that IP addresses are not duplicated - If this happens one or both machines with a duplicate address will stop working.

Another possibility is getting your address assigned to you automatically over the net via DHCP protocol. Enable DHCP function, and reset the machine. If your network is set up for this service, you will get an IP address assigned over the network. If you don't get an address in about 30 seconds, you probably don't have DHCP.

IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in Figure 4-8 appears.

Figure 4-8: IP configuration interface

IP Configuration

DHCP : Disable ▾

IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254

Apply
Help

This page includes the following fields:

OBJECT	DESCRIPTION
DHCP	<p>Enable or disable the DHCP client function.</p> <p>When DHCP function is enabled, the Managed Switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks Apply, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.</p>
IP Address	<p>Assign the IP address that the network is using.</p> <p>If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and display it in this column.</p> <p>The default IP is 192.168.0.100 or the user has to assign an IP address manually when DHCP Client is disabled.</p>
Subnet Mask	<p>Assign the subnet mask to the IP address.</p> <p>If DHCP client function is disabled, the user has to assign the subnet mask in this column field.</p>
Gateway	<p>Assign the network gateway for the switch.</p> <p>If DHCP client function is disabled, the user has to assign the gateway in this column field.</p> <p>The default gateway is 192.168.0.254.</p>

SNMP Configuration

SNMP Overview

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

Figure 4-9: SNMP configuration interface

GE-DS-242-PoE

GE Security

MENU

- Home
- System
 - System Information
 - IP Configuration
 - SNMP Configuration
 - Firmware Upgrade
 - Configuration Backup
 - Factory Default
 - System Reboot
- Port Configuration
 - Configuration Backup
 - Factory Default
 - System Reboot
- Layer 2 Features
- Security
- QoS
- Power over Ethernet

SNMP Configuration

System Options

Name:	GE-DS-242-PoE
Location:	No Location
Contact:	No Contact
SNMP Status:	Enable <input checked="" type="checkbox"/>

Apply Help

Community Strings

Current Strings:	New Community String:
private__read-write-all public__read-all-only	String: <input type="text"/>
<< Add <<	<input type="radio"/> RO <input type="radio"/> RW
Remove	

Trap Managers

Current Managers:	New Manager:
(none)	IP Address: <input type="text"/>
<< Add <<	Community: <input type="text"/>
Remove	

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

- **Network management stations (NMSs):** Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **SNMP Agents:** Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.

- **Management information base (MIB):** A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol:** A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Overview

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

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

SNMP Community

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

- Write = private
- Read = public

System Options

Use this page to define management stations. You can also define a name, location, and contact person for the Managed Switch.

Figure 4-10: SNMP configuration interface

SNMP Configuration

System Options

Name:	GE-DS-242-PoE
Location:	No Location
Contact:	No Contact
SNMP Status:	Enable <input checked="" type="checkbox"/>

Apply Help

Community Strings

Current Strings:		New Community String:
private__read-write-all public__read-all-only	<< Add << Remove	String: <input type="text"/> <input checked="" type="radio"/> RO <input type="radio"/> RW

Trap Managers

Current Managers:	New Manager:

This page includes the following fields:

OBJECT	DESCRIPTION
System Name	<p>An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign.</p> <p>The allowed string length is 0 to 255.</p>
System Location	<p>The physical location of this node (e.g., telephone closet, 3rd floor).</p> <p>The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.</p>
System Contact	<p>The textual identification of the contact person for this managed node, together with information on how to contact this person.</p> <p>The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.</p>
SNMP Status	<p>Indicates the SNMP mode operation. Possible modes are:</p> <ul style="list-style-type: none"> Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.

Community Strings

Community strings serve as passwords and can be entered as one of the following:

Figure 4-11: Community strings interface

This page includes the following fields:

OBJECT	DESCRIPTION
Community Strings	<p>Here you can define the new community string set and remove the unwanted community string.</p> <ul style="list-style-type: none"> String: Fill the name string. RO: Read only. Enables requests accompanied by this community string to display MIB-object information. RW: Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
ADD button	Press the button to add the management SNMP community strings on the Managed Switch.
REMOVE button	Press the button to remove the management SNMP community strings that you defined before on the Managed Switch.

Trap Managers

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

Figure 4-12: Trap managers interface

This page includes the following fields:

OBJECT	DESCRIPTION
IP Address	Enter the IP address of the trap manager.
Community	Enter the community string for the trap station.

Firmware Upgrade

It provides the functions allowing the user to update the switch firmware via the Trivial File Transfer Protocol (TFTP) server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

TFTP Firmware Upgrade

The Firmware Upgrade page provides the functions to allow a user to update the Managed Switch firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The screen in Figure 4-13 appears.

Use this menu to download a file from specified TFTP server to the Managed Switch.

Figure 4-13: Firmware Upgrade interface

The screenshot shows a web interface titled "Firmware Upgrade" with a subtitle "TFTP Firmware Upgrade". Below the subtitle, there are two input fields: "TFTP Server IP Address" and "Firmware File Name". At the bottom of the form, there are two buttons: "Apply" and "Help".

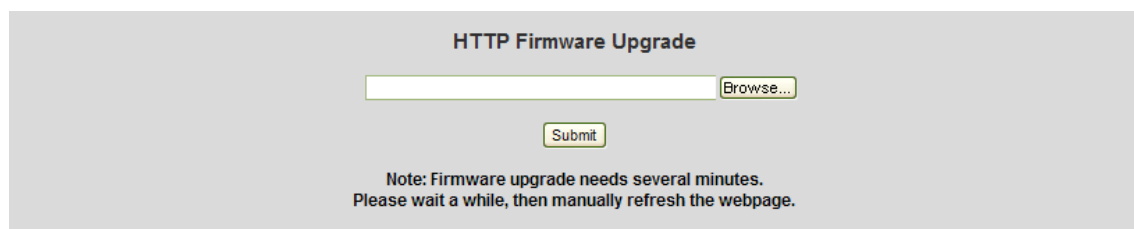
This page includes the following fields:

OBJECT	DESCRIPTION
TFTP Server IP Address	Type in your TFTP server IP.
Firmware File Name	Type in the name of the firmware image file to be updated.

HTTP Firmware Upgrade

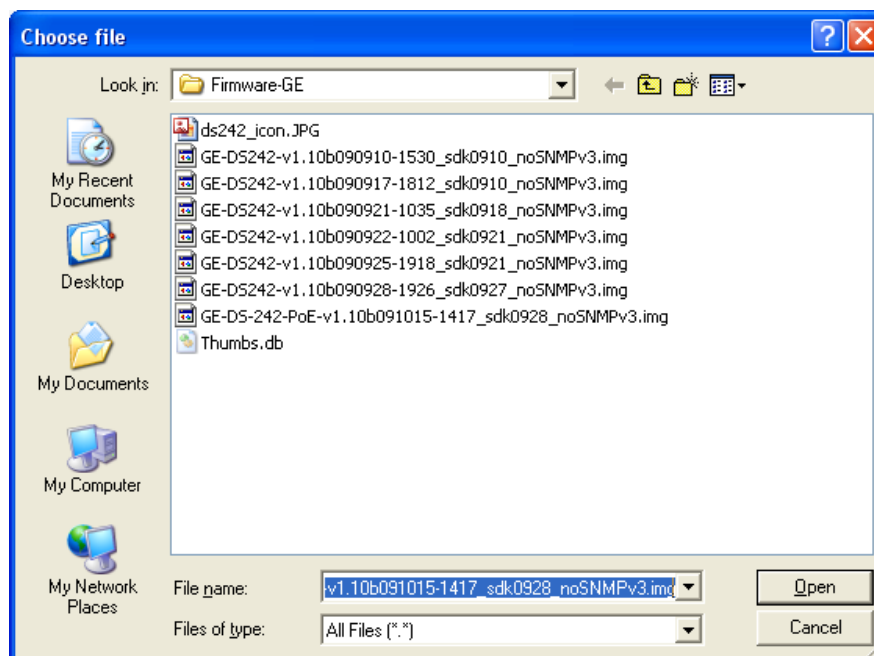
The HTTP Firmware Upgrade page contains fields for downloading system image files from the Local File browser to the device. The Web Firmware Upgrade screen in Figure 4-14 appears.

Figure 4-14: HTTP Firmware Upgrade interface



To open Firmware Upgrade screen, perform the following:

1. Click **System** -> **Web Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in Figure 4-14.
3. Click the "**Browse**" button of the main page, the **Choose file window** will appear.
4. Select the firmware file, then click the **Open** button to load the file.



The Firmware upgrade process takes several minutes. Please wait a while, and then manually refresh the webpage.

Configuration Backup

TFTP Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the Managed Switch will download back the flash image.

Figure 4-15: Configuration Restore interface

The screenshot shows the 'Configuration Restore' web interface. At the top, there are two tabs: 'TFTP Restore Configuration' (active) and 'TFTP Backup Configuration'. Under the active tab, there are two input fields: 'TFTP Server IP Address' and 'Restore File Name'. Below these fields are 'Apply' and 'Help' buttons. A horizontal line separates this section from the 'HTTP Config File Restore' section below. This section has a single input field followed by a 'Browse...' button, and a 'submit' button at the bottom.

This page includes the following fields:

OBJECT	DESCRIPTION
TFTP Server IP Address	Type in your TFTP server IP.
Restore File Name	Type in the correct file name for restoring.

TFTP Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

Figure 4-16: Configuration Backup interface

The screenshot shows the 'Configuration Backup' web interface. At the top, there are two tabs: 'TFTP Restore Configuration' and 'TFTP Backup Configuration' (active). Under the active tab, there are two input fields: 'TFTP Server IP Address' and 'Backup File Name'. Below these fields are 'Apply' and 'Help' buttons. A horizontal line separates this section from the 'HTTP Config File Backup' section below. This section contains a single line of text: 'Click here to download configuration file'.

This page includes the following fields:

OBJECT	DESCRIPTION
TFTP Server IP Address	Type in your TFTP server IP.
Backup File Name	Type in the file name.

Factory Default

Reset Switch to default configuration. Click the **reset** button to restore all configurations to the default value.

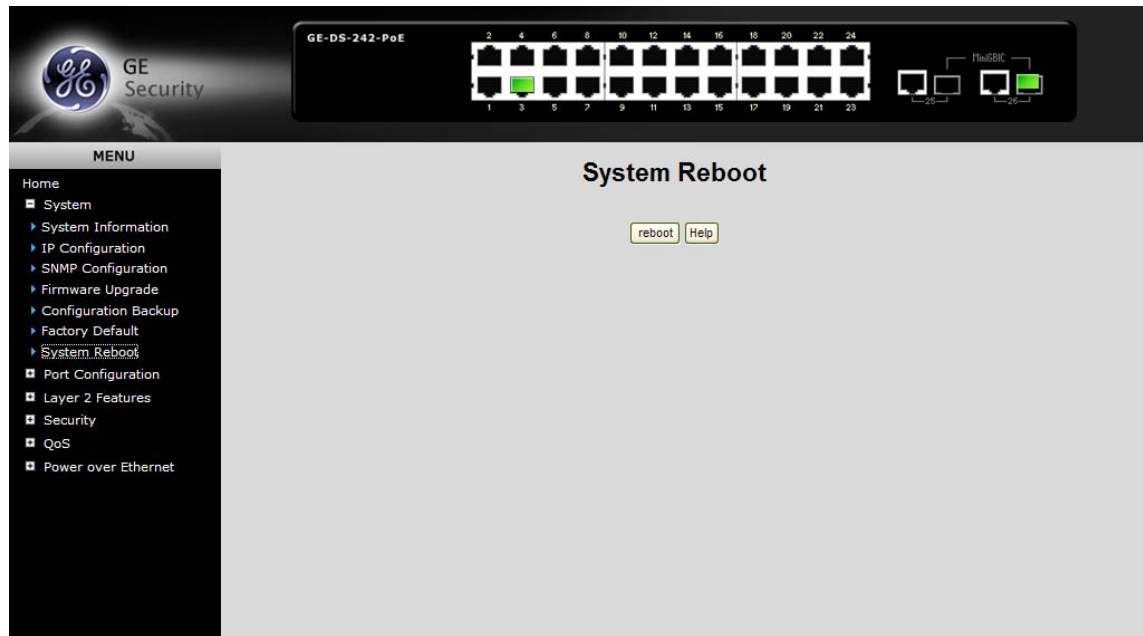
Figure 4-17: Factory Default interface



System Reboot

Reboot the Switch with a software reset. Click the **reboot** button to reboot the system.

Figure 4-18: System Reboot interface



Port Configuration

In Port control you can configure the settings of each port to control the connection parameters, the status of each port is listed below.

Figure 4-19: Port Control interface

Port	State	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)		Security	BSF	Jumbo Frame
						Ingress	Egress			
Port23										
Port24	Enable	Auto	100	Full	Enable	0	0	<input type="checkbox"/>	Enable	Enable
Port25										
Port26										

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			
Port24	On	Down	Auto	100	Full	Off	Off	Off	Off	On	On

This page includes the following fields:

OBJECT	DESCRIPTION
Port	Use the scroll bar and click on the port number to choose the port to be configured.
State	Current port state. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet.
Negotiation	Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
Speed	It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
Duplex	It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
Flow Control	Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.

OBJECT	DESCRIPTION
Rate Control (Unit: 128KBbps)	<p>Port-1 ~ Port-24, supports by-port ingress and egress rate control.</p> <p>For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. Device will perform flow control or backpressure to confine the ingress rate to meet the specified rate.</p> <ul style="list-style-type: none"> Ingress: Type the port effective ingress rate. The valid range is 0 ~ 8000. The unit is 128K. 0: disable rate control. 1 ~ 8000: valid rate value Egress: Type the port effective egress rate. The valid range is 0 ~ 8000. The unit is 128K. 0: disable rate control. 1 ~8000: valid rate value.
Security	<p>A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally.</p> <p>User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, then click Apply button to change on this page.</p>
BSF	<p>User can disable/Enable port broadcast storm filtering option by port.</p> <p>The filter mode and filter packets type can be select in Switch Setting > Misc Config page.</p>
Jumbo Frame	<p>User can disable/Enable port jumbo frame option by port. When port jumbo frame is enable, the port forward jumbo frame packet.</p>

Port Status

This page displays current port configurations and operating status - it is a ports' configurations summary table. Via the summary table, you can learn the status of each port at a glance, like Port Link Up/Link Down status, negotiation, Link Speed, Rate Control, Duplex mode and Flow Control.

Figure 4-20: Port Status interface

Port Status

The following information provides a view of the current status of the unit.

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit:128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			
Port1	On	Up	Auto	100	Full	Off	Off	Off	Off	On	On
Port2	On	Down	---	---	---	---	Off	Off	Off	On	On
Port3	On	Down	---	---	---	---	Off	Off	Off	On	On
Port4	On	Down	---	---	---	---	Off	Off	Off	On	On
Port5	On	Down	---	---	---	---	Off	Off	Off	On	On
Port6	On	Down	---	---	---	---	Off	Off	Off	On	On
Port7	On	Down	---	---	---	---	Off	Off	Off	On	On
Port8	On	Down	---	---	---	---	Off	Off	Off	On	On
Port9	On	Down	---	---	---	---	Off	Off	Off	On	On
Port10	On	Down	---	---	---	---	Off	Off	Off	On	On
Port11	On	Down	---	---	---	---	Off	Off	Off	On	On
Port12	On	Down	---	---	---	---	Off	Off	Off	On	On
Port13	On	Down	---	---	---	---	Off	Off	Off	On	On
Port14	On	Down	---	---	---	---	Off	Off	Off	On	On
Port15	On	Down	---	---	---	---	Off	Off	Off	On	On
Port16	On	Down	---	---	---	---	Off	Off	Off	On	On
Port17	On	Down	---	---	---	---	Off	Off	Off	On	On
Port18	On	Down	---	---	---	---	Off	Off	Off	On	On
Port19	On	Down	---	---	---	---	Off	Off	Off	On	On
Port20	On	Down	---	---	---	---	Off	Off	Off	On	On
Port21	On	Down	---	---	---	---	Off	Off	Off	On	On
Port22	On	Down	---	---	---	---	Off	Off	Off	On	On
Port23	On	Down	---	---	---	---	Off	Off	Off	On	On
Port24	On	Down	---	---	---	---	Off	Off	Off	On	On
Port25	On	Down	---	---	---	---	Off	Off	Off	On	On
Port26	On	Up	Auto	1000	Full	Off	Off	Off	Off	On	On

Port Statistics

The following chart provides the current statistic information, which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

Figure 4-21: Port Statistics interface

Port Statistics									
The following information provides a view of the current status of the unit.									
Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
Port1	On	Up	123578	0	1400302	0	0	0	390768
Port2	On	Down	0	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0	0
Port4	On	Down	414866	0	97918	0	0	0	150
Port5	On	Down	0	0	0	0	0	0	0
Port6	On	Down	0	0	0	0	0	0	0
Port7	On	Down	0	0	0	0	0	0	0
Port8	On	Down	0	0	0	0	0	0	0
Port9	On	Down	0	0	0	0	0	0	0
Port10	On	Down	0	0	0	0	0	0	0
Port11	On	Down	0	0	0	0	0	0	0
Port12	On	Down	0	0	0	0	0	0	0
Port13	On	Down	0	0	0	0	0	0	0
Port14	On	Down	0	0	0	0	0	0	0
Port15	On	Down	0	0	0	0	0	0	0
Port16	On	Down	0	0	0	0	0	0	0

This page includes the following fields:

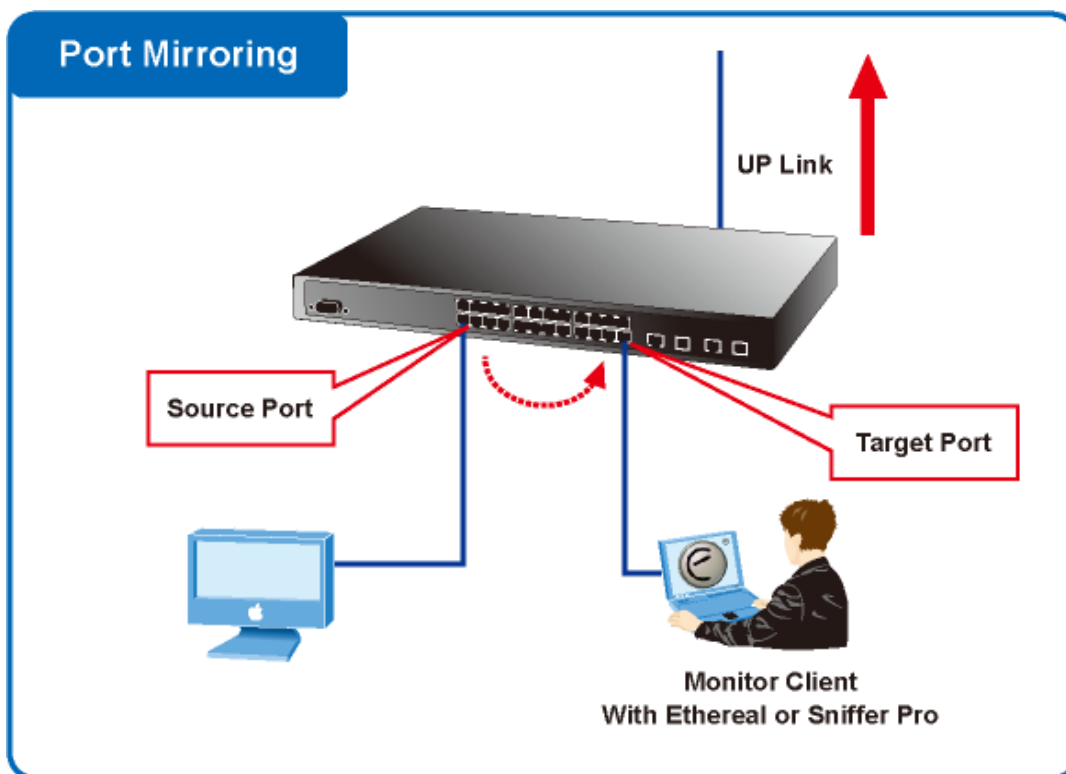
OBJECT	DESCRIPTION
Port	The port number.
Link	The status of linking-'Up' or 'Down'
State	Set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
Tx Good Packet	The counts of transmitting good packets via this port.
Tx Bad Packet	The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
Rx Good Packet	The counts of receiving good packets via this port.
Rx Bad Packet	The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
Tx Abort Packet	The aborted packet while transmitting.
Packet Collision	The counts of collision packet.

OBJECT	DESCRIPTION
Packet Dropped	The counts of dropped packet.
Rx Bcast Packet	The counts of broadcast packet.
Rx Mcast Packet	The counts of multicast packet.

Port Sniffer

The Port Sniffer (mirroring) is a method for monitor traffic in switched networks. Traffic through a port can be monitored by one specific port. That is, traffic goes in or out a monitored port will be duplicated into sniffer port.

Figure 4-22: Port Mirror application



Configuring the port mirroring by assigning a source port from which to copy all packets and a destination port where those packets will be sent.

Figure 4-23: Port Sniffer interface

The screenshot shows the 'Port Sniffer' configuration interface. At the top, there are two dropdown menus: 'Sniffer Type' set to 'BOTH' and 'Analysis Port' set to 'Port1'. Below these is a table with two columns: 'Port' and 'Monitor'. The 'Port' column lists ports from Port1 to Port13. The 'Monitor' column contains radio buttons. Port1 has an unselected radio button, Port2 has a selected radio button (indicated by a green dot), and Ports 3 through 13 have unselected radio buttons.

Port	Monitor
Port1	<input type="radio"/>
Port2	<input checked="" type="radio"/>
Port3	<input type="radio"/>
Port4	<input type="radio"/>
Port5	<input type="radio"/>
Port6	<input type="radio"/>
Port7	<input type="radio"/>
Port8	<input type="radio"/>
Port9	<input type="radio"/>
Port10	<input type="radio"/>
Port11	<input type="radio"/>
Port12	<input type="radio"/>
Port13	<input type="radio"/>

This page includes the following fields:

OBJECT	DESCRIPTION
	Select a sniffer mode:
Sniffer Type	<ul style="list-style-type: none"> • Disable • Rx • Tx • Both
Analysis (Monitoring) Port	It means Analysis port can be used to see the traffic on another port you want to monitor. You can connect Analysis port to LAN analyzer or netxray.
Monitored Port	The port you want to monitor. The monitor port traffic will be copied to Analysis port. You can select one monitor ports in the switch. User can choose which port that they want to monitor in only one sniffer type.

NOTE:

1. When the Mirror Mode set to RX or TX and the Analysis Port be selected, the packets to and from the Analysis Port will not be transmitted. The Analysis Port will accept only COPIED packets from the Monitored Port.
2. If you want to disable the function, you must select monitor port to none.

VLAN Configuration

VLAN Overview

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

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

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

NOTE:

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Managed Switch supports IEEE 802.1Q (tagged-based) and Port-Base VLAN setting in web management page. In the default configuration, VLAN support is "802.1Q".

Port-based VLAN

Port-based VLAN limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLAN, NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies

on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

IEEE 802.1Q VLANs

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

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

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

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

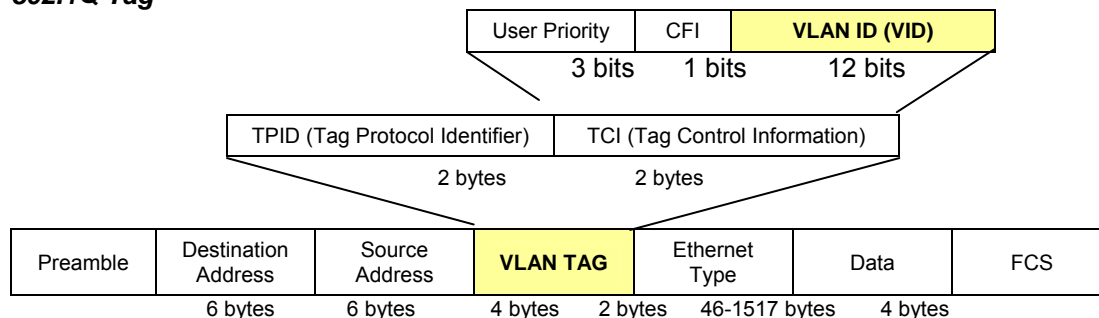
Some relevant terms:

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

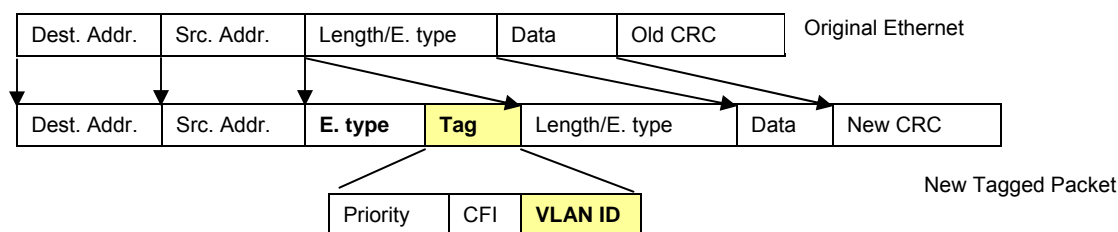
802.1Q VLAN Tags

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

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

802.1Q Tag

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

Adding an IEEE802.1Q Tag**Port VLAN ID**

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

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

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

for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

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

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

Default VLANs

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

VLAN and Link Aggregation Groups

In order to use VLAN segmentation in conjunction with port link aggregation groups, you can first set the port link aggregation group(s), and then you may configure VLAN settings. If you wish to change the port link aggregation grouping with VLAN already in place, you will not need to reconfigure the VLAN settings after changing the port link aggregation group settings. VLAN settings will automatically change in conjunction with the change of the port link aggregation group settings.

Static VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The Managed Switch supports Port-based and 802.1Q (Tagged-based) VLAN in web management page. In the default configuration, VLAN support is "802.1Q".

Figure 4-24: Static VLAN interface

Static VLAN

VLAN Operation Mode: 802.1Q ▼

- No VLAN
- Port Based VLAN
- 802.1Q

VLAN Group | **VLAN Filter**

VLAN Information

DEFAULT	1
---------	---

Add Edit Delete PrePage NextPage Help

NOTE:

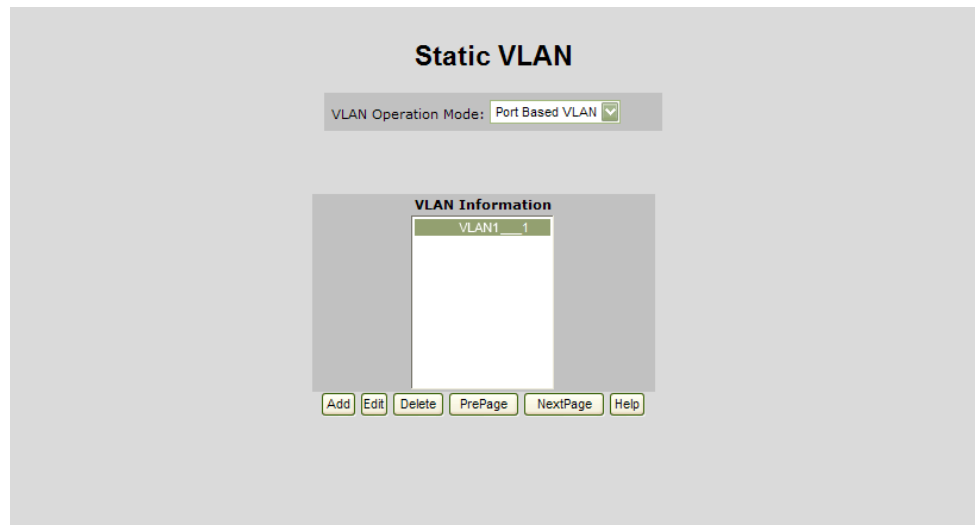
1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Switch supports Port-based VLAN and IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

Port-Based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLANs, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

Figure 4-25: Port-based VLAN interface



Create a VLAN and add member ports to it

1. Click the hyperlink "VLAN" \ "Static VLAN" to enter the VLAN configuration interface.
2. Select **"Port Based VLAN"** at the VLAN Operation Mode, to enable the port-based VLAN function.
3. Click **"Add"** to create a new VLAN group. See Figure 4-26 appears.
4. Type a name and Group ID for the new VLAN, the available range is 2-4094.
5. From the Available ports box, select ports to add to the Managed Switch and click **Add**.
6. Click **Apply**.
7. You will see the VLAN Group displays.
8. If the port-based VLAN groups list over one page, please click **"Next Page"** to view other VLAN groups on other page.
9. Use the **"Delete"** button to delete unwanted port-based VLAN groups
10. Use the **"Edit"** button to modify existing port-based VLAN groups.

By adding ports to the VLAN you have created one port-based VLAN group completely.

Figure 4-26: Static VLAN interface

This page includes the following fields:

OBJECT	DESCRIPTION
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.
Group ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and available range is 2-4094.
Port	Indicate port 1 to port 26.
Member	Add Defines the interface as a Port-Based member of a VLAN.
	Remove Forbidden ports are not included in the VLAN.

NOTE: All unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create and delete Tag-based VLAN. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can't be deleted.

Understanding the nomenclature of the Switch

- IEEE 802.1Q Tagged and Untagged

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

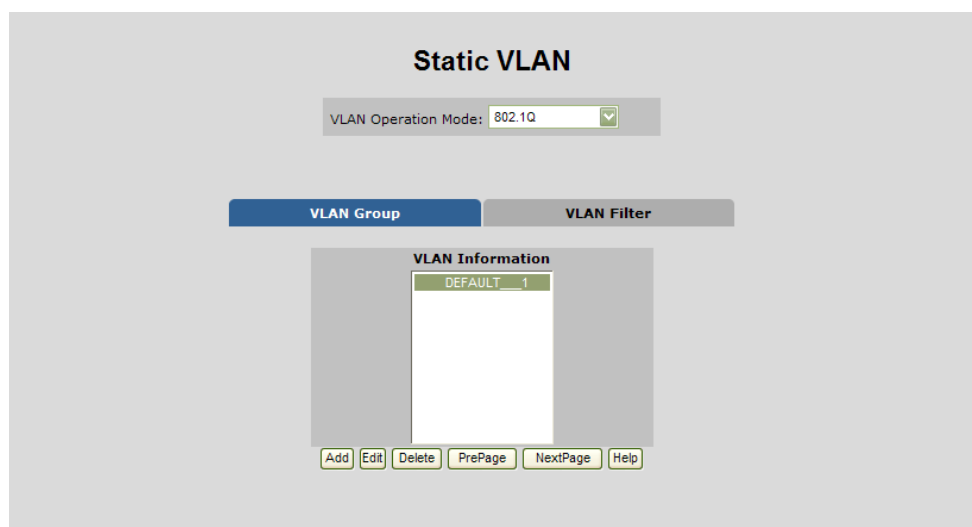
Tagged	Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag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

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

VLAN Group Configuration

- VLAN Group Configuration

Figure 4-27: VLAN Group Configuration interface



1. Click the hyperlink "**VLAN**" \ "**Static VLAN**" to enter the VLAN configuration interface.
2. Select "**802.1Q**" in the **VLAN Operation Mode**, to enable the 802.1Q VLAN function.
3. Click **Add** to create a new VLAN group or **Edit** to management exist VLAN groups. Then the VLAN Group column appears.
4. Input a VLAN group ID and available range is 2-4094.

Figure 4-28: VLAN Group Configuration interface

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group | **VLAN Filter**

VLAN Name: DEFAULT

VID: 1

Add >>

<< Remove

Port1
Port2
Port3
Port4
Port5
Port6
Port7
Port8
Port9
Port10
Port11
Port12

☒ CPU Port

Apply Help

5. Select specific port as member port. The screen in Figure 4-29 appears.

Figure 4-29: 802.1Q VLAN Setting Web Page screen

VLAN Name: DEFAULT	
VLAN ID: 1	
UnTag Member	
Port1	Untag
Port2	Untag
Port3	Untag
Port4	Untag
Port5	Untag
Port6	Untag
Port7	Untag
Port8	Untag
Port9	Untag
Port10	Untag
Port11	Untag
Port12	Untag
Port13	Untag
Port14	Untag
Port15	Untag
Port16	Untag
Port17	Untag
Port18	Untag
Port19	Untag
Port20	Untag
Port21	Untag
Port22	Untag
Port23	Untag
Port24	Untag
Port25	Untag
Port26	Untag

Apply

This page includes the following fields:

OBJECT	DESCRIPTION
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.
VLAN ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and available range is 2-4094.
Port	Indicate port 1 to port 26.
UnTag Member	Untag Packets forwarded by the interface are untagged.
	Tag Defines the interface as a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.

- After setup completed, please press "**Apply**" button to take effect.
- Please press "**Back**" for return to VLAN configuration screen to add other VLAN group, the screen in Figure 4-28 appears.
- If there are many groups that over the limit of one page, you can click **Next** to view other VLAN groups.
- Use the **Delete** button to delete unwanted VLAN.
- Use the **Edit** button to modify existing VLAN group.

NOTE: Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can't be deleted.

VLAN Filter

- 802.1Q VLAN Port Configuration

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

This section provides 802.1Q Ingress Filter of each port from the Switch, the screen in Figure 4-30 appears.

Figure 4-30: 802.1Q Ingress filter interface

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filters

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)

Ingress Filtering Rule 2
(Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1	1	Enable	Disable
Port2			
Port3			
Port4			

Apply
Default
Help

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port2	1	ENABLE	DISABLE

This page includes the following fields:

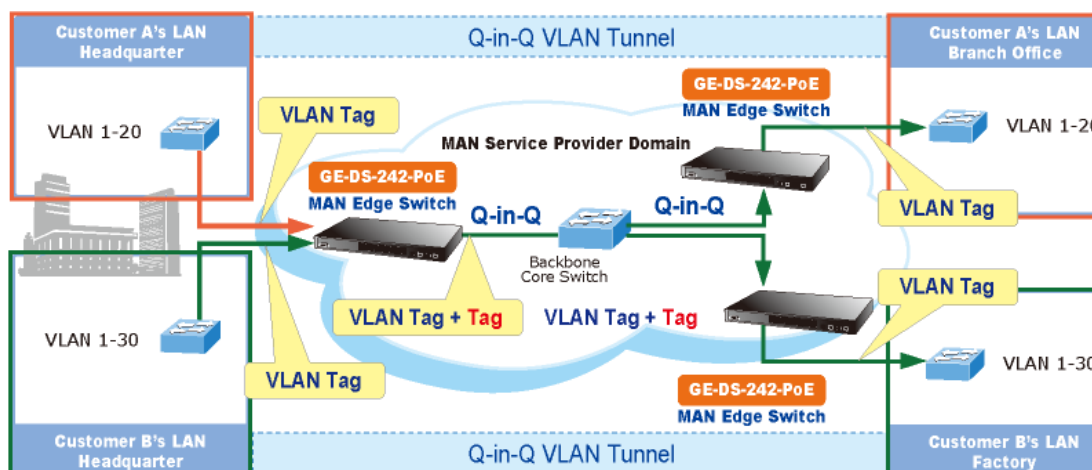
OBJECT	DESCRIPTION
NO	Indicate port 1 to port 26.
PVID	<p>Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging.</p> <p>The switch each port allows user to set one VLAN ID, the range is 1~255, default VLAN ID is 1.</p> <p>The VLAN ID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.</p>
Ingress Filtering 1	<p>Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN.</p> <p>Enable: Forward only packets with VID matching this port's configured VID.</p> <p>Disable: Disable Ingress filter function.</p>
Ingress Filtering 2	<p>Drop untagged frame.</p> <p>Disable: Acceptable all Packet.</p> <p>Enable: Only packet with match VLAN ID can be permission to go through the port.</p>
Apply button	Press the button to save configurations.

802.1Q VLAN

IEEE 802.1Q Tunneling (Q-in-Q)

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

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



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

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

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

Q-in-Q Port Setting

The QinQ VLAN \ QinQ Port Setting screen in Figure 4-31 appears.

Figure 4-31: Q-in-Q Port Setting interface

QinQ VLAN		
QinQ Port Setting		QinQ Tunnel Setting
QinQ Enable		
QinQ Tpid <input type="text" value="8100"/>		
Port	QinQ	QinQ Uplink
Port1	<input type="checkbox"/>	<input type="checkbox"/>
Port2	<input type="checkbox"/>	<input type="checkbox"/>
Port3	<input type="checkbox"/>	<input type="checkbox"/>
Port4	<input type="checkbox"/>	<input type="checkbox"/>
Port5	<input type="checkbox"/>	<input type="checkbox"/>
Port6	<input type="checkbox"/>	<input type="checkbox"/>
Port7	<input type="checkbox"/>	<input type="checkbox"/>
Port8	<input type="checkbox"/>	<input type="checkbox"/>
Port9	<input type="checkbox"/>	<input type="checkbox"/>
Port10	<input type="checkbox"/>	<input type="checkbox"/>
Port11	<input type="checkbox"/>	<input type="checkbox"/>

This page includes the following fields:

OBJECT	DESCRIPTION
QinQ	Enable Sets the Managed Switch to QinQ mode, and allows the QinQ tunnel port to be configured.
	Disable The Managed Switch operates in its normal VLAN mode. The default is for the Managed Switch to function in Disable mode.
QinQ TPID	The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel access port. <ul style="list-style-type: none"> 802.1Q Tag : 8100 vMAN Tag : 88A8 Default : 802.1Q Tag.
Port QinQ	Check: Sets the Port to QinQ mode. Or the port operates in its normal VLAN mode. Default: Un-check.

OBJECT	DESCRIPTION
QinQ Uplink	Check Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network.
	Cancel Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.

Q-in-Q Tunnel Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support QinQ is called a QinQ user-port. A port configured to support QinQ Uplink is called a QinQ uplink-port.

Figure 4-32: Q-in-Q Tunnel Setting interface

QinQ VLAN

QinQ Port Setting QinQ Tunnel Setting

Tunnel ID	Tunnel1	<< Get
Tunnel VID	0	

<< Add << Remove>>

Port1
Port2
Port3
Port4
Port5
Port6
Port7
Port8
Port9

Apply Delete Help

To configure QinQ Port

1. Enable global QinQ function: select **QinQ** enable "**Enable**".
2. Fill QinQ Tpid.
3. Enable port QinQ function: select QinQ checkbox for special port.
4. Enable port QinQ Uplink function: select QinQ Uplink checkbox for special port.

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

Theory

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

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

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1W Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

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

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees - from any combination of ports contained within a single switch, in user specified groups.

- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

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

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

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

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

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

The communication between switches via BPDUs results in the following:

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

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

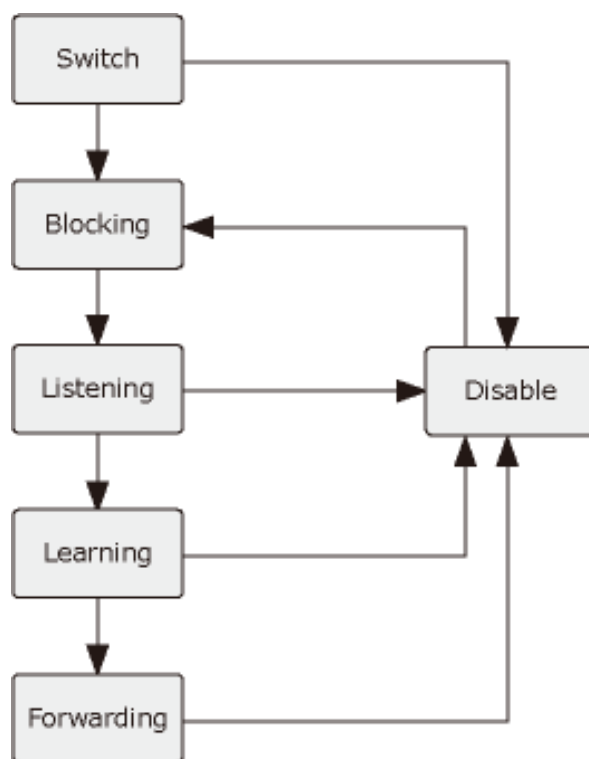
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout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

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

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

A port transitions from one state to another as follows:

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

Figure 4-33: STP Port State Transitions

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

STP Parameters

STP Operation Levels

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

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

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

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

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

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

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

Default Spanning-Tree Configuration

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

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

Observe the following formulas when setting the above parameters:

- **Max. Age _ 2 x (Forward Delay - 1 second)**
- **Max. Age _ 2 x (Hello Time + 1 second)**

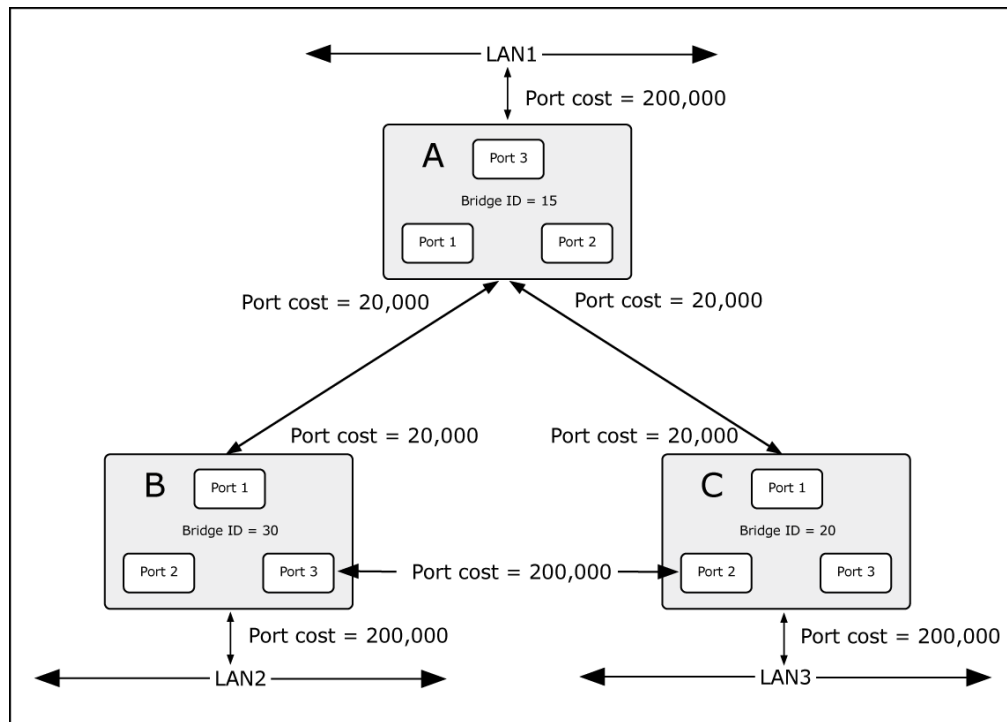
Illustration of STP

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

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

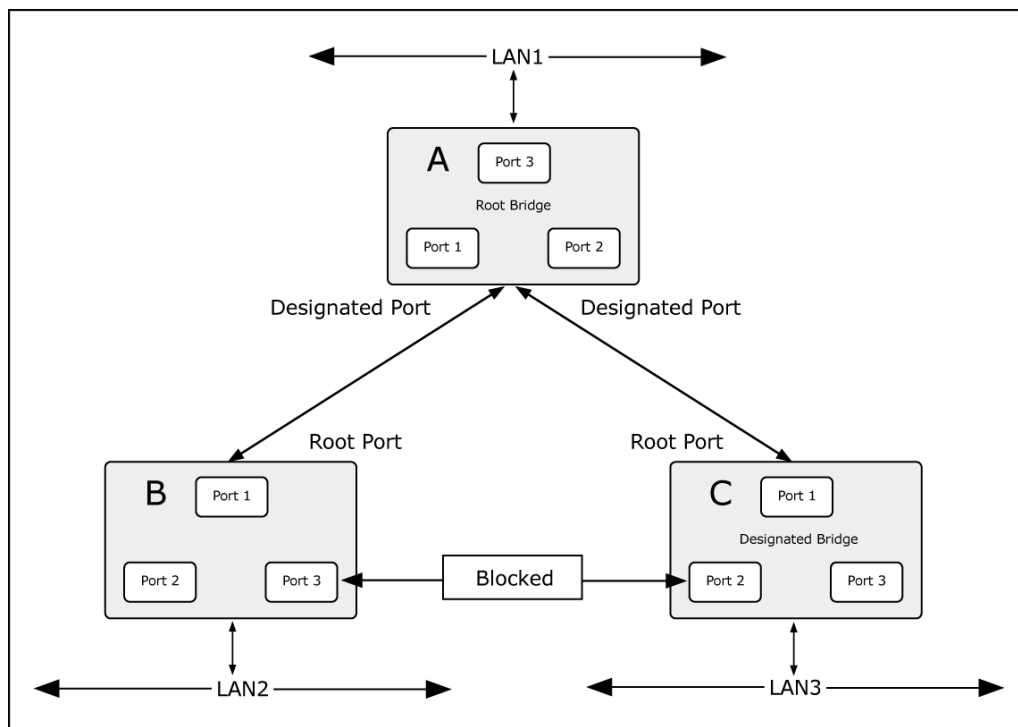
Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

Figure 4-34: Before Applying the STA Rules



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

Figure 4-35: After Applying the STA Rules



The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

RSTP System Configuration

This section provides RSTP-System Configuration from the Switch, the screen in Figure 4-36 appears.

- The user can view spanning tree information of Root Bridge.
- The user can modify RSTP state. After modification, click the **Apply** button.

Figure 4-36: RSTP System Configuration interface

The screenshot displays the 'Spanning Tree' configuration page. It features two tabs: 'System Configuration' (active) and 'PerPort Configuration'. Under 'System Configuration', there is a section titled 'Configure Spanning Tree Parameters' with a table of settings. Below this table are 'Apply' and 'Help' buttons. At the bottom, there is a 'Root Bridge Information' section with a table showing the current root bridge's details.

Configure Spanning Tree Parameters	
STP State (Default DISABLE)	<input type="checkbox"/>
STP protocol version (Default RSTP)	RSTP
Priority (0-61440; Default 32768)	32768
Maximum Age (6-40; Default 20)	20
Hello Time (1-10; Default 2)	2
Forward Delay (4-30; Default 15)	15

Apply Help

Root Bridge Information	
Priority	32768
MAC Address	00:30:4F:75:F2:AA
Root Path Cost	0

This page includes the following fields:

OBJECT	DESCRIPTION
RSTP mode	The user must enable the RSTP function first before configuring the related parameters.
Protocol Version	A value used to specify the spanning tree protocol, the original spanning tree protocol (STP, 802.1d) or the rapid spanning tree protocol (RSTP, 802.1w).
Priority (0-61440)	The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age (6-40)	The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
Hello Time (1-10)	The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
Forward Delay Time (4-30)	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

NOTE: Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time.

$2 \times (\text{Forward Delay Time value} - 1) > \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1).$

NOTE: Each switch in a spanning-tree adopts the Hello Time, Forward Delay time, and Max Age parameters of the root bridge, regardless of how it is configured.

Root Bridge Information

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

The displayed table contains a row for each RSTP bridge instance, where the column displays the following information:

The RSTP Bridge Status screen in Figure 4-37 appears.

Figure 4-37: RSTP Bridge Status page screenshot

Root Bridge Information	
Priority	32768
MAC Address	00:30:4F:75:F2:AA
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

This page includes the following fields:

Object	Description
Priority	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
MAC Address	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Root Port	The switch port currently assigned the root port role.
Maximum Age	Path Cost to the Designated Root for the Root Bridge.
Hello Time	Minimum time between transmissions of Configuration BPDUs.
Forward Delay	Derived value of the Root Port Bridge Forward Delay parameter.

Port Configuration

This web page provides the port configuration interface for RSTP. You can assign higher or lower priority to each port. Rapid spanning tree will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

Figure 4-38: RSTP Port Configuration interface

Spanning Tree

System Configuration
PerPort Configuration

Configure Spanning Tree Port Parameters

Port Number	Path Cost (1-200000000)	Priority (0 - 240; Default 128)	Admin Edge (Default NO)	Admin Non-STP (Default NO)	Admin P2P (Default AUTO)
Port1					
Port2					
Port3	200000	128	NO	NO	AUTO
Port4					
Port5					

Apply
Help

STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	200000	128	Forwarding	NO	NO	YES
Port2	2000000	128	Disabled	NO	NO	NO
Port3	2000000	128	Disabled	NO	NO	NO
Port4	2000000	128	Disabled	NO	NO	NO

This page includes the following fields:

OBJECT	DESCRIPTION
Path Cost	<p>The cost of the path to the other bridge from this transmitting bridge at the specified port.</p> <p>Enter a number 1 through 200,000,000.</p>
Priority	<p>Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240.</p> <p>The value of priority must be the multiple of 16.</p>
Admin P2P	<p>The rapid state transitions possible within RSTP are dependent upon whether the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively.</p> <ul style="list-style-type: none"> • YES means the port is regarded as a point-to-point link. • NO means the port is regarded as a shared link. • AUTO means the link type is determined by the auto-negotiation between the two peers..
Admin Edge	<p>The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "YES" status.</p>
Admin Non STP	<p>The port includes the STP mathematic calculation.</p> <ul style="list-style-type: none"> • YES is not including STP mathematic calculation. • NO is including the STP mathematic calculation.

NOTE: Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 802.1w standard exceeds 65,535, the default is set to 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Table 4-1: Recommended STP Path Cost Range

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

Table 4-2: Recommended STP Path Cost Range

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

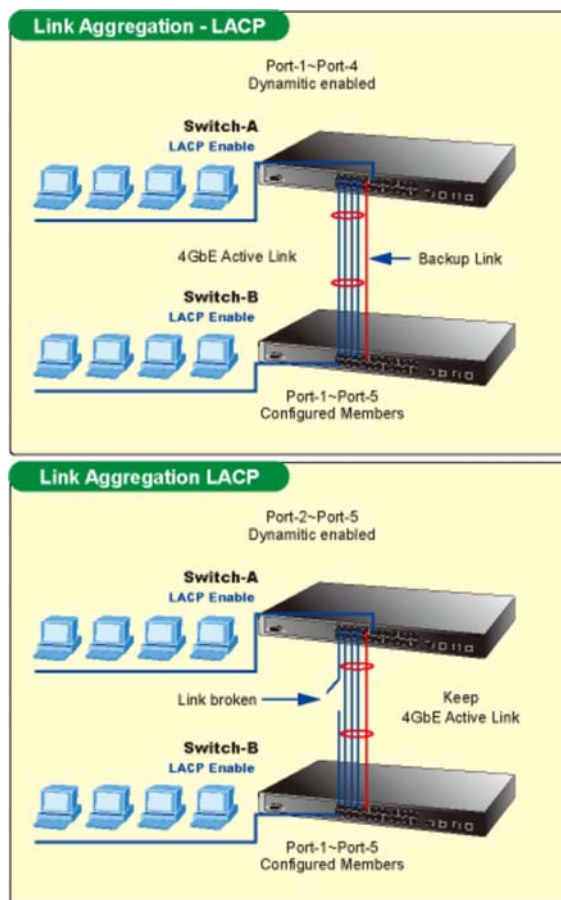
Trunking

Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. The Managed Switch supports two types of port trunk technology:

- Static Trunk
- LACP

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, more detail information refers to IEEE 802.3ad.

Figure 4-39: Aggregator setting



This section provides Port Trunk-Aggregator settings for each port from the Managed Switch, the screen in Figure 4-40 appears.

Figure 4-40: Port Trunk-Aggregator setting interface (two ports are added to the left field with LACP enabled)

The screenshot shows the 'Trunking' configuration page with the 'Aggregator Setting' tab selected. The 'LACP' checkbox is checked, and the 'System Priority' is set to 32768. The 'Group ID' is set to 1, 'LACP' is set to 'Enable', and 'Work Ports' is set to 2. A list of ports (Port1 to Port9) is on the right, with Port23 and Port24 selected in the left field. Buttons for '<< Add <<', 'Remove>>', 'Apply', 'Delete', and 'Help' are at the bottom.

This page includes the following fields:

OBJECT	DESCRIPTION
System Priority	A value which is used to identify the active LACP. The Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
Group ID	There are 13 trunk groups to be selected. Assign the "Group ID" to the trunk group.
LACP	<ul style="list-style-type: none"> Enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. Disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
Work ports	This column field allows the user to type in the total number of active port up to four. With LACP static trunk group, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group (non-LACP), the number of work ports must equal the total number of group member ports.

NOTE: A trunk group, including member ports split between two switches, has to enable the LACP function of the two switches.

Aggregator Information

When you setup the LACP aggregator, you will see relational information here.

LACP disabled

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of Aggregator Information.

Figure 4-41: Assigning 2 ports to a trunk group with LACP disabled

Trunking

Aggregator Setting | **Aggregator Information** | State Activity

LACP ☐ System Priority 32768

Group ID 1 << Get

LACP Disable

Work Ports 2

Port23 Port24 << Add << Remove>>

Port16 Port17 Port18 Port19 Port20 Port21 Port22 Port23 Port24 Port25 Port26

Apply Delete Help

Figure 4-42: Static Trunking Group information

Trunking

Aggregator Setting | **Aggregator Information** | State Activity

The following information provides a view of LACP current status.

Static Trunking Group

Group Key 1

Port_No 23 24

This page includes the following fields:

OBJECT	DESCRIPTION
Group Key	This is a read-only column field that displays the trunk group ID.
Port member	This is a read-only column field that displays the members of this static trunk group.

LACP enabled

Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of Aggregator Information.

- **Switch 1 configuration**

1. Set **System Priority** of the trunk group. The default is 1.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable **LACP**.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of Work Ports changes automatically.

Figure 4-43: Aggregation Information of Switch 1

The screenshot shows the 'Trunking' configuration interface. The 'Aggregator Information' tab is active. It displays the following configuration:

- LACP:** Checked (checkbox).
- System Priority:** 1.
- Group ID:** 1 (selected from a dropdown).
- LACP:** Enable (selected from a dropdown).
- Work Ports:** 2.
- Port List:** A list of ports from Port1 to Port11. Port1 and Port2 are currently selected.
- Buttons:** '<< Add <<', 'Remove >>', and '<< Get' are located near the port list.
- Footer:** 'Apply', 'Delete', and 'Help' buttons.

5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

- **Switch 2 configuration**
 6. Set **System Priority** of the trunk group. For example: 32768.
 7. Select a **trunk group ID** by pull down the drop-down menu bar.
 8. Enable **LACP**.
 9. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

Figure 4-44: Switch 2 configuration interface

10. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches have been configured.

Figure 4-45: Switch 1 Aggregator Information

Group1						
Actor			Partner			
Priority	1		32768			
MAC	00304f75f2ab		00304f10c976			
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT1	258	1	selected	PORT3	513	1
PORT2	258	1	selected	PORT4	513	1

State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click the **Apply** button, the port state activity will change to Passive.

Figure 4-46: State Activity of Switch 1

Trunking			
Aggregator Setting		Aggregator Information	State Activity
Port	LACP State Activity	Port	LACP State Activity
1	<input checked="" type="checkbox"/> Active	2	<input checked="" type="checkbox"/> Active
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A

This page includes the following fields:

OBJECT	DESCRIPTION
Active	The port automatically sends LACP protocol packets.
Passive	The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

Figure 4-47: State Activity of Switch 2

Trunking

Aggregator Setting		Aggregator Information		State Activity	
Port	LACP State Activity	Port	LACP State Activity		
1	N/A	2	N/A		
3	<input checked="" type="checkbox"/> Active	4	<input checked="" type="checkbox"/> Active		
5	N/A	6	N/A		
7	N/A	8	N/A		
9	N/A	10	N/A		
11	N/A	12	N/A		
13	N/A	14	N/A		
15	N/A	16	N/A		
17	N/A	18	N/A		
19	N/A	20	N/A		
21	N/A	22	N/A		
23	N/A	24	N/A		

NOTE: A link having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

Forwarding and Filtering

The frames of Ethernet Packets contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

Dynamic MAC Table

Entries in the MAC Table are shown on this page. The Dynamic MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address. You can view all of the dynamic MAC addresses learned by the listed port.

Figure 4-48: Dynamic MAC Address interface

Forwarding and Filtering

Dynamic MAC Table Static MAC Table MAC Filtering

Click "Clear" will clear Dynamic addresses from the switch .

Dynamic addresses currently learned on the switch are listed below.

NO	MAC	PORT	VID	TYPE
1	00:1A:64:12:CD:51	1	1	Dynamic
2	00:14:51:98:01:70	1	1	Dynamic
3	00:0E:2E:76:ED:FD	1	1	Dynamic
4	00:30:4F:52:A1:DD	1	1	Dynamic
5	00:30:4F:A1:01:A9	1	1	Dynamic
6	00:14:5E:DC:93:CD	1	1	Dynamic
7	00:14:85:03:F7:80	1	1	Dynamic
8	00:19:21:5C:1E:FB	1	1	Dynamic
9	00:1B:78:12:8E:E9	1	1	Dynamic
10	00:15:5D:01:09:0A	1	1	Dynamic
11	00:14:5E:7F:97:F8	1	1	Dynamic
12	00:14:5E:16:1D:16	1	1	Dynamic

MAC Table Entries

OBJECT	DESCRIPTION
NO	The index of the MAC address entry.
MAC	The MAC address of the entry.
PORT	The ports that are members of the entry.
VID	The VLAN ID of the entry.
Type	Indicates whether the entry is a static or dynamic entry.

- Click **"Clear"** to clear the dynamic MAC addresses information of the current port shown on the screen.

Static MAC Table

You can add a static MAC address that remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add / modify / delete a static MAC address.

Add the Static MAC Address

You can add a static MAC address in the switch MAC table here.

Figure 4-49: Static MAC Addresses interface

Forwarding and Filtering

Dynamic MAC Table Static MAC Table MAC Filtering

Dynamic addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address	PORT	VID
00:30:4F:11:22:33	1	1

MAC Address: 00:30:4F:22:33:44

Port num: Port20

VLAN ID: 1

Add Delete Help

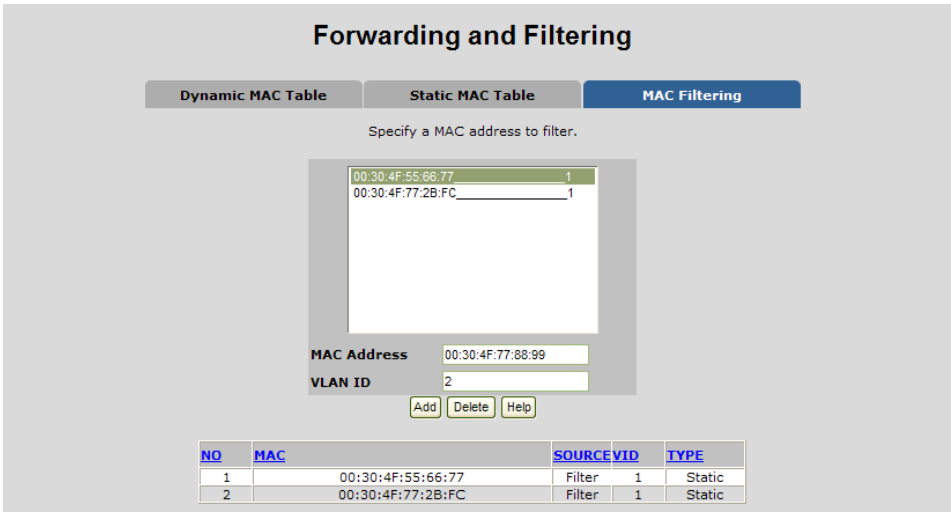
This page includes the following fields:

OBJECT	DESCRIPTION
MAC Address	Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
Port Num	Pull down the selection menu to select the port number.
VLAN ID	The VLAN ID for the entry.

MAC Filtering

By filtering MAC address, the switch can easily filter the pre-configured MAC address and increase the security. You can add and delete filtering MAC address.

Figure 4-50: MAC Filtering interface



This page includes the following fields:

OBJECT	DESCRIPTION
MAC Address	Enter the MAC address that you want to filter.
VLAN ID	The VLAN ID for the entry.

IGMP Snooping

Theory

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The Internet Group Management Protocol (IGMP) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'querier'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

Figure 4-51: Multicast Service

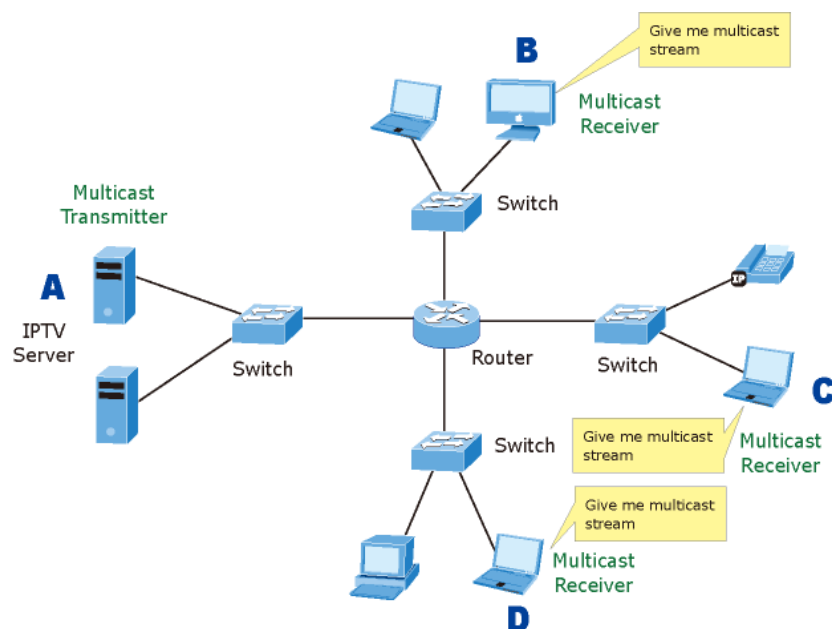


Figure 4-52: Multicast flooding

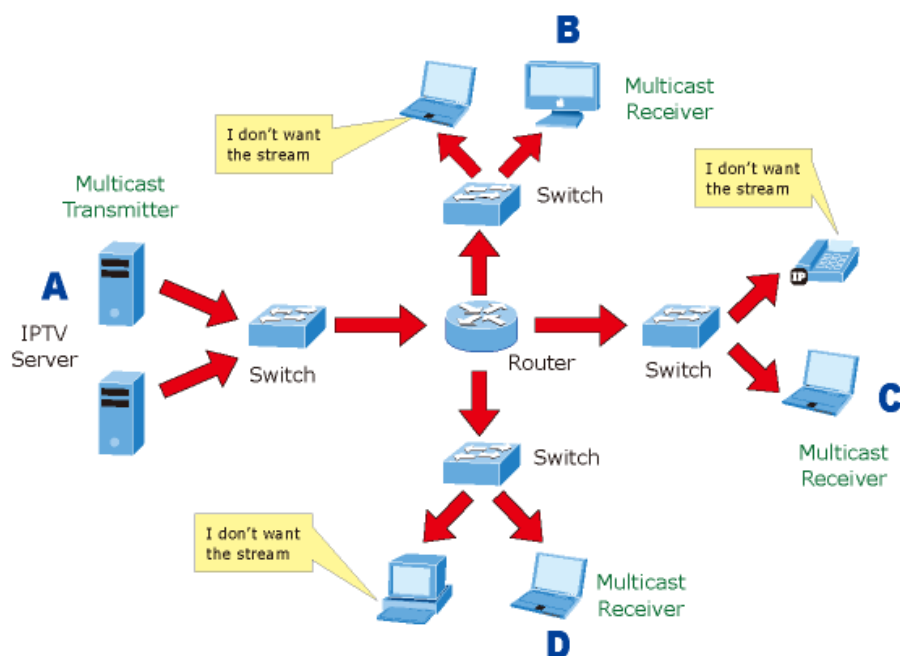
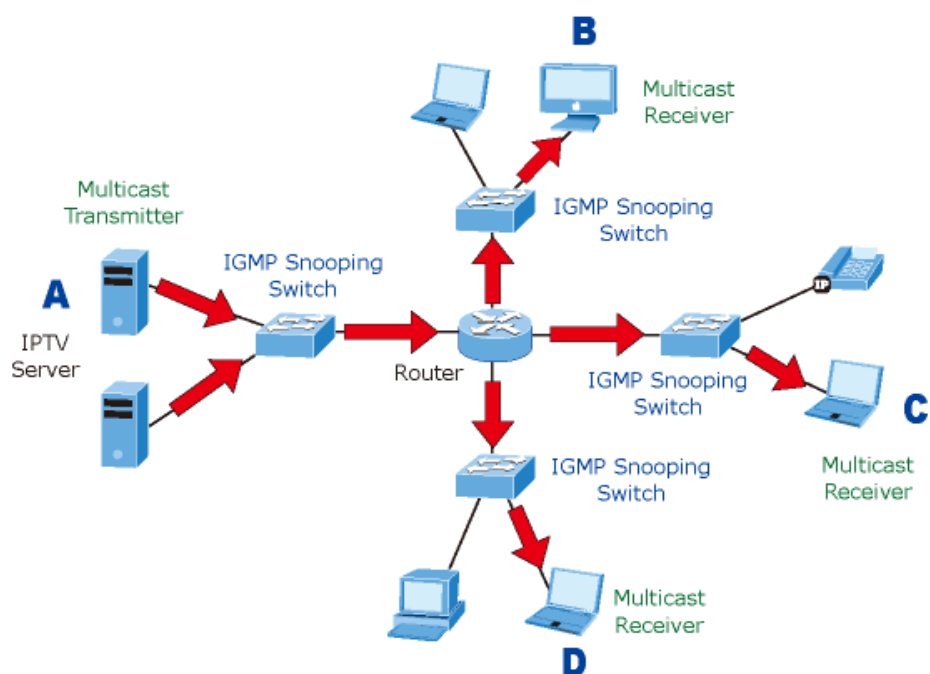


Figure 4-53: IGMP Snooping multicast stream control



IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

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

The IGMP Type codes are shown below:

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

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

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

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

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

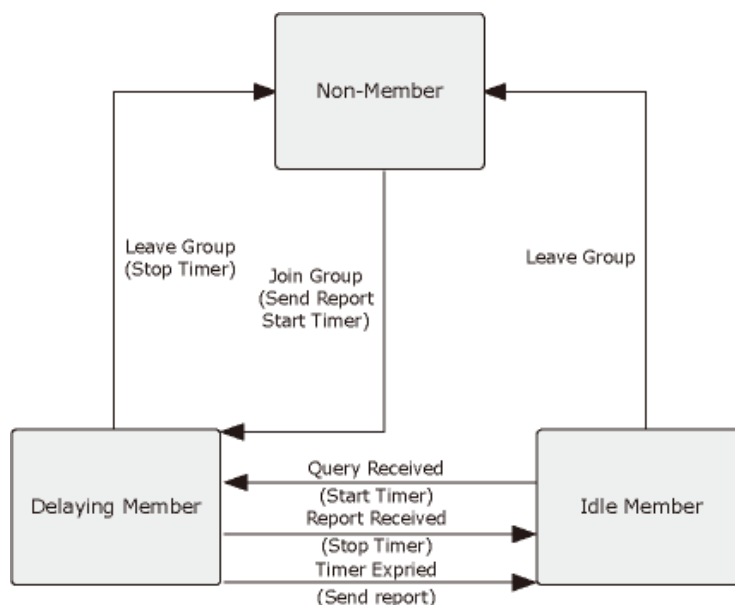
Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

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

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

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

Figure 4-54: IGMP State Transitions



IGMP Querier

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

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

IGMP Configuration

The Switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then the IGMP snooping information displays. IP multicast addresses range are from 224.0.0.0 through 239.255.255.255.

Figure 4-55: IGMP Configuration interface

This page includes the following fields:

OBJECT	DESCRIPTION
IGMP Protocol	Enable or disable the IGMP protocol.
IGMP Fastleave	Enable or disable Fast Leave on the port.
IGMP Querier	Enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.

NOTE: Fast Leave:

The Managed Switch can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the fastleave function is enabled for the parent VLAN. This allows the Managed switch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific query to that interface.

QoS Configuration

Understand QoS

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

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

You can use QoS on your system to:

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

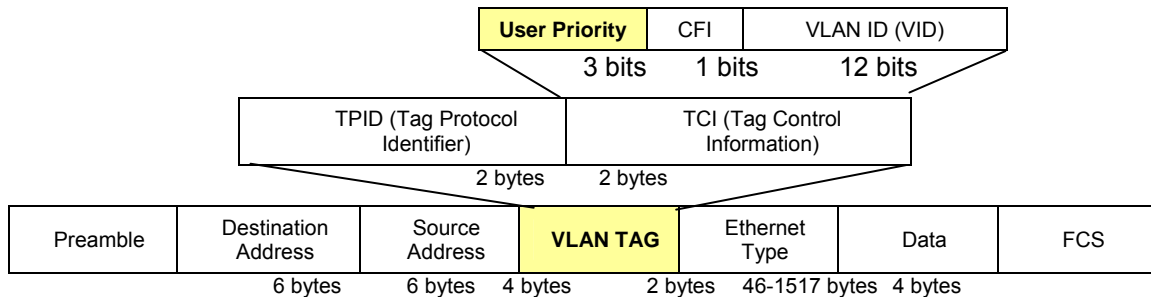
The QoS page of the Switch contains three types of QoS mode - the CoS mode, TOS mode or Port-based mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- **CoS / 802.1p Tag Priority Mode** -The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **TOS / DSCP Mode** - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- **Port-Based Priority Mode** - Any packet received from the specify high priority port will treated as a high priority packet.

QoS Configuration

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. When CoS / 802.1p Tag Priority is applied, the Switch recognizes 802.1Q VLAN tag packets and extracts the VLAN tagged packets with User Priority value.

802.1Q Tag and 802.1p priority



Set up the COS priority level. With the drop-down selection item of Priority Type above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

Priority Queue Service settings

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. In 802.1p compliant devices, a tag inserted into the packet header is used to identify the priority level of data packets.

The Switch supports Static Port Ingress priority and four queues. The screen in Figure 4-56 appears.

Figure 4-56: QoS Configuration - 802.1pPriority

This page includes the following fields:

OBJECT	DESCRIPTION
First Come First Service	The sequence of packets sent is depend on arrival order.
All High before Low	The high priority packets sent before low priority packets.
Weighted Round Robin	Select the preference given to packets in the switch's higher-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest : 4 SecHigh : 2 SecLow : 1 Lowest means that the switch sends 8 highest priority packets before sending 4 second high priority packet, before sending 2 second low priority packet, before sending 1 lowest priority packet.
802.1p priority [0-7]	Set up the COS priority level 0~7—High, Middle, Low, Lowest.

NOTE: 802.1p Priority:

Priority classifiers of the Switch forward packet. COS range is from 0 to 7. Seven is the high class. Zero is the less class. The user may configure the mapping between COS and Traffic classifiers.

QoS PerPort Configuration

Configure the priority level for each port. With the drop-down selection item of Priority Type above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

Figure 4-57: QoS Configuration - Port-Based Priority

QoS Configuration

QoS Configuration **PerPort Configuration**

Configure Port Priority

Port Number	Port Priority
Port1	Disable
Port2	Disable
Port3	Disable
Port4	Disable
Port5	Disable

Apply

Port Priority

PortNum	Priority
Port1	Disable
Port2	Disable
Port3	Disable
Port4	Disable
Port5	Disable

This page includes the following fields:

OBJECT	DESCRIPTION
Port Number:	Indicate port 1 to port 26.
Port Priority:	Each port has 8 priority levels—0~7 or Disable to be chosen. 7 is the highest priority.

TOS/DSCP

TOS/DSCP priority is obtained through a 6-bit Type-of-Service (TOS) or Differentiated Service Code Point (DSCP) to 3-bit priority mapping.

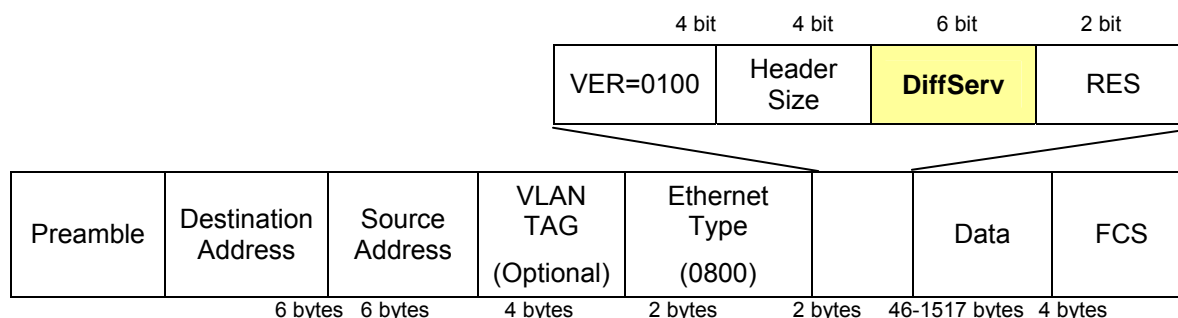
The Type of Service (TOS) octet in the IPv4 header is divided into three parts; Precedence (3 bits), TOS (4 bits), and MBZ (1 bit). The Precedence bits indicate the importance of a packet, whereas the TOS bits indicate how the network should make tradeoffs between throughput, delay, reliability, and cost (as defined in RFC 1394). The MBZ bit (for "must be zero") is currently unused and is either set to zero or just ignored.

0	1	2	3	4	5	6	7
Precedence			TOS			MBZ	

Pv4 Packet Header Type of Service Octet

The four TOS bits provide 15 different priority values, however only five values have a defined meaning.

DiffServ Code Point (DSCP) - is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network. DSCP are defined in RFC2597 for classifying traffic into different service classes. The Managed Switch extracts the codepoint value of the DS field from IPv4 packets and identifies the priority of the incoming IP packets based on the configured priority.



The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP retains backward compatibility with the three precedence bits so that non-DSCP compliant, TOS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

TOS/DSCP Configuration

The TOS/DSCP page provides fields for defining output queue to specific DSCP fields. When TCP/IP's TOS/DSCP mode is applied, the Managed Switch recognizes TCP/IP Differentiated Service Codepoint (DSCP) priority information from the DS-field defined in RFC2474.

Enable TOS/DSCP for traffic classification and then the DSCP to priority mapping column is configurable, as Figure 4-8 shows:

Figure 4-58: QoS Configuration - TOS Priority

DSCP	Priority
DSCP0	0
DSCP1	0
DSCP2	0
DSCP3	0
DSCP4	0

DSCP	Priority	DSCP	Priority
DSCP0	0	DSCP1	0
DSCP2	0	DSCP3	0
DSCP4	0	DSCP5	0
DSCP6	0	DSCP7	0

This page includes the following fields:

OBJECT	DESCRIPTION
TOS/DSCP	Enable / Disable internal traffic class (0~7) to map the corresponding IP DSCP value.
DSCP	The values of the IP DSCP header field within the incoming packet. 0~63.
Priority	Specify which 802.1p priority to map the corresponding IP DSCP. The value is 0~7.

TOS/DSCP Port Configuration

Set up IP TOS / DSCP mapping to 802.1p priority when receiving IPv4/IPv6 packets, the Managed Switch allow to by port configuring the QoS Status. This TOS/DSCP Port Configuration page is to configure the IP TOS/DSCP mapping on the port and display the current port status. The screen in Figure 4-59 appears.

Figure 4-59 : QoS Configuration - TOS/DSCP Port Status

Port Number	TOS/DSCP Status
Port1	Disable
Port2	
Port3	
Port4	
Port5	

PortNum	TOS/DSCP Port Status
Port1	Disable
Port2	Disable
Port3	Disable
Port4	Disable
Port5	Disable

This page includes the following fields:

OBJECT	DESCRIPTION
Port Number	Indicate port 1 to port 26.
TOS/DSCP Status	Enable / Disable TOS/DSCP map to 802.1p priority on specify port.

Access Control List

The Access Control List (ACL) is a concept in computer security used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identifier. Access Control List (ACL) is a mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted or denied to access the resource. The screen in following screen appears.

Packets can be forwarded or dropped by ACL rules include Ipv4 or non-Ipv4. The Managed Switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

Packet Type / Bindings can be selected to ACL for Ipv4 or Non-Ipv4.

Figure 4-60: Access Control List (ACL) Web Page screen

Access Control List

Group Id	<input type="text" value="1"/> (1~220)		
Action	Permit <input checked="" type="checkbox"/>		
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID <input type="text" value="1"/> (1~4094; Any means Vid=0 if uses binding)		
Packet Type / Binding	<input checked="" type="radio"/> IPv4 <input type="radio"/> Non-IPv4 <input type="radio"/> Binding		
Src IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>	Ether Type <input type="text" value="Any"/> Type# <input type="text"/>	MAC Address <input type="text" value="00:11:22:33:44:55"/>
Dst IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>	IP Address <input type="text" value="0.0.0.0"/>	
IP Fragment	<input checked="" type="checkbox"/> Unchecked		Port Id <input type="text" value="1"/> (1~26)
L4 Protocol	<input checked="" type="radio"/> Any <input type="text" value="Protocol#"/> <input type="radio"/> TCP <input type="text" value="Any"/> <input type="text" value="Port#"/> <input type="radio"/> UDP <input type="text" value="Any"/> <input type="text" value="Port#"/>		
Port Id	<input type="text" value="0"/> (1~26, 0: don't care)		
Current List	<div style="border: 1px solid black; height: 40px;"></div>		

This page includes the following fields:

IPv4 ACL

OBJECT	DESCRIPTION	DEFAULT VALUE
Group ID	1 ~ 247 (max. 247 ACL group).	
Action	Permit / Deny. Permit: Permit packet cross switch. Deny: Drop packet.	Permit
VLAN	Any / VID. Any: Any VLAN id. VID: 1~4094. A certain VLAN id.	Any
Packet Type	IPv4 / Non-IPv4 / Binding IPv4: Set Ipv4 packet field. Non-IPv4: Set non-Ipv4 packet field. Binding: Set binding entry.	IPv4

OBJECT	DESCRIPTION	DEFAULT VALUE
Src IP Address	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>Any / IP and Mask</p> <p>Any: Any IP address.</p> <p>IP : A certain IP address.</p> <p>Mask: <code>***.***.***.***</code></p> <p>* is represent a digit from 0~9,</p> <p>*** is range from 0 to 255</p> <p>Notice: This is not subnet mask.</p>	Any
Dst IP Address	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>Any / IP and Mask</p> <p>Any: Any IP address.</p> <p>IP : A certain IP address.</p> <p>Mask: <code>***.***.***.***</code></p> <p>* is represent a digit from 0~9,</p> <p>*** is range from 0 to 255</p>	Any
IP Fragment	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>Uncheck / Check</p> <p>Uncheck: Not check IP fragment field.</p> <p>Check: Check IP fragment field.</p>	Uncheck
L4 Protocol	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>Any / ICMP(1) / IGMP(2) / TCP(6) / UDP(17)</p>	Any
Protocol	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>0~255.</p> <p>If protocol not find in L4 Protocol field, you can direct assign number.</p>	
TCP	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>Any / FTP(21) / HTTP(80)</p>	Any
Port	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>0~65535</p> <p>If TCP port not find in TCP field, you can direct assign number.</p>	
UDP	<p>Set this field if Packet Type is IPv4, else ignore.</p> <p>Any / DHCP(67) / TFTP(69) / NetBios(137)</p>	Any

OBJECT	DESCRIPTION	DEFAULT VALUE
Port	Set this field if Packet Type is IPv4, else ignore. 0~65535 If UDP port not find in UDP field, you can direct assign number.	
Port Id	Source port id, from 1~26, 0 means don't care.	0
Current List	You create ACL and Binding groups.	

Non-IPv4 ACL

In Packet Type / Binding box should select Non-IPv4

OBJECT	DESCRIPTION	DEFAULT VALUE
Group ID	1 ~ 247 (max. 247 ACL group)	
Action	Permit / Deny. Permit: Permit packet cross switch. Deny: Drop packet.	Permit
VLAN	Any / VID. Any: Any VLAN ID. VID: 1~4094. A certain VLAN ID.	Any
Packet Type	IPv4 / Non-IPv4 / Binding IPv4: Set Ipv4 packet field. Non-IPv4: Set non-Ipv4 packet field. Binding: Set binding entry.	IPv4
Ether Type	Set this field if Packet Type is Non-IPv4, else ignore.) Any / ARP(0x0806) / IPX(0x8137)	Any
Type	Set this field if Packet Type is Non-IPv4, else ignore.) 0~0xFFFF If ether type not find in Ether Type field, you can direct assign number.	
Current List	You create ACL and Binding groups.	

Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN id and port id to bind, and device can cross switch if all conditions match.

Use binding function; we should enable it first in following page.

In Packet Type / Binding box should select Binding.

OBJECT	DESCRIPTION	DEFAULT VALUE
Group ID	1 ~ 247 (max. 247 ACL group)	
Action	Permit / Deny. Permit : Permit packet cross switch. Deny: Drop packet.	Permit
VLAN	Any / VID. Any: Any Vlan id. VID: 1~4094. A certain vlan id.	Any
Packet Type	IPv4 / Non-IPv4 / Binding IPv4: Set Ipv4 packet field. Non-IPv4: Set non-Ipv4 packet field. Binding: Set binding entry.	IPv4
MAC Address	**.**.**.**.**.**.*** * is represent a digit from 0~9 and A~F, *** is range from 0 to FF.	00:11:22:33:44:55
IP Address	***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255.	0.0.0.0
Port Id	Source port id, from 1~26.	1
Current List	You create ACL and Binding groups.	

MAC Limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

MAC Limit Configuration

The Layer 2 MAC Limit function can be per-port configured for security management purposes. When the port is in MAC Limit mode, the port will be "locked" without permission of address learning. Only the incoming packets with Source MAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses.

Figure 4-61: MAC Limit - Configure MAC Limit

MAC Limit

Configure MAC Limit

MAC Limit ☒

Port Number Limit (1-64, 0 to turn off MAC limit)

Port1 ☐ Port2 ☐ Port3 ☐ Port4 ☐ Port5 ☐

15

Apply Help

MAC Limit Port Status

Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off

This page includes the following fields:

OBJECT	DESCRIPTION
MAC Limit	Enable or disable MAC limit function for the Managed Switch.
Port Number	Indicate port 1 to port 26.
Limit	The maximum number of per-port MAC addresses to be learned (1-64, 0 to disable this port's MAC limit function).

MAC Limit Port Status

This table displays current MAC Limit status of each port.

Figure 4-62: MAC Limit - MAC Limit Port Status

MAC Limit Port Status	
Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off
Port7	off
Port8	off
Port9	off
Port10	off
Port11	off
Port12	off
Port13	off
Port14	off
Port15	off

This page includes the following fields:

OBJECT	DESCRIPTION
Port Number	Indicate port 1 to port 26.
Limit	Display the current MAC Limit configuration and status of each port.

802.1X Configuration

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

Understanding IEEE 802.1X Port-Based Authentication

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

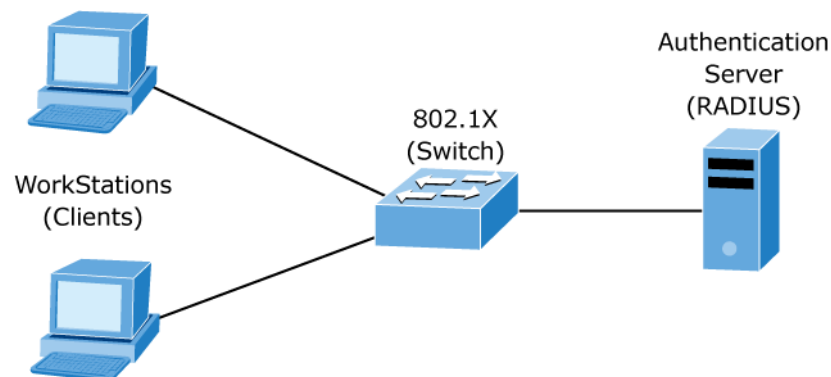
Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

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

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

Figure 4-63: 802.1x device role



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

- **Authentication server** - performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- **Switch (802.1X device)** - controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

- **Authentication Initiation and Message Exchange**

The switch or the client can initiate authentication. If you enable authentication on a port by using the `dot1x port-control auto` interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

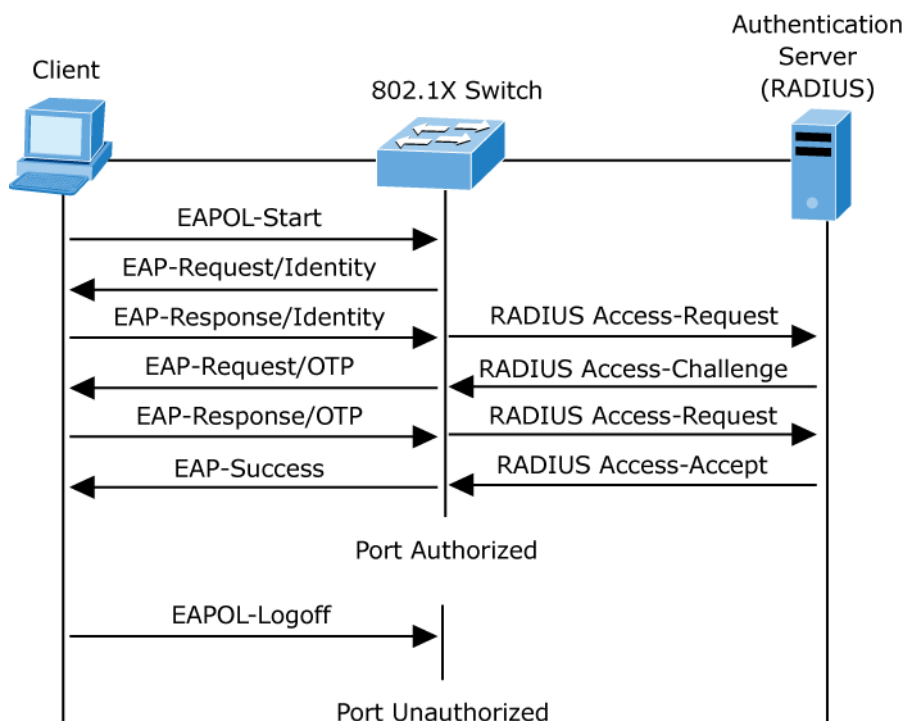
However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

NOTE: If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-64" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 4-64: EAP message exchange



- Ports in Authorized and Unauthorized States

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

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

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

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

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

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

System Configuration

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

To enable 802.1x, from System \ System Information \ Misc Config then you still to fill in the authentication server information:

Figure 4-65: System information \ Misc Configuration\ 802.1x Protocol

Turn On Port Interval: 0 seconds (0~3600 seconds, interval time between turning off and turning on port for flooding CPU port, 0:disable)

Broadcast Storm Filter Mode: OFF

Broadcast Storm Filter Packet select

☐ Broadcast Packets

☐ IP Multicast

☐ Control Packets

☐ Flooded Unicast/Multicast Packets

Collisions Retry Forever : 16

Hash Algorithm : CRC-Hash

IP/MAC Binding : Disable

802.1x Protocol : Enable

Apply Default Help

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

Figure 4-66: 802.1x System Configuration interface

802.1x Configuration

System Configuration PerPort Configuration Misc Configuration

Configure 802.1x Parameters

Radius Server IP:	192.168.0.99
Server Port:	1812
Accounting Port:	1813
Shared Key:	
NAS Identifier:	NAS_L2_SWITCH

Apply Help

This page includes the following fields:

OBJECT	DESCRIPTION
IEEE 802.1x Protocol:	Enable or disable 802.1x protocol.
Radius Server IP:	Assign the RADIUS Server IP address.
Server Port:	Set the UDP destination port for authentication requests to the specified RADIUS Server.
Accounting Port:	Set the UDP destination port for accounting requests to the specified RADIUS Server.

OBJECT	DESCRIPTION
Shared Key:	Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
NAS, Identifier:	Set the identifier for the RADIUS client.
IEEE 802.1x Protocol:	Enable or disable 802.1x protocol.

4.12.3 802.1x Port Configuration

In this page, you can select the specific port and configure the authorization state. The state provides No Authorization, Force Authorized, Force unauthorized, and Authorize.

Figure 4-67: 802.1x Per Port Setting interface

802.1x Configuration

System Configuration
Port Configuration
Misc Configuration

Configure 802.1x Per Port State

Port Number	Port State
<div style="border: 1px solid #ccc; padding: 2px;"> Port1 ▲ Port2 □ Port5 ▼ Port6 ▼ Port7 ▼ </div>	<div style="border: 1px solid #ccc; padding: 2px;"> Au ▼ </div>

Port Status

PortNum	State
Port1	No
Port2	No
Port5	No
Port6	No
Port7	No
Port8	No
Port9	No

This page includes the following fields:

OBJECT	DESCRIPTION
FU (Force Unauthorized)	The specified port is required to be held in the unauthorized state.
FA (Force Authorized)	The specified port is required to be held in the authorized state.

OBJECT	DESCRIPTION
Authorize	The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
No	The specified port works without complying with 802.1x protocol.

Misc Configuration

In this page, you can change the default configuration for the 802.1x standard:

Figure 4-68: 802.1x Misc Configuration interface

802.1x Configuration	
System Configuration PerPort Configuration Misc Configuration	
Configure 802.1x misc configuration	
Quiet period:	60
Tx period:	15
Supplicant timeout:	30
Server timeout:	30
Max requests:	2
Reauth period:	3600
Apply Help	





This page includes the following fields:

OBJECT	DESCRIPTION
Quiet Period:	Used to define periods of time during which it will not attempt to acquire a supplicant. Default time is 60 seconds.
TX Period:	Set the period the port waits for retransmit next EAPOL PDU during an authentication session. Default value is 30 seconds.
Supplicant Timeout:	Set the period of time the switch waits for a supplicant response to an EAP request. Default value is 30 seconds.
Server Timeout:	Set the period of time the switch waits for a server response to an authentication request. Default value is 30 seconds.
Max Requests:	Set the number of authentication that must time-out before authentication fails and the authentication session ends. Default value is 2 times.
Reauth period:	Set the period of time which clients connected must be re-authenticated. Default value is 3600 seconds.

Power Over Ethernet

Providing up to 24 PoE, in-line power interface, the GE-DS-242-PoE PoE Switch can easily build a power central-controlled IP phone system, IP Camera system, AP group for the enterprise. For instance, 24 camera / AP can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without the power-socket limitation, the PoE Switch makes the installation of cameras or WLAN AP more easily and efficiently.

Power over Ethernet Powered Device

 <p>3~5 watts</p>	<p>Voice over IP phones</p> <p>Enterprise can install POE VoIP Phone, ATA and other Ethernet/non-Ethernet end-devices to the central where UPS is installed for un-interrupt power system and power control system.</p>
 <p>6~12 watts</p>	<p>Wireless LAN Access Points</p> <p>Museum, Sightseeing, Airport, Hotel, Campus, Factory, Warehouse can install the Access Point any where with no hesitation</p>
 <p>10~12 watts</p>	<p>IP Surveillance</p> <p>Enterprise, Museum, Campus, Hospital, Bank, can install IP Camera without limits of install location – no need electrician to install AC sockets.</p>
 <p>3~12 watts</p>	<p>PoE Splitter</p> <p>PoE Splitter split the PoE 48V DC over the Ethernet cable into 5/9/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.</p>

Power Management

In a power over Ethernet system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure to powered devices (PDs), which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system may a prior be planed with a PSU capable of supplying less power than the total potential power consumption of all the PoE ports in the system. In order to maintain the majority of ports active, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current. The input power consumption is equal to the system's aggregated power consumption. The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected. When this value is exceeded, ports will be deactivated, according to user-defined priorities. The power budget is managed according to the following user-definable parameters: maximum available power, ports priority, maximum allowable power per port.

The Over Temperature Protection of the PoE Switch offers a safety and stable PoE operating by limit the output power according to detected temperature to prevent destructive breakdown due to un-expected overheating.

This section provides PoE (Power over Ethernet) Configuration and PoE output status of PoE Switch, screen in Figure 4-69 appears.

Figure 4-69: PoE Configuration

PoE Configuration

PoE PSU Status	On
PoE Temperature Unit 1	28C/35F
PoE Temperature Unit 2	30C/37.5F
Over Temperature Protection	Disable
Power Limit Mode	No Limit

Note :
 1. Total Limit mode : Port 1~24 up to 380W
 2. Priority Limit mode : Delieve power by priority
 3. No Limit mode : Disable power limit function

Power Allocation: 0% 0 W / 380 W

Port	PoE Function	Priority	Device Class	Current [mA]	Consumption [W]	Power Limit
1	Enable	Critical	--	0	0	15.4
2	Enable	Critical	--	0	0	15.4
3	Enable	Critical	--	0	0	15.4
4	Enable	Critical	--	0	0	15.4
5	Enable	Critical	--	0	0	15.4

This page includes the following fields:

OBJECT	DESCRIPTION
PoE PSU Status	PoE PSU Status shows status of power supply for PoE output.
PoE Temperature Unit 1	Display the current operating temperature of PoE chip unit 1. The unit 1 is in charge of PoE Port-1~Port-12
PoE Temperature Unit 2	Display the current operating temperature of PoE chip unit 2. The unit 1 is in charge of PoE Port-13~Port-24

OBJECT	DESCRIPTION
Over Temperature Protection	<p>Enable / Disable over temperature protection.</p> <p>When the PoE temperature unit 1 / unit2 over 70 degree C then PoE power budget will be changed by 3 segments as following.</p> <ul style="list-style-type: none"> Over 70 Degree C power budget 180 Watts Over 73 Degree C power budget 170 Watts Over 76 Degree C power budget 160 Watts
Power limit mode	<p>Allow to configure power limit mode of Web Smart Device. It can choose :</p> <ul style="list-style-type: none"> Port Priority Deliver PoE power by port priority setting Total Limit. Set limit value of the total POE port provided power to the PDs.
Power Allocation	Show the total watts usage of PoE Switch.
PoE Function	Can enable or disable the PoE function.
Priority	<p>Set port priority for the POE power management</p> <p>It can choose the "port priority", value is :</p> <ul style="list-style-type: none"> Critical High Low <p>High priority is "Critical".</p>
Device class	<p>Class 0 is the default for PDs. However, to improve power management at the PSE, the PD may opt to provide a signature for Class 1 to 3.</p> <p>The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes. A PD shall return Class 0 to 3 in accordance with the maximum power draw as specified by Table 4.1.</p>
Current(mA)	It shows the PoE device current Amp.
Consumption [W]	It shows the PoE device current watt.
Power Limit	<p>It can limit the port PoE supply watts.</p> <p>Per port maximum value must less 15.4, total ports values must less than the Power Reservation value.</p> <p>Once power overload detected, the port will auto shut down and keep on detection mode until PD's power consumption lower than the power limit value.</p>

NOTE: For GE-DS-242-PoE, the total PoE power reservation from Port-1~24 is up to 380W.

- PD Classifications

A PD may be classified by the PSE based on the classification information provided by the PD. The intent of PD classification is to provide information about the maximum power required by the PD during operation. Class 0 is the default for PDs. However, to improve power management at the PSE, the PD may opt to provide a signature for Class 1 to 3.

The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes.

A PD shall return Class 0 to 3 in accordance with the maximum power draw as specified by Table 4-3.

Table 4-13-1: Device class

Class	Usage	Range of maximum power used by the PD
0	Default	0.44 to 12.95 Watts
1	Optional	0.44 to 3.84 Watts
2	Optional	3.84 to 6.49 Watts
3	Optional	6.49 to 12.95 Watts
4	Not Allowed	Reserved for Future Use

NOTE: Class 4 is defined but is reserved for future use. A Class 4 signature cannot be provided by a compliant PD.

Chapter 5

Console Management

Login in the Console Interface

To configure the system via console mode, connect a serial cable to a COM port on a PC or notebook computer and to RJ-45 type serial (console) port of the Managed Switch. The console port of the Managed Switch is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

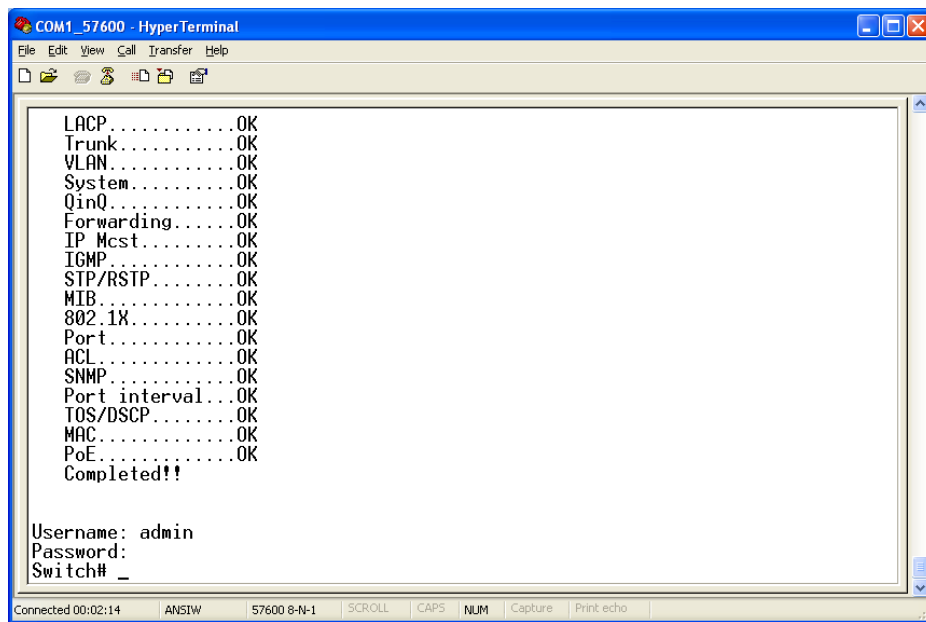
To get more information about how to connect to the console interface of GE-DS-242-PoE with HyperTerminal please refer to the GE-DS-242-PoE Installation Sheet.

Once the terminal has connected to the device, power on the GE-DS-242-PoE, the terminal will display that it is running testing procedures.

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

Username: **admin**

Password: **admin**

Figure 5-1: GE-DS-242-PoE Console Login screen

NOTE: For security reasons, please change and memorize the new username and password after this first setup.

Username Max: 6, Min: 1 characters.

Password Max: 6, Min: 1 characters.

Only enter commands in lowercase letters in console interface.

Configure IP address

The GE-DS-242-PoE Managed Switch is shipped with default IP address as follows.

IP Address : **192.168.0.100**

Subnet Mask : **255.255.255.0**

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

Show the current IP address

1. On "Switch# " prompt, enter "configure".
2. On "Switch(config)# " prompt, enter "show ip".
3. The screen displays the current IP address, Subnet Mask and Gateway. As show in Figure 5-2.

Figure 5-2: Show IP information screen

```

COM1_57600 - HyperTerminal
File Edit View Call Transfer Help

QinQ.....OK
Forwarding.....OK
IP Mcast.....OK
IGMP.....OK
STP/RSTP/MSTP...OK
MIB.....OK
802.1X.....OK
Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

Username: admin
Password:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# _

Connected 00:07:05  ANSIW  57600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo

```

Configure IP address

1. On "Switch(config)# " prompt, enter the following commands and press <Enter>. As show in Figure 5-3.

Switch(config)# ip address 192.168.1.100 255.255.255.0

Switch(config)# ip default-gateway 192.168.1.254

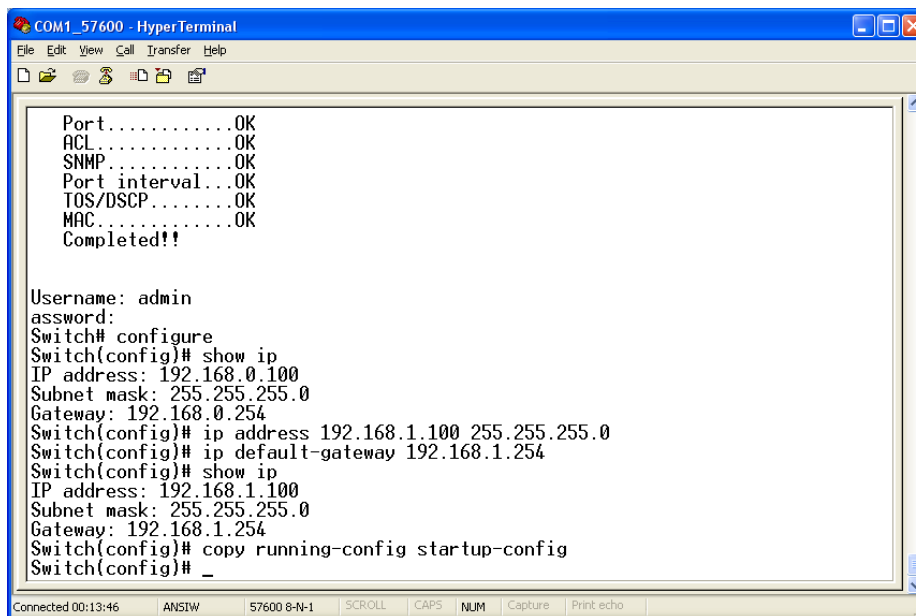
The previous commands would apply the follow settings for the Switch.

IP: 192.168.1.100

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

Figure 5-3: Set IP address screen



```
COM1_57600 - HyperTerminal
File Edit View Call Transfer Help
Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

Username: admin
assword:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# ip address 192.168.1.100 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
Switch(config)# show ip
IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Gateway: 192.168.1.254
Switch(config)# copy running-config startup-config
Switch(config)# _
```

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

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

NOTE: If you are not familiar with console command or the related parameter, enter "help" anytime in console to get the help description.

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

Commands Level

The following table lists the CLI commands and descriptions.

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	<p>The user commands available at the user level are a subset of those available at the privileged level.</p> <p>Use this mode to:</p> <ul style="list-style-type: none"> • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in User EXEC mode.	switch#	Enter disable to exit.	<p>The privileged command is the advanced mode.</p> <p>Use this mode to</p> <ul style="list-style-type: none"> • Display advanced function status • Save configuration
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	<p>Use this mode to configure those parameters that are going to be applied to your switch.</p>

Chapter 6

Command Line Interface

Operation Notice

To enter the "configuration" mode, you need to be in the privileged mode, and then types in the command **configure**:

```
Switch# configure
```

```
Switch (config) #
```

Command Line Editing

Key Function

<Ctrl>-B	; ← Moves the cursor back one character.
<Ctrl>-D	Deletes the character at the cursor.
<Ctrl>-E	Jumps to the end of the current command line.
<Ctrl>-F	; → Moves the cursor forward one character.
<Ctrl>-K	Deletes from the cursor to the end of the command line.
<Ctrl>-N	; ↓ Enters the next command line in the command history.
<Ctrl>-P	; ↑ Enters the previous command line in the command history.
<Ctrl>-U	Deletes from the cursor to the beginning of the command line.
<Ctrl>	-W Deletes the last word typed.
<Esc> B	Moves the cursor backward one word.
<Esc> D	Deletes from the cursor to the end of the word.
<Esc> F	Moves the cursor forward one word.
<Backspace>	Delete the character before the cursor.
	Delete the character at the cursor.

The following generic function keys provide functions in all of the menus:

Command Help

You may enter ? at any command mode, and the CLI will return possible commands at that point, along with some description of the command.

System Commands

Command	Description
show running-config	Display the running configuration of the switch.
copy running-config startup-config	Backup the switch configurations.
erase startup-config	Reset to default factory settings at next boot time.
clear arp	<ip-addr> specifies the IP address to be cleared. If no IP address is entered, the entire ARP cache is cleared.
show arp	Show the IP ARP translation table.
ping	Send ICMP ECHO_REQUEST to network hosts. Parameters: <1..999> specifies the number of repetitions. If not entered, it will continue to ping until you press <Ctrl>-C to stop.

Switch Static Configuration

Port Configuration and show status

port state

Description:

Turn the port state on or off.

Syntax:

port state <on | off> [<port-list>]

Parameters:

<port-list> specifies the ports to be turn on or off. If not entered, all ports are turn on or off.

port nego

Description:

Set port negotiation.

Syntax:

port nego <force | auto | nway-force> [<port-list>]

Parameters:

<port-list> specifies the ports to be set.If not entered, all ports are set.

port speed

Description:

Set port speed (in mbps) and duplex.

Syntax:

port speed <10 | 100 | 1000> <full | half> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port flow**Description:**

Enable or disable port flow control.

Syntax:

port flow <enable | disable> <enable | disable> [<port-list>]

Parameters:

The first <enable | disable> enables or disables flow control in full duplex mode.

The second <enable | disable> enables or disables flow control in half duplex mode.

<port-list> specifies the ports to be set. If not entered, all ports are set.

port rate**Description:**

Set port effective ingress or egress rate.

Syntax:

port rate <ingress | egress> <0..8000> [<port-list>]

Parameters:

<0..8000> specifies the ingress or egress rate.<0..8000>

<port-list> specifies the ports to be set. If not entered, all ports are set.

port priority**Description:**

Set port priority.

Syntax:

port priority <disable | low | high> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port jumboframe**Description:**

Set port jumbo frame. When port jumbo frame is enable, the port forward jumbo frame packet

Syntax:

port jumboframe <enable | disable> [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

show port status**Description:**

Show port status, including port State, Link, Trunking, VLAN, Negotiation, Speed, Duplex, Flow control, Rate control ,Priority, Security, BSF control.

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

```
-----
```

```
Port 1 Information
```

```
-----
```

```
State: on
```

```
Link: down
```

```
Trunking: none
```

```
VLAN: DEFAULT
```

```
Priority: disable
```

```
Security: off
```

```
-----
```

```
Port 2 Information
```

```
-----
```

```
State: on
```

```
Link: down
```

```
Trunking: none
```

```
VLAN: DEFAULT
```

```
Priority: disable
```

```
Security: off
```

```
-----
```

```
Port 3 Information
```

```
State: on
```

```
Link: down
```

```
--More--
```

show port statistics

Description:

Show port statistics, including TxGoodPkt, TxBadPkt, RxGoodPkt, RxBadPkt, TxAbort, Collision, and DropPkt.

Parameters:

<port-id> specifies the port to be shown.

```
Switch(config)# show port statistics
```

```
Port 1 Information
```

```
TxGoodPkt: 0
```

```
TxBadPkt: 0
```

```
RxGoodPkt: 0
```

```
RxBadPkt: 0
```

```
TxAbort: 0
```

```
Collision: 0
```

```
DropPkt: 0
```

```
Port 2 Information
```

```
TxGoodPkt: 0
```

```
TxBadPkt: 0
```

```
RxGoodPkt: 0
```

```
RxBadPkt: 0
```

```
TxAbort: 0
```

```
Collision: 0
```

```
DropPkt: 0
```

```
-----
```

```
Port 3 Information
```

```
-----
```

```
--More--
```

show port protection

Description:

Show protected port information.

```
Switch(config)# show port protection
```

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

Port	Protected	Group
1	off	1
2	off	1
3	off	1
4	off	1
5	off	1
6	off	1
7	off	1
8	off	1
9	off	1
10	off	1
11	off	1
12	off	1
13	off	1
14	off	1
15	off	1
16	off	1
17	off	1
18	off	1
19	off	1
20	off	1

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

21		off		1
22		off		1
25		off		1
26		off		1
Trk1		off		1

Trunk Configuration

Trunk allows the switch to combine ports so that they function like a single high-speed link. It can be used to increase the bandwidth to some devices to provide a high-speed link. For example, trunk is useful when making connections between switches or connecting servers to the switch. Trunk can also provide a redundant link for fault tolerance. If one link in the trunk failed, the switch can balance the traffic among the remaining links.

NOTE: The 10/100 Mbps port cannot be trunked with gigabit port (port 25~26). All ports in the same trunk group will be treated as a single port. If a trunk group exists, the ports belonging to that trunk will be replaced by "TRUNK #" in the VLAN configuration screen. The following example configures port 25~26 as "TRUNK 1."

Trunking Commands

show trunks

Description:

Show trunking information.

```
Switch(config)# show trunk
Group ID | LACP | Ports | LACP Active
-----+-----+-----+-----
1 | Yes | 23,24 | 23,24
```

trunk add

Description:

Add a new trunk group.

Syntax:

trunk add <trunk-id> <lacp | no-lacp> <port-list> <active-port-list>

Parameters:

<trunk-id> specifies the trunk group to be added.

Lacp

Description:

Specifies the added trunk group to be LACP enabled.

Syntax:

lacp

no-lacp specifies the added trunk group to be LACP disabled.

Parameters:

<port-list> specifies the ports to be set.

<active-port-list> specifies the ports to be set to LACP active.

no trunk

Description:

Delete an existing trunk group.

Syntax:

no trunk *<trunk-id>*

Parameters:

<trunk-id> specifies the trunk group to be deleted

LACP Commands

[no] lacp

Description:

Enable/disable LACP.

lacp system-priority

Description:

Set LACP system priority.

Syntax:

lacp system-priority *<1..65535>*

Parameters:

<1..65535> specifies the LACP system priority.

no lacp system-priority**Description:**

Set LACP system priority to the default value 32768.

show lacp status**Description:**

Show LACP enable/disable status and system priority.

show lacp**Description:**

Show LACP information.

```
Switch(config)# show lacp status  
LACP is enabled.  
LACP system priority: 32768
```

show lacp agg**Description:**

Show LACP aggregator information.

Syntax:

show lacp agg <trunk-id>

Parameters:

<trunk-id> specifies the trunk group to be shown.

show lacp port**Description:**

Show LACP information by port.

Syntax:

show lacp port <port-id>

Parameters:

<port-id> specifies the port to be shown.

NOTE: If VLAN group exists, all of the members of static trunk group must be in same VLAN group.

VLAN Configuration

Virtual LANs

A Virtual LAN (VLAN) is a logical network group that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN within a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically. A station can belong to more than one VLAN group. VLAN prevents users from accessing network resources of another on the same LAN, thus the users can not see the hard disks and printers of another user in the same building. VLAN can also increase the network performance by reducing the broadcast traffic and enhance the security of the network by isolating groups.

The GE-DS-242-PoE supports two types of VLANs:

- Port-based
- IEEE 802.1Q (tag) -based

Only one of the two VLAN types can be enabled at one time.

Port-based VLANs are VLANs where the packet forwarding decision is made based on the destination MAC address and its associated port. You must define the outgoing ports allowed for each port when you use port-based VLANs. In port-based VLANs, the packets received from one port can only be sent to the ports which are configured to the same VLAN. As shown in the following figure, the switch administrator configured port 1~2 as VLAN 1 and port 3~4 as VLAN 2. The packets received from port 1 can only be forwarded to port 2. The packets received from port 2 can only be forwarded to port 1. That means the computer A can send packets to computer B, and vice versa. The same situation also occurred in VLAN 2. The computer C and D can communicate with each other. However, the computers in VLAN 1 can not see the computers in VLAN 2 since they belonged to different VLANs.

IEEE 802.1Q (tag) -based VLANs enable the Ethernet functionality to propagate tagged packets across the bridges and provides a uniform way for creating VLAN within a network then span across the network. For egress packet, you can choose to tag it or not with the associated VLAN ID of this port. For ingress packet, you can forward this packet to a specific port as long as it is also in the same VLAN group.

The 802.1Q VLAN works by using a tag added to the Ethernet packets. The tag contains a VLAN Identifier (VID) which belongs to a specific VLAN group. And ports can belong to more than one VLAN.

The difference between a port-based VLAN and a tag-based VLAN is that the tag-based VLAN truly divided the network into several logically connected LANs. Packets rambling around the switches can be forwarded more intelligently. In the figure shown below, by identifying the tag, broadcast packets coming from computer A in VLAN1 at sw1 can be forwarded directly to VLAN1.

However, the switch could not be so smart in the port-based VLAN mechanism. Broadcast packets will also be forwarded to port 4 of sw2. It means the port-based VLAN can not operate a logical VLAN group among switches.

The GE-DS-242-PoE supports both Port-based VLAN and Tag-based (802.1Q) VLAN modes. The default configuration is tag-based (802.1Q) VLAN. In the 802.1Q VLAN, initially, all ports on the switch belong to default VLAN, VID is 1.

NOTE: You cannot delete the default VLAN group in 802.1Q VLAN mode.

VLAN Mode: Port-based

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode (disabled|port-based|dot1q)

Parameters:

(disabled | port-based | dot1q) specifies the VLAN mode.

NOTE: Change the VLAN mode for every time, user have to restart the switch for valid value.

Advanced 802.1Q VLAN Configuration

Ingress filters configuration

When a packet was received on a port, you can govern the switch to drop it or not if it is an untagged packet. Furthermore, if the received packet is tagged but not belonging to the same VALN group of the receiving port, you can also control the switch to forward or drop the packet. The example below configures the switch to drop the packets not belonging to the same VLAN group and forward the packets not containing VLAN tags.

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode (disabled|port-based|dot1q)

Parameters:

(disabled | port-based | dot1q) specifies the VLAN mode.

NOTE: Change the VLAN mode for every time, user have to restart the switch for valid value.

vlan mode

Description:

Add or edit VLAN entry.

Syntax:

vlan add <1-4094> NAME (cpu-port|no-cpu-port) LIST [LIST]

Parameters:

<1-4094> specifies the VLAN id or Group id (if port based VLAN mode)

NAME specifies the VLAN group name.

(cpu-port|no-cpu-port) specifies the CPU port belong this VLAN group.

LIST specifies the ports to be set to VLAN members.

[LIST] specifies the ports to be set to tagged members. If not entered, all members set to untagged.

```
e.g.. switch(config)# vlan add 1 vlan1 cpu-port 1-4
```

This VLAN entry has four members (from port1 to port4) and all members are untagged.

no vlan

Description:

Delete VLAN entry.

Syntax:

no vlan <1-4094>

Parameters:

<1-4094> specifies the VLAN id or group id (if port based VLAN).

e.g. no vlan 1

show vlan

Description:

Show VLAN entry information.

Syntax:

show vlan [<1-4094>]

Parameters:

<1-4094> specifies the VLAN id, null means all valid entries.

e.g.

```
Switch(config)# show vlan 1
```

```
VLAN      : 1
```

```
Type      : Static
```

```
Creation Time (sec.): 43
```

```
CPU Port   : Yes
```

```
Port | Member
```

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

```
Port1 | Untagged
```

```
Port2 | Untagged
```

```
Port3 | Untagged
```

```
Port4 | Untagged
```

```
Port5 | Untagged
```

```
Port6 | Untagged
```

```
Port7 | Untagged
```

```
Port8 | Untagged
```

```
Port9 | Untagged
```

```
Port10 | Untagged
```

```
Port11 | Untagged
```

```
Port12 | Untagged
```

```
Port13 | Untagged
```

```
Port14 | Untagged
```

```
Port15 | Untagged
```

```
Port16 | Untagged
```

```
--More--
```

```
Port17 | Untagged
```

```
Port18 | Untagged
```

```
Port19 | Untagged
```

```
Port20 | Untagged
```

```
Port21 | Untagged
```

```
Port22 | Untagged
```

```
Port25 | Untagged
```

```
Port26 | Untagged
```

```
Trk1 | Untagged
```


show vlan static**Description:**

Show static VLAN entry information.

show vlan pvid**Description:**

Show port default VLAN id.

Syntax:

show vlan pvid [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all port's PVID will be showed.

e.g.

```
Switch(config)# show vlan pvid
```

```
Port | PVID
```

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

```
Port1 | 1
```

```
Port2 | 1
```

```
Port3 | 1
```

```
Port4 | 1
```

```
Port5 | 1
```

```
Port6 | 1
```

```
Port7 | 1
```

```
Port8 | 1
```

```
Port9 | 1
```

```
Port10 | 1
```

```
Port11 | 1
```

```
Port12 | 1
```

```
Port13 | 1
```

```
Port14 | 1
```

```
Port15 | 1
```

```
Port16 | 1
```

```
Port17 | 1
```

```
Port18 | 1
```

```
Port19 | 1
```

```
Port20 | 1
```

```
Port21 | 1
```

```
--More--
```

```
Port22 | 1
```

```
Port25 | 1
```

```
Port26 | 1
```

```
Trk1 | 1
```

vlan filter**Description:**

Set ingress filter rules.

Syntax:

vlan filter (enable | disable) (enable | disable) LIST

Parameters:

(enable | disable) specifies the non-members packet will be forwarded or not. If set enable, forward only packets with VID matching this port's configured VID.

(enable | disable) specifies the untagged frame will be dropped or not. If set enable, drop untagged frame.

show vlan filter**Description:**

Show VLAN filter setting.

Syntax:

show vlan filter [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all ports' filter rules will be shown.

```
Switch(config)# show vlan filter
```

```
Port | Rule 1 | Rule 2
```

```
Filter (nonmbr) (untag)
```

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

```
Port1 | Drop | Forward
```

```
Port2 | Drop | Forward
```

```
Port3 | Drop | Forward
```

```
Port4 | Drop | Forward
```

```
Port5 | Drop | Forward
```

```
Port6 | Drop | Forward
```

```
Port7 | Drop | Forward
```

```
Port8 | Drop | Forward
```

```
Port9 | Drop | Forward
```

```
Port10 | Drop | Forward
```

```
Port11 | Drop | Forward
```

```
Port12 | Drop | Forward
```

```
Port13 | Drop | Forward
```

```
Port14 | Drop | Forward
```

```
Port15 | Drop | Forward
```

```
Port16 | Drop | Forward
```

```
Port17 | Drop | Forward
```

```
Port18 | Drop | Forward
```

```
Port19 | Drop | Forward
```

```
Port20 | Drop | Forward
```

```
--More--
```

```
Port21 | Drop | Forward
```

```
Port22 | Drop | Forward
```

```
Port25 | Drop | Forward
```

```
Port26 | Drop | Forward
```

```
Trk1 | Drop | Forward
```

Misc Configuration

no mac-age-time

Description:

Set MAC address age-out time.

Syntax:

[no] mac-age-time Enable or disable MAC address age-out.

mac-age-time <6..1572858>

Parameters:

<6..1572858> specifies the MAC address age-out time. Must be divisible by 6. Type the number of seconds that an inactive MAC address remains in the switch's address table.

show mac-age-time

Description:

Show MAC address age-out time.

broadcast

Description:

Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/16

Syntax:

broadcast mode <off | 1/2 | 1/4 | 1/8 | 1/16 | >

broadcast select

Description:

Select the Broadcast storm filter packet type:

Unicast/Multicast: Flood unicast/multicast filter

Control Packets: Control packets filter

IP multicast: IP multicast packets filter

Broadcast Packets: Broadcast Packets filter

Syntax:

broadcast select <unicast/multicast | control packet | ip multicast | broadcast >

Collision-Retry

Description:

Collision-Retry setting

Syntax:

Collision-Retry < off | 16 | 32 | 48 >

Parameters:

16\32\48 – In Half-Duplex, collision-retry maximum is 16\32\48 times and packet will be dropped if collisions still happen

Disable – In Half-Duplex, if collision occurs, will retry forever (Default).

Administration Configuration

Change Username / Password

hostname

Description:

Set switch name.

Syntax:

hostname <name-str>

Parameters:

<name-str> specifies the switch name. If you would like to have spaces within the name, use quotes ("") around the name.

no hostname

Reset the switch name to factory default setting.

[no] password

Description:

Set or remove username and password for manager or operator.

Syntax:

[no] password <manager | operator | all>

Parameters:

The manager username and password is also used by the web UI.

IP Configuration

User can configure the IP setting and fill in a new value.

ip address

Description:

Set IP address and subnet mask.

Syntax:

ip address *<ip-addr> <ip-mask>*

ip default-gateway

Description:

Set the default gateway IP address.

Syntax:

ip default-gateway *<ip-addr>*

show ip

Description:

Show IP address, subnet mask, and the default gateway.

show info

Description:

Shows basic information, including system info, MAC address, and versions.

```
Switch(config)# show info
Model name: GE-DS-242-PoE
Description: 24-Port 10/100Mbps + 2G TP/SFP Combo Managed Switch
MAC address: 00:30:4F:44:55:66
Firmware version: 2.08
CLI version: 1.07
802.1x: disabled
IGMP: enabled
LACP: enabled
```


dhcp**Description:**

Set switch as dhcp client, it can get ip from dhcp server.

NOTE: If you set this command, the switch will reboot.

show dhcp**Description:**

Show dhcp enable/disable.

Reboot switch

boot**Description:**

Reboot (warm-start) the switch.

Reset to Default

erase startup-config**Description:**

Reset configurations to default factory settings at next boot time.

TFTP Update Firmware

copy tftp firmware

Description:

Download firmware from TFTP server.

Syntax:

copy tftp firmware *<ip-addr>* *<remote-file>*

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

Restore Configure File

copy tftp <running – config | flash>

Description:

Retrieve configuration from the TFTP server. If the remote file is the text file of CLI commands, use the keyword running-config.

If the remote file is the configuration flash image of the switch instead, use the keyword flash.

Syntax:

copy tftp <running-config | flash> *<ip-addr>* *<remote-file>*

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

Backup Configure File

copy <running – config | flash> tftp

Description:

Send configuration to the TFTP server. If you want to save the configuration in a text file of CLI commands, use the keyword `running-config`. If you want to save the configuration flash image instead, use the keyword `flash`.

Syntax:

copy <running-config | flash> tftp <ip-addr> <remote-file>

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

MAC limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an “opening” is available, the switch stores the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

User can configure the MAC limit setting and fill in the new value.

mac-limit

Description:

Enable MAC limit.

no mac-limit

Description:

Disable MAC limit.

Mac-limit

Description:

Set port MAC limit value, 0 to turn off MAC limit of port.

Syntax:

Mac-limit <port-list> <1-64>

show mac-limit

Description:

Show MAC limit information, including MAC limit enable/disable, per-port MAC limit setting.

Port Mirroring Configuration

Port monitoring is a feature to redirect the traffic occurred on every port to a designated monitoring port on the switch. With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In the Managed Switch, you can specify one port to be the monitored ports and any single port to be the monitoring port. You also can specify the direction of the traffic that you want to monitor. After properly configured, packets with the specified direction from the monitored ports are forwarded to the monitoring port.

NOTE: The default Port Monitoring setting is disabled.

mirror-port

Description:

Set port monitoring information. (RX only|TX only|both RX and TX)

Syntax:

mirror-port <rx | tx | both> <port-id> <port-list>

Parameters:

rx specifies monitoring rx only.

tx specifies monitoring tx only.

both specifies monitoring both rx and tx.

<port-id> specifies the analysis port ID. This port receives traffic from all monitored ports.

<port-list> specifies the monitored port list.

show mirror-port

Description:

Show port monitoring information.

Quality of Service

There are four transmission queues with different priorities in the Managed Switch: Highest, SecHigh, SecLow and Lowest. The Managed Switch will take packets from the four queues according to its QoS mode setting. If the QoS mode was set to "Disable", the Managed Switch will not perform QoS on its switched network. If the QoS mode was set to "High Empty Then Low", the Managed Switch will never exhaust packets from a queue until the queues with higher priorities are empty. If the QoS mode was set to "weight ratio", the Managed Switch will exhaust packets from the queues according to the ratio. The default value of QoS mode is "weight 8:4:2:1." That means the switch will first exhaust 8 packets from the queue with highest priority, and then exhaust 4 packets from the queue with second high priority, and so on.

When the switch received a packet, the switch has to decide which queue to put the received packet into. In the Managed Switch, it will put received packets into queues according to the settings of "802.1p Priority" and "Static Port Ingress Priority." When the received packet is an 802.1p tagged packet, the switch will put the packet into a queue according to the 802.1p Priority setting.

Otherwise, the switch will put the packet into a queue according the setting of Static Port Ingress Priority.

- **802.1p Priority:** the 802.1p packet has a priority tag in its packet header. The range of the priority is 7~0. The Managed Switch can specify the mapping between 802.1p priority and the four transmission queues. In the default setting, the packets with 802.1p priority 0~1 are put into the queue with lowest priority, the packets with 802.1p priority 2~3 are put into queue with second low priority, and so on.
- **Static Port Ingress Priority:** each port is assigned with one priority 7~0. The priority of the packet received from one port is set to the same priority of the receiving port. When the priority of the received packet was determined, the packet is treated as an 802.1p packet with that priority and will be put into a queue according to the 802.1p Priority setting.

QoS Configuration

QoS mode:

- **First Come First Service:** The sequence of packets sent is depending on arrive orders.
- **All High before Low:** The high priority packets sent before low priority packets.
- **WRR: Weighted Round Robin.** Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher

priority packets sent before one lower priority packet is sent. For example, 8 Highest:4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.

- QoS level: 0~7 priority level can map to highest, second-high, second-low, lowest queue.

qos priority

Description:

Set 802.1p priority.

Syntax:

qos priority <first-come-first-service | all-high-before-low | weighted-round-robin>

Parameters:

[<highest-weight>][<sechighweight>][<sec low -weight>] [<lowest-weight>]

e.g. qos priority weighted-round-robin 8,4,2,1.

qos level

Description:

Set priority levels to highest, second-high, second-low and lowest.

Syntax:

qos level < highest | second-high | second-low | lowest > <level-list>

Parameters:

<level-list> specifies the priority levels to be high or low.

Level must be

between 1 and 7.

e.g. qos level highest 7

e.g. qos level lowest 4

show qos**Description:**

Show QoS configurations, including 802.1p priority, priority level.

e.g.

```
Switch(config)# show qos
QoS configurations:
QoS mode: weighted round robin
Highest weight: 8
Second High weight: 4
Second Low weight: 2
Lowest weight: 1
802.1p priority[0-7]:
Lowest  Lowest  SecLow  SecLow  SecHigh  SecHigh  Highest  Highest
```

Per Port Priority

port priority**Description:**

Set port priority.

Syntax:

port priority <disable | [0-7]> [*<port-list>*]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

e.g. port priority disable 1-5

MAC Address Configuration

clear mac-address-table

Description:

Clear all dynamic MAC address table entries.

mac-address-table static

Description:

Set static unicast or multicast MAC address. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

mac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

no mac-address-table static mac-addr

Description:

Delete static unicast or multicast MAC address table entries.

Syntax:

no mac-address-table static mac-addr <vlan-id>

show mac-address-table

Description:

Display MAC address table entries.

```
Switch(config)# show mac-address-table
```

MAC Address	VLAN	Type	Source
00:08:B6:00:06:90	1	Dynamic	25
00:40:63:00:65:30	1	Dynamic	Trk1
00:03:63:F7:80:7F	1	Dynamic	25

show mac-address-table static**Description:**

Display static MAC address table entries.

show mac-address-table multicast**Description:**

Display multicast-related MAC address table.

smac-address-table static**Description:**

Set static unicast or multicast MAC address in secondary MAC address table. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

smac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

show smac-address-table**Description:**

Display secondary MAC address table entries.

show smac-address-table multicast**Description:**

Display multicast-related secondary MAC address table.

[no] filter**Description:**

Set MAC address filter. The packets will be filtered if both of the destination MAC address and the VLAN tag matches the filter entry. If the packet does not have a VLAN tag, then it matches an entry with VLAN ID 1.

Syntax:

[no] filter <mac-addr> <vlan-id>

show filter**Description:**

Display filter MAC address table.

STP/RSTP Commands

[no] spanning-tree

Description:

Enable or disable spanning-tree.

spanning-tree forward-delay

Description:

Set spanning tree forward delay used, in seconds.

Syntax:

spanning-tree forward-delay <4-30>

Parameters:

<4-30> specifies the forward delay, in seconds. Default value is 15.

NOTE: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$.

spanning-tree hello-time

Description:

Set spanning tree hello time, in seconds.

Syntax:

spanning-tree hello-time <1-10>

Parameters:

<1-10> specifies the hello time, in seconds. Default value is 2.

NOTE: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$.

spanning-tree maximum-age**Description:**

Set spanning tree maximum age, in seconds.

Syntax:

spanning-tree maximum-age <6-40>

Parameters:

<6-40> specifies the maximum age, in seconds. Default value is 20.

NOTE: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$.

spanning-tree priority**Description:**

Set spanning tree bridge priority.

Syntax:

spanning-tree priority <0-61440>

Parameters:

<0-61440> specifies the bridge priority. The value must be in steps of 4096.

spanning-tree port path-cost**Description:**

Set spanning tree port path cost.

Syntax:

spanning-tree port path-cost <1-200000000> [<port-list>]

Parameters:

<1-200000000> specifies port path cost.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree port priority

Description:

Set spanning tree port priority.

Syntax:

spanning-tree port priority <0-240> [<port-list>]

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

<port-list> specifies the ports to be set. Null means all ports.

show spanning-tree

Description:

Show spanning-tree information.

show spanning-tree port

Description:

Show spanning tree per port information.

Syntax:

show spanning-tree port [<port-list>]

Parameters:

<port-list> specifies the port to be shown. Null means all ports.

The remaining commands in this section are only for system with RSTP (rapid spanning tree, 802.1w) capability:

spanning-tree debug

Description:

Enable or disable spanning tree debugging information.

spanning-tree protocol version**Description:**

Change spanning tree protocol version.

Syntax:

spanning-tree protocol-version <stp | rstp>

Parameters:

stp specifies the original spanning tree protocol (STP,802.1d).

rstp specifies rapid spanning tree protocol (RSTP,802.1w).

[no] spanning-tree port mcheck**Description:**

Force the port to transmit RST BPDUs.

No format means not force the port to transmit RST BPDUs.

Syntax:

[no] spanning-tree port mcheck [<port-list>]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port**Description:**

Set the port to be edge connection. No format means set the port to be non-edge connection.

Syntax:

[no] spanning-tree port edge-port [<port-list>]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp

Description:

Disable or enable spanning tree protocol on this port.

Syntax:

[no] spanning-tree port non-stp [<port-list>]

Parameters:

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree point-to-point mac

Description:

Set the port to be point to point connection.

Syntax:

spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]

Parameters:

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

<port-list> specifies the ports to be set. Null means all ports.

show spanning-tree

Description:

Show spanning-tree information of CIST.

show spanning-tree port

Description:

Show spanning tree port information of CIST.

Syntax:

show spanning-tree port [<port-list>]

Parameters:

<port-list> specifies the port to be shown. Null means all ports.

SNMP

Any Network Management running the simple Network Management Protocol (SNMP) can be management with the switch.

System Options

Snmp /no snmp

Description:

Enable or disable SNMP.

Show snmp status

Description:

Show the enable or disable status of SNMP.

Snmp system-name

Description:

Set agent system name string.

Syntax:

snmp system-name <name-str>

Parameters:

<name-str> specifies the system name string.

e.g. snmp system-name SWITCH

Snmp system-location

Description:

Set agent location string.

Syntax:

snmp system-location <location-str>

Parameters:

<location-str> specifies the location string.

e.g. snmp system-location office

Snmp system-contact

Description:

Set agent system contact string.

Syntax:

snmp system-contact <contact-str>

Parameters:

<contact-str> specifies the contact string.

e.g. snmp system-contact abc@sina.com

show snmp system

Description:

Show SNMP system information.

Community Strings

snmp community

Description:

Set SNMP community string.

Syntax:

snmp community <read-sysinfo-only | read-all-only | read-write-all><community-str>

Parameters:

<community-str> specifies the community string.

e.g. snmp community read-all-only public

no snmp community

Description:

Delete SNMP community string.

Syntax:

no snmp community <community-str>

Parameters:

<community-str> specifies the community string.

e.g. no snmp community public

show snmp community

Description:

Show SNMP community strings.

Trap Managers

snmp trap

Description:

Set SNMP trap receiver IP address, community string, and port number.

Syntax:

snmp trap <ip-addr> [<community-str>] [<1..65535>]

Parameters:

<ip-addr> specifies the IP address.

<community-str> specifies the community string.

<1..65535> specifies the trap receiver port number.

e.g. snmp trap 192.168.200.1 public

no snmp trap

Description:

Remove trap receiver IP address and port number.

Syntax:

no snmp trap <ip-addr> [<1..65535>]

Parameters:

<ip-addr> specifies the IP address.

<1..65535> specifies the trap receiver port number.

e.g. no snmp trap 192.168.200.1

show snmp trap

Description:

Show all trap receivers.

IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.

igmp

Description:

Enable/disable IGMP snooping.

Syntax:

[no] igmp

igmp fastleave

Description:

Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report, else wait one sec.

Syntax:

[no] igmp fastleave

igmp querier

Description:

Enable/disable IGMP snooping querier.

Syntax:

[no] igmp querier

igmp crossVLAN

Description:

Enable/disable IGMP snooping CrossVLAN

Syntax:

[no] igmp CrossVLAN

igmp debug

Description:

Enable/disable IGMP snooping debugging output.

Syntax:

[no] igmp debug

show igmp

Description:

Show IGMP snooping information.

Syntax:

show igmp <status | router | groups | table>

Parameters:

status specifies IGMP snooping status and statistics information.

router specifies IGMP snooping router's IP address.

groups specifies IGMP snooping multicast group list.

table specifies IGMP snooping IP multicast table entries.

igmp clear_statistics

Description:

Clear IGMP snooping statistics counters.

802.1x Protocol

dot1x

Description:

Enable or disable 802.1x.

Syntax:

[no] dot1x

radius-server host

Description:

Set radius server IP, port number, and accounting port number.

Syntax:

radius-server host <ip-addr> <1024..65535> <1024..65535>

Parameters:

<ip-addr> specifies server's IP address.

The first <1024..65535> specifies the server port number.

The second <1024..65535> specifies the accounting port number.

radius-server key

Description:

Set 802.1x shared key.

Syntax:

radius-server key <key-str>

Parameters:

<key-str> specifies shared key string.

radius-server nas

Description:

Set 802.1x NAS identifier.

Syntax:

radius-server nas <id-str>

Parameters:

<id-str> specifies NAS identifier string.

show radius-server

Description:

Show radius server information, including radius server IP, port number, accounting port number, shared key, NAS identifier,

dot1x timeout quiet-period

Description:

Set 802.1x quiet period. (default: 60 seconds)

Syntax:

dot1x timeout quiet-period <0..65535>

Parameters:

<0..65535> specifies the quiet period, in seconds.

dot1x timeout tx-period

Description:

Set 802.1x Tx period. (default: 15 seconds).

Syntax:

dot1x timeout tx-period <0..65535>

Parameters:

<0..65535> specifies the Tx period, in seconds.

dot1x timeout supplicant**Description:**

Set 802.1x supplicant timeout (default: 30 seconds)

Syntax:

dot1x timeout supplicant <1..300>

Parameters:

<1..300> specifies the supplicant timeout, in seconds.

dot1x timeout radius-server**Description:**

Set radius server timeout (default: 30 seconds).

Syntax:

dot1x timeout radius-server <1..300>

Parameters:

<1..300> specifies the radius server timeout, in seconds.

dot1x max-req**Description:**

Set 802.1x maximum request retries (default: 2 times).

Syntax:

dot1x max-req <1..10>

Parameters:

<1..10> specifies the maximum request retries.

dot1x timeout re-authperiod**Description:**

Set 802.1x re-auth period (default: 3600 seconds).

Syntax:

dot1x timeout re-authperiod <30..65535>

Parameters:

<30..65535> specifies the re-auth period, in seconds.

show dot1x

Description:

Show 802.1x information, quiet period, Tx period, supplicant timeout, server timeout, maximum requests, and re-auth period.

dot1x port

Description:

Set 802.1x per port information.

Syntax:

dot1x port <fu | fa | au | no> <port-list>

Parameters:

fu specifies forced unauthorized.

fa specifies forced authorized.

au specifies authorization.

no specifies disable authorization.

<port-list> specifies the ports to be set.

show dot1x port

Description:

Show 802.1x per port information.

Access Control List

Packets can be forwarded or dropped by ACL rules include Ipv4 or non-Ipv4. The Managed Switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

Ipv4 ACL commands

no acl

Description:

Delete ACL group.

Syntax:

no acl <1-220>

Parameters:

<1-220> specifies the group id.

e.g. no acl 1

no acl count

Description:

Reset the ACL group count.

Syntax:

no acl count <GroupId>

Parameters:

GroupId: <1-220> specifies the group id.

show acl

Description:

Show ACL group information.

Syntax:

show acl [<1-220>]

Parameters:

<1-220> specifies the group id, null means all valid groups.

e.g.

Switch(config)# show acl 1

Group Id : 1

```
Switch(config)# show acl 1
```

```
Group Id : 1
```

```
-----
```

```
Action : Permit
```

```
Rules:
```

```
Vlan ID : Any
```

```
IP Fragment : Uncheck
```

```
Src IP Address : Any
```

```
Dst IP Address : Any
```

```
L4 Protocol : Any
```

```
Port ID : Any
```

```
Hit Octet Count : 165074
```

```
Hit Packet count : 472
```

acl (add|edit) <1-220> (permit|deny) <0-4094> ipv4 <0-255>

Description:

Add or edit ACL group for Ipv4.

Syntax:

**acl (add|edit) <1-220> (permit|deny) <0-4094> ipv4 <0-255> A.B.C.D A.B.C.D
A.B.C.D A.B.C.D (check|unCheck) <0-65535> <0-26>**

Parameters:

(add|edit) specifies the operation.

<1-220> specifies the group id.

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN id. 0 means don't care.

<0-255> specifies the IP protocol. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

A.B.C.D specifies the Destination IP Address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

(check|unCheck) specifies the IP Fragment. check: Check IP fragment field; unCheck: Not check IP fragment field.

<0-65535> specifies the Destination port number if TCP or UDP. 0 means don't care.

<0-26> specifies the Port id. 0 means don't care.

e.g.

```
Switch(config)# acl add 1 deny 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0.0 0.0.0.0 unCheck 0 0
```

This ACL rule will drop all packet from IP is 192.168.1.1 with VLAN id=1 and IPv4.

acl (add|edit) <1-220> (qosvoip) <0-4094>**Description:**

Add or edit ACL group for Ipv4.

Syntax:

acl (add|edit) <1-220> (qosvoip) <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF> <0-FFFF>

Parameters:

(add|edit) specifies the operation.

<1-220> specifies the group id.

(qosvoip) specifies the action, do qos voip packet adjustment.

<0-4094> specifies the VLAN id. 0 means don't care.

<0-1F> specifies the port ID value.

<0-1F> specifies the port ID mask.

<0-FF> specifies the protocol value.

<0-FF> specifies the protocol mask.

<0-FFFF> specifies the source port value.

<0-FFFF> specifies the source port mask.

<0-FFFF> specifies the destination port value.

<0-FFFF> specifies the destination mask.

e.g. acl add 1 qosvoip 1 7 1 1 0 0 0 0 0

Non-Ipv4 ACL commands

no acl <1-220> and **show acl [<1-220>]** commands are same as Ipv4 ACL commands.

```
acl (add|edit) <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>
```

Description:

Add or edit ACL group for non-Ipv4.

Syntax:

```
acl (add|edit) <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>
```

Parameters:

(add|edit) specifies the operation.

<1-220> specifies the group id.

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN id. 0 means don't care.

<0-65535> specifies the Ether Type. 0 means don't care.

e.g. acl add 1 deny 0 nonipv4 2054. This ACL rule will drop all packets for either type is 0x0806 and non-IPv4.

Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN id and port id to bind, and device can cross switch if all conditions match.

SIP/SMAC binding commands

bind

Description:

Enable binding function.

no bind

Description:

Disable binding function.

no bind

Description:

Delete Binding group.

Syntax:

no bind <1-220>

Parameters:

<1-220> specifies the group id.

e.g. no bind 1

show bind**Description:**

Show Binding group information.

Syntax:

show bind [<1-220>]

Parameters:

<1-220> specifies the group id, null means all valid groups.

e.g. show bind 1

bind add**Description:**

Add Binding group.

Syntax:

bind add <1-220> A:B:C:D:E:F <0-4094> A.B.C.D <1-26>

Parameters:

<1-220> specifies the group id.

A.B.C.D specifies the MAC address.

<0-4094> specifies the VLAN id. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the IP Address.

<1-26> specifies the Port id.

e.g.

```
Switch(config)# bind add 1 00:11:22:33:44:55 0 192.168.1.1 1
```

This Binding rule will permit all packet cross switch from device's IP is 192.168.1.1 and MAC is 00:11:22:33:44:55 and this device connect to switch port id=1.

Power over Ethernet Commands

show poe	Show System Power over Ethernet information
show poe status	Show PoE port information
poe temperature-protection	Enabling or disabling the PoE power supply over temperature protection
poe limit-mode	Configure System PoE power limit mode information
poe enable	Enabling or disabling the port POE injects function
poe priority	Set port priority for the power supply management
poe maximum-power	Enabling or disabling per port power output limit

Display System PoE status

show poe

Description:

Show System Power over Ethernet information

Command Level

Global Configuration

Example:

```
Switch(config)# show poe

Maximum Available Power      :190Watts
System Operation Status      : on
PoE Power Consumption        : 55 watts
Usage Threshold              : 21%
PoE Power limit mode         : Port Priority
```

show poe status**Description:**

Show per PoE port information

Command Level

Global Configuration

Syntax:

show poe status [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

Example 1:

Switch(config)# show poe status 1							
Port	Admin	Oper	Priority	Power Limit[W]	Current Consumption [W]	Current[mA]	Device Class
Port1	Enable	on	Low	15.4	13.4	279	0

Example 2:

Switch(config)# show poe status							
Port	Admin	Oper	Priority	Power Limit[W]	Current Consumption [W]	Current[mA]	Device Class
Port1	Enable	on	Low	15.4	13.4	279	0
Port2	Enable	on	Low	15.4	11.3	236	0
Port3	Enable	on	Low	15.4	6.5	135	3
Port4	Enable	off	Low	15.4	0	0	0
Port5	Enable	off	Low	15.4	0	0	0
Port6	Enable	off	Low	15.4	0	0	0
Port7	Enable	off	Low	15.4	0	0	0
Port8	Enable	off	Low	15.4	0	0	0
Port9	Enable	off	Low	15.4	0	0	0
Port10	Enable	off	Low	15.4	0	0	0

Configure PoE Over Temperature Protection

poe temperature-protection enable[x4]

Description:

Configure PoE over temperature protection to enable or disable

Command Level

Global Configuration

Syntax:

poe temperature-protection { enable / disable }

Parameters:

<Enable > Enable PoE power budget change automatically by detected PoE unit temperature

<Disable > Disable PoE power budget change automatically

NOTE: PoE temperature-protection working in Priority mode or Total Limit mode only.

Configure PoE - System

poe limit-mode

Description:

Configure System PoE power limit mode information

Command Level

Global Configuration

Syntax:

poe limit-mode { Port-Priority / Total-Limit }

[no] poe limit-mode

Parameters:

<Port Priority> Deliver PoE power by port priority setting

<Total Limit> Set limit value of the total POE port provided power to the PDs.

NOTE: "no poe limit-mode" = No Limit.

Example:

```
Switch(config)# poe limit-mode port-priority
```

```
Switch (config)# show poe
```

Maximum Available Power	:190Watts
System Operation Status	: on
PoE Power Consumption	: 55 watts
Usage Threshold	: 21%
PoE Power limit mode	: Port Priority

```
Switch (config)# no poe limit-mode
```

```
Switch (config)# show poe
```

Maximum Available Power	:190Watts
System Operation Status	: on
PoE Power Consumption	: 55 watts
Usage Threshold	: 21%
PoE Power limit mode	: No Limit

Configure PoE -- Port

poe enable

Description:

Enabling or disabling the port POE injects function.

Command Level:

Global Configuration

Syntax:

poe enable [<port-list>]

[no] poe enable [<port-list>]

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

Example:

```
Switch(config)# poe enable 1
```

```
Switch(config)# show poe status 1
```

Port	Admin	Oper	Priority	Power Limit[W]	Current Consumption [W]	Current[mA]	Device Class
Port1	Enable	on	High	15.4	13.4	279	0

```
Switch(config)# no poe enable 1
```

```
Switch(config)# show poe status 1
```

Port	Admin	Oper	Priority	Power Limit[W]	Current Consumption [W]	Current[mA]	Device Class
Port1	Disable	off	High	15.4	--	--	0

poe priority**Description:**

Set port priority for the power supply management.

The command is configurable while "poe limit-mode" is set to "Port Priority"

Command Level:

Global Configuration

Syntax:

poe priority { Critical | High | Low} [<port-list>]

Parameters:

{Critical | High | Low}

- Critical - Indicates that operating the powered device is high.
- High- Indicates that operating the powered device has medium priority.
- Low- Indicates that operating the powered device has low priority

<port-list> specifies the ports to be set. If not entered, all ports are set.

Example:

```
Switch(config)# poe priority low 1
```

```
Switch(config)# show poe status 1
```

Port	Admin	Oper	Priority	Power Limit[W]	Current Consumption [W]	Current[mA]	Device Class
Port1	Enable	on	Low	15.4	13.4	279	0

poe maximum-power**Description:**

Enabling or disabling per port power output limit.

The command is configurable while "poe limit-mode" is set to "Total-Limit"

Command Level:

Global Configuration

Syntax:

poe maximum-power <1~15.4> [<port-list>]

no poe mximum-power [<port-list>]

Parameters:

<1~15.4>

<port-list> specifies the ports to be set. If not entered, all ports are set.

Example:

```
Switch(config)# poe maximum-power 10 1
```

```
Switch (config)# show poe status 1
```

Port	Admin	Oper	Priority	Power Limit[W]	Current Consumption [W]	Current[mA]	Device Class
Port1	Enable	on	Low	10	00		0

Chapter 7

Switch Operation

Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of a node in the network, including the MAC address, port no, etc. This information comes from the learning process of the Ethernet Switch.

Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

Forwarding & Filtering

When one packet comes from some port of the Industrial Fast Ethernet Switch, it will also check the destination address besides the source address. The Industrial Fast Ethernet Switch will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port from which this packet comes in. And these ports will transmit this packet to the network it is connected to. If found, and the destination address is located at a different port from where this packet comes in, the Industrial Fast Ethernet Switch will forward this packet to the port where this destination address is located, according to the information from address table. But, if the destination address is located at the same port from where this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability.

Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Industrial Switch stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets can occur. This is the best choice when a network needs efficiency and stability.

The Industrial Fast Ethernet Switch scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existing hubs, which nearly always improve overall performance. An Ethernet Switch can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Industrial Fast Ethernet Switch, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain, reducing the overall load on the network.

The Industrial Fast Ethernet Switch performs "Store-and-Forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

Auto-negotiation

The STP ports on the Industrial Fast Ethernet Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

Chapter 8

Power Over Ethernet

Overview

What is PoE?

Based on the global standard IEEE 802.3af, PoE is a technology for wired Ethernet, the most widely installed local area network technology adopted today. PoE allows the electrical power necessary for the operation of each end-device to be carried by data cables rather than by separate power cords. New network applications, such as IP Cameras, VoIP Phones, and Wireless Networking, can help enterprises improve productivity. It minimizes wires that must be used to install the network for offering lower cost, and less power failures.

IEEE802.3af also called Data Terminal equipment (DTE) power via Media dependent interface (MDI) is an international standard to define the transmission for power over Ethernet. The 802.3af is delivering 48V power over RJ-45 wiring. Besides 802.3af also define two types of source equipment: Mid-Span and End-Span.

- Mid-Span

Mid-Span device is placed between legacy switch and the powered device. Mid-Span is tap the unused wire pairs 4/5 and 7/8 to carry power, the other four is for data transmit.

- End-Span

End-Span device is direct connecting with power device. End-Span could also tap the wire 1/2 and 3/6.

PoE System Architecture

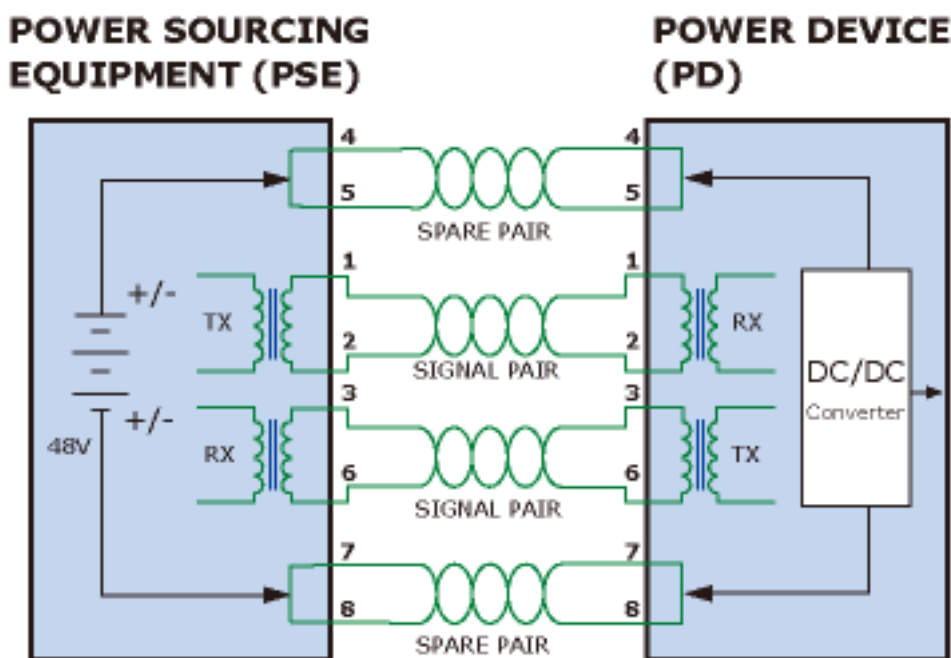
The specification of PoE typically requires two devices: the Powered Source Equipment (PSE) and the Powered Device (PD). The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

How Power is Transferred Through the Cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-T. The specification allows two options for using these cables for power, shown in Figure 8-1 and Figure 8-2:

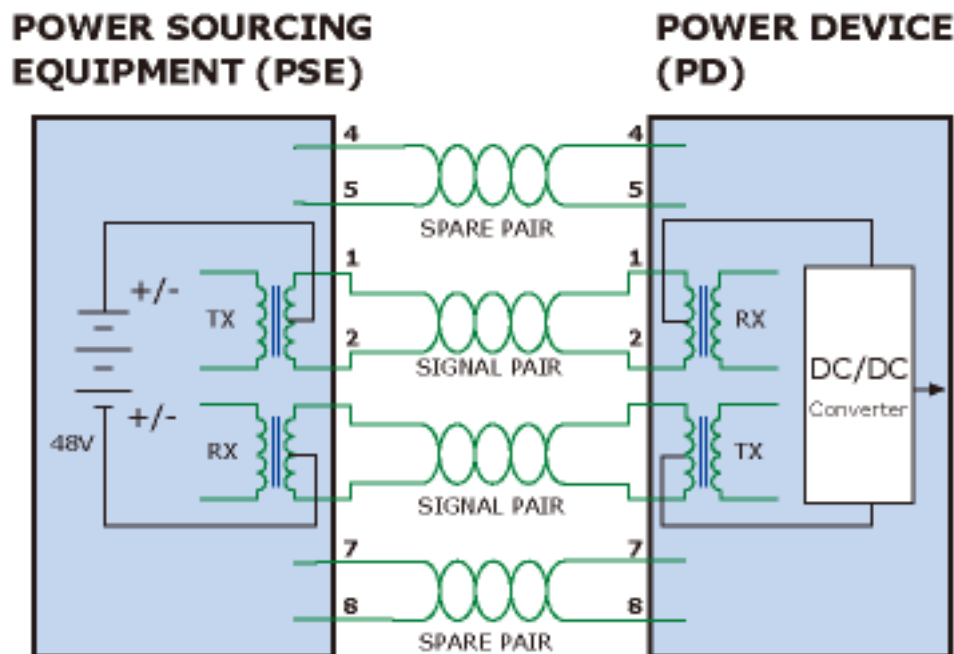
The spare pairs are used. Figure 8-1 shows the pair on pins 4 and 5 connected together and forming the positive supply, and the pair on pins 7 and 8 connected and forming the negative supply. (In fact, a late change to the spec allows either polarity to be used).

Figure 8-1: Power Supplied over the Spare Pins



The data pairs are used. Since Ethernet pairs are transformer coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without upsetting the data transfer. In this mode of operation the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.

Figure 8-2: Power Supplied over the Data Pins



When to install PoE?

Consider the following scenarios:

- You're planning to install the latest VoIP Phone system and you want to minimize cabling building costs.
- The company staff has been clamoring for a wireless access point in the picnic area behind the building so they can work on their laptops through lunch, but of electrical power to the outside is not available.
- Management asks for IP Surveillance Cameras and business access systems throughout the facility, but they would rather avoid another installation bill.

References:

IEEE Std 802.3af-2003 (Amendment to IEEE Std 802.3-2002, including IEEE Std 802.3ae-2002), 2003 Page(s):0_1-121

White Paper on Power over Ethernet (IEEE802.3af)

http://www.poweroverethernet.com/articles.php?article_id=52

Microsemi /PowerDsine

<http://www.microsemi.com/PowerDsine/>

Linear Tech

<http://www.linear.com/>

The PoE Provision Process

While adding PoE support to networked devices is relatively painless, it should be realized that power cannot simply be transferred over existing CAT-5 cables. Without proper preparation, doing so may result in damage to devices that are not designed to support provision of power over their network interfaces.

The PSE is the manager of the PoE process. In the beginning, only small voltage level is induced on the port's output, till a valid PD is detected during the Detection period. The PSE may choose to perform classification, to estimate the amount of power to be consumed by this PD. After a time-controlled start-up, the PSE begins supplying the 48 VDC level to the PD, till it is physically or electrically disconnected. Upon disconnection, voltage and power shut down.

Since the PSE is responsible for the PoE process timing, it is the one generating the probing signals prior to operating the PD and monitoring the various scenarios that may occur during operation.

All probing is done using voltage induction and current measurement in return.

Stages of powering up a PoE link

Stage	Action	Volts specified per 802.3af	Volts managed by chipset
Detection	Measure whether powered device has the correct signature resistance of 15–33 kΩ	2.7–10.0	1.8–10.0
Classification	Measure which power level class the resistor indicates	14.5–20.5	12.5–25.0
Startup	Where the powered device will startup	>42	>38
Normal operation	Supply power to device	36–57	25.0–60.0

Line Detection

Before power is applied, safety dictates that it must first be ensured that a valid PD is connected to the PSE's output. This process is referred to as "line detection", and involves the PSE seeking a specific, 25 KOhm signature resistor. Detection of this signature indicates that a valid PD is connected, and that provision of power to the device may start.

The signature resistor lies in the PD's PoE front-end, isolated from the rest of the the PD's circuitries till detection is certified.

Classification

Once a PD is detected, the PSE may optionally perform classification, to determine the maximal power a PD is to consume. The PSE induces 15.5-20.5 VDC, limited to 100 mA, for a period of 10 to 75 ms responded by a certain current consumption by the PD, indicating its power class.

The PD is assigned to one of 5 classes: 0 (default class) indicates that full 15.4 watts should be provided, 1-3 indicate various required power levels and 4 is reserved for future use. PDs that do not support classification are assigned to class 0. Special care must be employed in the definition of class thresholds, as classification may be affected by cable losses.

Classifying a PD according to its power consumption may assist a PoE system in optimizing its power distribution. Such a system typically suffers from lack of power resources, so that efficient power management based on classification results may reduce total system costs.

Start-up

Once line detection and optional classification stages are completed, the PSE must switch from low voltage to its full voltage capacity (44-57 Volts) over a minimal amount of time (above 15 microseconds).

A gradual startup is required, as a sudden rise in voltage (reaching high frequencies) would introduce noise on the data lines.

Once provision of power is initiated, it is common for inrush current to be experienced at the PSE port, due to the PD's input capacitance. A PD must be designed to cease inrush current consumption (of over 350 mA) within 50 ms of power provision startup.

Operation

During normal operation, the PSE provides 44-57 VDC, able to support a minimum of 15.4 watts power.

Power Overloads

The IEEE 802.3af standard defines handling of overload conditions. In the event of an overload (a PD drawing a higher power level than the allowed 12.95 Watts), or an outright short circuit caused by a failure in cabling or in the PD, the PSE must shut down power within 50 to 75 milliseconds, while limiting current drain during this period to protect the cabling infrastructure. Immediate voltage drop is avoided to prevent shutdown due to random fluctuations.

Power Disconnection Scenarios

The IEEE 802.3af standard requires that devices powered over Ethernet be disconnected safely (i.e. power needs be shut down within a short period of time following disconnection of a PD from an active port).

When a PD is disconnected, there is a danger that it will be replaced by a non-PoE-ready device while power is still on. Imagine disconnecting a powered IP phone utilizing 48 VDC, then inadvertently plugging the powered Ethernet cable into a non-PoE notebook computer. What's sure to follow is not a pretty picture.

The standard defines two means of disconnection, DC Disconnect and AC Disconnect, both of which provide the same functionality - the PSE shutdowns power to a disconnected port within 300 to 400ms. The upper boundary is a physical human limit for disconnecting one PD and reconnecting another.

DC Disconnect

DC Disconnect detection involves measurement of current. Naturally, a disconnected PD stops consuming current, which can be inspected by the PSE. The PSE must therefore disconnect power within 300 to 400 ms from the current flow stop. The lower time boundary is important to prevent shutdown due to random fluctuations.

AC Disconnect

This method is based on the fact that when a valid PD is connected to a port, the AC impedance measured on its terminals is significantly lower than in the case of an open port (disconnected PD).

AC Disconnect detection involves the induction of low AC signal in addition to the 48 VDC operating voltage. The returned AC signal amplitude is monitored by the PSE at the port terminals. During normal operation, the PD's relatively low impedance lowers the returned AC signal while a sudden disconnection of this PD will cause a surge to the full AC signal level and will indicate PD disconnection.

Chapter 9

Troubleshooting

This chapter contains information to help you solve common problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet Switch was set up according to the instructions in this manual.

The Link LED is not lit

Solution:

Check the cable connection and remove duplex mode of the Ethernet Switch

Some stations cannot talk to other stations located on the other port

Solution:

Check the VLAN settings, trunk settings, or port enabled / disabled status.

Performance is bad

Solution:

Check the full duplex status of the Ethernet Switch. If the Ethernet Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

Why the Switch doesn't connect to the network

Solution:

1. Check the LNK/ACT LED on the switch
2. Try another port on the Switch
3. Make sure the cable is installed properly

4. Make sure the cable is the right type
5. Turn off the power. After a while, turn on power again

100Base-TX port link LED is lit, but the traffic is irregular

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

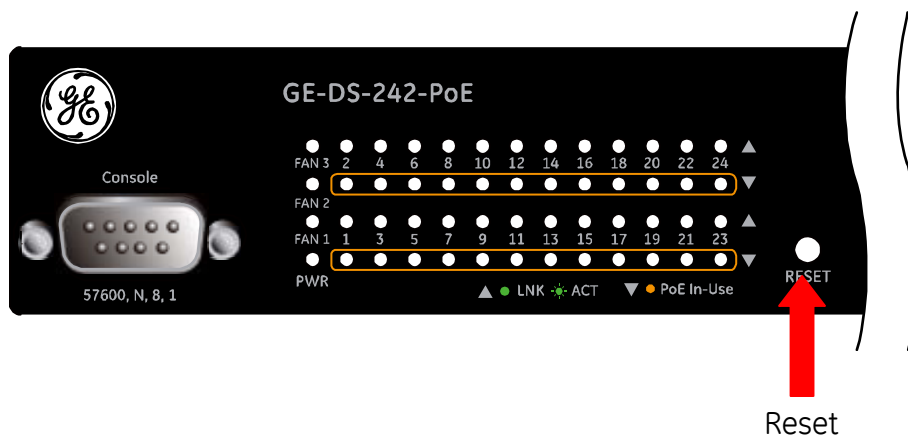
Switch does not power up

Solution:

1. AC power cord not inserted or faulty
2. Check that the AC power cord is inserted correctly
3. Replace the power cord If the cord is inserted correctly, check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

While IP Address be changed or forgotten admin password –

To reset the IP address to the default IP Address “192.168.0.100” or reset the password to default value. Press the hardware **reset button** at the front panel about **10 seconds**. After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



Appendix A

RJ-45 Pin Assignment

Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

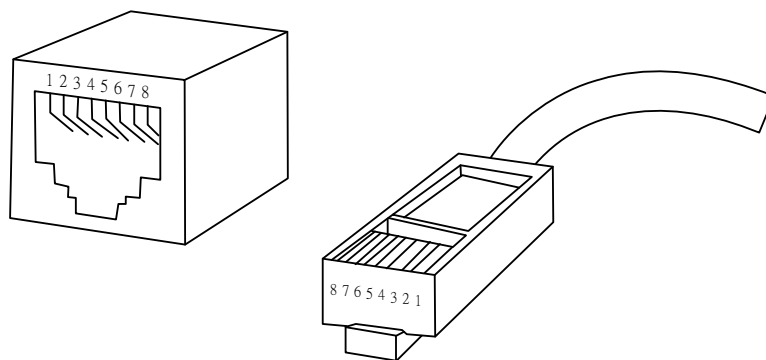
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI	MDI-X
	Media Dependant Interface	Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

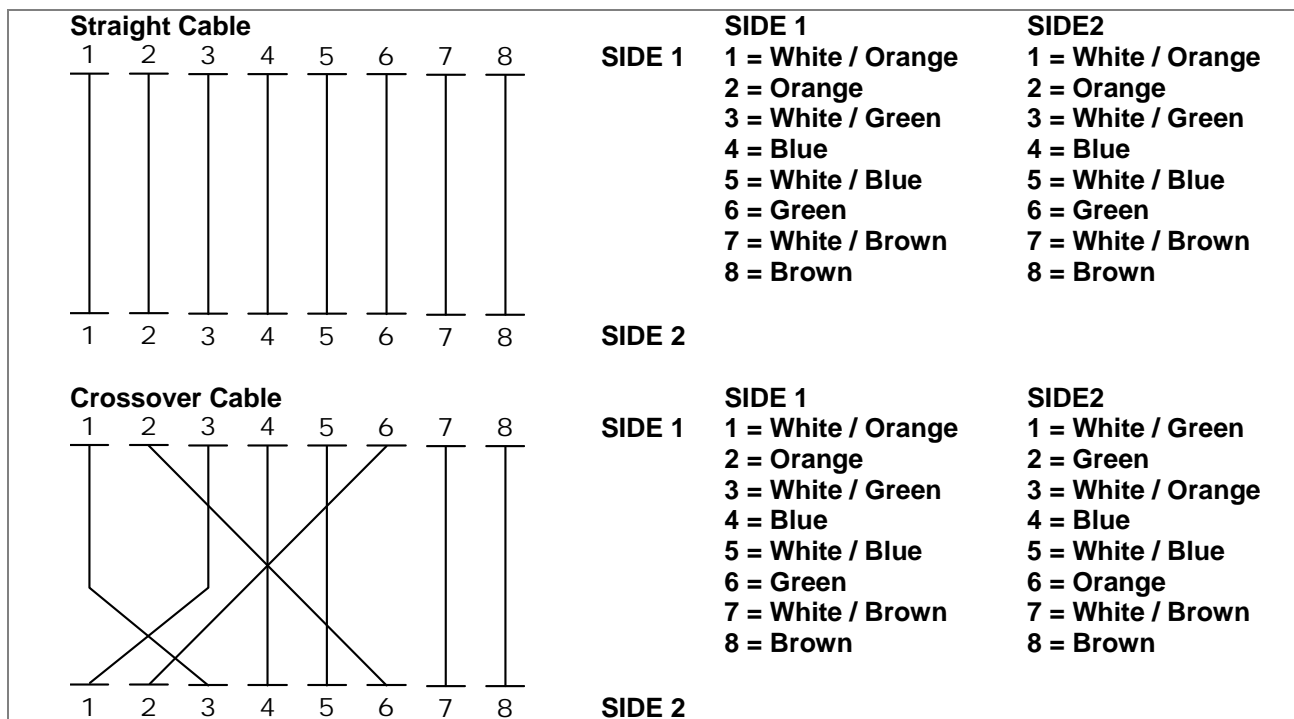
The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

Figure 101: Straight-Through and Crossover Cable



Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.