




GE-DSG-244/DSSG-244 and 244- PoE 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	<p>  N4131</p>
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></p> <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 5
- Product Specification 9

Chapter 2 Installation 13

- Hardware Description 14
- Switch Installation 22
- Stack Installation 27

Chapter 3 Switch Management 33

- Requirements 33
- Management Access Overview 34
- The Administration Console 35
- Web Management 37
- SNMP-Based Network Management 38
- Protocols 38
- Management Architecture 39

Chapter 4 Web-Based Management 41

- About Web-based Management 41
- System 46
- Simple Network Management Protocol 61
- Port Management 71
- Link Aggregation 80
- VLAN 88
- Rapid Spanning Tree Protocol 102
- Quality of Service 118
- Multicast 134
- IEEE 802.1X Network Access Control 143
- Access Control Lists 167
- Address Table 194
- Port Security 198
- LLDP 200
- Network Diagnostics 207
- Stacking - GE-DSSG-244 / GE-DSSG-244-PoE 209
- Power Over Ethernet 222

Chapter 5 Command Line Interface 233

Accessing the CLI 233

Telnet login 237

Chapter 6 Command Line Mode 239

Link Aggregation Command 256

VLAN Configuration Command 263

Spanning Tree Protocol Command 270

Multicast Configuration Command 277

Quality of Service Command 283

802.1x Port Access Control Command 292

Access Control List Command 300

MAC Address Table Command 305

LLDP Command 310

Stack Management Command 315

Power over Ethernet Command 318

Chapter 7 Switch Operation 325

Chapter 8 Power Over Ethernet Overview 329

What is PoE? 329

PoE System Architecture 330

The PoE Provision Process 332

Stages of powering up a PoE link 332

Power Disconnection Scenarios 334

Chapter 9 Troubleshooting 335

Appendix A RJ-45 Pin Assignment 339

Switch's RJ-45 Pin Assignments 339

10/100Mbps, 10/100Base-TX 340

Appendix B Glossary 343

Chapter 1

Introduction



GE DSSG-244-PoE

The GE Security Layer 2 Managed Gigabit Switch series – the GE-DSG-244 and GE-DSSG-244 series switches are all multiple port Gigabit Ethernet Switched with SFP fiber optical connective ability and robust layer 2 features. The description of these models is below:

GE-DSG-244	24-Port 10/100/1000Base-T with 4 Shared SFP Managed Gigabit Switch
GE-DSSG-244-POE	24-Port 10/100/1000Base-T PoE Managed Stackable Switch
GE-DSSG-244	24-Port 100/1000Base-X with 8 Shared TP Managed Stackable Switch

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
Two rack-mounting brackets with attachment screws	X2
Power cord	x1
Rubber feet	X4
RS-232 cable	x1
50cm stack cable (GE-DSSG-244 Series only)	x1

If any of these items 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 / Cost-effective / Telecom class Gigabit solution for Enterprise backbone and Data Center Networking

The GE Security Managed Switch is a L2/L4 Managed Gigabit Switch. Since Gigabit network interface had become the basic equipment and requirement of Enterprise and Network Servers, with 68Gbps switching fabric, the Managed Switch can handle extremely large amounts of data in a secure topology linking to a backbone or high capacity servers. The powerful QoS and Network Security features meet the needs of effective data traffic control for Campus and Enterprise, such VoIP, video streaming and multicast application.

High Performance

The Managed Switch provides 24 10/100/1000Mbps Gigabit Ethernet ports with 4-shared Gigabit SFP slots. It boasts a high performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as 68Gbps, which greatly simplifies the task of upgrading the LAN for bandwidth increase.

Robust Layer 2 Features

The Managed Switch can be programmed for basic switch management functions such as port speed configuration, Port aggregation, VLAN, Spanning Tree protocol, QoS, bandwidth control and IGMP Snooping. The Managed Switch provides 802.1Q Tagged VLAN, Q-in-Q VLAN trunking and private VLAN; the VLAN groups allowed on the Managed Switch will be maximally up to 255. Via supporting port aggregation, the Managed Switch allows the operation of a high-speed trunk combining multiple ports, up to eight groups of maximum to 8-ports for trunking, and it supports fail-over as well.

Excellent Traffic Control

GE Security GE-DSG-244/GE-DSSG-244 series is loaded with powerful traffic management and QoS features to enhance services offered by telecoms. The functionality includes QoS features such as wire-speed Layer 4 traffic classifiers and bandwidth limiting that are particularly useful for multi-tenant unit, multi business units, Telco, or Network Service Provide applications. It also empowers enterprises to take full advantage of limited network resources and guarantees the best performance at VoIP and Video conferencing transmission.

Efficient Management

For efficient management, the series of Managed Switches is equipped with console, WEB and SNMP management interfaces. With its built-in Web-based management, it offers an easy-to-use, platform-independent management and configuration facility. The Managed Switch supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software. Text-based management can also be accessed via Telnet and the console port.

Powerful Security

The Managed Switch offers comprehensive Access Control List (ACL) for enforcing security. Its protection mechanisms also comprise of port-based 802.1x and MAC-based user and device authentication. The port-security is effective in limiting the number of client pass-throughs, so that network administrators can now construct highly secured corporate networks in considerably less time and effort than before.

Flexibility and Extension solution

The mini-GBIC slots are compatible with 1000Base-SX/LX and WDM SFP (Small Form-factor Pluggable) fiber-optic modules. The distance can be extended from 550 meters (Multi-Mode fiber) up to above 10/30/70 kilometers (Single-Mode fiber or WDM fiber). They are well suited for use within the enterprise data centers and distributions.

Reliability Stacking Management

The GE-DSSG-244 Series Managed Switch provides a switch stacking function to manage up to 16 switches using a single IP address. That helps network managers to easily configure switches via one single IP address instead of connecting and setting each unit one by one. Through its high bandwidth tunnel and stacking technology, it gives enterprise, service provider and enterprise level flexible control over port density, uplinks and switch stack performance. Up to 384 Gigabit Ethernet ports can be managed by a stacking group and you can add ports and functionality as needed. The stacking technology also enables the advantages of chassis-based switches to be integrated into GE-DSSG-244 Series Managed Switch, but without the expensive up-front costs.

Advanced Features and Centralized Power Management for Enterprise and Campus PoE Networking (PoE Model)

The GE Security GE-DSSG-244-POE series PoE Switch provides 24 10/100/1000Mbps Power-over-Ethernet (PoE, IEEE 802.3af compliant) ports, which optimize the installation and power management of network devices such as wireless access points (AP), Voice over IP (VoIP) phones, and security video cameras. The PoE capabilities also help to reduce deployment costs for network devices such as wireless AP as there are no restrictions of power outlet locations. Power and data switching are integrated into one unit and delivered over a single cable. This eliminates cost for additional AC wiring and reduces installation time.

Fiber Optical Long-Reach Networking - GE-DSSG-244

To fulfill the needs of a large scale network deployment, the GE-DSSG-244 provides 24 100/1000 dual-speed SFP slots, 8 shared Gigabit TP ports, and 2 dedicated High-Speed HDMI-like interfaces for stacking with the series of switches. By applying the GE-DSSG series Switch, up to 16 units, 384 fiber-optical ports can be managed by a stacking group. You can add ports and functionality as needed. The 2 built-in stacking ports provide 5Gbps bandwidth and up to 20Gbps Bi-directional speed and it

can handle extremely large amounts of data in a secure topology linking to a backbone or a high capacity network server. The stacking technology also enables the chassis-based switches to be integrated into GE-DSSG series Managed Switch but without the expensive up-front cost.

The following table lists the major hardware difference between the series models:

Model		GE-DSG-244	GE-DSSG-244	GE-DSSG-244-POE
Interface	10/100/1000 T	24	8	24
	1000SX/LX	4	24, 100FX compatible	4
Power over Ethernet		-	-	IEEE 802.3af
PoE Budget		-	-	220W
Stack Capability		-	Hardware stacking, up to 16 units	

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-BASED MANAGEMENT	Explains how to manage the Managed Switch by Web interface
COMMAND LINE INTERFACE	Explains how to manage the Managed Switch by Command Line interface
COMMAND LINE MODE	An extensive listing of all commands and their description
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
APPENDIX B	Glossary

Product Features

- **Physical Port**

- GE-DSG-244
 - 24-Port 10/100/1000Base-T Gigabit Ethernet RJ-45
 - 4 mini-GBIC/SFP slots, shared with Port-21 to Port-24
 - RS-232 DB9 console interface for switch basic management and setup
- GE-DSSG-244-POE
 - 24-Port 10/100/1000Base-T Gigabit Ethernet RJ-45 with IEEE 802.3af PoE Injector
 - 4 mini-GBIC/SFP slots, shared with Port-21 to Port-24
 - RS-232 DB9 console interface for Switch basic management and setup
 - 2 High-performance 5GbE Stacking interface24-Port 10/100Base-TX RJ-45 with PoE Injector
- GE-DSSG-244
 - 24 100/1000Base-X mini-GBIC/SFP slots
 - 8-Port 10/100/1000Base-T Gigabit Ethernet RJ-45, shared with Port-1 to Port-8
 - RS-232 DB9 console interface for Switch basic management and setup
 - 2 High-performance 5GbE Stacking interface

- **Layer 2 Features**

- Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
- Supports Auto-negotiation and half duplex/full duplex modes for all 10Base-T/100Base-TX and 1000Base-T ports
- Auto-MDI/MDI-X detection for each RJ-45 port
- Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
- High performance of Store-and-Forward architecture, broadcast storm control and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
- 8K MAC address table, automatic source address learning and ageing
- 1392Kbytes embedded memory for packet buffers
- Support VLANs:

- IEEE 802.1Q Tagged VLAN
 - Up to 255 VLANs groups, out of 4041 VLAN IDs
 - Provides Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
 - Private VLAN Edge (PVE)
- Support Spanning Tree Protocol:
 - STP, IEEE 802.1D (Classic Spanning Tree Protocol)
 - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
- 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)
- Provides Port Mirror (many-to-1)
- Port Mirroring to monitor the incoming or outgoing traffic on a particular port
- **Quality of Service**
 - 4 priority queues on all switch ports
 - Supports for strict priority and weighted round robin (WRR) CoS policies
 - Ingress Shaper and Egress Rate Limit per port bandwidth control
 - Traffic-policing policies on the switch port
- **Multicast**
 - Supports IGMP Snooping v1 and v2
 - Querier mode support
- **Security**
 - IEEE 802.1x Port-Based / MAC-Based network access authentication
 - IP-based Access Control List (ACL)
 - MAC-based Access Control List
- **Management**
 - WEB-based, Telnet, Console Command Line management
 - Access through SNMPv1, v2c and v3 security set and get requests.

- Built-in Trivial File Transfer Protocol (TFTP) client
- BOOTP and DHCP for IP address assignment
- Firmware upload/download via HTTP / TFTP
- SNTP (Simple Network Time Protocol)
- **Stacking (GE-DSSG-244 and GE-DSSG-244-PoE)**
 - Hardware stack up to 16 units and 384 ports
 - Stacking architecture supports Chain and Ring mode
 - Mirror across stack
 - Link Aggregation groups spanning multiple switches in a stack
 - Hardware learning with MAC table synchronization across stack
- **Power over Ethernet (GE-DSSG-244-POE Only)**
 - 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

Product Specification

Product	GE-DSG-244	GE-DSSG-244-PoE	GE-DSSG-244
Hardware Specification			
Copper Ports	24 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports	24 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports with IEEE 802.3af PoE injector	8 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports, shared with Port-1 to Port-8
SFP/mini-GBIC Slots	4 SFP interfaces, shared with Port-21 to Port-24; 100Base-FX SFP transceiver compatible	4 SFP interfaces, shared with Port-21 to Port-24; 100Base-FX SFP transceiver compatible	24 SFP interfaces, 1000Base-SX/LX and 100Base-FX SFP transceiver compatible
Switch Processing Scheme	Store-and-Forward		
Switch Fabric	48Gbps	68Gbps	68Gbps
Address Table	8K entries		
Share data Buffer	1392 kilobytes		
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex		
Jumbo Frame	10Kbytes		
LED	System: Power Ports: 1000 Link/Act 10/100 Link/Act SFP Link	System: Power, Master Ports: 10/100/1000 Link/Act, PoE In-Use, SFP Link, Stack Port Link Alert: FAN alert	System: Power, Master Ports: 1000 Link/Act, 10/100 Link/Act, SFP Link, Stack Port Link
Dimension	17.32" x 7.87" x 1.75"	17.32" x 11.81" x 1.75"	17.32" x 7.87" x 1.75"
Weight	5.93 lbs	9.92 lbs	6.61 lbs
Power over Ethernet			
PoE Standard	---	IEEE 802.3af Power over Ethernet / PSE	---

PoE Power Supply	---	End-Span	---
PoE Power Output	---	Per Port 48V DC, 350mA . Max. 15.4 watts	---
Power Pin Assignment	---	1/2(+), 3/6(-)	---
PoE Power Budget	---	220 Watts	---
Number of PD@7Watts	---	24	---
Number of PD@15.4Watts	---	14	---
Stacking			
Stacking Ports	---	Two 5Gbps HDMI-Like interface	
Stacking Numbers	---	16	
Stacking Bandwidth	---	10Gbps (Full-Duplex)	
Stack ID Display	---	7-Segment LED Display (1~9, A~F,0)	
Stack Topology	---	Ring / Chain / Back-to-Back stack	
Layer 2 function			
System Configuration	Console, Telnet, Web Browser, SNMPv1, v2c and v3		
Port configuration	Port disable/enable. Auto-negotiation 10/100/1000Mbps full and half duplex mode selection. Flow Control disable / enable. Bandwidth control on each port.		
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.		
VLAN	802.1Q Tagged Based VLAN ,up to 255 VLAN groups Q-in-Q Private VLAN		
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Support 12 groups of 16-Port trunk support		
QoS	Traffic classification based, Strict priority and WRR 4-level priority for switching - Port Number - 802.1p priority - DS/TOS field in IP Packet		
IGMP Snooping	IGMP (v1/v2) Snooping, up to 8K multicast Groups IGMP Querier mode support		

Access Control List	IP-Based ACL / MAC-Based ACL Up to 256 entries
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD-MIB RFC3411 SNMP-Frameworks-MIB IEEE802.1X PAE LLDP MAU-MIB Power over Ethernet

ELECTRICAL SPECIFICATION

Model		GE-DSG-244	GE-DSSG-244-PoE	GE-DSSG-244
AC Power Input Voltage:		100 ~ 240VAC, 50 / 60Hz, Auto-sensing.		
Power Consumption	110V	22.2 Watts / 75.7 BTU	29.3 Watts / 99.9 BTU	15.5 Watts
(System on):	220V	23Watts / 78.43 BTU	30.2 Watts / 102.98 BTU	16 Watts
Power Consumption	110V	29.3 Watts / 100 BTU	39 Watts / 132.99 BTU	46 Watts
(Full Load):	220V	30.2 Watts / 102.98 BTU	40 Watts / 136.4 BTU	45.5 Watts
Power Consumption	110V	---	Max. 290 Watts / 988.9 BTU	---
(PoE Full Load):	220V	---	Max. 288 Watts / 982 BTU	---

ENVIRONMENTAL SPECIFICATION

Operating:

Temperature: 0°C ~ 50 degree C

Relative Humidity: 20% ~ 95% (non-condensing)

Storage:

Temperature: -20°C ~ 70 degree C

Relative Humidity: 20% ~ 95% (non-condensing)

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 LED indicators.

Before connecting any network device to the Managed Switch, please read this chapter completely.

Hardware Description

Switch Front Panel

The unit front panel provides a simple interface for monitoring the Managed Switch. Figures 2-1 through 2-3 show the front panels of the Managed Switches.

Figure 2-1: GE-DSG-244 Front Panel



Figure 2-2: GE-DSSG-244-PoE Front Panel



Figure 2-3: GE-DSSG-244 Front Panel



Gigabit TP Interface

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

Gigabit SFP Slots

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

Console Port

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

Reset Button

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

Reset Button Pressed and Released	Function
About 1~3 second	Reboot the Managed Switch
Until the PWR LED lit off	Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as below: <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

Stack ID (GE-DSSG-244 Series only)

Each GE-DSSG-244 series Managed Stackable Switch on a stack must have a unique "Stack ID". There are 16 degrees (0~9, A~F) in the rotary switch. The Stack ID is configured via Web or CLI management interface. Use the Stack ID to identify the location of the real device.

NOTE: Stack ID is not equal to the Master Priority that is configured in the management interface.

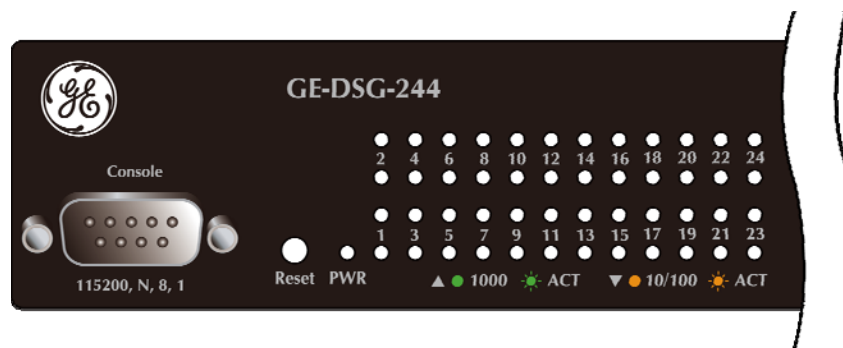
Master LED (GE-DSSG-244 Series only)

If master switch is fail or disconnected to the switch by stack port, the switch with least switch ID will become master.

LED Indications

The front panel LEDs indicates instant status of port links, data activity, system operation, Stack status and system power, helps monitor and troubleshoot when needed. The front panel LEDs are shown in Figures 2-4 through 2-6.

Figure 2-4: GE-DSG-244 LED indication



System

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

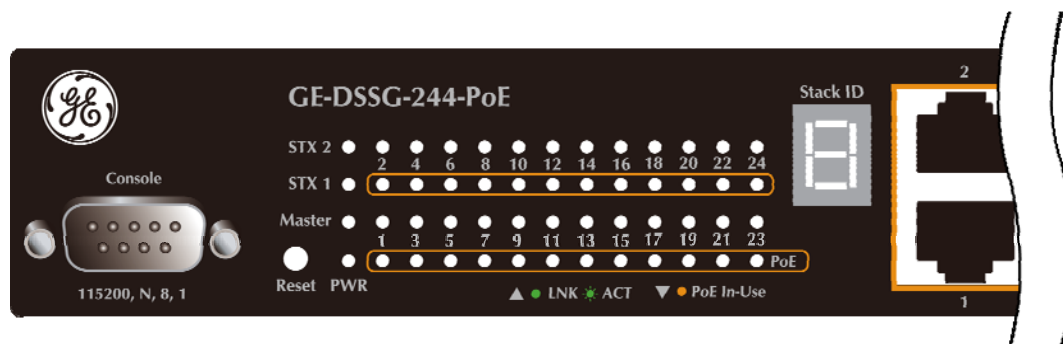
10/100/1000Base-T interfaces

LED	Color	Function
1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established with speed 1000Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If 10/100 LNK/ACT LED is light, it indicates that the port is operating at 10Mbps or 100Mbps If 10/100 LNK/ACT LED is Off, it indicates that the port is link down
10/100 LNK/ACT	Orange	Lights: To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If 1000 LNK/ACT LED is light, it indicates that the port is operating at 1000Mbps If 1000 LNK/ACT LED is Off, it indicates that the port is link down

1000Base-SX/LX SFP interfaces (Shared Port-21~Port-24)

LED	Color	Function
1000 LNK	Green	Lights: To indicate the link through that SFP port is successfully established with speed 1000Mbps with Gigabit SFP transceiver or 100Mbps with 100Base-FX SFP transceiver
		Off: To indicate that the SFP port is link down

Figure 2-5: GE-DSSG-244-PoE LED indication



System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch is powered on. Blink to indicate the System is running under booting procedure.
Master	Green	Lights to indicate that the Switch is the Master of the stack group
STX1	Green	Lights to indicate the stacking link through that port is successfully established.
STX2	Green	Lights to indicate the stacking link through that port is successfully established.

Alert

LED	Color	Function
PWR Alert	Green	Lights to indicate that the power supply failure
FAN1 Alert	Green	Lights to indicate that the FAN1 failure
FAN2 Alert	Green	Lights to indicate that the FAN2 failure
FAN3 Alert	Green	Lights to indicate that the FAN3 failure

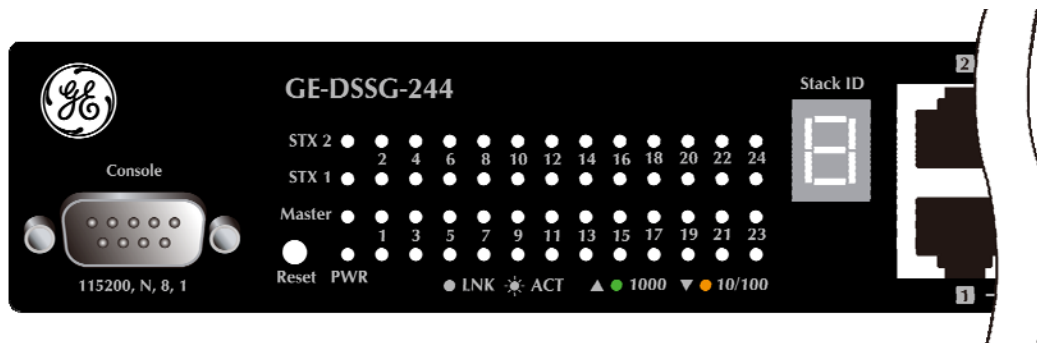
10/100/1000Base-T interfaces

LED	Color	Function
10/100/1000 LNK/ACT	Green	Lights: To indicate the link through that port is successfully established with speed 10Mbps or 100Mbps or 1000Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If L10/100 NK/ACT LED light-> indicate that the port is operating at 10Mbps or 100Mbps If LNK/ACT LED Off -> indicate that the port is link down
PoE In-Use	Orange	Lights: To indicate the port is providing 48VDC in-line power
		Off: To indicate the connected device is not a PoE Powered Device (PD)

1000Base-SX/LX SFP interfaces (Shared Port-21~Port-24)

LED	Color	Function
1000 LNK	Green	Lights: To indicate the link through that SFP port has been successfully established with speed 1000Mbps
		Off: To indicate that the SFP port is link downs

Figure 2-6: GE-DSSG-244 LED indication



System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
Master	Green	Lights to indicate that the Switch is the Master of the stack group
STX1	Green	Lights to indicate the stacking link through that port has been successfully established.
STX2	Green	Lights to indicate the stacking link through that port has been successfully established.

10/100/1000Base-T interfaces

LED	Color	Function
10/100/1000 LNK/ACT	Green	Lights: To indicate the link through that port has been successfully established with speed 10Mbps or 100Mbps or 1000Mbps
		Blink: To indicate that the switch is actively sending or receiving data over that port.
		Off: If 10/100 LNK/ACT LED is light, it indicates that the port is operating at 10Mbps or 100Mbps If 10/100 LNK/ACT LED is Off, it indicates that the port is link down
PoE In-Use	Orange	Lights: To indicate the port is providing 48VDC in-line power
		Off: To indicate the connected device is not a PoE Powered Device (PD)

1000Base-SX/LX SFP interfaces (Shared Port-21~Port-24)

LED	Color	Function
1000 LNK	Green	Lights: To indicate the link through that SFP port is successfully established with speed 1000Mbps with Gigabit SFP transceiver or 100Mbps with 100Base-FX SFP transceiver
		Off: To indicate that the SFP port is link down

7-Segment LED Display

Stack ID (1~9, A~F, 0): To indicate the Switch ID of each GE-DSSG-244 series Managed Switch. Switch IDs are used to uniquely identify the Managed Switches within a stack. The Switch ID of each Managed Switch is shown on the display on the front of the Managed Switch and is used widely in the web pages as well as in the CLI commands of the Stack group.

Stack ID	1	2	3	4	5	6	7	8	9	A.	B.	C.	D.	E.	F.	0
Switch ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Switch Rear Panel

The rear panel of the Managed Switch indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50-60Hz. Figure 2-7 to Figure 2-9 shows the rear panel of these Managed Switches.

Figure 2-7: GE-DSG-244 Rear panel

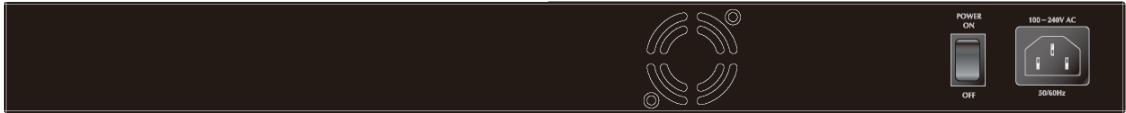


Figure 2-8: GE-DSSG-244-PoE Rear panel



Figure 2-9: GE-DSSG-244 Rear panel



AC Power Receptacle

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

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

POWER NOTICE:

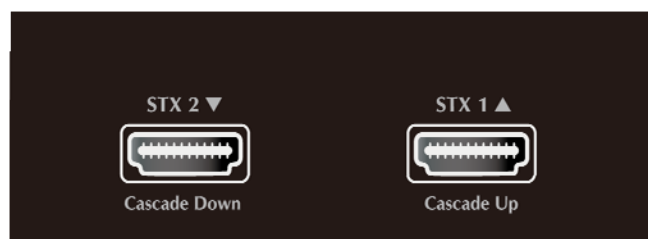
1. The Managed Switch is a power-required device: it will not work unless it is receiving power. If your networks must be active at all times, it is recommended that the Switch be connected to a UPS (Uninterruptable Power Supply) to prevent data loss or downtime.
 2. In some areas, installing a surge 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.
-

Stack Ports (GE-DSSG-244 series)

There are two High-Performance stack ports on the rear panel. One is STX1 / Cascade Down and the other is STX2 / Cascade UP.

- When stacked, the STX1 / Cascade Down port should connect to the other switch's STX2 / Cascade UP port and the STX2 / Cascade UP port should connect to other switch's STX1 / Cascade Down out.
- You can just use attached GE Security connector to stack.
- The HDMI LIKE stacking cables are Cross-overed HDMI cables; only attached GE Security stack cables can be used.
- Plug-and-play connection.

Figure 2-10: GE-DSSG-244 Stack Ports



Switch Installation

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

Desktop Installation

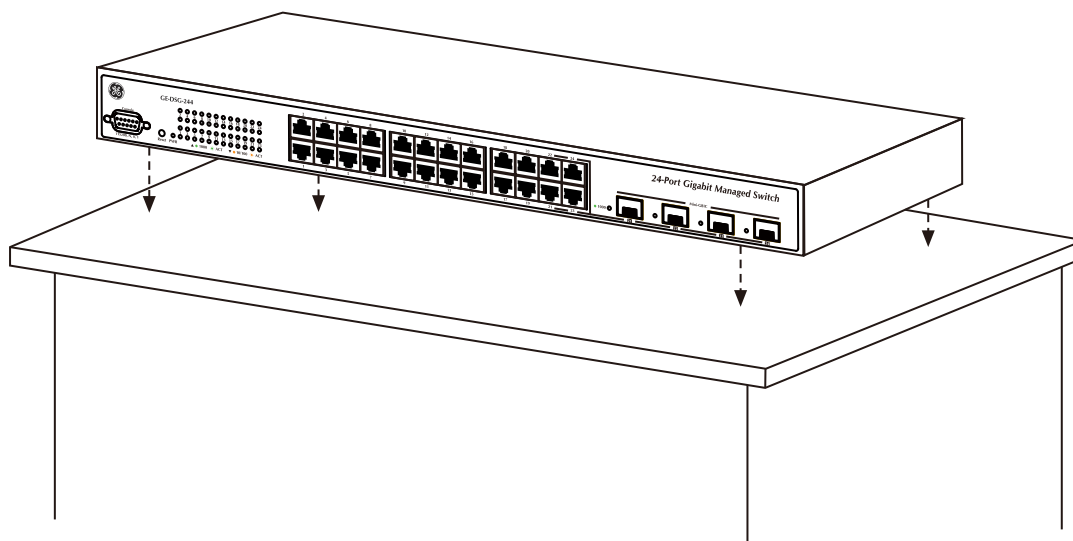
Use the following steps to install the Managed Switch on a desktop or shelf:

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 2-11.

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

Figure 2-11: Typical placement of GE-DSG-244 on desktop



NOTE: When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Features and Product Specifications.

Connection to the Managed Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please refer to the Cabling Specification section.

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 such as printer servers, workstations or 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.

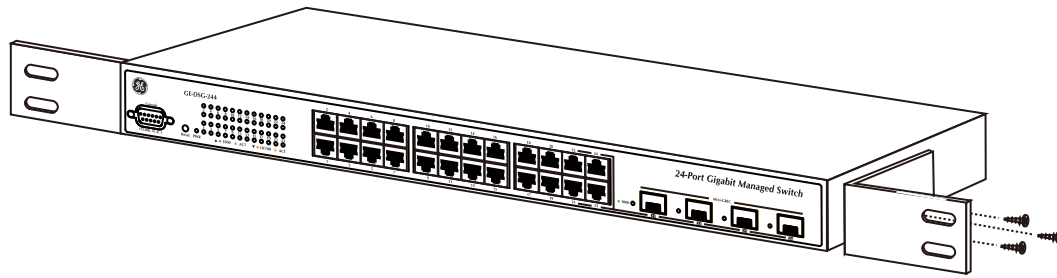
Step 1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front.

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 2-12 shows how to attach brackets to one side of the Managed Switch.

Figure 2-12: Attaching rack-mount brackets to the GE-DSG-244

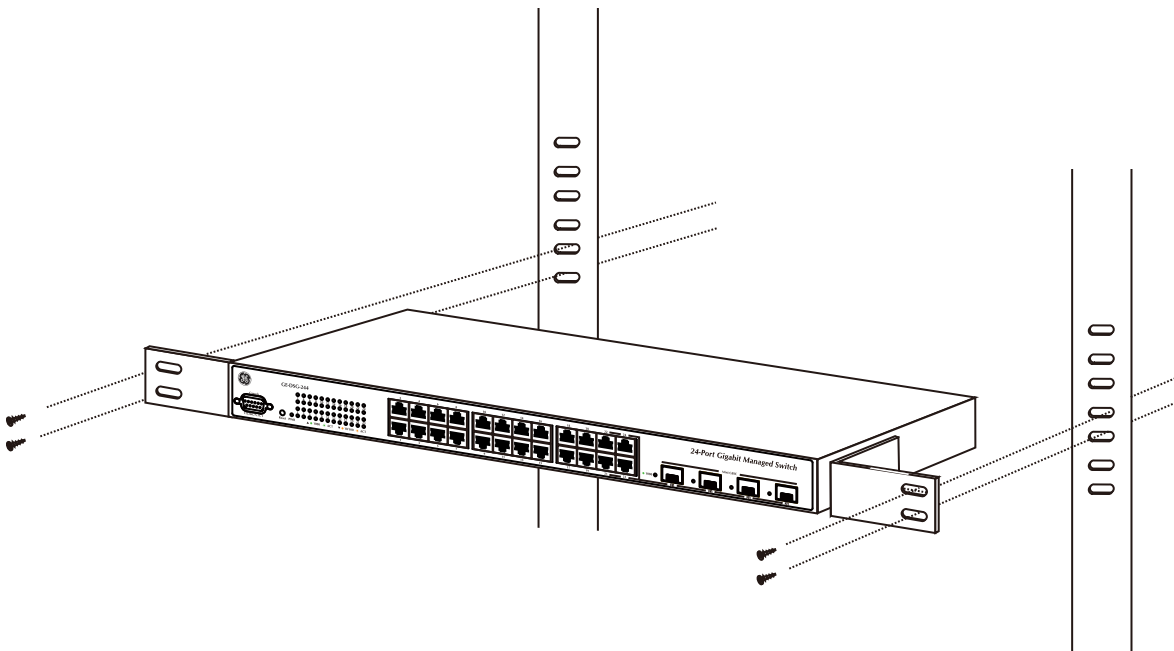


Step 3: Secure the brackets tightly, but do not over tighten screws.

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 2-13.

Figure 2-13: Mounting the GE-DSG-244 in a rack



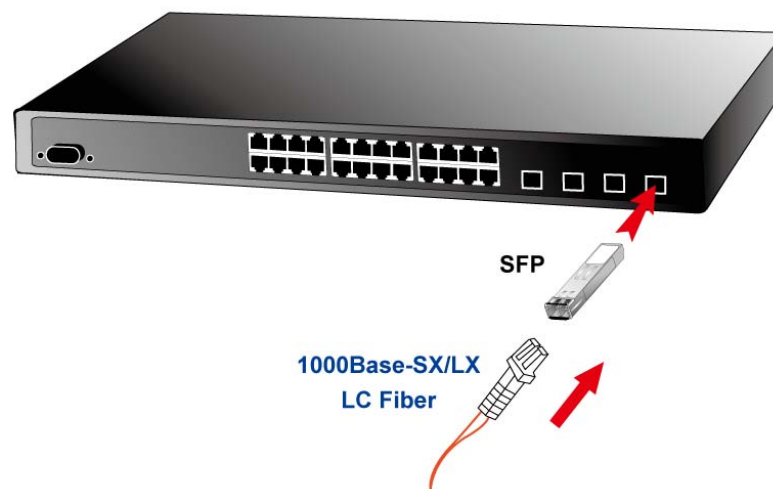
Step 6: Follow steps 4 and 5 of the Desktop Installation section to connect the network cabling and supply power to the Managed Switch.

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/from any SFP port without powering down the Managed Switch, as shown in Figure 2-14.

Figure 2-14: 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 may 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 1000Base-LX SFP transceiver, use single-mode fiber cable (one side must be male duplex LC connector type).

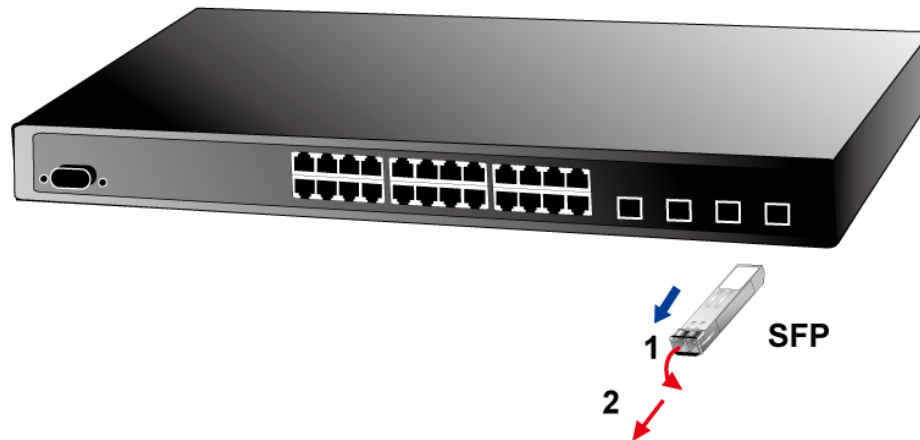
Connect the fiber cable:

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 "Force 1000" is needed.

Remove the transceiver module

1. Make sure there is no network activity by consulting or checking 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 2-15: Pulling out the SFP transceiver



CAUTION: Never pull out the module without pull 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 Switch.

Stack Installation

GE-DSSG-244

The GE-DSSG-244 series Managed Switch provides a switch stacking function to manage up to 16 switches using a single IP address. And up to 384 Gigabit Ethernet ports can be managed by a stacking group and you can add ports and functionality as needed. You can add GE-DSSG-244 series switches as needed to support more network clients, knowing that your switching fabric will scale to meet increasing traffic demands.

Two types of stack topologies are supported by the GE-DSSG-244 series:

- Chain topology (same as a disconnected ring)
- Ring topology

Please see the following figure for a sample connection.

Figure 2-16: Chain Stack topology

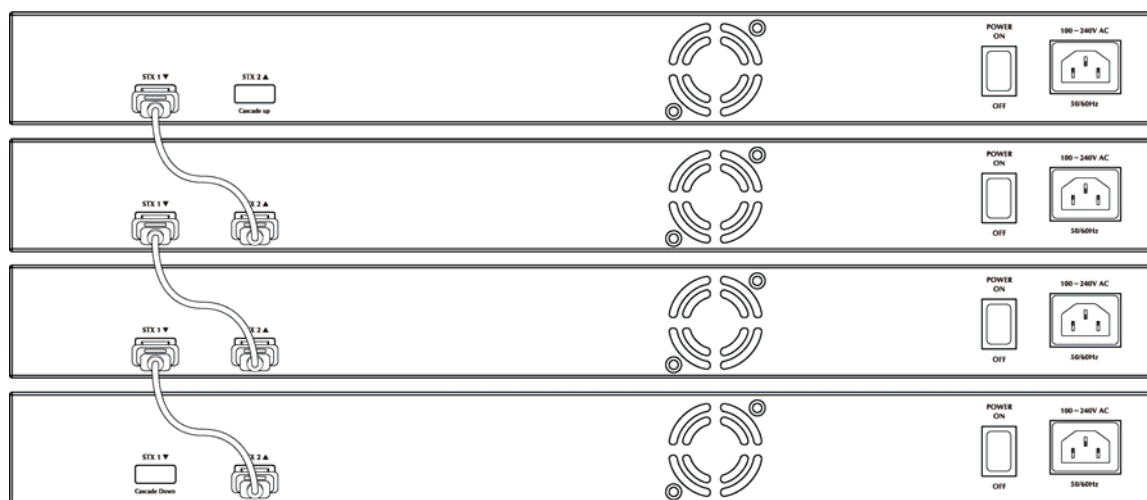
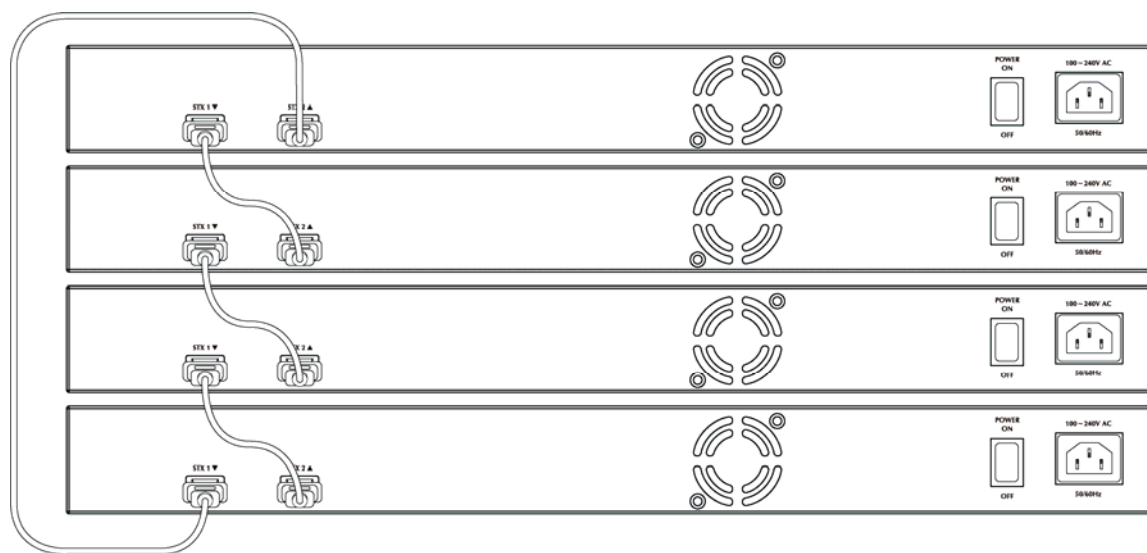


Figure 2-17: Ring Stack topology



Connecting Stacking cable

Before attempting to connect stacking ports, verify that you have the required stack cables. The following cables are used to connect stacked switches:

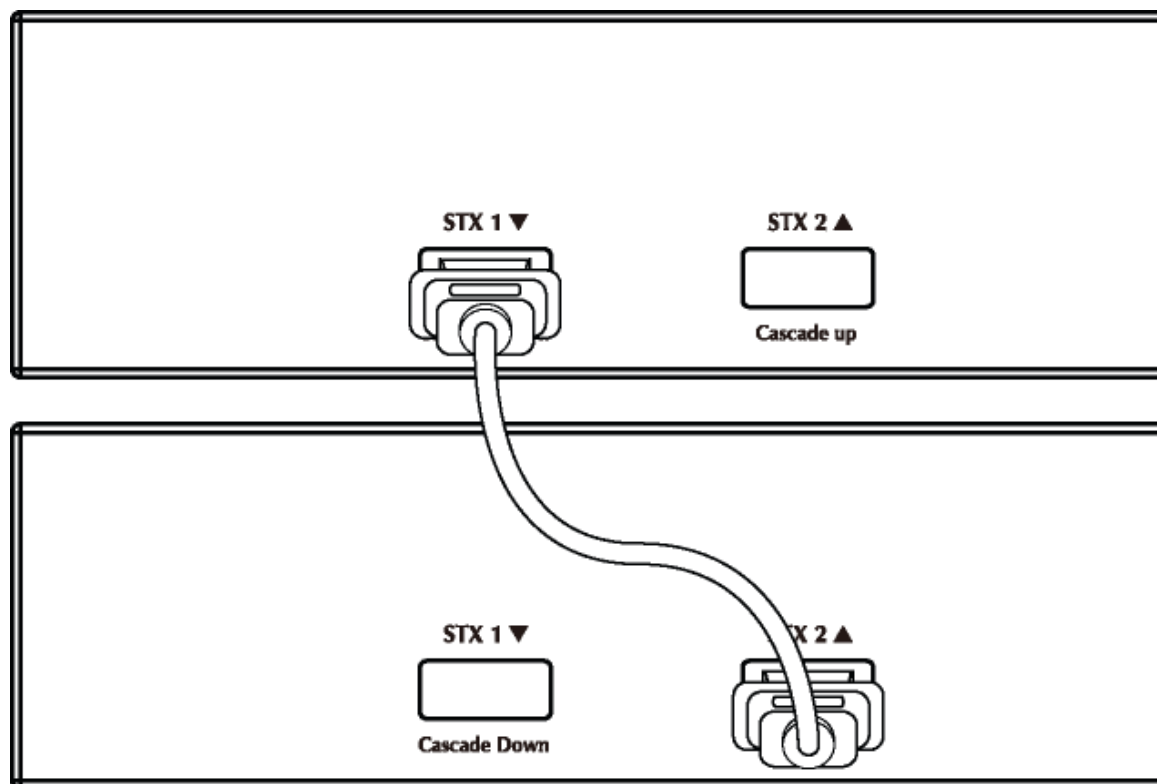
- 50cm, Short stack cable -used to connect adjacent GE-DSSG-244 series switches.
- 200cm, Long / Redundant stack cable - used to connect the top and bottom GE-DSSG-244 series switches of a stack.

There are two high-performance HDMI-like Stack ports on the rear panel for proprietary management stack. Only attached GE Security cross-overed HDMI cable can be used.

STEP-1: Plug one end of the cable in the "STX1 / Cascade Down" port and the other end to the "STX2 / Cascade UP" port of next device.

STEP-2: Repeat the step for every device in the stack cluster, then ending at last switch.

Figure 2-18: Stacking connection



STEP-3: If you wish to implement stack redundancy, use the longer stack cable to connect the stack port marked "STX1 / Cascade Down" on the bottom switch to the port marked "STX2 / Cascade Up" on the top switch of the stack.

NOTE: The stack port is for management and data packets to be transmitted between other GE-DSSG-244 series stackable switches, the stack ports can't be configured with Layer 2 features via management interface.

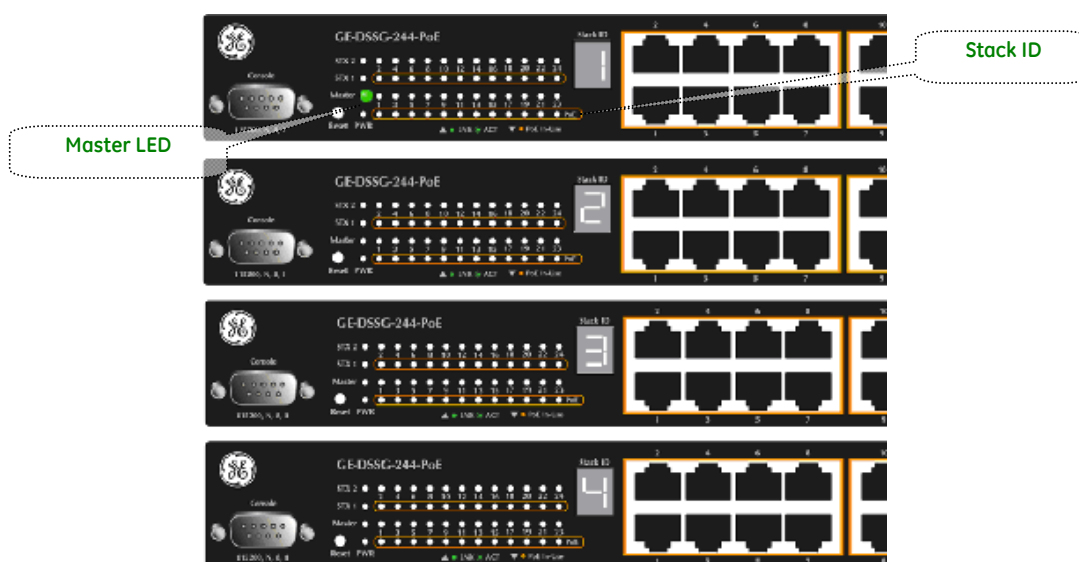
STEP-4: Power up the stack switches.

Management Stacking

The stack operation of the GE-DSSG-244 series Managed Switch supports Plug and Play Stacking connection and auto stack configuration.

STEP-5: Once the stack start operation, the Stack master is automatically elected without any configure. A lit green “Master” LED on the front panel indicates the Stack master.

Figure 2-19: Stack Master with "Master" LED lit



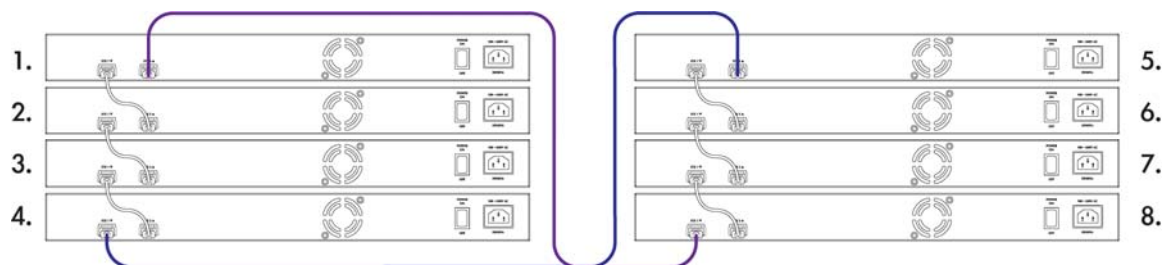
STEP-6: When a GE-DSSG-244 series Switch is added to the stack, a Switch ID is automatically assigned to the GE-DSSG-244 series Switch. Choosing a different Switch ID on the Stack Configuration page can modify the automatic SID assignment. This method allows Switch IDs to be assigned so that it is easier for the user to remember the ID of each switch.

STEP-7: Connect the RS-232 serial cable to the console port on the front of the stack master, and then login the GE-DSSG-244 series Switch to start the switch management.

NOTE: The stack switch with least priority ID or MAC Address number will become Master. Only Master switch's management interface (console, telnet, web and SNMP) is accessible.

It's allowed to build a stack of up to 16 GE Security GE-DSSG-244 series Switches. If there is the space limitation or power issue and you wish to stack all the switches in different racks, use long stack cables to connect two stacks.

Figure 2-20: Separated Stack connection



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 connect
- Network cables - Use standard network (UTP) cables with RJ45 connectors.
- Above Workstation installed with WEB Browser and JAVA runtime environment Plug-in.

NOTE: We recommend using Internet Explorer 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. The following table compares the three management methods.

Table 3-1: Management Methods Comparison

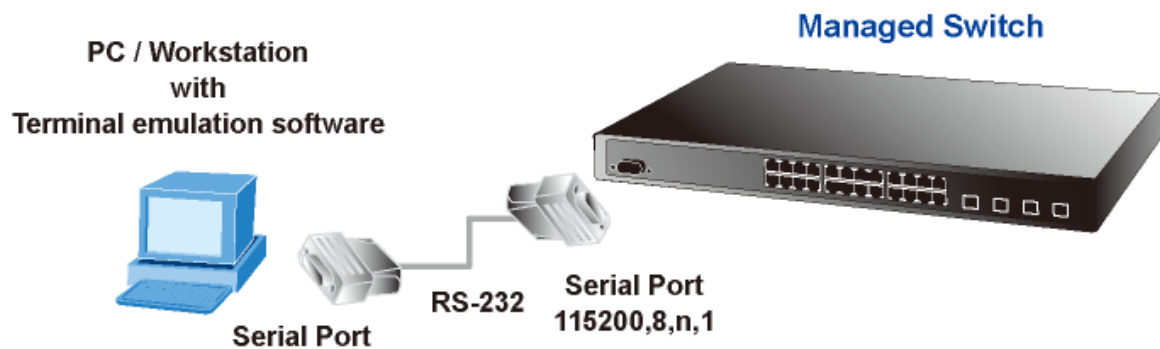
Method	Advantages	Disadvantages
Console	No IP address or subnet needed Text-based Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems Secure	Must be near switch or use dial-up connection Not convenient for remote users Modem connection may prove to be unreliable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

The 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 3-1: 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.

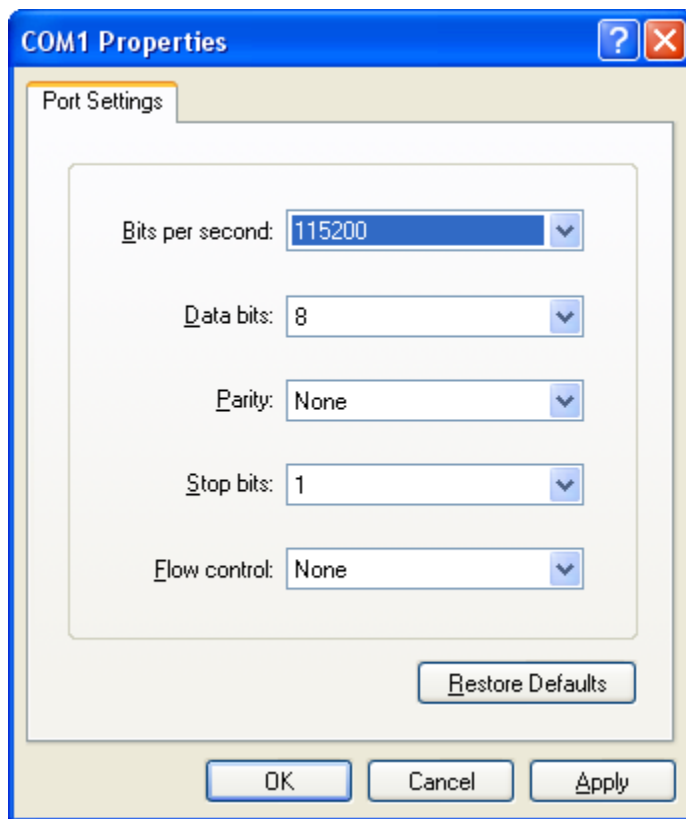
When using this management method, a straight DB9 RS-232 cable is required to connect the switch to the PC.

1. Click **START**, then **Programs/Accessories** and then **Hyper Terminal**.

When the following screen appears, make sure that the COM port should be configured as:

- 115200 bps
- 8 data bits
- No parity
- 1 stop bit
- Flow Control = None

Figure 3-2: COM1 Properties window



2. Once the terminal has connected to the device, power on the GE-DSG series Managed Industrial Switch, the terminal will display that it is running testing procedures.
3. Then, the system asks for the login password. The factory default username and password is below. The login screen appears.

User name: **admin**

Password: **admin**

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.

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 3-3: Web management setup

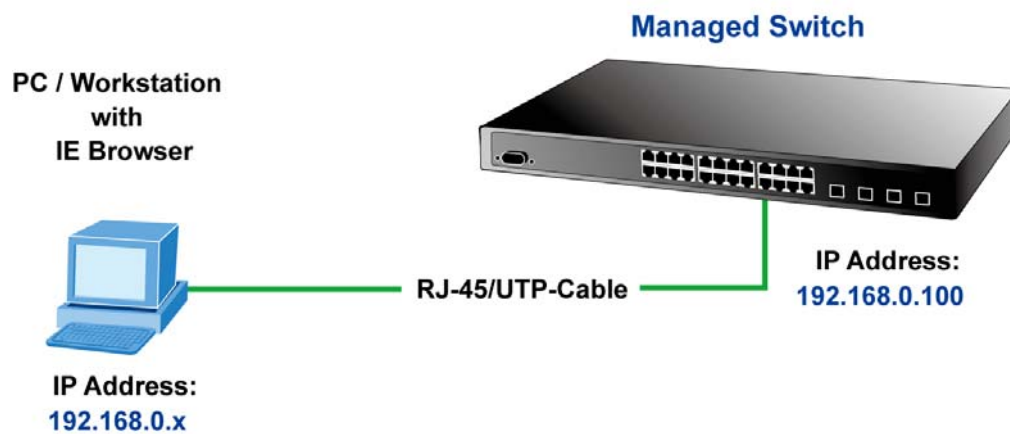


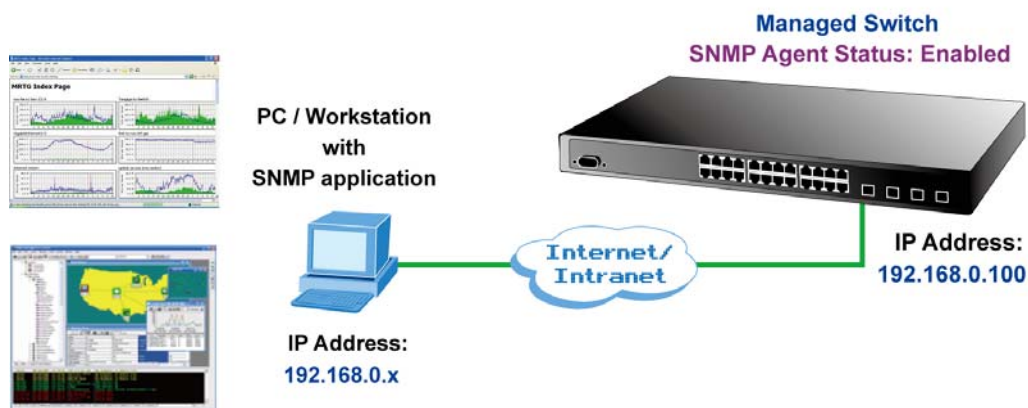
Figure 3-4: Web main screen of Managed Switch



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 3-5: SNMP management setup



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 of Web browser).

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

Chapter 4

Web-Based Management

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.

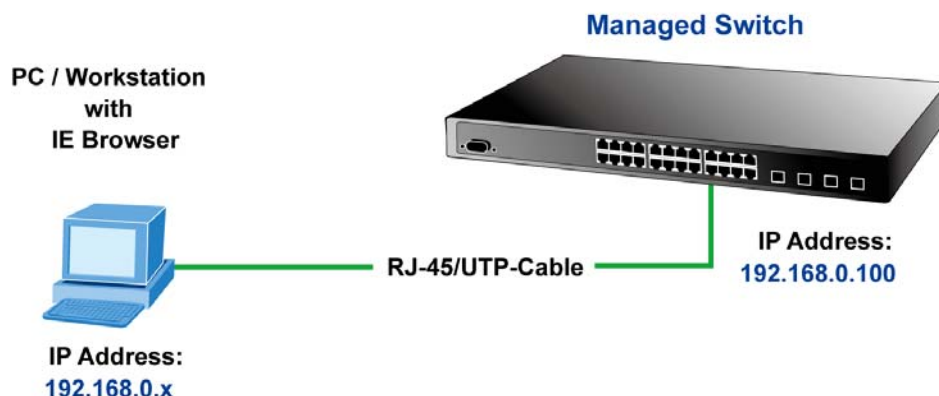
NOTE: By default, IE6.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

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.

Figure 4-1: Web management setup



Logging on the Switch

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

http://192.168.0.100

2. When the 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 shown in Figure 4-2 appears.

Default User name: **admin**

Default Password: **admin**

Figure 4-2: Login screen



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

Figure 4-3: Web main page



4. The Switch Menu on the left of the Web page lets 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:

- It is recommended to use Internet Explorer 6.0 or above to access Managed Switch.
- A changed IP address takes effect immediately after clicking on the **Save** button, and you will need to use the new IP address to access the Web interface.
- For security reasons, 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 GE-DSG / GE-DSSG-244 series 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.

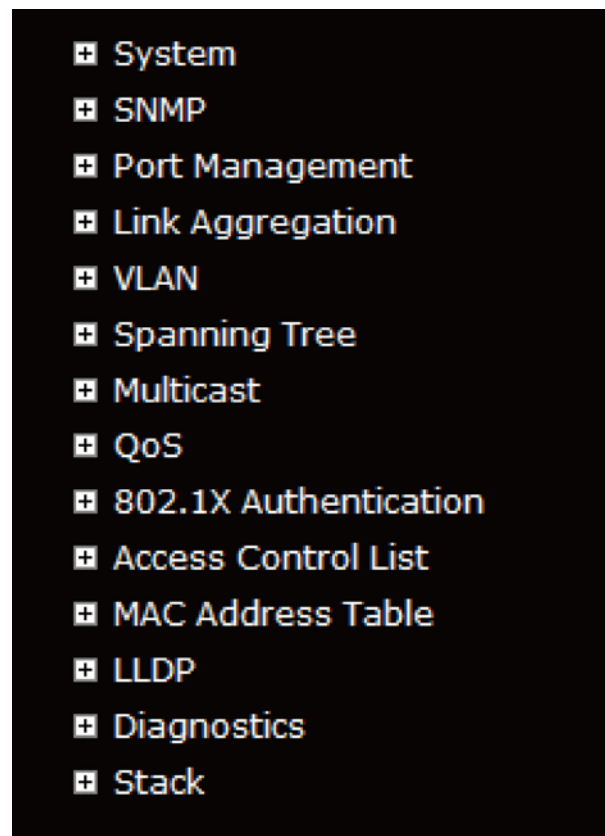
The port states are illustrated as follows:

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-DSG/GE-DSSG-244 series 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
User Authentication	Allows configuring the system password required to access the web pages or log in from CLI.
SNTP Configuration	Simple Network Time Protocol. Configures SNTP client settings, including broadcast mode or a specified list of servers
Web Firmware Upgrade	Upgrade the firmware via Web browser
TFTP Firmware Upgrade	Upgrade the firmware via TFTP server
Configuration Save	Save/view the switch configuration to remote host
Configuration Upload	Upload the switch configuration from remote host
Factory Default	Reset the configuration of the Managed Switch
System Reboot	Restarts the switch

System Information

The System Info page provides information for the current device information. System Info page helps a switch administrator to identify the hardware MAC address, software version and system uptime.

Figure 4-6: System Information page screenshot

System Information

System	
Contact	
Name	GE-DSSG-244
Location	
Hardware	
MAC Address	00-30-4f-24-24-24
Power Status	AC Power
Temperature	44.0 C - 111.2 F
Time	
System Date	2009-10-21 Wed 05:59:26 +0000
System Uptime	6d 02:24:43

Switch ID	Software Version
1	v1.0b090925

Auto-refresh ☐

This page includes the following fields:

Object	Description
Contact	The system contact configured in SNMP \ System Information \ System Contact.
Name	The system name configured in SNMP \ System Information \ System Name.
Location	The system location configured in SNMP \ System Information \ System Location
MAC Address	The MAC Address of this switch.
System Date	The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.
System Uptime	The period of time the device has been operational.
Switch ID	The switch ID. (GE-DSSG-244 series Only)
Software Version	The software version of the switch.
Software Date	The date when the switch software was produced.

Buttons

Auto-refresh: check this box to enable an automatic refresh of the page at regular intervals.

Refresh: click to refresh the page; any changes made locally will be undone.

For the GE-DSSG-244 series stackable switch, the System Information page add additional column to identify the current switch ID of stack member switches in a stack group. The screen as below appears

Figure 4-7: System Information

System Information

System	
Contact Name	GE-DSSG-244-PoE
Location	

Hardware	
MAC Address	00-30-4f-76-26-93
Power Status	AC Power
Temperature	47.0 C - 116.6 F

Time	
System Date	1970-01-01 Thu 00:03:38 +0000
System Uptime	0d 00:03:38

Switch ID	Software Version
1	v1.0b090925
2	v1.0b090925
3	v1.0b090925

Auto-refresh ☐

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

	Configured	Current
DHCP Client	<input type="checkbox"/>	<button>Renew</button>
IP Address	10.1.1.241	10.1.1.241
IP Mask	255.255.255.0	255.255.255.0
IP Router	10.1.1.254	10.1.1.254
VLAN ID	1	1

Save Reset

The Current column is used to show the active IP configuration.

Object	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	Provide the IP address of this switch in dotted decimal notation.
IP Mask	Provide the IP mask of this switch dotted decimal notation.
IP Router	Provide the IP address of the router in dotted decimal notation.
SNTP Server	Provide the IP address of the SNTP Server in dotted decimal notation.
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
Timezone Offset	Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.

Buttons

Click **SAVE** to save changes.

Click **RESET** to undo any changes made locally and revert to previously saved values.

User Authentication

This page allows you to configure the system password required to access the web pages or log in from CLI. After setup completed, please press "Save" button to take effect. Please login to the web interface with new password, the screen in Figure 4-8 appears.

Figure 4-8: IP configuration interface



The screenshot shows a web interface titled "User Authentication". It features three text input fields stacked vertically, labeled "Old Password", "New Password", and "Confirm New Password". Below these fields is a single "Save" button. The interface has a light gray background.

This page includes the following fields:

Object	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126. It will not display as it is typed, only asterisks (*) will show. Passwords are alphanumeric characters in length, and are case sensitive.
Confirm New Password	The new password must be entered twice to catch typing errors. To confirm that you entered it correctly, this field will not display, but will show asterisks (*)

NOTE: After change the default password, if you forget the password. Press the "Reset" button in the front panel of the Managed Switch over 10 seconds and then release, the current setting includes VLAN, will be lost and the Managed Switch will restore to the default mode.

SNTP Configuration

In the System sub-function menu, you can see the SNTP Configuration, by which you can configure the time settings for the Managed Switch. You can specify SNTP Servers and set GMT Timezone. The SNTP Configuration screen in Figure 4-9 appears.

Figure 4-9: SNTP Configuration page screenshot

SNTP Configuration	
SNTP Server	asia.pool.ntp.org
Timezone	(GMT+0)Casablanca, Monrovia, Dublin, Edinburgh, Lisbon, Lond
System Date	2009-10-21 Wed 06:56:00 +0000
System Uptime	6d 03:20:42

Save Reset

This page includes the following fields:

Object	Description
SNTP Server	Provide the IP address of the SNTP Server in dotted decimal notation. Enter a user-defined SNTP server IP addresses or hostname. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
Timezone Offset	Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
System Date	Display the current local date and time (UTC) of the last SNTP request or receipt of an unsolicited message. The field format is Year-Month-Day HH : MM : SS. For example, 2008-08-20 21:15:03
System Uptime	Display the time passed since the device boot up.

NOTE: The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. A network SNTP server performs time synchronization. SNTP operates only as a client, and cannot provide time services to other systems.

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

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

<http://ntp.isc.org/bin/view/Servers/WebHome>

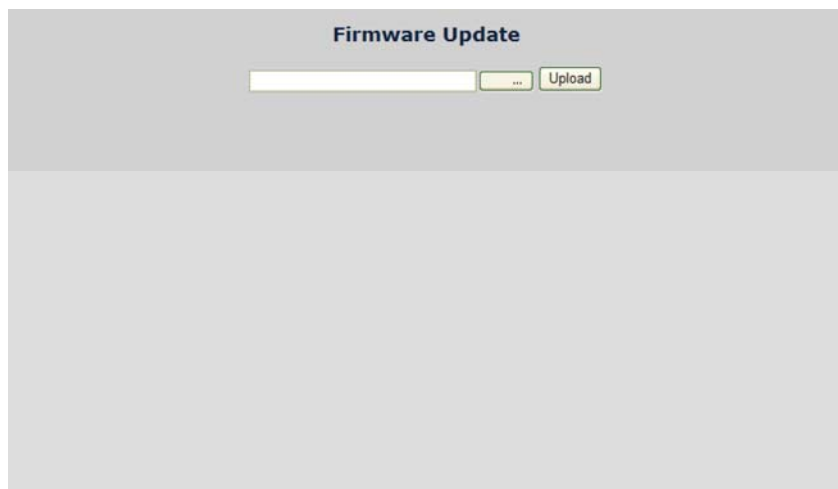
<http://ntp.isc.org/bin/view/Servers/NTPPoolServers>

<http://support.microsoft.com/kb/262680/en-us>.

Web Firmware Upgrade

The Web Firmware Upgrade page contains fields for downloading system image files from the Local File browser to the device. The Web Firmware Upgrade screen in Figure 4-10 appears.

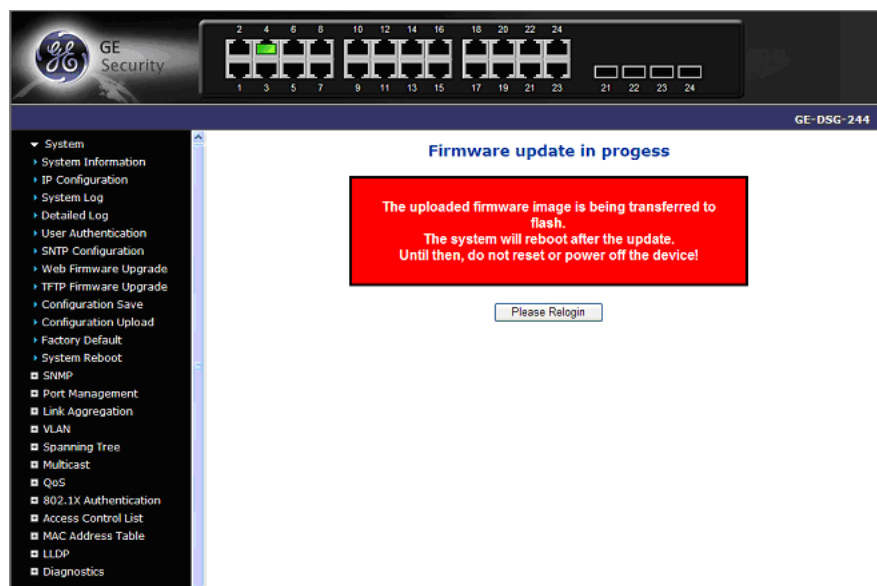
Figure 4-10: Web Firmware Upgrade page screenshot



To execute a Firmware Upgrade do the following:

1. Click System -> Web Firmware Upgrade.
2. The Firmware Upgrade screen is displayed as in Figure 4-10.
3. Click the "Browse" button of the main page; the system would pop up the file selection menu to choose firmware.
4. Select the firmware file and then click "Upload", the Software Upload Progress would show the file upload status.
5. Once the software has been loaded to the system successfully. The following screen appears. Click the "Please Relogin" button to activate the new software immediately. The system will load the new software after reboot.

Figure 4-11: Software successfully loaded notice screen



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 4-12 appears.

Figure 4-12: TFTP Firmware Upgrade interface

TFTP Firmware Update

TFTP Server IP	192.168.0.52
Firmware file name	GE-DSSG-244_v10b

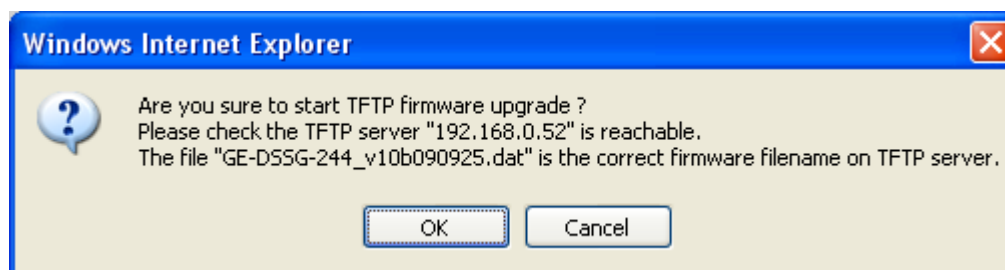
This page includes the following fields:

Object	Description
TFTP Server IP	Fill in your TFTP server IP address.
Filename	The name of firmware image. (Maximum length: 24 characters)
Upgrade button	Press the button for upgrade the switch firmware.

To open Firmware Upgrade screen, perform the following:

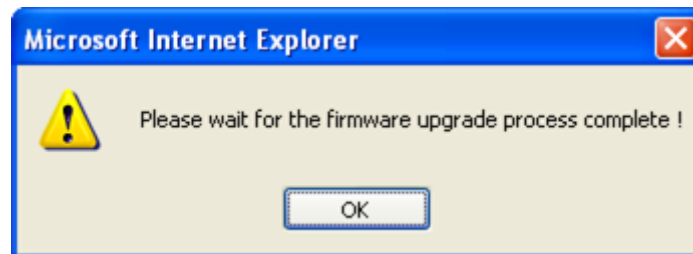
1. Click System -> TFTP Firmware Upgrade.
2. The Firmware Upgrade screen is displayed as in Figure 4-12.
3. Fill in the TFTP server IP Address and the firmware file name, click the "Upgrade" button of the main page, the system would pop up the confirm message shown in Figure 4-13.

Figure 4-13: TFTP Firmware upgrade pop-up message



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

Figure 4-14: Firmware upgrade pop-up message



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

NOTE: DO NOT Power OFF the switch until the update progress is complete.

NOTE: Do not quit the Firmware Upgrade page without pressing the "OK" button - after the image be loaded. Or the system won't apply the new firmware. User has to repeat the firmware upgrade processes again.

Configuration Save

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The screen in Figure 4-15 appears.

Figure 4-15: Configuration Save page screenshot



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

Header tags: `<?xml version="1.0"?>` and `<configuration>`. These tags are mandatory and must be present at the beginning of the file.

Section tags: `<platform>`, `<global>` and `<switch>`. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.

Module tags: `<ip>`, `<mac>`, `<port>` etc. These tags identify a module controlling specific parts of the configuration.

Group tags: `<port_table>`, `<vlan_table>` etc. These tags identify a group of parameters, typically a table.

Parameter tags: `<mode>`, `<entry>` etc. These tags identify parameters for the specific section, module and group. The `<entry>` tag is used for table entries.

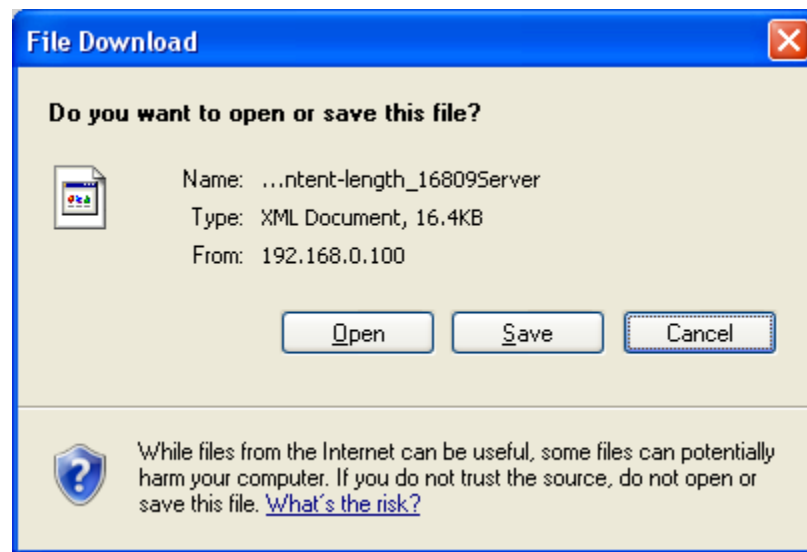
Configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may then be modified using an editor and loaded to a switch.

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

Save Configuration

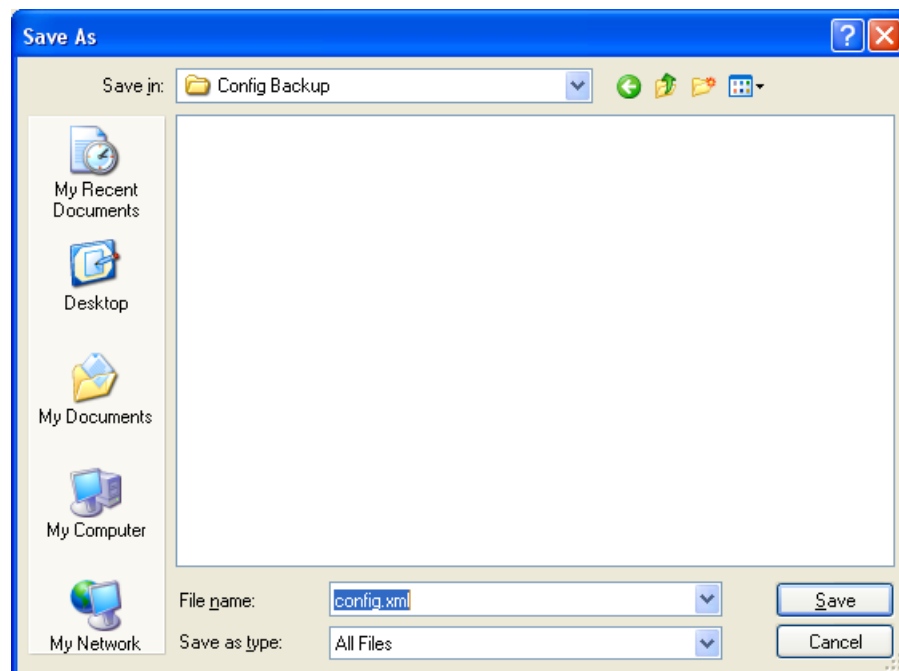
1. Press the "Save Configuration" button to save the current configuration in manager workstation. The following screens in Figure 4-16 and 4-17 appear.

Figure 4-16: File Download screen



2. Choose the file save path in management workstation.

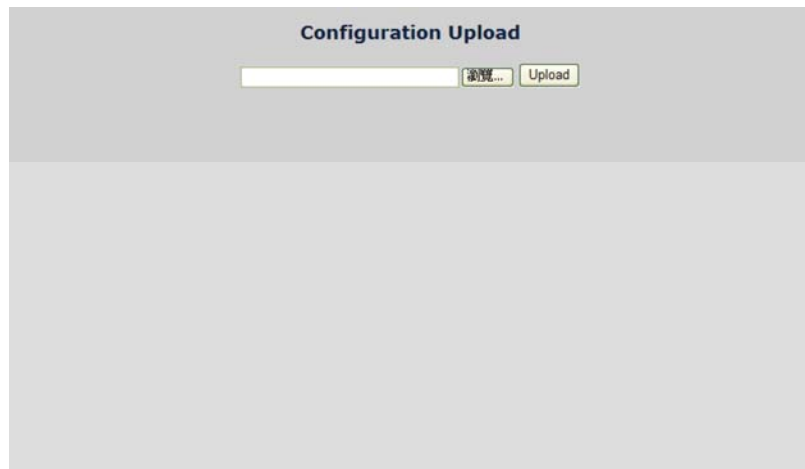
Figure 4-17: File save screen



Configuration Upload

This function allows backup and reload the current configuration of the Managed Switch to the local management station. The screen in Figure 4-18 appears.

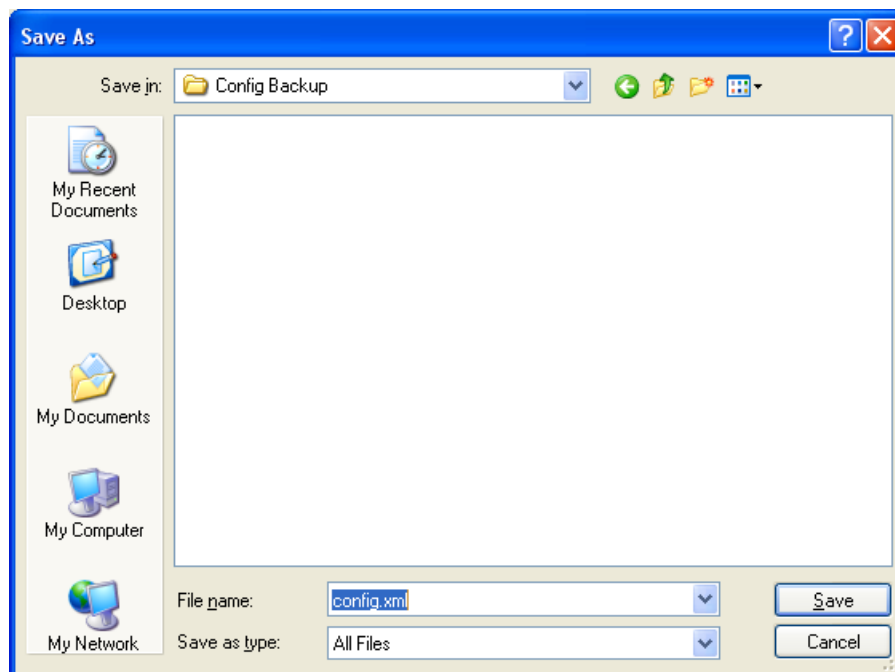
Figure 4-18: Configuration Upload page screenshot



Configuration Upload

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

Figure 4-19: Windows file selection menu popup



2. Select the configuration file then click "Upload", the bottom of the browser shows the upload status.

3. When finished the message appears "Transfer Completed".

Factory Default

The Factory Reset button can reset the Managed Switch back to the factory default mode. Be aware that the entire configuration will be reset; include the IP address of the Managed Switch. Once the Factory Reset item is pressed, the screen in Figure 4-20 appears.

Figure 4-20: Factory Default Reset screen

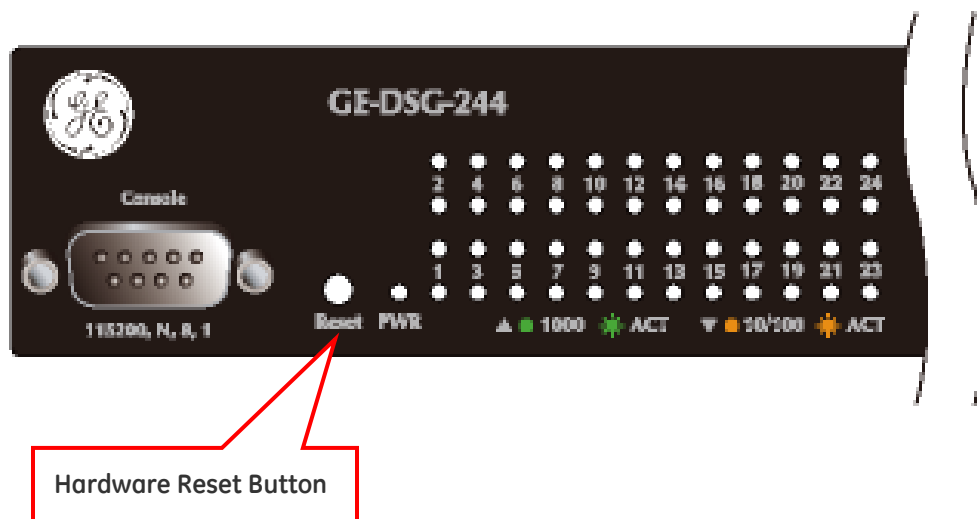


After the "Factory" button is pressed and rebooted, the system will load the default IP settings as following:

- Default IP address: 192.168.0.100
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.0.254
- The other settings have been reset back to disable or none.

NOTE: To reset the Managed Switch to the Factory default setting, you can also press the hardware reset button at the front panel about 10 seconds. After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.

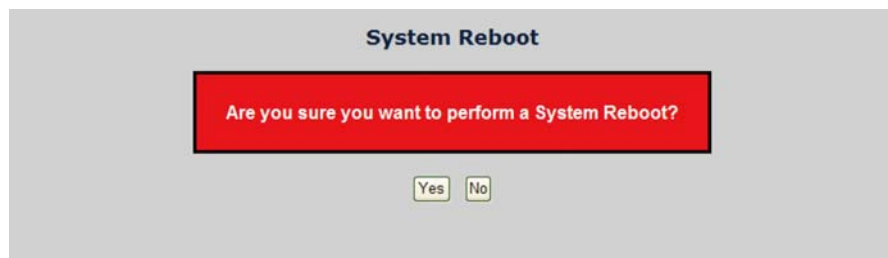
Figure 4-21: Hardware Rest Button



System Reboot

The Reboot page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user have to re-login to the WEB interface about 60 seconds later, the screen in Figure 4-22 appears.

Figure 4-22: System Reboot page screenshot



You can also check the SYS LED at the front panel to identify the System is load completely or not. If the SYS LED is blinking, then it is in the firmware load stage; if the SYS LED light on, you can use the WEB browser to login the Switch.

Simple Network Management Protocol

SNMP Overview

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

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

- **Network management stations (NMSs):** Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents:** Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB):** A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol:** A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP 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

SNMP System Configuration

Configure SNMP on this page.

The SNMP System Configuration screen in Figure 4-23 appears.

Figure 4-23: SNMP System Configuration page screenshot

SNMP System Configuration	
Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Save Reset

This page includes the following fields:

Object	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associate with SNMPv3 community's table.

Write Community	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associate with SNMPv3 community's table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-F's are not allowed. Change of the Engine ID will clear all original local users.

SNMP System Information Configuration

The switch system information is provided here.

The System Information Configuration screen in Figure 4-24 appears.

Figure 4-24: System Information Configuration page screenshot

This page includes the following fields:

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

SNMP Trap Configuration

Configure SNMP trap on this page.

The SNMP Trap Configuration screen in Figure 4-25 appears.

Figure 4-25: SNMP Trap Configuration page screenshot

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

Save Reset

This page includes the following fields:

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

Object	Description
Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMPv3 Configuration

SNMPv3 Accesses Configuration

Configure SNMPv3 accesses table on this page. The entry index key are Group Name, Security Model and Security Level.

The SNMPv3 Accesses Configuration screen in Figure 4-26 appears.

Figure 4-26: SNMPv3 Accesses Configuration page screenshot

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view	None
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

This page includes the following fields:

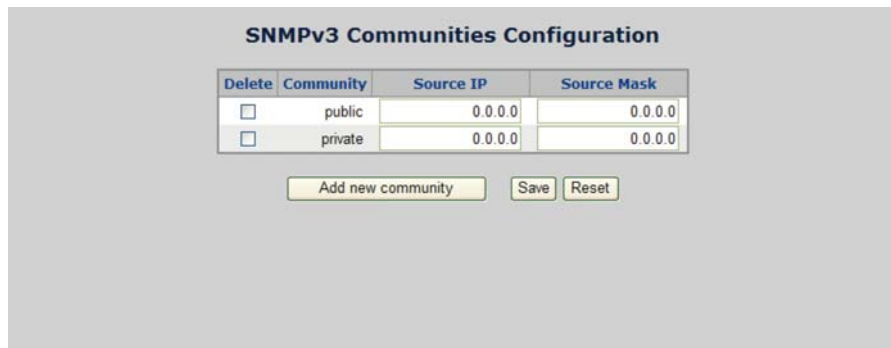
Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates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

SNMPv3 Communities Configuration

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

The SNMPv3 Communities Configuration screen in Figure 4-27 appears.

Figure 4-27: SNMPv3 Communities Configuration page screenshot



The screenshot shows the 'SNMPv3 Communities Configuration' page. It features a table with four columns: 'Delete', 'Community', 'Source IP', and 'Source Mask'. There are two rows of data: one for 'public' and one for 'private', both with '0.0.0.0' in the Source IP and Source Mask fields. Below the table are three buttons: 'Add new community', 'Save', and 'Reset'.

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

Buttons: Add new community, Save, Reset

This page includes the following fields:

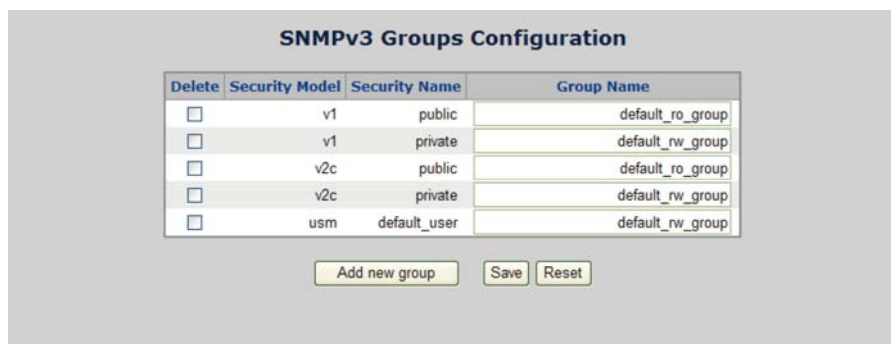
Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Source IP	Indicates the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

SNMPv3 Groups Configuration

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

The SNMPv3 Groups Configuration screen in Figure 4-28 appears.

Figure 4-28: SNMPv3 Groups Configuration page screenshot



The screenshot shows the 'SNMPv3 Groups Configuration' page. It features a table with four columns: 'Delete', 'Security Model', 'Security Name', and 'Group Name'. There are five rows of data: two for 'v1' (public and private), two for 'v2c' (public and private), and one for 'usm' (default_user). The Group Name field contains values like 'default_ro_group' and 'default_rw_group'. Below the table are three buttons: 'Add new group', 'Save', and 'Reset'.

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Buttons: Add new group, Save, Reset

This page includes the following fields:

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

SNMPv3 Users Configuration

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

The SNMPv3 Users Configuration screen in Figure 4-29 appears.

Figure 4-29: SNMPv3 Users Configuration page screenshot

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

This page includes the following fields:

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

SNMPv3 Views Configuration

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

The SNMPv3 Views Configuration screen in Figure 4-30 appears.

Figure 4-30: SNMPv3 Views Configuration page screenshot

This page includes the following fields:

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

Port Management

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

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

Port Configuration

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

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

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

The Port Configuration screen in Figure 4-31 appears.

Figure 4-31: Port Configuration page screenshot

Port Configuration for Switch 1

Total Power Usage: 47%

Port	Link	Speed		Flow Control			Maximum Frame	Excessive Collision Mode	Power Control	
		Current	Configured	Current Rx	Current Tx	Configured			Usage	Configured
1	Down	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	41%	Enabled ▼
2	Down	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	41%	Enabled ▼
3	Down	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	41%	Enabled ▼
4	Down	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	41%	Enabled ▼
5	Down	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	41%	Enabled ▼
6	Down	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	41%	Enabled ▼
7	100fdx	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	41%	Enabled ▼
8	1Gfdx	Auto	▼	X	X	<input type="checkbox"/>	9600	Discard ▼	92%	Enabled ▼
9	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
10	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
11	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
12	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
13	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
14	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
15	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
16	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
17	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
18	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
19	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
20	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
21	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
22	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
23	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			
24	Down	Auto	▼	X	X	<input type="checkbox"/>	9600			

Save Reset Refresh

This page includes the following fields:

Object	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	<p>Select any available link speed for the given switch port. Draw the menu bar to select the mode.</p> <p>Auto Speed - Setup Auto negotiation.</p> <p>10 half - Force sets 10Mbps/Half-Duplex mode.</p> <p>10 Full - Force sets 10Mbps/Full-Duplex mode.</p> <p>100 half - Force sets 100Mbps/Half-Duplex mode.</p> <p>100 full - Force sets 100Mbps/Full-Duplex mode.</p> <p>1000 full - Force sets 1000Mbps/Full-Duplex mode.</p> <p>Disable - Shutdown the port manually.</p>
Flow Control	<p>When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner.</p> <p>When a fixed-speed setting is selected, that is what is used.</p> <p>Current Rx column indicates whether pause frames on the port are obeyed.</p> <p>Current Tx column indicates whether pause frames on the port are transmitted.</p> <p>The Rx and Tx settings are determined by the result of the last Auto-Negotiation.</p> <p>Check the configured column to use flow control.</p> <p>This setting is related to the setting for Configured Link Speed.</p>
Maximum Frame	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Excessive Collision Mode	<p>Configure port transmit collision behavior.</p> <p>Discard: Discard frame after 16 collisions (default).</p> <p>Restart: Restart backoff algorithm after 16 collisions.</p>

Object	Description
Power Control	<p>The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port.</p> <p>Disabled: All power savings mechanisms disabled.</p> <p>ActiPHY: Link down power savings enabled.</p> <p>Dynamic: Link up power savings enabled.</p> <p>Enabled: Link up and link down power savings enabled.</p>
Total Power Usage	Total power usage in board, measured in percent.

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

Port Statistics Overview

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

The Port Statistics Overview screen in Figure 4-32 appears.

Figure 4-32: Port Statistics Overview page screenshot

Port Statistics Overview for Switch 1

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	0	0	0	0	0	0	0	0
2	890	85	119654	52257	5	0	5	0	121
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	5202636	568702	730401984	276389608	3	0	3	0	7095
8	466314	5002757	199898909	660350309	0	0	0	0	345
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
ST1	0	0	0	0	0	0	0	0	0
ST2	0	0	0	0	0	0	0	0	0

Auto-refresh ☐

The displayed counters are:

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

Detailed Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belongs to the currently selected stack unit, as reflected by the page header.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. The Detailed Port Statistics screen in Figure 4-33 appears.

Figure 4-33: Detailed Port Statistics Port 1 page screenshot

Detailed Port Statistics for Switch 1 Port 1			
Auto-refresh <input type="checkbox"/> Refresh Clear Port 1 ▼			
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	0	Tx Low	0
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

This page includes the following fields:

Receive Total and Transmit Total

Object	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Object	Description
Rx Drops	The number of frames dropped due to lack of receiving buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short frames received with valid CRC.
Rx Oversize	The number of long frames received with valid CRC.
Rx Fragments	The number of short ¹ frames received with invalid CRC.
Rx Jabber	The number of long ² frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

Receive Error Counters

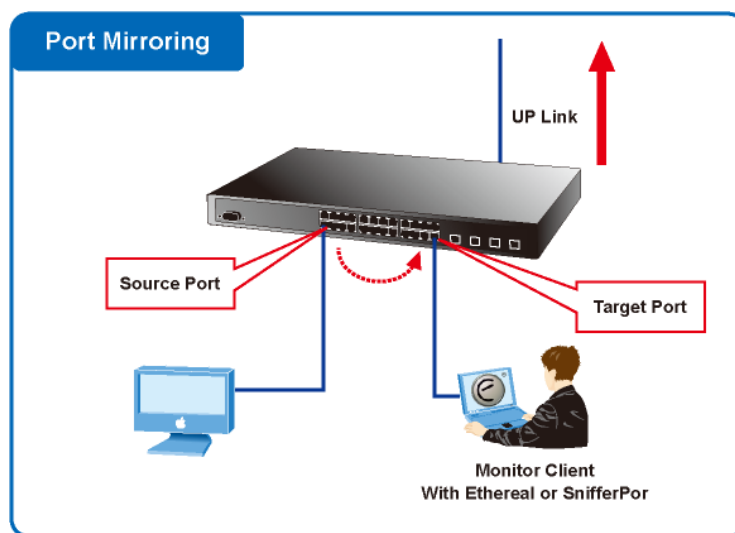
Object	Description
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

Port Mirroring Configuration

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

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

Figure 4-34: Port Mirror application



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

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

Mirror Port Configuration

The Port Mirror Configuration screen in Figure 4-35 and Figure 4-36 appears.

- GE-DSG Standalone Switch

Figure 4-35: Port Mirror Configuration page screenshot

Port Mirror Configuration

Stack Global Settings

Port to mirror to: Disabled

Switch to mirror to: Switch 1

Mirror Port Configuration for Switch 1

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

Save Reset

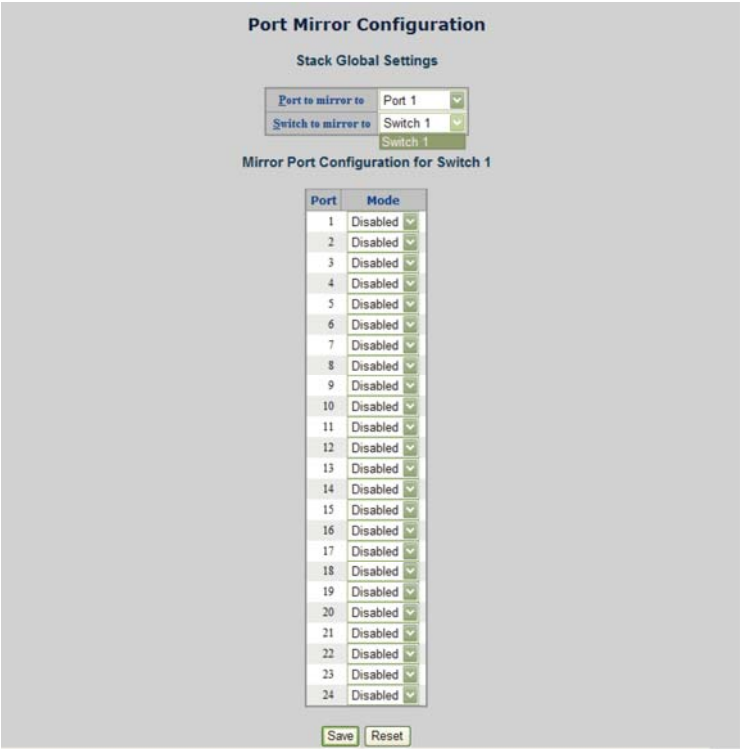
This page includes the following fields:

Object	Description
Port to mirror to	Frames from ports that have either source or destination mirroring enabled are mirrored to this port. Disabled disables mirroring.
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode.
Rx only	Frames received at this port are mirrored to the mirroring port. Frames transmitted are not mirrored.
Tx only	Frames transmitted from this port are mirrored to the mirroring port. Frames received are not mirrored.
Disabled	Neither frames transmitted nor frames received are mirrored.
Enabled	Frames received and frames transmitted are mirrored to the mirror port.

GE-DSSG-244 series Stackable Switch

The GE-DSSG-244 series Stackable switch supports port mirror function over stack switch.

Figure 4-36: Port Mirror Configuration page screenshot



This page includes the following fields:

Object	Description
Switch to mirror to	Frames from ports that have either source or destination mirroring enabled are mirrored to this switch.

SFP Module Information

You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status, such as the transceiver type, speed, wavelength and supports distance of SFP module on a specific interface. You can also use the hyperlink of the port number to check the statistics on a specific interface.

Figure 4-37: SFP Module Information page screenshot

SFP Module Information for Switch 1

Port	Type	Speed	Wave Length(nm)	Distance(m)
1	---	---	---	---
2	---	---	---	---
3	---	---	---	---
4	---	---	---	---
5	---	---	---	---
6	---	---	---	---
7	---	---	---	---
8	---	---	---	---
9	---	---	---	---
10	---	---	---	---
11	---	---	---	---
12	---	---	---	---
13	---	---	---	---
14	---	---	---	---
15	---	---	---	---
16	---	---	---	---
17	---	---	---	---
18	---	---	---	---
19	---	---	---	---
20	---	---	---	---
21	---	---	---	---
22	---	---	---	---
23	---	---	---	---
24	---	---	---	---

Auto-refresh ☐

This page includes the following fields:

Object	Description
Type	Display the type of current SFP module, the possible types are: 1000Base-SX 1000Base-LX 100Base-FX
Speed	Display the speed of current SFP module, the speed value or description is get from the SFP module. Different vendors SFP modules might show different speed information
Wave Length(nm)	Display the wavelength of current SFP module, the wavelength value is get from the SFP module. Use this column to check if the wavelength values of two nodes are the matched while the fiber connection is failed.
Distance(m)	Display the supports distance of current SFP module, the distance value is getting from the SFP module.

Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

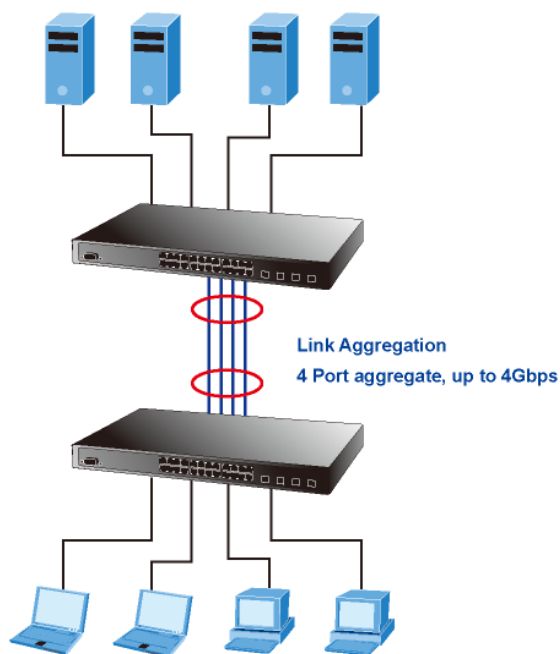
Aggregated Links can be assigned manually (Port Trunk) or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

The device supports the following Aggregation links:

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

Figure 4-38: Link Aggregation



The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high-speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ-45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 16 ports to be aggregated at the same time. The Managed Switch support Gigabit Ethernet ports (up to 12 groups). If the group is defined as a LACP static link aggregation group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregation group, then the number of ports must be the same as the group member ports.

The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reordering of frames within a flow is therefore not possible. The aggregation code is based on the following information:

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

Normally, all 5 contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 16 member ports. Any quantity of link aggregations may be configured for the device (only limited by the quantity of ports on the device.) To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

Static Aggregation Configuration

This page is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relate to the currently selected stack unit, as reflected by the page header.

Hash Code Contributors

Figure 4-39: Aggregation Mode Configuration page screenshot

		Port Members																							
Locality	Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Global	1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Global	2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Local	1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Local	2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Local	3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Local	4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Object	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the

Object	Description
	Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Static Aggregation Group Configuration

The Aggregation Group Configuration screen in Figure 4-40 appears.

Figure 4-40: Aggregation Group Configuration page screenshot

Aggregation Group Configuration for Switch 1

		Port Members																							
Locality	Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	Normal																								
Global	1																								
Global	2																								
Local	1																								
Local	2																								
Local	3																								
Local	4																								
Local	5																								
Local	6																								
Local	7																								
Local	8																								
Local	9																								
Local	10																								
Local	11																								
Local	12																								

Save Reset</

This page includes the following fields:

Object	Description
Locality	<p>Indicates the aggregation group type. This field is only valid for stackable switches.</p> <p>Global: The group members may reside on different units in the stack. The device supports two 8-port global aggregations.</p> <p>Local: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.</p>
Group ID	<p>Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.</p>
Port Members	<p>Each switch port is listed for each group ID. Select a radio button to</p>

Object	Description
	include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group.

LACP Configuration

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

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. The LACP port settings relate to the currently selected stack unit, as reflected by the page header. The LACP Port Configuration screen in Figure 4-41 appears.

Figure 4-41: LACP Port Configuration page screenshot

LACP Port Configuration for Switch 1

Port	LACP Enabled	Key	Role
1	<input type="checkbox"/>	Auto	Active
2	<input type="checkbox"/>	Auto	Active
3	<input type="checkbox"/>	Auto	Active
4	<input type="checkbox"/>	Auto	Active
5	<input type="checkbox"/>	Auto	Active
6	<input type="checkbox"/>	Auto	Active
7	<input type="checkbox"/>	Auto	Active
8	<input type="checkbox"/>	Auto	Active
9	<input type="checkbox"/>	Auto	Active
10	<input type="checkbox"/>	Auto	Active
11	<input type="checkbox"/>	Auto	Active
12	<input type="checkbox"/>	Auto	Active
13	<input type="checkbox"/>	Auto	Active
14	<input type="checkbox"/>	Auto	Active
15	<input type="checkbox"/>	Auto	Active
16	<input type="checkbox"/>	Auto	Active
17	<input type="checkbox"/>	Auto	Active
18	<input type="checkbox"/>	Auto	Active
19	<input type="checkbox"/>	Auto	Active
20	<input type="checkbox"/>	Auto	Active
21	<input type="checkbox"/>	Auto	Active
22	<input type="checkbox"/>	Auto	Active
23	<input type="checkbox"/>	Auto	Active
24	<input type="checkbox"/>	Auto	Active

Save Reset

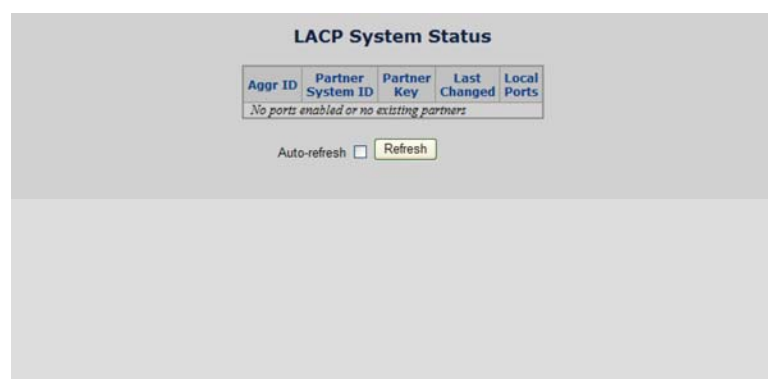
This page includes the following fields:

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

LACP System Status

This page provides a status overview for all LACP instances. The LACP Status page displays the current LACP aggregation Groups and LACP Port status. The LACP System Status screen in Figure 4-42 appears.

Figure 4-42: LACP System Status page screenshot



This page includes the following fields:

Object	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".

LACP Port Status

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

The LACP Port Status screen in Figure 4-43 appears.

Figure 4-43: LACP Port Status page screenshot

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-

Auto-refresh ☐

This page includes the following fields:

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

LACP statistics

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

The LACP statistics screen in Figure 4-44 appears.

Figure 4-44: LACP Port statistics page screenshot

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-

Auto-refresh ☐ Refresh

This page includes the following fields:

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

VLAN

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.

NOTES:

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

3. The Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

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

IEEE 802.1Q VLAN

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

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

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

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

This Managed Switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs

- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

IEEE 802.1Q VLAN Standard

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

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

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

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

Some relevant terms:

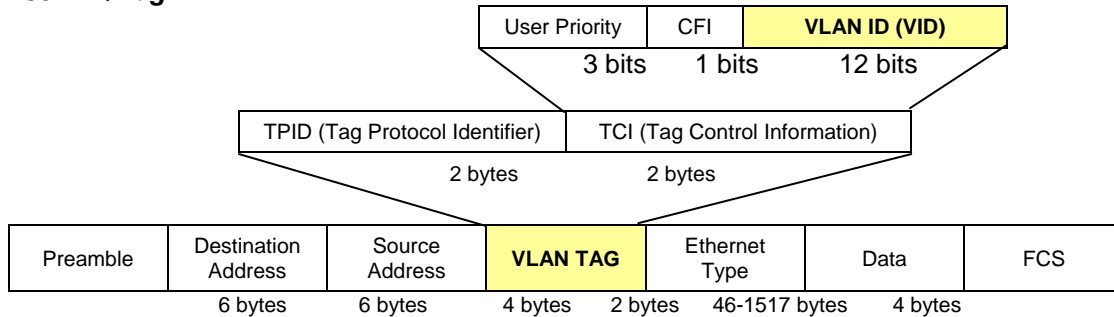
- Tagging - The act of putting 802.1Q VLAN information into the header of a packet.
- Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

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

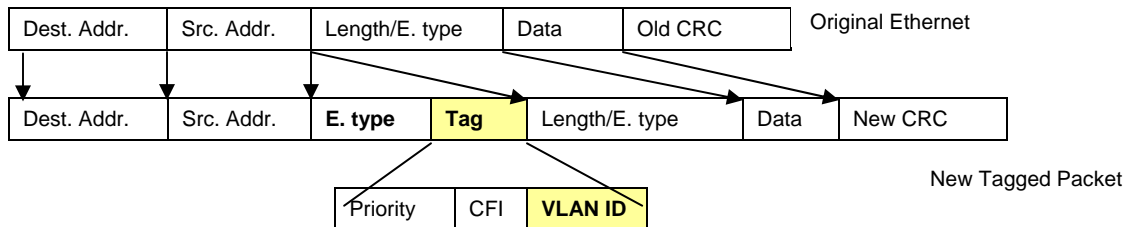
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



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

Adding an IEEE802.1Q Tag



Port VLAN ID

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

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

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

the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

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

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

Default VLANs

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

Assigning Ports to VLANs

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

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

Port Overlapping

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

Untagged VLANs

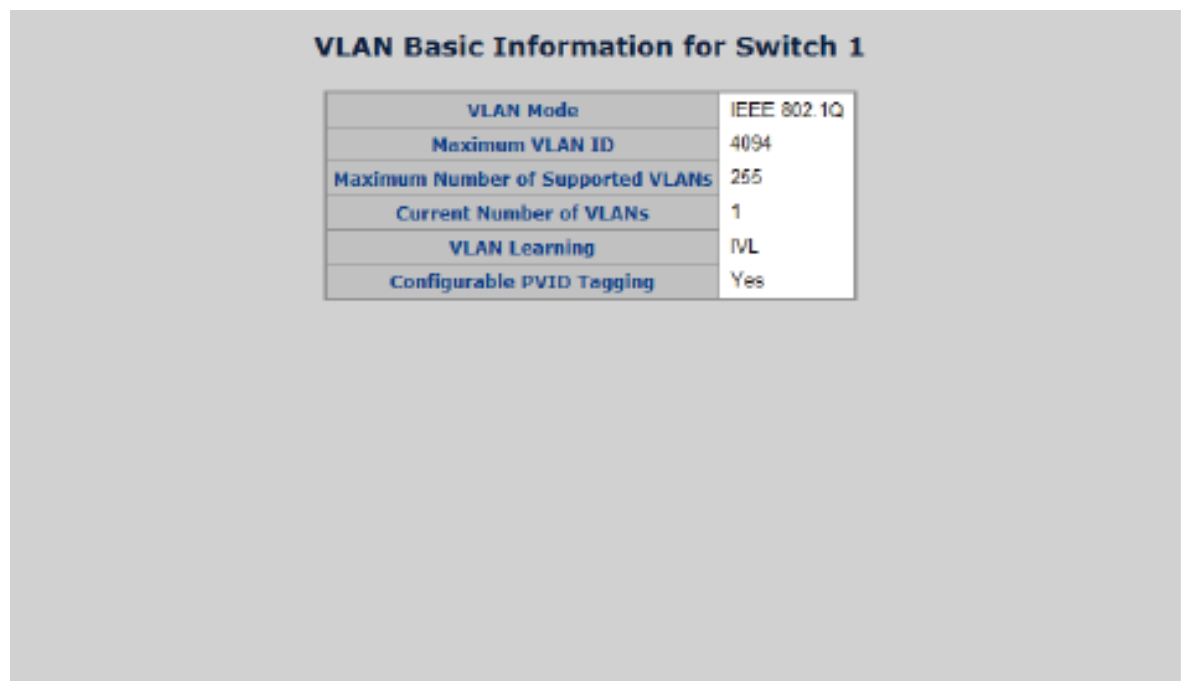
Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same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

VLAN Basic Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the Managed Switch.

The VLAN Basic Information screen in Figure 4-51 appears.

Figure 4-45: VLAN Basic Information page screenshot



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

This page includes the following fields:

Object	Description
VLAN Mode	Display the current VLAN mode used by this Managed Switch Port-Based

IEEE 802.1Q VLAN	
Maximum VLAN ID	Maximum VLAN ID recognized by this Managed Switch.
Maximum Number of Supported VLANs	Maximum number of VLANs that can be configured on this Managed Switch.
Current number of VLANs	Display the current number of VLANs
VLAN Learning	Display the VLAN learning mode. The Managed Switch supports IVL (IVL Independent vlan learning).

VLAN Port Configuration

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

Understand nomenclature of the Switch

- IEEE 802.1Q Tagged and Untagged

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

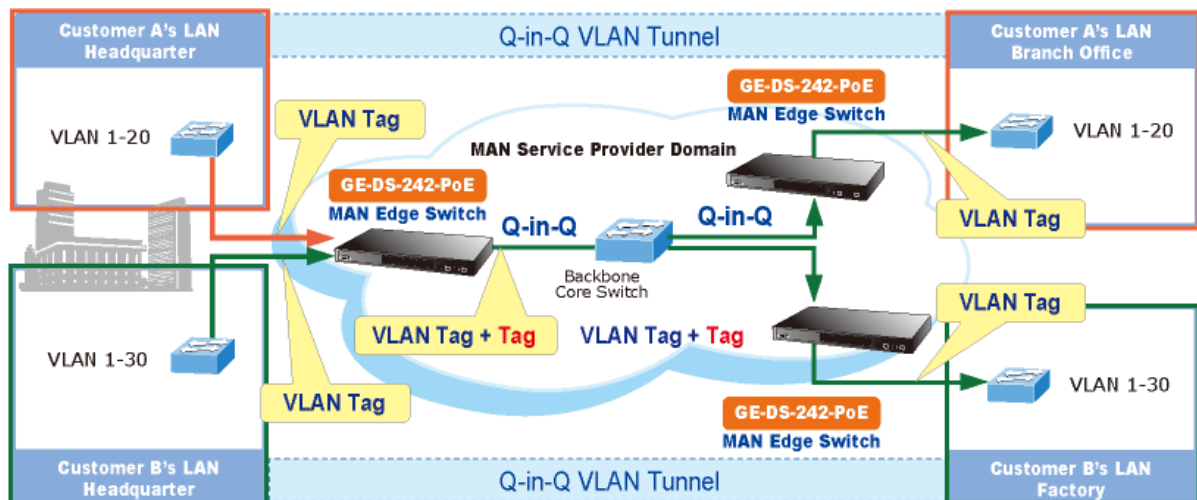
Tagged	Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag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

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

IEEE 802.1Q Tunneling (Q-in-Q)

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

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



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.

VLAN Port Configuration

The VLAN Port Configuration screen in Figure 4-46 appears.

Figure 4-46: VLAN Port Configuration page screenshot

VLAN Port Configuration for Switch 1

VLAN Mode IEEE 802.1Q

Port	PVID	Ingress Filtering	Acceptable Frame Type	Link Type	Q-in-Q Mode	Set out layer VLAN tag ether type
1	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
2	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
3	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
4	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
5	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
6	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
7	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
8	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
9	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
10	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
11	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
12	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
13	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
14	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
15	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
16	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
17	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
18	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
19	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
20	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
21	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
22	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
23	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag
24	1	<input type="checkbox"/>	All	UnTag	Disable	802.1Q Tag

Save Reset

This page includes the following fields:

Object	Description
Port	This is the logical port number for this row.
PVID	<p>Allow assign PVID for selected port. The range for the PVID is 1-4094.</p> <p>The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.</p>
Ingress Filtering	Enable ingress filtering for a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
Accept Frame Type	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
Link Type	<p>Allow 802.1Q Untagged or Tagged VLAN for selected port.</p> <p>When adding a VLAN to selected port, it tells the switch whether to keep or remove the tag from a frame on egress.</p> <p>Untag: outgoing frames without VLAN-Tagged.</p> <p>Tagged: outgoing frames with VLAN-Tagged.</p>
Q-in-Q Mode	<p>Sets the Managed Switch to QinQ mode, and allows the QinQ tunnel port to be configured. The default is for the Managed Switch to function in Disable mode.</p> <p>Disable The port operates in its normal VLAN mode. (This is the default.)</p> <p>MAN Port: Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network.</p> <p>Customer Port: Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.</p>
Set Out layer VLAN tag ether type	<p>The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel access port.</p> <p>802.1Q Tag : 8100</p> <p>vMAN Tag : 88A8</p> <p>Default : 802.1Q Tag</p>

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

VLAN Membership Configuration

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices.

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN. The VLAN Membership Configuration screen in Figure 4-47 appears.

Figure 4-47: VLAN Membership Configuration page screenshot

VLAN Membership Configuration for Switch 1

		Port Members																							
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

This page includes the following fields:

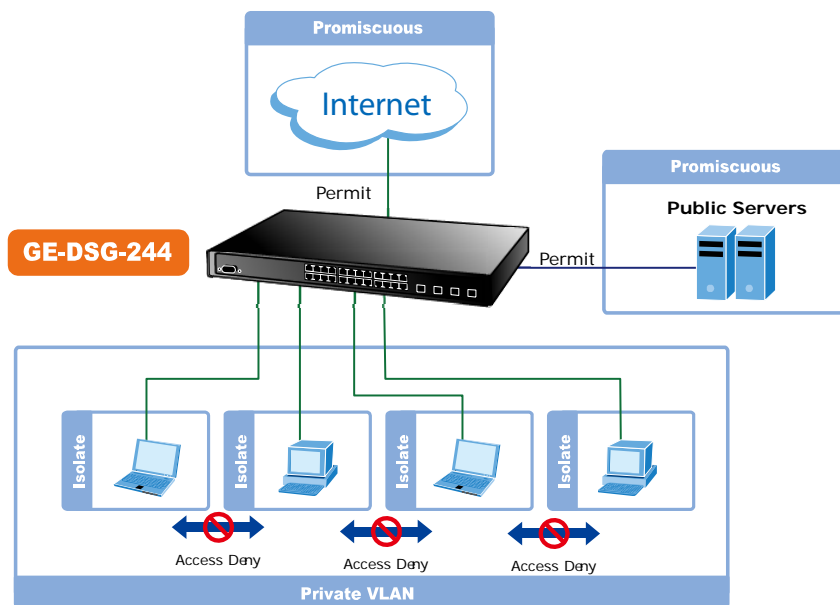
Object	Description
Delete	To delete a VLAN entry, check this box. The entry will be deleted on all stack switch units during the next Save.
VLAN ID	Indicates the ID of this particular VLAN.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check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

Private VLAN Configuration

Overview

When a VLAN is configured to be a private VLAN, communication between ports within that VLAN can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the same VLAN, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other.



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

- Promiscuous ports
 - Ports from which traffic can be forwarded to all ports in the private VLAN
 - Ports which can receive traffic from all ports in the private VLAN
- Isolated ports
 - Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN
 - Ports which can receive traffic from only promiscuous ports in the private VLAN

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

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

Figure 4-48: Private VLAN Configuration page screenshot

Port Isolation Configuration for Switch 1

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

This page includes the following fields:

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

Rapid Spanning Tree Protocol

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.

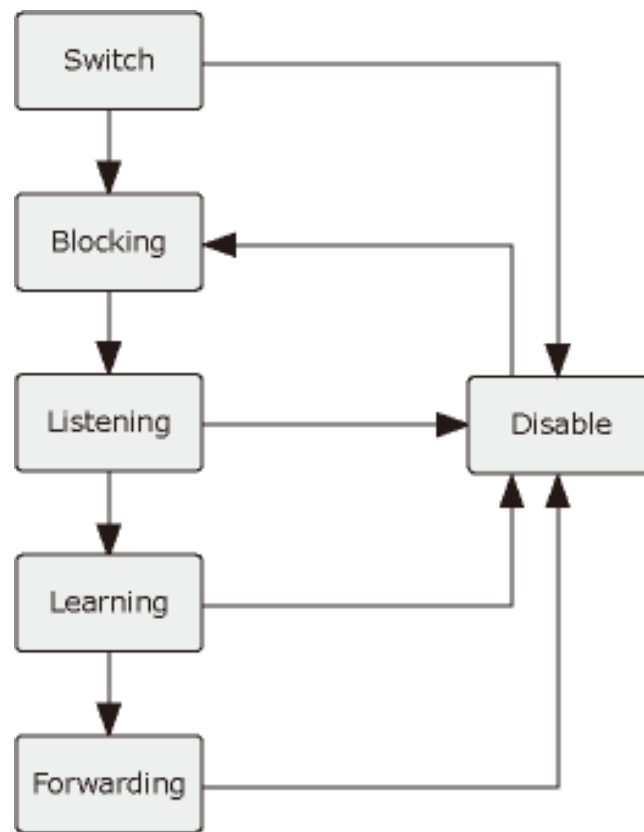
Each port on a switch using STP exists in one of the following five states:

- 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 4-49: 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 level:

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

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

Default Spanning-Tree Configuration

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

User-Changeable STA Parameters

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

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

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

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

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

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

NOTE: Observe the following formulas when setting the above parameters:

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

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

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

Illustration of STP

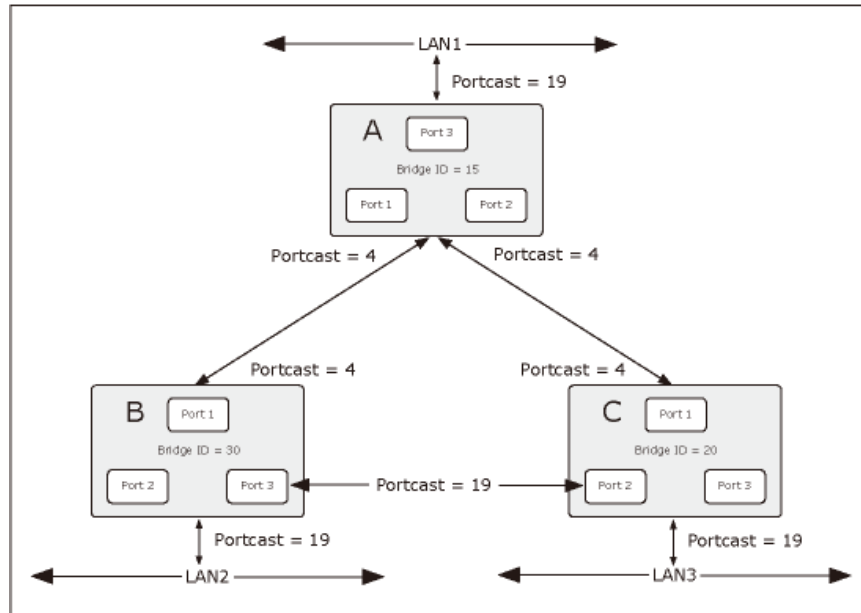
A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

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

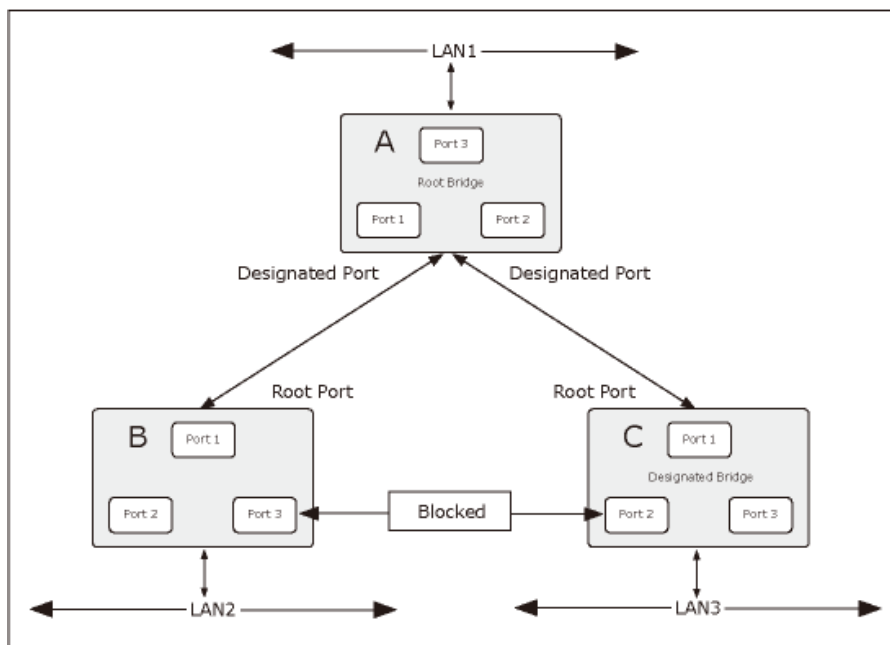
the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

Figure 4-50: Before Applying the STA Rules



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

Figure 4-51: 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 = 4) 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 = 19). 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 page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch or switch Stack. The Managed Switch support the following Spanning Tree protocols:

Compatible -- Spanning Tree Protocol (STP): Provides a single path between end stations, avoiding and eliminating loops.

Normal -- Rapid Spanning Tree Protocol (RSTP): Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.

The RSTP System Configuration screen in Figure 4-52 appears.

Figure 4-52: RSTP System Configuration page screenshot

RSTP System Configuration	
System Priority	32768
Max Age	20
Forward Delay	15
Protocol Version	Normal

Save Reset

This page includes the following fields:

Object	Description
System Priority	A value used to represent the priority component of a Bridge Identifier.
Max Age	<p>The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 200 seconds.</p> <p>-Default: 20</p> <p>-Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$.</p> <p>-Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$</p>
Forward Delay	<p>The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds</p> <p>-Default: 15</p> <p>-Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$</p> <p>-Maximum: 30</p>
Protocol Version	<p>The STP compatibility mode setting.</p> <p>Normal – Rapid STP (802.1w): Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.</p> <p>Compatible – Classis STP (802.1d): Provides a single path between end stations, avoiding and eliminating loops.</p>

NOTE: The Gigabit Ethernet Switch implement the Rapid Spanning Protocol as the default spanning tree protocol. While select **“Compatibles”** mode, the system uses the RSTP (802.1w) to be compatible with and co work with another STP (802.1d)’s BPDU control packets.

RSTP Bridge Status

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 4-53 appears.

Figure 4-53: RSTP Bridge Status page screenshot

VLAN ID	Active Ports	Bridge ID	Root			Topology Flag
			ID	Port	Cost	
1	0	32769:00-30-4f-24-24-24	32769:00-30-4f-24-24-24	-	0	Steady
0	0	32768:00-30-4f-24-24-24	32768:00-30-4f-24-24-24	-	0	Steady

Auto-refresh ☐

This page includes the following fields:

Object	Description
VLAN ID	The VLAN ID associated with this Bridge instance. This is also a link to the RSTP Detailed Bridge Status.
Active Ports	The number switch ports active in the RSTP bridge instance (aggregated ports count only as one).
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the <i>root</i> port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.

RSTP Port Configuration

This page allows the user to inspect the current RSTP port configurations, and possibly change them as well.

This page contains settings for aggregations and physical ports. The aggregation settings are stack global.

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

Figure 4-54: RSTP Port Configuration interface

RSTP Port Configuration

Aggregated Ports Configuration (Stack Global)

RSTP Enabled	Path Cost	Priority
<input type="checkbox"/>	Auto	128

Physical Ports Configuration for Switch 1

Port	RSTP Enabled Check all <input type="checkbox"/>	Path Cost	Priority	Edge	Point2point
1	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
13	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
14	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
15	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
16	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
17	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
18	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
19	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
20	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
21	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
22	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
23	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto
24	<input type="checkbox"/>	Auto	128	<input checked="" type="checkbox"/>	Auto

Save Reset

This page includes the following fields:

Object	Description
Port	The switch port number of the logical RSTP port.
RSTP Enabled	Controls whether RSTP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: 128 Range: 0-240, in steps of 16
Edge	Controls whether the port is known to connect directly to edge devices. (<i>no Bridges attached</i>). The Edge flag is cleared by receipt of any BPDUs on the port. Transitioning to the forwarding state is faster for edge ports than for other ports. (This applies to physical ports only. Aggregations are always <i>Non-Edge</i>).
Point2Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always <i>forced Point2Point</i>).

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

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

Table 4-3: Default STP Path Costs

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

RSTP Port Status

This page displays the RSTP port status for port physical ports in the currently selected switch.

The RSTP Port Status screen in Figure 4-55 appears.

Figure 4-55: RSTP Port Status page screenshot

RSTP Port Status for Switch 1

Port	Role	State	Bridge
1	Non-STP	Non-STP	-
2	Non-STP	Non-STP	-
3	Non-STP	Non-STP	-
4	Non-STP	Non-STP	-
5	Non-STP	Non-STP	-
6	Non-STP	Non-STP	-
7	Non-STP	Non-STP	-
8	Non-STP	Non-STP	-
9	Non-STP	Non-STP	-
10	Non-STP	Non-STP	-
11	Non-STP	Non-STP	-
12	Non-STP	Non-STP	-
13	Non-STP	Non-STP	-
14	Non-STP	Non-STP	-
15	Non-STP	Non-STP	-
16	Non-STP	Non-STP	-
17	Non-STP	Non-STP	-
18	Non-STP	Non-STP	-
19	Non-STP	Non-STP	-
20	Non-STP	Non-STP	-
21	Non-STP	Non-STP	-
22	Non-STP	Non-STP	-
23	Non-STP	Non-STP	-
24	Non-STP	Non-STP	-

Auto-refresh ☐

This page includes the following fields:

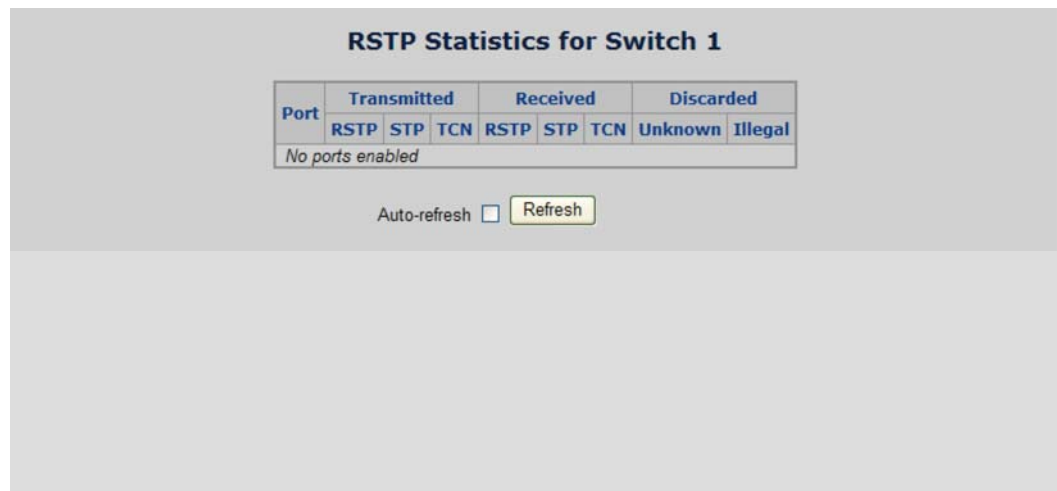
Object	Description
Port	The switch port number of the logical RSTP port.
Role	<p>The current RSTP port role. The port role can be one of the following values:</p> <p>Disabled</p> <p>Alternate</p> <p>Backup</p> <p>Root</p> <p>Designated</p> <p>Non-STP.</p>
State	<p>The current RSTP port state. The port state can be one of the following values:</p> <p>Disabled</p> <p>Blocking</p> <p>Learning</p> <p>Forwarding</p> <p>Non-STP.</p>
Bridge	The RSTP Bridge instance (VLAN ID). This is also a link to the RSTP Detailed Bridge Status, if the port is RSTP enabled.

RSTP Port Statistics

This page displays the RSTP port statistics counters for port physical ports in the currently selected switch.

The RSTP Port Statistics screen in Figure 4-56 appears.

Figure 4-56: RSTP Statistics page screenshot



This page includes the following fields:

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

Quality of Service

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.

QoS Terminology

- Classifier-classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- DiffServ Code Point (DSCP) - is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- Service Level-defines the priority that will be given to a set of classified traffic. You can create and modify service levels.

- Policy-comprises a set of "rules" that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- QoS Profile-consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- Rules-comprises a service level and a classifier to define how the Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

QoS Control List Configuration

This page lists the QCEs for a given QCL.

- Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.
- The classification is controlled by a QoS assigned to each port.
- A QCL consists of an ordered list of up to 12 QCEs.
- Each QCE can be used to classify certain frames to a specific QoS class.
- This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS Class for the port.

The QoS Control List Configuration screen in Figure 4-57 appears.







Figure 4-57: QoS Control List Configuration page screenshot

QoS Control List Configuration

QCL # 1

QCE Type	Type Value	Traffic Class
+		

This page includes the following fields:

Object	Description
QCL #	Select a QCL to display a table that lists all the QCEs for that particular QCL.
QCE Type	<p>Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported:</p> <p>Ethernet Type: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header.</p> <p>VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged.</p> <p>TCP/UDP Port: IPv4 TCP/UDP source/destination port.</p> <p>DSCP: IPv4 and IPv6 DSCP.</p> <p>ToS: The 3-precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field).</p> <p>Tag Priority: User Priority. Only applicable if the frame is VLAN tagged or priority tagged.</p>
Type Value	<p>Indicates the value according to its QCE type.</p> <p>Ethernet Type: The field shows the Ethernet Type value.</p> <p>VLAN ID: The field shows the VLAN ID.</p> <p>TCP/UDP Port: The field shows the TCP/UDP port range.</p> <p>DSCP: The field shows the IPv4/IPv6 DSCP value.</p>
Traffic Class	The QoS class associated with the QCE.
Modification Buttons	<p>You can modify each QCE in the table using the following buttons:</p> <p>: Inserts a new QCE before the current row.</p> <p>: Edits the QCE.</p> <p>: Moves the QCE up the list.</p> <p>: Moves the QCE down the list.</p> <p>: Deletes the QCE.</p> <p>: The lowest plus sign adds a new entry at the bottom of the list of QCL.</p>

QoS Control Entry Configuration

Configure a new QoS Control Entry on this page.

Frames can be classified by up to 4 different QoS classes: **Low**, **Normal**, **Medium**, and **High**.

The classification is controlled by a QCL assigned to each port.

A QCL consists of an ordered list of up to **12** QCEs.

Each QCE can be used to classify certain frames to a specific QoS Class.

This classification can be based on parameters such as **VLAN ID**, **UDP/TCP port**, **IPv4/IPv6 DSCP** or **Tag Priority**. Frames not matching any of the QCEs are classified to the default QoS Class for the port.

The QCE Configuration screen in Figure 4-58 appears.

Figure 4-58: QoS Configuration page screenshot

This page includes the following fields:

Object	Description
QCE Type	<p>Select the available type for the specific QCE.</p> <p>Ethernet Type: Matches the received frame's EtherType against the QCE Key.</p> <p>VLAN ID: Matches the frame's VID against the QCE Key.</p> <p>TCP/UDP Port: Matches the destination port and the source port against the QCE Key.</p> <p>DSCP: Matches the received IPv4/IPv6 DSCP value (6 bits) against the two DSCP values in the QCE Key.</p> <p>ToS: Uses the precedence part of the IPv4/IPv6 ToS (3 bits) as an index to the eight QoS Class values in the QCE Key.</p> <p>Tag Priority: Uses the User Priority value (3 bits) as an index to the eight QoS Class values in the QCE Key.</p>

Object	Description
Type Value	<p>Configure the values according to the QCE type you select.</p> <p>Ethernet Type: The allowed values for this type range from 0x600 (1536) to 0xFFFF (65535).</p> <p>VLAN ID: The allowed values for this type range from 1 to 4095.</p> <p>TCP/UDP Port Range: Specify whether there is a range or a specific port number. The port range allowed is from 0 to 65535.</p> <p>DSCP: The allowed range is 0 to 63. ToS or Tag Priority do not have type value settings.</p>
Traffic Class	<p>Select a traffic class of Low, Normal, Medium, or High to apply to the QCE.</p> <p>If the QCE type is ToS or Tag Priority, there are 8 rows of traffic class that can be configured for each priority.</p>

Port QoS Configuration

This page allows you to configure QoS settings for each port.

- Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.
- The classification is controlled by a QCL that is assigned to each port.
- A QCL consists of an ordered list of up to 12 QCEs.
- Each QCE can be used to classify certain frames to a specific QoS class.
- This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.
- Frames not matching any of the QCEs are classified to the default QoS class for the port.
- The settings relate to the currently selected stack unit, as reflected by the page header.

The Port QoS Configuration screen in Figure 4-59 appears.

Figure 4-59: Port QoS Configuration page screenshot

Port QoS Configuration

Stack Global Settings

Number of Classes 4

Settings for Switch 1

Port	Default Class	QCL #	User Priority	Queuing Mode	Queue Weighted			
					Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Strict Priority	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8
13	Low	1	0	Strict Priority	1	2	4	8
14	Low	1	0	Strict Priority	1	2	4	8
15	Low	1	0	Strict Priority	1	2	4	8
16	Low	1	0	Strict Priority	1	2	4	8
17	Low	1	0	Strict Priority	1	2	4	8
18	Low	1	0	Strict Priority	1	2	4	8
19	Low	1	0	Strict Priority	1	2	4	8
20	Low	1	0	Strict Priority	1	2	4	8
21	Low	1	0	Strict Priority	1	2	4	8
22	Low	1	0	Strict Priority	1	2	4	8
23	Low	1	0	Strict Priority	1	2	4	8
24	Low	1	0	Strict Priority	1	2	4	8

This page includes the following fields:

Object	Description
Number of Classes	Configure the number of traffic classes as "1", "2", or "4". The default value is "4".
Port	The logical port for the settings contained in the same row.
Default Class	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
QCL #	Select which QCL to use for the port.
User Priority	Select the default user priority for this port when adding a Tag to the untagged frames.

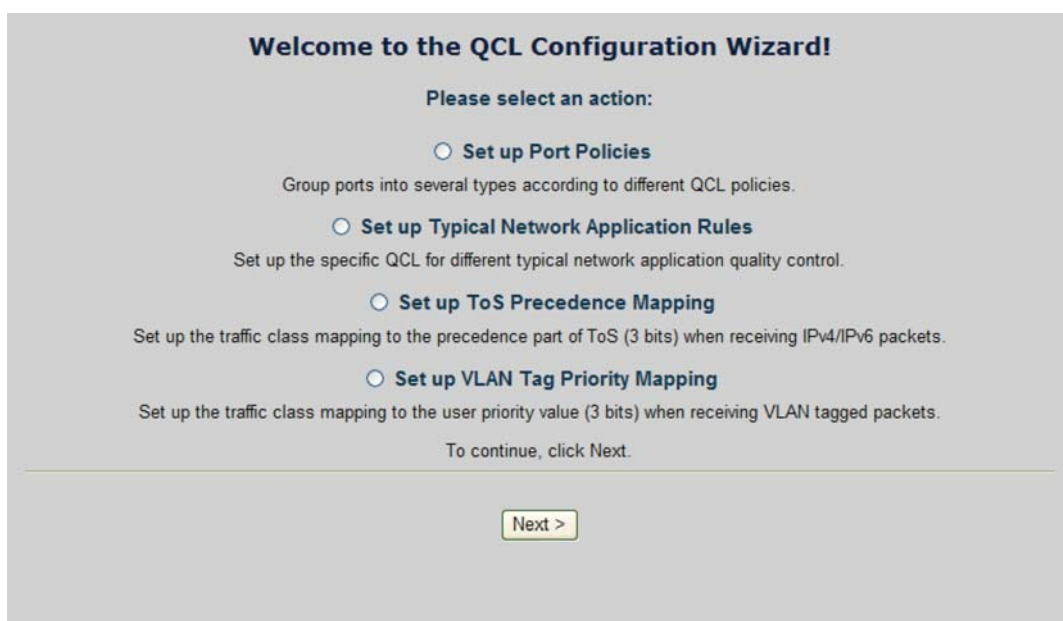
Queuing Mode	Select which Queuing mode for this port.
Queue Weighted	Setting Queue weighted (Low: Normal: Medium: High) if the "Queuing Mode" is "Weighted".

QCL Configuration Wizard

This handy wizard helps you set up a QCL quickly.

The QCL Configuration Wizard screen in Figure 4-60 appears.

Figure 4-60: Port QoS Configuration page screenshot



This page includes the following fields:

Object	Description
Set up Port Policies	Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules	Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping	Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping	Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

Set up Policy Rules

Group ports into several types according to different QCL policies. The settings relate to the currently selected stack unit, as reflected by the page header. The screen in Figure 4-61 appears.

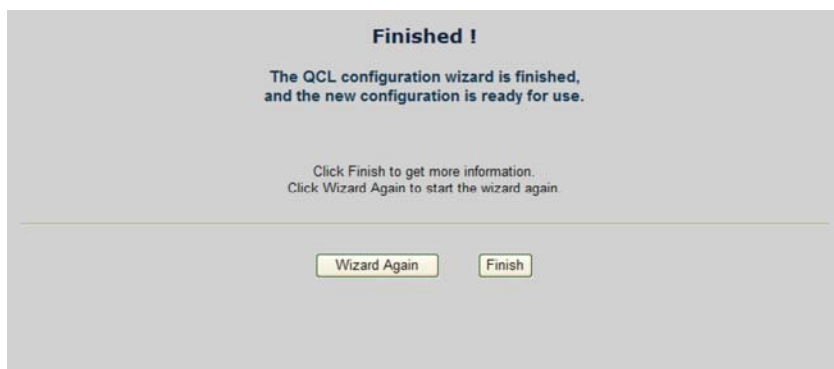
Figure 4-61: Set up Policy Rules page screenshot

	Port Members																							
QCL ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

This page includes the following fields:

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

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



Set up Typical Network Application Rules

Set up the specific QCL for different typical network application quality control.

STEP-1

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

Figure 4-62: Set up Typical Network Application Rules page screenshot

This page includes the following fields:

Object	Description
Audio and Video	<p>Indicates the common servers that apply to the specific QCE .</p> <p>The common servers are:</p> <p>QuickTime 4 Server</p> <p>MSN Messenger Phone</p> <p>Yahoo Messenger Phone</p> <p>Napster</p> <p>Real Audio</p>
Games	Indicates the common games that apply to the specific QCE.
User Definition	<p>Indicates the user definition that applies to the specific QCE. The user definitions are:</p> <p>Ethernet Type: Specify the Ethernet Type filter for this QCE. The allowed range is 0x600 to 0xFFFF.</p> <p>VLAN ID: VLAN ID filter for this QCE. The allowed range is 1 to 4095.</p> <p>UDP/TCP Port: Specify the TCP/UDP port filter for this QCE. The allowed range is 0 to 65535.</p> <p>DSCP: Specify the DSCP filter for this QCE. The allowed range is 0 to 63.</p>

Buttons

Cancel Wizard: Click to cancel the wizard.

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

Next >: Click to continue the wizard.

STEP-2

According to your selection on the previous page, this wizard will create specific QCEs (QoS Control Entries) automatically.

First select the QCL ID for these QCEs, and then select the traffic class. Different parameter options are displayed depending on the frame type that you selected.

Figure 4-63: Set up Typical Network Application Rules page 2 screenshot

Set up Typical Network Application Rules

According to your selection on the previous page, this wizard will create specific QCEs (QoS Control Entries) automatically.

First select the QCL ID for these QCEs, and then select the traffic class. Different parameter options are displayed, depending on your selection.

QCL ID

1

Traffic Class

Low

Low

Normal

Medium

High

Cancel Wizard

< Back

Next >

This page includes the following fields:

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

Set up ToS Precedence Mapping

Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets. The screen in Figure 4-64 appears.

Figure 4-64: Set up ToS Precedence Mapping page screenshot

Set up ToS Precedence Mapping

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

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

This page includes the following fields:

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

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

QoS Control List Configuration

QCL # 1

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

Set up VLAN Tag Priority Mapping

Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets. The screen in Figure 4-65 appears.

Figure 4-65: Set up VLAN Tag Priority Mapping

Set up VLAN Tag Priority Mapping

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

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

Cancel Wizard < Back Next >

This page includes the following fields:

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

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



QoS Statistics

This page provides statistics for the different queues for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header. The QoS Statistics screen in Figure 4-66 appears.

Figure 4-66: QoS Statistics page screenshot

QoS Statistics for Switch 1

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	876	0	0	0	0	0	9	85
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	68423963	431542	0	0	0	0	9406	189409
8	433865	68204050	0	0	0	0	103222	1245
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
ST1	0	0	0	0	0	0	0	0
ST2	0	0	0	0	0	0	0	0

Auto-refresh ☐ Refresh Clear

This page includes the following fields:

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

Bandwidth Control

Configure the switch port rate limit for Policers and Shapers on this page. The settings relate to the currently selected stack unit, as reflected by the page header. The screen Bandwidth Control in Figure 4-67 appears.

Figure 4-67: Bandwidth Control page screenshot

Bandwidth Control Configuration for Switch 1

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
9	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
10	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
11	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
12	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
13	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
14	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
15	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
16	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
17	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
18	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
19	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
20	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
21	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
22	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
23	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps
24	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	500	kbps

This page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row.
Policer Enabled	Enable or disable the port policer. The default value is "Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is

Object	Description
	"Mbps"
Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Shaper Unit	Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is "kbps".

Storm Control Configuration

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

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

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

The Storm Control Configuration screen in Figure 4-68 appears.

Figure 4-68: Storm Control Configuration page screenshot

The screenshot shows the "Storm Control Configuration" page. It contains a table with three columns: "Frame Type", "Status", and "Rate (pps)". There are three rows for "Unicast", "Multicast", and "Broadcast". Each row has a checkbox in the "Status" column and a dropdown menu in the "Rate (pps)" column. Below the table are "Save" and "Reset" buttons.

Frame Type	Status	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Save Reset

This page includes the following fields:

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

Multicast

IGMP Snooping

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

About the Internet Group Management Protocol (IGMP) Snooping

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

Figure 4-69: Multicast Service

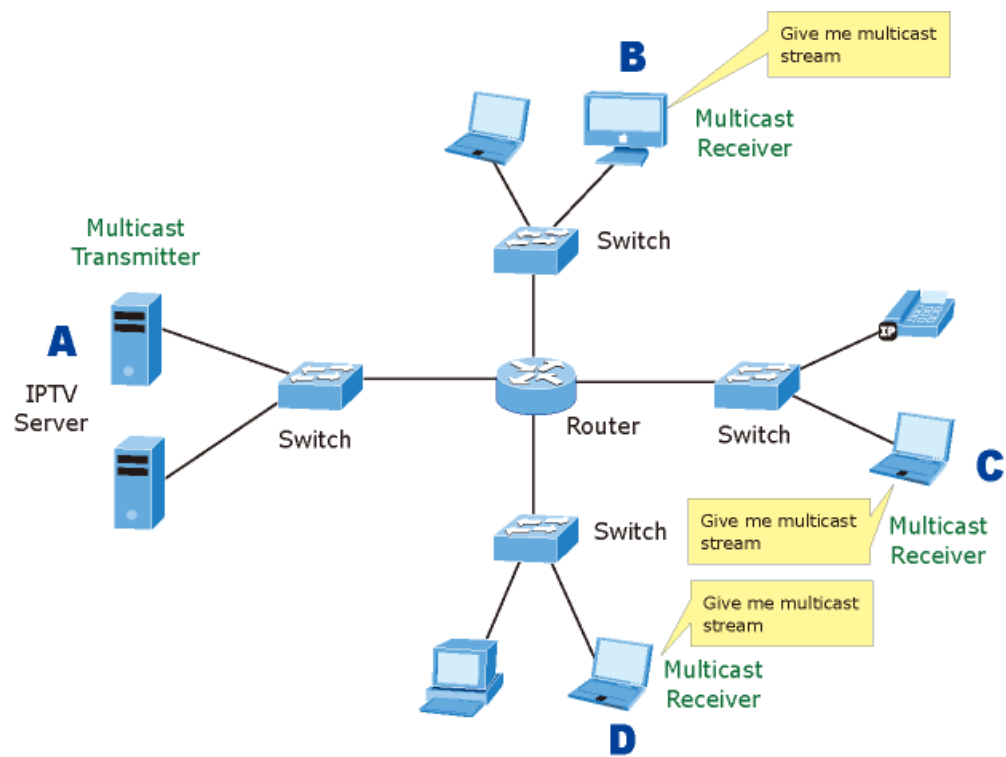


Figure 4-70: Multicast flooding

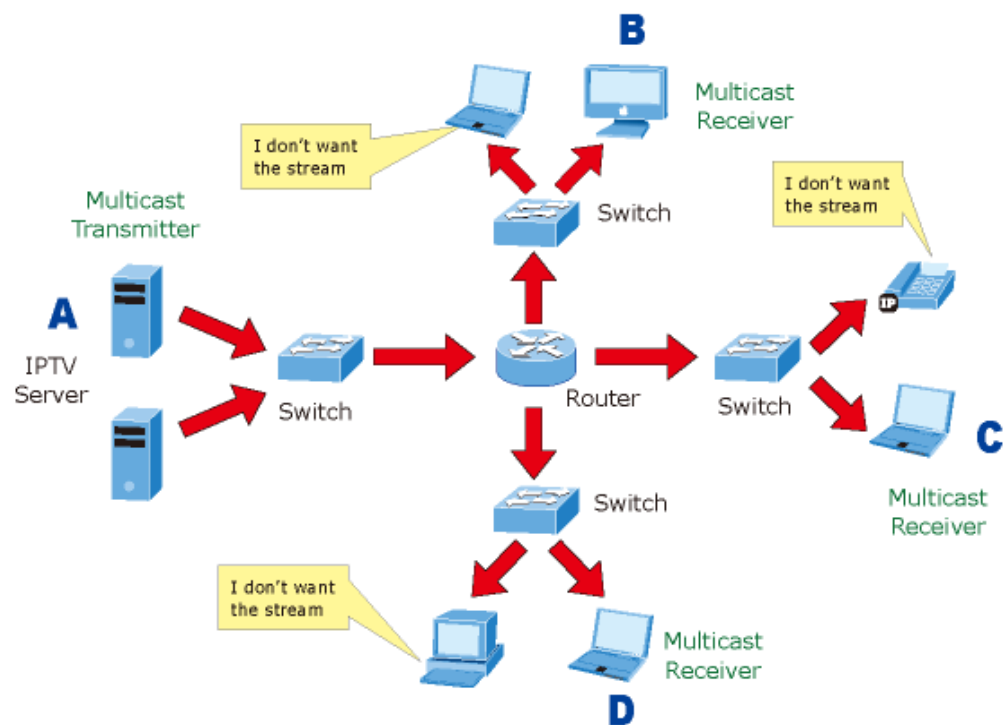
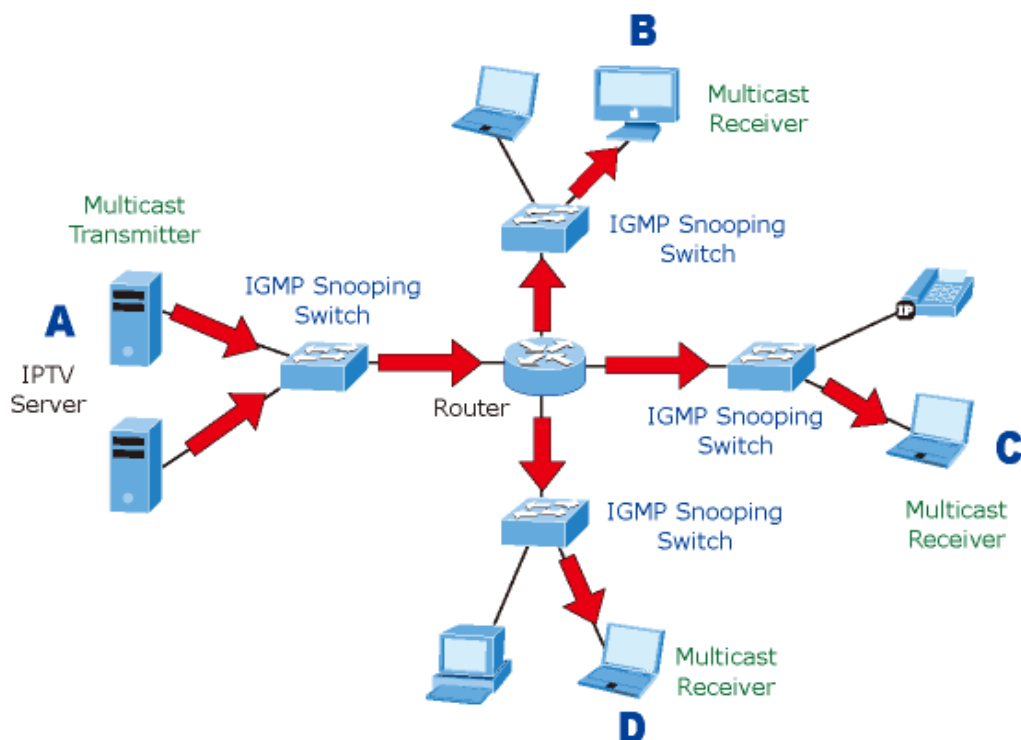


Figure 4-71: IGMP Snooping multicast stream control



IGMP Versions 1 and 2

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

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

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

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

The IGMP Type codes are shown below:

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

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

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

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

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

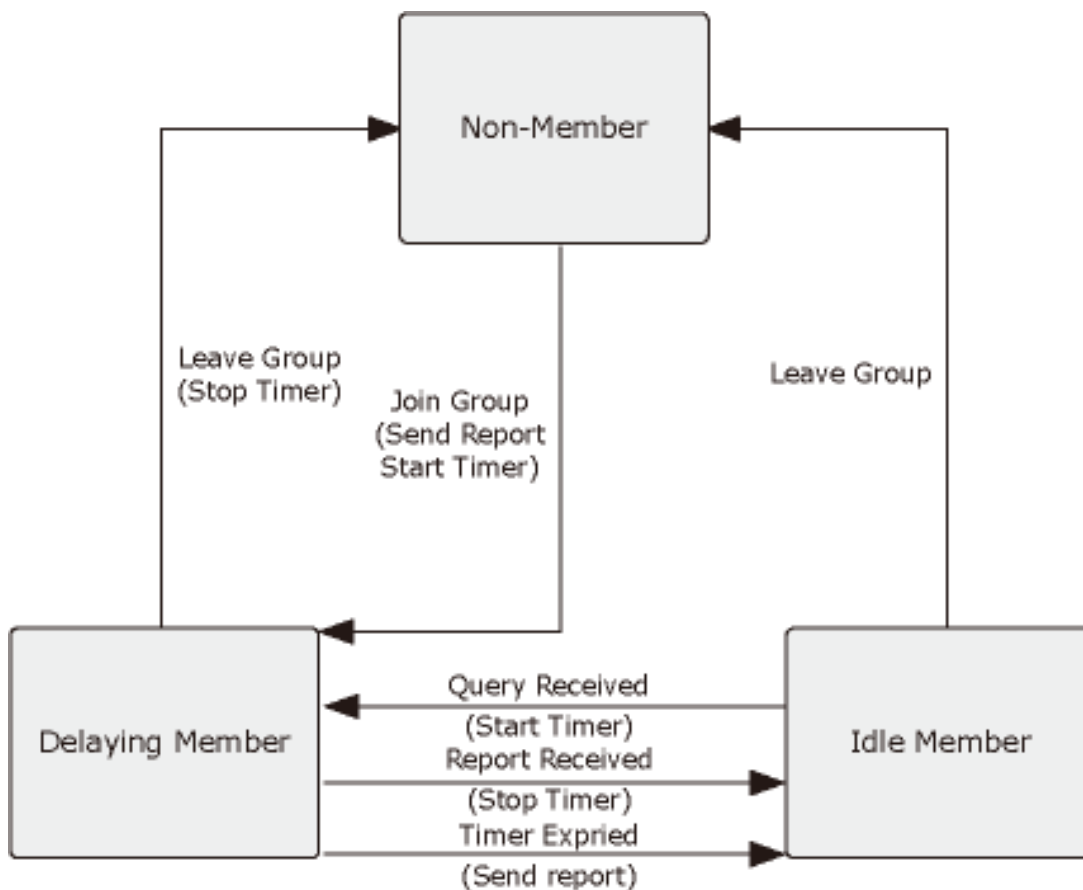
Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

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

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

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

Figure 4-72: 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 Snooping Configuration

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

The IGMP Snooping Configuration screen in Figure 4-73 appears.

Figure 4-73: IGMP Snooping Configuration page screenshot

IGMP Snooping

IGMP Protocol:	Enable
IGMP fastleave:	Enable
IGMP Querier:	Enable
Multicast Group	
Ip_Address	VID
MemberPort	
Apply	

This page includes the following fields:

Object	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.

IGMP Port Related Configuration

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

The IGMP Port Related Configuration screen in Figure 4-74 appears.

Figure 4-74: IGMP Port Related Configuration page screenshot

IGMP Port Related Configuration for Switch 1

Port	Router Port	Fast Leave
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	<input type="checkbox"/>

This page includes the following fields:

Object	Description
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the Fast Leave on the port.

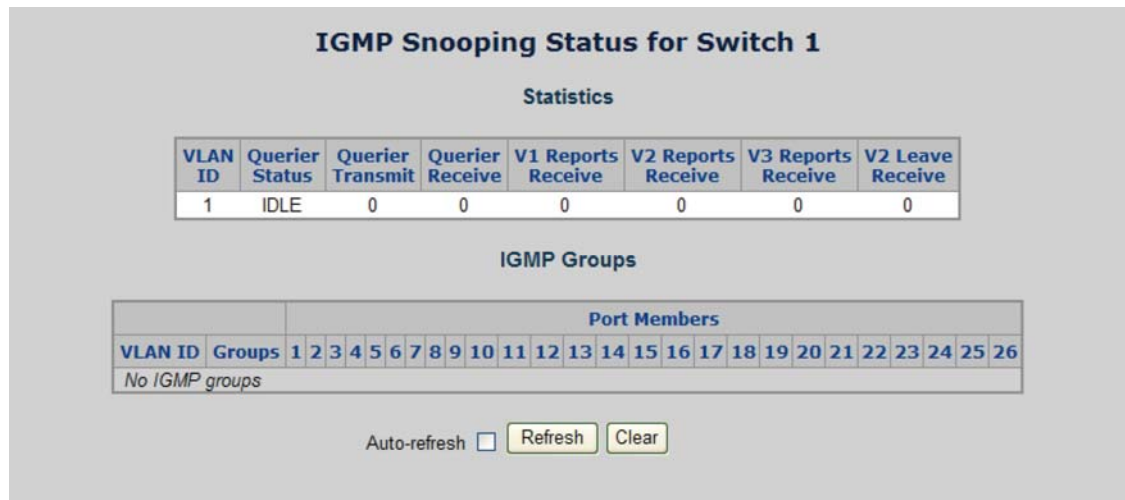
IGMP Snooping Status

This page provides IGMP Snooping status.

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

The IGMP Snooping status screen in Figure 4-75 appears.

Figure 4-75: IGMP Snooping status page screenshot



This page includes the following fields:

Object	Description
VLAN ID	The VLAN ID of the entry.
Groups	The present IGMP groups. Max. are 128 groups for each VLAN.
Port Members	The ports that are members of the entry.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Transmit	The number of Transmitted Querier.
Querier Receive	The number of Received Querier.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.

Multicast Address Table

The Multicast Address Table screen in Figure 4-76 appears.

Figure 4-76: Multicast Address Table page screenshot

[illegible]

This page includes the following fields:

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

IEEE 802.1X Network Access Control

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

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.

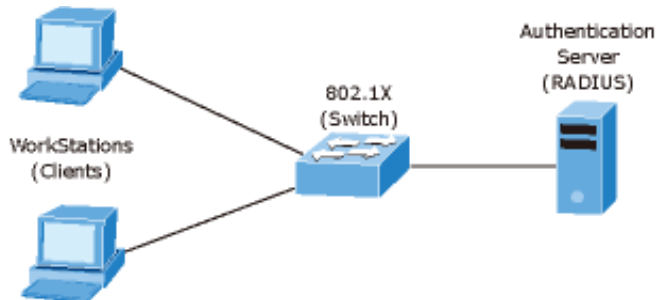
This section includes this conceptual information:

- 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 4-77: 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.

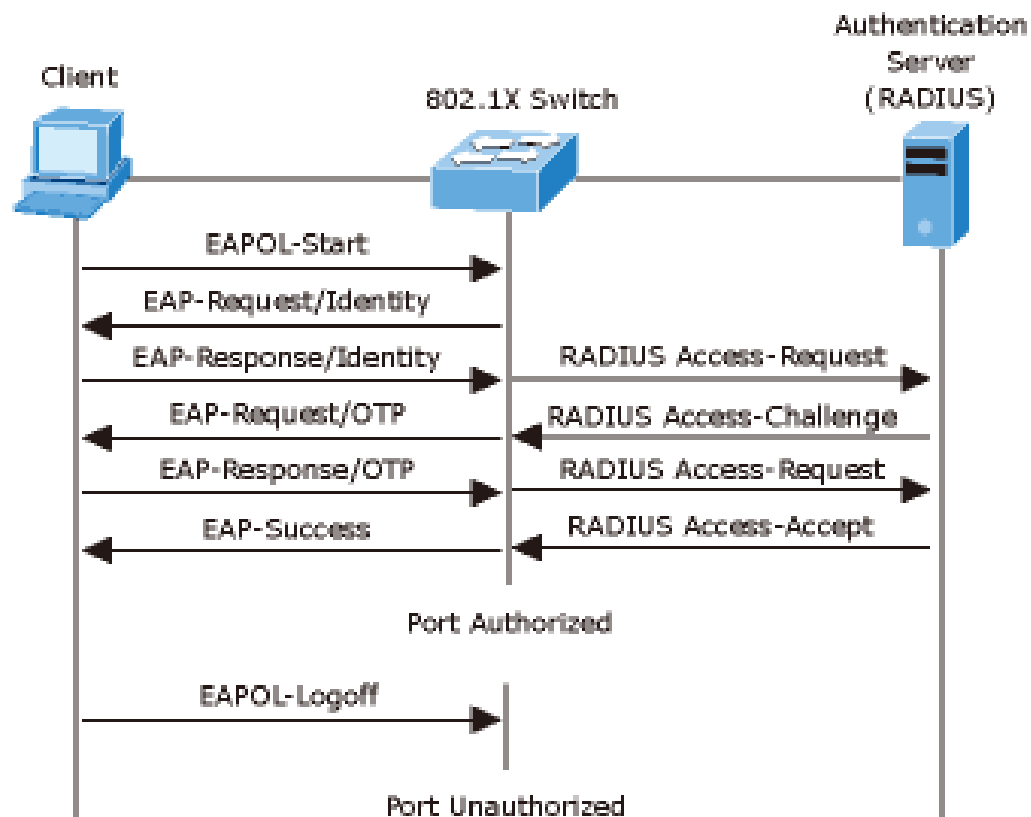
However, if during boot up, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

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 4-78" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 4-78: 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.

802.1X System Configuration

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

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

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

The 802.1X System Configuration screen in Figure 4-79 appears.

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

Figure 4-79: 802.1X Configuration page screenshot

802.1X Configuration for Switch 1

System Configuration (Stack Global)

Mode	Disabled
RADIUS IP	0.0.0.0
RADIUS Secret	
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAP Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds

Save Reset Refresh

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

This page includes the following fields:

Object	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switchstack. If globally disabled, all ports are allowed forwarding of frames.
RADIUS IP	The IP address of the RADIUS Server expressed in dotted decimal notation. If the RADIUS IP changes while the protocol is globally enabled, then all ports/clients will get reinitialized.
RADIUS Secret	The secret - up to 29 characters long - shared between the RADIUS Server and the switchstack.
Reauthentication Enabled	<p>If checked, clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port.</p> <p>For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).</p>
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

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

802.1X and MAC-Based Authentication Port Configuration

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

The 802.1X Port Configuration screen in Figure 4-80 appears.

Figure 4-80: 802.1X Port Configuration page screenshot

802.1X Port Configuration for Switch 1

Port	Admin State	Port State	Max Clients		Restart	
1	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
2	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
3	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
4	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
5	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
6	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
7	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
8	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
9	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
10	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
11	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
12	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
13	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
14	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
15	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
16	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
17	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
18	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
19	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
20	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
21	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
22	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
23	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize
24	Authorized	802.1X Disabled	All	1536	Reauthenticate	Reinitialize

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

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

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

Object	Description
	<p>Admin State is "Auto" or "MAC-Based".</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized.</p> <p>Reinitialize: Forces a reinitialization of the port/clients and thereby a reauthentication immediately. The port/clients will transfer to the unauthorized state while the reauthentication is ongoing.</p>

802.1X Port Status

This page provides an overview of the current IEEE 802.1X port states for the selected switch. The 802.1X Port Status screen in Figure 4-81 appears.

Figure 4-81: 802.1X Status page screenshot

Port	State	Last Source	Last ID
1	802.1X Disabled		
2	802.1X Disabled		
3	802.1X Disabled		
4	802.1X Disabled		
5	802.1X Disabled		
6	802.1X Disabled		
7	802.1X Disabled		
8	802.1X Disabled		
9	802.1X Disabled		
10	802.1X Disabled		
11	802.1X Disabled		
12	802.1X Disabled		
13	802.1X Disabled		
14	802.1X Disabled		
15	802.1X Disabled		
16	802.1X Disabled		
17	802.1X Disabled		
18	802.1X Disabled		
19	802.1X Disabled		
20	802.1X Disabled		
21	802.1X Disabled		
22	802.1X Disabled		
23	802.1X Disabled		
24	802.1X Disabled		

Auto-refresh ☐ Refresh

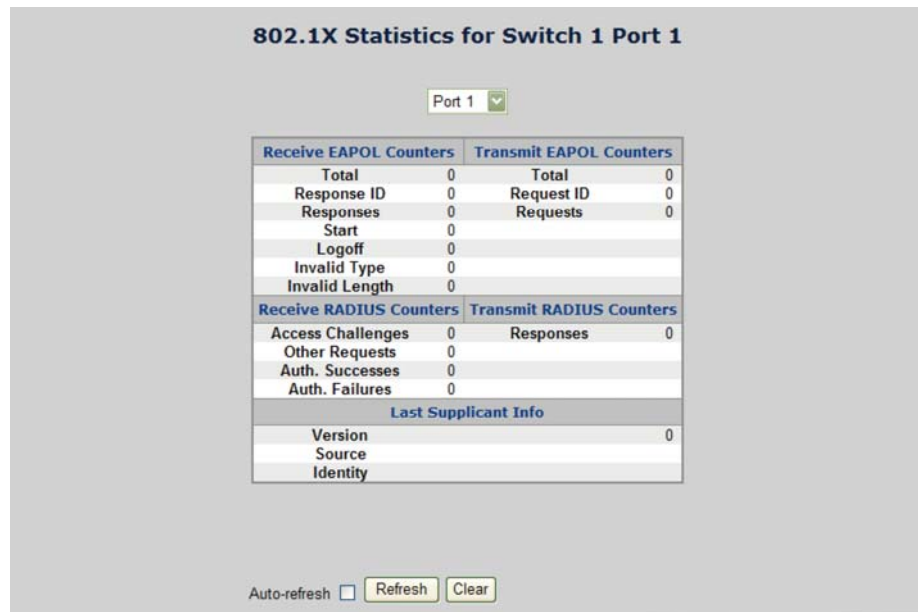
This page includes the following fields:

Object	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
State	The current state of the port. Refer to IEEE 802.1X Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for port-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame for port-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

802.1X and MAC-Based Authentication Statistics

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected RADIUS statistics, only. Use the port select box to select which port details to be displayed. The 802.1X and MAC-Based Authentication Statistics screen in Figure 4-82 appears.

Figure 4-82: 802.1X Statistics Port 1 page screenshot



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

EAPOL Counters

These counters are not available for MAC-based ports.

Supplicant frame counter statistics. There are seven receiving frame counters and three transmitting frame counters.

EAPOL Counters			
Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAP Resp/ID frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response

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

RADIUS Counters

RADIUS Server frame counter statistics.

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

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

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

RADIUS Counters			
Direction	Name	IEEE Name	Description
			<p>Indicates that the RADIUS server has communication with the switch.</p> <p>MAC-based:</p> <p>Counts all Access Challenges received from the RADIUS server for this port (left-most table) or client (right-most table).</p>
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	<p>Port-based:</p> <p>Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the RADIUS server chose an EAP-method.</p> <p>MAC-based:</p> <p>Not applicable.</p>
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	<p>Port- and MAC-based:</p> <p>Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the RADIUS server.</p>
Rx	Auth. Failures	dot1xAuthBackendAuthFailures	<p>Port- and MAC-based:</p> <p>Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the RADIUS server.</p>
Tx	Responses	dot1xAuthBackendResponses	<p>Port-based:</p> <p>Counts the number of times that the switch attempts to send a supplicant's first response packet to the RADIUS server. Indicates the switch attempted communication with the RADIUS server. Possible retransmissions are not counted.</p> <p>MAC-based:</p> <p>Counts all the RADIUS packets sent from the switch towards the RADIUS server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</p>

Last Supplicant/Client Info

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

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

Last Supplicant/Client Info		
Name	IEEE Name	Description
Version	dot1xAuthLastEapolFrameVersion	Port-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Source	dot1xAuthLastEapolFrameSource	Port-based: The source MAC address carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity or (Last) Client	-	Port-based: The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame. MAC-based: The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).

Clients attached to this port

This table is only available for MAC-based ports

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

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

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

Windows Platform RADIUS Server Configuration

Setup the RADIUS server and assign the client IP address to the Managed switch. In this case, field in the default IP Address of the Managed Switch with 192.168.0.100. And also make sure the shared secret key is as same as the one you had set at the Managed Switch's 802.1x system configuration - 12345678 at this case.

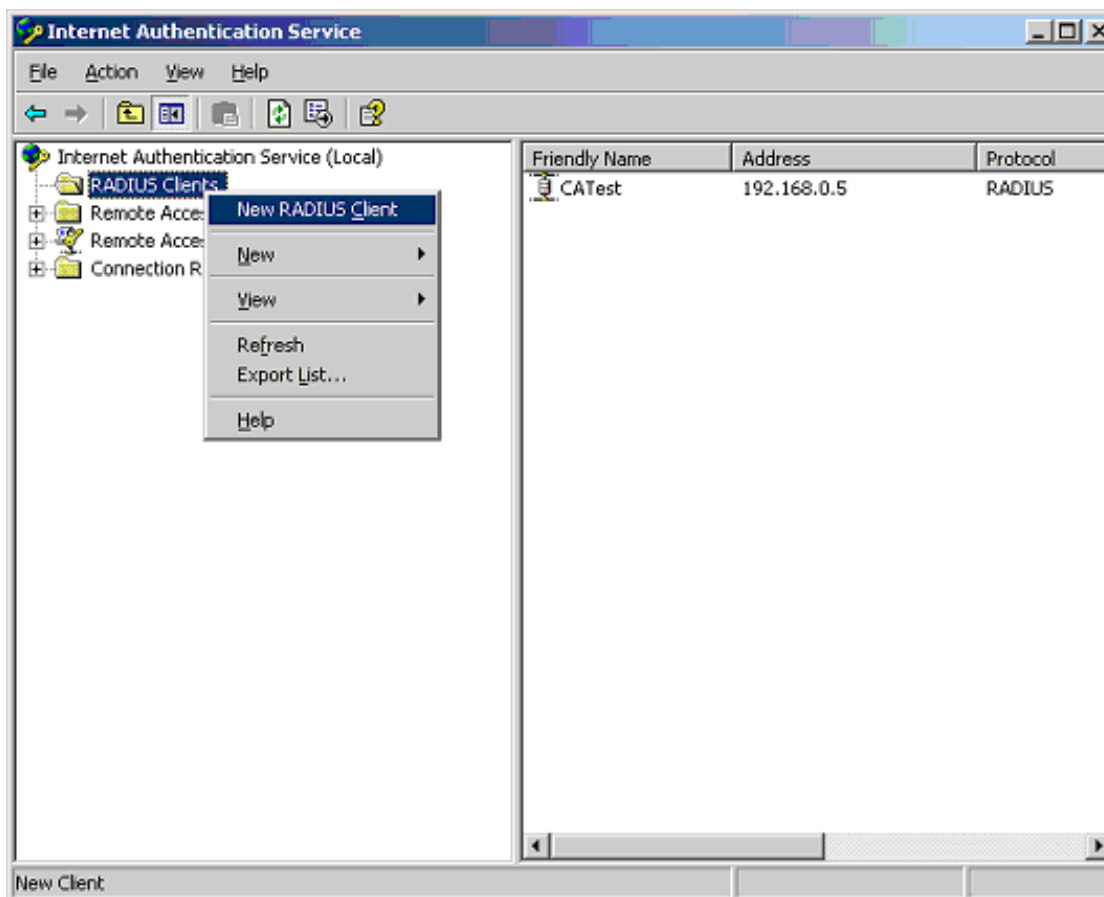
1. Enable the 802.1x Authentication Mode and configure the IP Address of remote RADIUS server and secret key.

Figure 4-83: 802.1x Configuration - System screenshot

802.1X Configuration	
System Configuration	
Mode	Enabled
RADIUS IP	192.168.0.200
RADIUS Secret	12345678
Reauthentication Enabled	<input checked="" type="checkbox"/>
Reauthentication Period	3600 seconds
EAP Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds

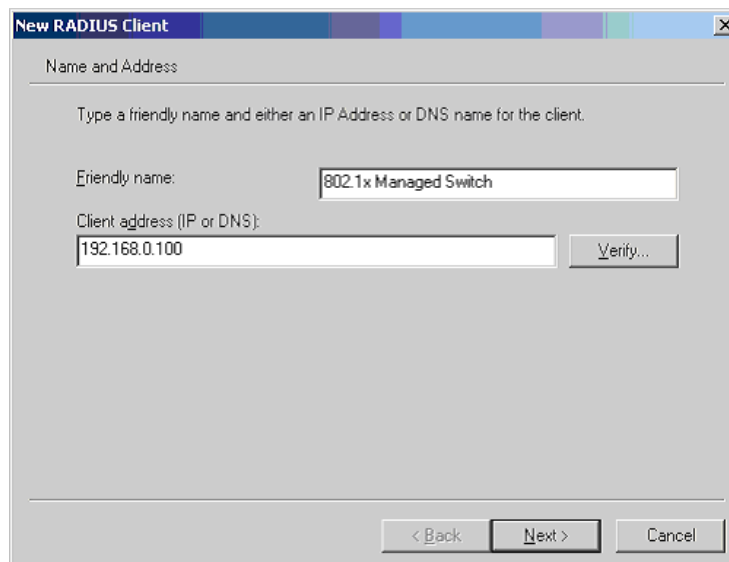
2. Add New RADIUS Client on the Windows 2003 server.

Figure 4-84: Windows Server - add new RADIUS client setting



3. Assign the client IP address to the Managed switch.

Figure 4-85: Windows Server - add new RADIUS client setting



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

Figure 4-86: Windows Server - add new RADIUS client setting

New RADIUS Client

Additional Information

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

Client-Vendor: RADIUS Standard

Shared secret:

Confirm shared secret:

☐ Request must contain the Message Authenticator attribute

< Back Finish Cancel

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

Figure 4-87: 802.1x Port Configuration

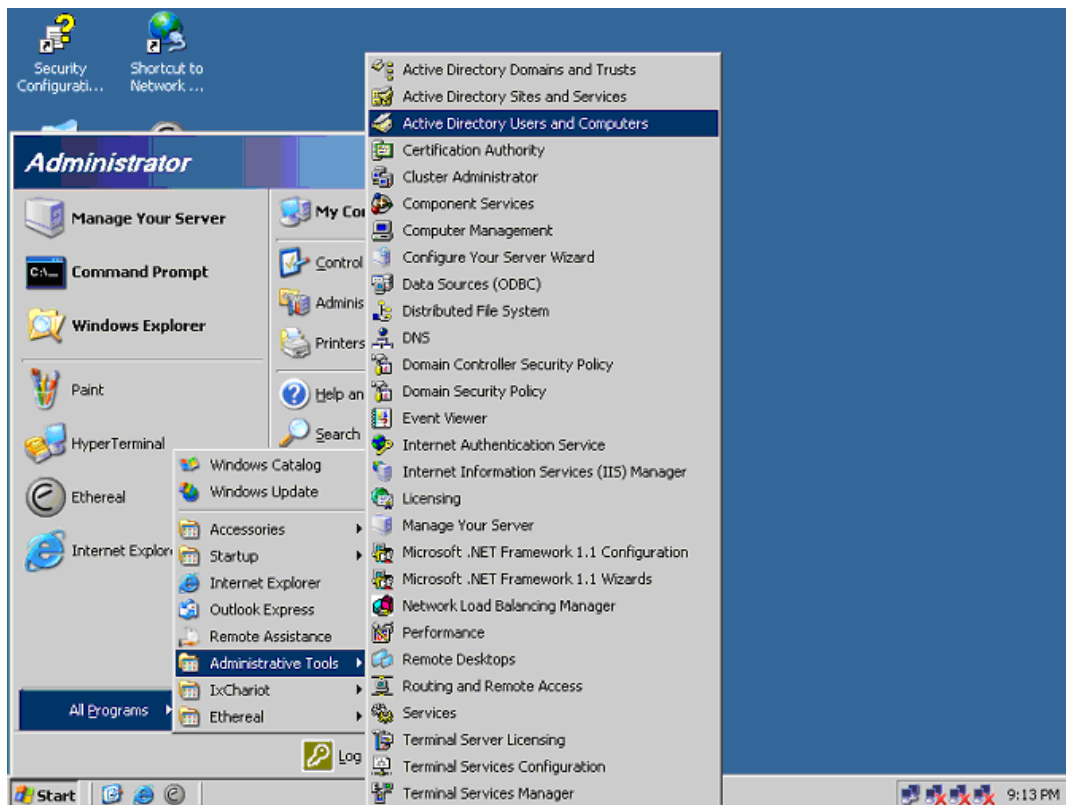
802.1X Port Configuration for Switch 1

Port	Admin State	Port State	Max Clients	Restart
1	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
2	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
3	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
4	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
5	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
6	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
7	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
8	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
9	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
10	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
11	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
12	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
13	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
14	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
15	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
16	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
17	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
18	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
19	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
20	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
21	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
22	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
23	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize
24	Authorized	802.1X Disabled	All	1536 Reauthenticate Reinitialize

Save Reset Refresh

6. Create user data. The establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2003 Server, and then:

Figure 4-88: Windows 2003 AD server setting path



7. Enter "Active Directory Users and Computers", create legal user data, the next, right-click a user what you created to enter properties, and what to be noticed:

Figure 4-89: Add User Properties screen

New Object - User

Create in: ca.test.pc/Users

First name: test Initials:

Last name:

Full name: test

User logon name: test @ca.test.pc

User logon name (pre-Windows 2000): CA\ test

< Back Next > Cancel

Figure 4-90: Add User Properties screen

New Object - User

Create in: ca.test.pc/Users

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

NOTE: Set the Ports Authenticate Status to "Force Authorized" if the port is connected to the RADIUS server or the port is an uplink port that is connected to another switch. Or once the 802.1X stat to work, the switch might not be able to access the RADIUS server.

802.1X Client Configuration

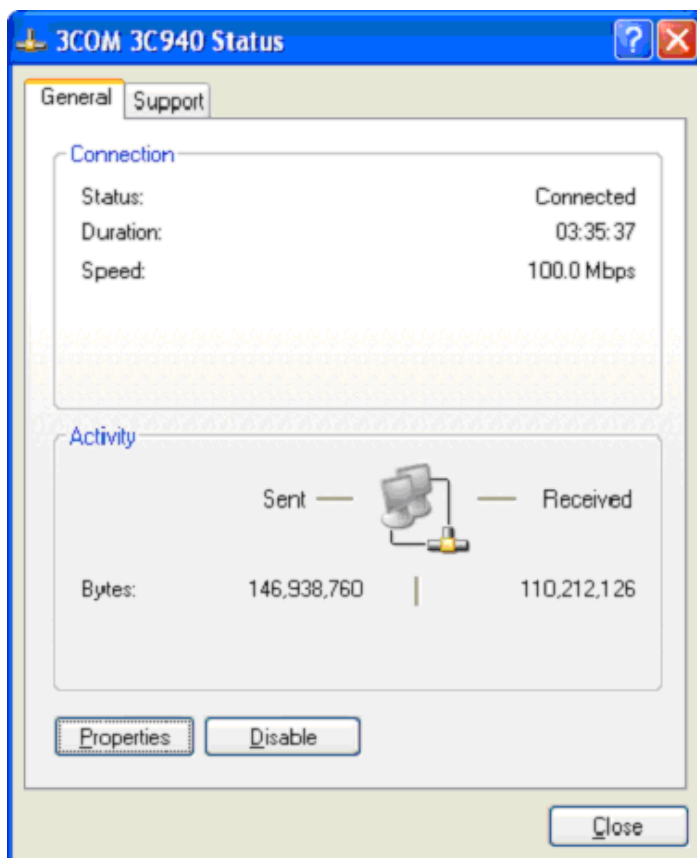
Windows XP is originally 802.1X support. As to other operating systems (windows 98SE, ME, 2000), an 802.1X client utility is needed. The following procedures show how to configure 802.1X Authentication in Windows XP.

Please note that if you want to change the 802.1x authentication type of a wireless client, i.e. switch to EAP-TLS from EAP-MD5, you must remove the current existing wireless network from your preferred connection first, and add it in again.

Configure Sample: EAP-MD5 Authentication

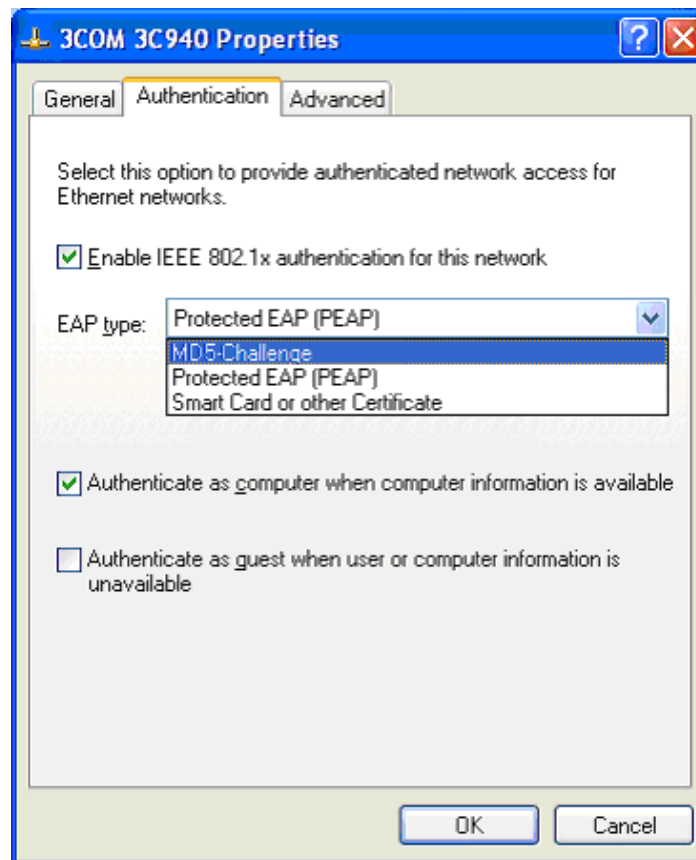
1. Go to **Start > Control Panel**, double-click on **"Network Connections"**.
2. Right-click on the Local Network Connection.
3. Click **"Properties"** to open up the Properties setting window.

Figure 4-91: Status window



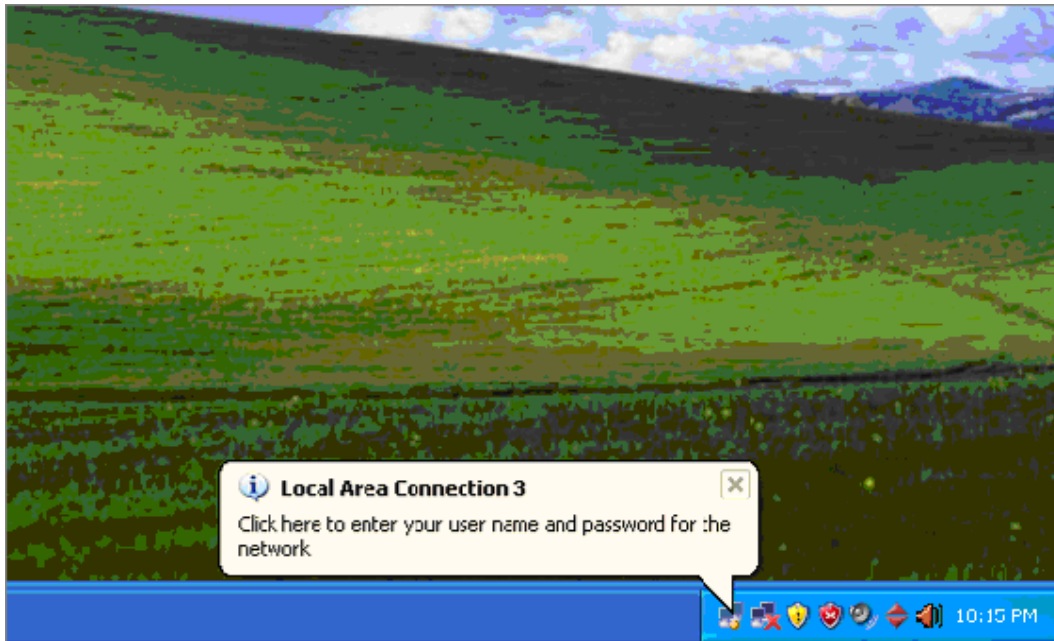
4. Select "Authentication" tab.
5. Select "Enable network access control using IEEE 802.1X" to enable 802.1x authentication.
6. Select "MD-5 Challenge" from the drop-down list box for EAP type.

Figure 4-92: Authentication Tab



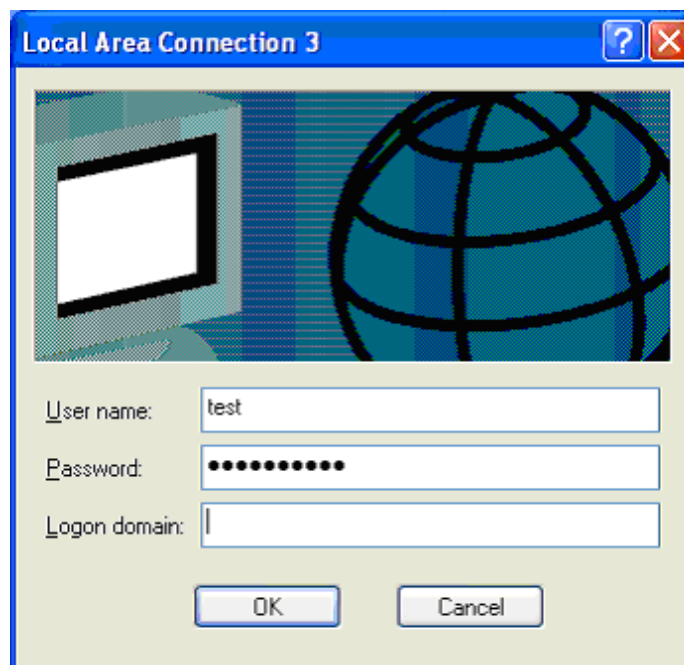
7. Click "OK".
8. When client has associated with the Managed Switch, a user authentication notice appears in system tray. Click on the **notice** to continue.

Figure 4-93: Windows client popup login request message



9. Enter the user name, password and the logon domain that your account belongs.
10. Click "OK" to complete the validation process.

Figure 4-94: Domain Logon window



Access Control Lists

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

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

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined for this Managed Switch. Each row describes the ACE that is defined.

- The maximum number of ACEs is 128.
- Click on the lowest plus sign to add a new ACE to the list.







The Access Control List Configuration screen in Figure 4-95 appears.

Figure 4-95: Access Control List Configuration page screenshot

The screenshot shows the 'Access Control List Configuration' interface. At the top, there's a title bar. Below it is a table with eight columns: 'Ingress Port', 'Frame Type', 'Action', 'Rate Limiter', 'Port Copy', 'Logging', 'Shutdown', and 'Counter'. Below the table, there are four buttons: 'Clear', 'Refresh', 'Auto-refresh' (with a checkbox), and 'Remove All'.

This page includes the following fields:

Object	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: Any: The ACE will match any ingress port. Policy: The ACE will match ingress ports with a specific policy. Port: The ACE will match a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. ARP : The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 15. When Disabled is displayed, the rate limiter operation is disabled.

Object	Description
Port Copy	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
Logging	Indicates the logging operation of the ACE. Possible values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Indicates the port shut down operation of the ACE. Possible values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using the following buttons:  : Inserts a new ACE before the current row.  : Edits the ACE row.  : Moves the ACE up the list.  : Moves the ACE down the list.  : Deletes the ACE.  : The lowest plus sign adds a new entry at the bottom of the ACE listings.

ACE Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.

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

Object	Description
Ingress Port	Select the ingress port for which this ACE applies. Any: The ACE applies to any port. Port n: The ACE applies to this port number, where n is the number of the switch port. Policy n: The ACE applies to this policy number, where n can range from 1 through 8.
Switch	Select the switch to which this ACE applies. Any: The ACE applies to any port. Switch n: The ACE applies to this switch number, where n is the number of the switch.
Frame Type	Select the frame type for this ACE. Any: Any frame can match this ACE. Ethernet Type: Only Ethernet Type frames can match this ACE. ARP: Only ARP frames can match this ACE. IPv4: Only IPv4 frames can match this ACE.
Action	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
Port Copy	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Logging	Specify the logging operation of the ACE. The allowed values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.

MAC Parameters

Object	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
SMAC Value	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

VLAN Parameters

Object	Description
VLAN ID Filter	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

Object	Description
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) ARP: Frame must have ARP/RARP opcode set to ARP. RARP: Frame must have ARP/RARP opcode set to RARP. Other: Frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) Request: Frame must have ARP Request or RARP Request OP flag set. Reply: Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. Any: No sender IP filter is specified. (Sender IP filter is "don't-care".) Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
Sender IP Address	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specify the target IP filter for this specific ACE. Any: No target IP filter is specified. (Target IP filter is "don't-care".) Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
Target IP Address	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

Object	Description
ARP SMAC Match	<p>Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.</p> <p>0: ARP frames where SHA is not equal to the SMAC address.</p> <p>1: ARP frames where SHA is equal to the SMAC address.</p> <p>Any: Any value is allowed ("don't-care").</p>
RARP SMAC Match	<p>Specify whether frames can hit the action according to their target hardware address field (THA) settings.</p> <p>0: RARP frames where THA is not equal to the SMAC address.</p> <p>1: RARP frames where THA is equal to the SMAC address.</p> <p>Any: Any value is allowed ("don't-care").</p>
IP/Ethernet Length	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.</p> <p>0: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry.</p> <p>1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
IP	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.</p> <p>0: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry.</p> <p>1: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
Ethernet	<p>Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.</p> <p>0: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry.</p> <p>1: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>

IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

Object	Description
IP Protocol Filter	<p>Specify the IP protocol filter for this ACE.</p> <p>Any: No IP protocol filter is specified ("don't-care").</p> <p>Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.</p> <p>ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.</p> <p>UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.</p> <p>TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.</p>
IP Protocol Value	<p>When "Specific" is selected for the IP protocol value, you can enter a specific value.. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.</p>
IP TTL	<p>Specify the Time-to-Live settings for this ACE.</p> <p>zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.</p> <p>non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
IP Fragment	<p>Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.</p> <p>No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.</p> <p>Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
IP Option	<p>Specify the options flag setting for this ACE.</p> <p>No: IPv4 frames where the options flag is set must not be able to match this entry.</p> <p>Yes: IPv4 frames where the options flag is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>

Object	Description
SIP Filter	<p>Specify the source IP filter for this ACE.</p> <p>Any: No source IP filter is specified. (Source IP filter is "don't-care".)</p> <p>Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.</p> <p>Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.</p>
SIP Address	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	<p>Specify the destination IP filter for this ACE.</p> <p>Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)</p> <p>Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.</p> <p>Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.</p>
DIP Address	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

ICMP Parameters

Object	Description
ICMP Type Filter	<p>Specify the ICMP filter for this ACE.</p> <p>Any: No ICMP filter is specified (ICMP filter status is "don't-care").</p> <p>Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.</p>
ICMP Type Value	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

Object	Description
ICMP Code Filter	<p>Specify the ICMP code filter for this ACE.</p> <p>Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").</p> <p>Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.</p>
ICMP Code Value	<p>When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.</p>

TCP/UDP Parameters

Object	Description
TCP/UDP Source Filter	<p>Specify the TCP/UDP source filter for this ACE.</p> <p>Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").</p> <p>Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.</p> <p>Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.</p>
TCP/UDP Source No.	<p>When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.</p>
TCP/UDP Source Range	<p>When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.</p>
TCP/UDP Destination Filter	<p>Specify the TCP/UDP destination filter for this ACE.</p> <p>Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").</p> <p>Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.</p> <p>Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.</p>

Object	Description
TCP/UDP Destination Number	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
TCP/UDP Destination Range	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
TCP FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. 0: TCP frames where the FIN field is set must not be able to match this entry. 1: TCP frames where the FIN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. 0: TCP frames where the SYN field is set must not be able to match this entry. 1: TCP frames where the SYN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP PSH	Specify the TCP "Push Function" (PSH) value for this ACE. 0: TCP frames where the PSH field is set must not be able to match this entry. 1: TCP frames where the PSH field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. 0: TCP frames where the ACK field is set must not be able to match this entry. 1: TCP frames where the ACK field is set must be able to match this entry. Any: Any value is allowed ("don't-care").

Object	Description
TCP URG	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <p>0: TCP frames where the URG field is set must not be able to match this entry.</p> <p>1: TCP frames where the URG field is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

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

ACL Configuration wizard

This handy wizard helps you set up an ACL quickly.

The ACL Configuration wizard screen in Figure 4-96 appears.

Figure 4-96: Access Control List Configuration page screenshot

Welcome to the ACL Configuration Wizard!

Please select an action:

☐ **Set up Policy Rules**
Set up the default policy rules for Client ports, Server ports, Network ports, and Guest ports.

☐ **Set up Port Policies**
Group ports into several types according to different ACL policies.

☐ **Set up Typical Network Application Rules**
Set up the specific ACL for different typical network application access control.

☐ **Set up Source MAC and Source IP Binding**
Strictly control the network traffic by only allowing incoming frames that match the source MAC and source IP on specific ports.

☐ **Set up DoS Attack Detection Rules**
Set up the specific ACL to detect DoS attack.

To continue, click Next.

Next >

This page includes the following fields:

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

Set up Policy Rules

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

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

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

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

Policy 5 for guest ports: Internet access only.

The screen in Figure 4-97 appears.

Figure 4-97: Set up Policy Rules page screenshot



Set up Port Policies

Group ports into several types according to different ACL policies.

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

The screen in Figure 4-98 appears.

Figure 4-98: Set up Port Policies page screenshot

Set up Port Policies for Switch 1

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

	Port Members																							
Policy ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1 (Default)	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
2 (Client)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3 (Server)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4 (Network)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5 (Guest)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

This page includes the following fields:

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

Set up Typical Network Application Rules

Set up the specific ACL for different typical network application access control. The screen in Figure 4-99 appears.

STEP-1: Selecting the Network Application Type:

Figure 4-99: Set up Typical network Application Rules page screenshot

Set up Typical Network Application Rules

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

Common Servers

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

Instant Messaging

☐ Google Talk ☐ MSN Messenger ☐ Yahoo Messenger

User Definition

☐ Ethernet Type ☐ UDP Port ☐ TCP Port

Others

☐ HTTPS ☐ ICMP ☐ Multicast IP Stream ☐ NetBIOS ☐ Ping Request ☐ Ping Reply ☐ SNMP ☐ SNMP Traps

Cancel Wizard < Back Next >

This page includes the following fields:

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

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

STEP-2: Define and Apply the Typical Network Application Rules:

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

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

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

The screen in Figure 4-100 appears.

Figure 4-100: Set up Typical network Application Rules screenshot

Set up Typical Network Application Rules

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

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

Different parameter options are displayed depending on your selections.

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








Cancel Wizard < Back Next >

This page includes the following fields:

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

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

Figure 4-101: Set up Typical network Application Rules screenshot

Access Control List Configuration								
Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter	
Any	IPv4/UDP 67 DHCP Client (In)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/UDP 67 DHCP Client (Out)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 5222 Google Talk (In)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 5222 Google Talk (Out)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	EType	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 443 HTTPS (In)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 443 HTTPS (Out)	Deny	Disabled	Disabled	Disabled	Disabled	0	
<div> Clear Refresh <input type="checkbox"/> Auto-refresh </div> <div> Remove All </div>								

Set up Source MAC and Source IP Binding

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

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

The screen in Figure 4-102 appears.

Figure 4-102: Set up Source MAC and Secure IP Binding page screenshot

Set up Source MAC and Source IP Binding for Switch 1

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

Port	Binding Enabled	Source MAC Address	Source IP Address
1	<input checked="" type="checkbox"/>	00-30-4F-AA-BB-CC	192.168.0.200
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
11	<input type="checkbox"/>		
12	<input type="checkbox"/>		
13	<input type="checkbox"/>		
14	<input type="checkbox"/>		
15	<input type="checkbox"/>		
16	<input type="checkbox"/>		
17	<input type="checkbox"/>		
18	<input type="checkbox"/>		
19	<input type="checkbox"/>		
20	<input type="checkbox"/>		
21	<input type="checkbox"/>		
22	<input type="checkbox"/>		
23	<input type="checkbox"/>		
24	<input type="checkbox"/>		

[Cancel Wizard](#) [< Back](#) [Next >](#)

This page includes the following fields:

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

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

Figure 4-103: New Configuration

Access Control List Configuration

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Logging	Shutdown	Counter	
Switch 1 - Port 1	SMAC/SIP Binding - 192.168.0.200	Permit	Disabled	Disabled	Disabled	Disabled	0	
Switch 1 - Port 1	SMAC/SIP Binding - 00-30-4f-aa-bb-cc	Permit	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/UDP 67 DHCP Client (In)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/UDP 67 DHCP Client (Out)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 5222 Google Talk (In)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 5222 Google Talk (Out)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	EType	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 443 HTTPS (In)	Deny	Disabled	Disabled	Disabled	Disabled	0	
Any	IPv4/TCP 443 HTTPS (Out)	Deny	Disabled	Disabled	Disabled	Disabled	0	

Clear Refresh ☐ Auto-refresh
Remove All

Set up DoS Attack Detection Rules

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

The screen in Figure 4-104 appears.

Figure 4-104: Set up DoS Attack Detection Rules page screenshot

Set up DoS Attack Detection Rules

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

☐ **UDP DoS - Fraggle**
A malicious attacker sending a large number of UDP packets with random ports to the target system.

☒ **ICMP DoS - Ping of Death**
A malicious attacker sending a malformed ICMP request packet larger than the 65,536 bytes to the target system.

☐ **ICMP DoS - Smurf**
A malicious attacker sending a malformed ICMP request packet with broadcast destination addresses to the target system.

Cancel Wizard < Back Next >

This page includes the following fields:

Object	Description
UDP DoS - Fraggle	A malicious attacker sending a large number of UDP packets with random ports to the target system. When the target system receives these packets, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the spoofed source address. Eventually leading it to be unreachable by other clients and the system will go down.
ICMP DoS - Ping of Death	A malicious attacker sending a malformed ICMP request packet larger than the 65,536 bytes to the target system. Some target systems cannot handle the packet larger than the maximum IP packet size, which often causes target system froze, crashed or rebooted.
ICMP DoS - Smurf	A malicious attacker sending a malformed ICMP request packet with broadcast destination addresses to the target system. After receiving the packet, all reachable hosts send an ICMP echo reply packet back to the spoofed source address. Thus, the target host will suffer from a larger amount of traffic generated.

Set up DoS Attack Detection Rules

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

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

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

Figure 4-105: Set up DoS Attack Detection Rules page screenshot

Set up DoS Attack Detection Rules

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

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

Different parameter options are displayed depending on your selections.

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

Cancel Wizard < Back Next >

This page includes the following fields:

Object	Description
Ingress Port	<p>Select the ingress port to which this ACE applies.</p> <p>Any: The ACE applies to any port.</p> <p>Port <i>n</i>: The ACE applies to this port number, where <i>n</i> is the number of the switch port.</p> <p>Policy <i>n</i>: The ACE applies to this policy number, where <i>n</i> can range from 1 through 8.</p>
Switch	<p>Select the switch to which this ACE applies.</p> <p>Any: The ACE applies to any port.</p> <p>Switch <i>n</i>: The ACE applies to this switch number, where <i>n</i> is the number of the switch.</p>

Object	Description
Action	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 15 . Disabled indicates that the rate limiter operation is disabled.
Logging	Specify the logging operation of the ACE. The allowed values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.

NOTE: The System Log memory size and logging rate is limited.

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

Figure 4-106: New Configuration

Access Control List Configuration

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

☐ Auto-refresh

ACL Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.

The ACL Rate Limiter Configuration screen in Figure 4-107 appears.

Figure 4-107: ACL Rate Limiter Configuration page screenshot

Rate Limiter ID	Rate (pps)
1	512
2	256
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1

Save Reset

This page includes the following fields:

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

ACL Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. The settings relate to the currently selected stack unit, as reflected by the page header.

The ACL Ports Configuration screen in Figure 4-108 appears.

Figure 4-108: ACL Ports Configuration page screenshot

ACL Ports Configuration for Switch 1

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Deny	Disabled	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	Disabled	8750
8	1	Permit	Disabled	Disabled	Disabled	Disabled	213
9	1	Permit	Disabled	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	Disabled	0
13	1	Permit	Disabled	Disabled	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	Disabled	Disabled	0
15	1	Permit	Disabled	Disabled	Disabled	Disabled	0
16	1	Permit	Disabled	Disabled	Disabled	Disabled	0
17	1	Permit	Disabled	Disabled	Disabled	Disabled	0
18	1	Permit	Disabled	Disabled	Disabled	Disabled	0
19	1	Permit	Disabled	Disabled	Disabled	Disabled	0
20	1	Permit	Disabled	Disabled	Disabled	Disabled	0
21	1	Permit	Disabled	Disabled	Disabled	Disabled	0
22	1	Permit	Disabled	Disabled	Disabled	Disabled	0
23	1	Permit	Disabled	Disabled	Disabled	Disabled	0
24	1	Permit	Disabled	Disabled	Disabled	Disabled	0

This page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is "Disabled".

Object	Description
Port Copy	Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is "Disabled".
Logging	<p>Specify the logging operation of this port. The allowed values are:</p> <p>Enabled: Frames received on the port are stored in the System Log.</p> <p>Disabled: Frames received on the port are not logged.</p> <p>The default value is "Disabled".</p> <p>Please note that the System Log memory size and logging rate is limited.</p>
Shutdown	<p>Specify the port shut down operation of this port. The allowed values are:</p> <p>Enabled: If a frame is received on the port, the port will be disabled.</p> <p>Disabled: Port shut down is disabled.</p> <p>The default value is "Disabled".</p>
Counter	Counts the number of frames that match this ACE.

Address Table

Switching of frames is based upon the DMAC address contained in the frame. The Managed Switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The network administrator configures the static entries if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

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

MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here. The MAC Address Table Configuration screen in Figure 4-109 appears.

Figure 4-109: MAC Address Table Configuration page screenshot

ACL Ports Configuration for Switch 1

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Deny	Disabled	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	Disabled	8750
8	1	Permit	Disabled	Disabled	Disabled	Disabled	213
9	1	Permit	Disabled	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	Disabled	0
13	1	Permit	Disabled	Disabled	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	Disabled	Disabled	0
15	1	Permit	Disabled	Disabled	Disabled	Disabled	0
16	1	Permit	Disabled	Disabled	Disabled	Disabled	0
17	1	Permit	Disabled	Disabled	Disabled	Disabled	0
18	1	Permit	Disabled	Disabled	Disabled	Disabled	0
19	1	Permit	Disabled	Disabled	Disabled	Disabled	0
20	1	Permit	Disabled	Disabled	Disabled	Disabled	0
21	1	Permit	Disabled	Disabled	Disabled	Disabled	0
22	1	Permit	Disabled	Disabled	Disabled	Disabled	0
23	1	Permit	Disabled	Disabled	Disabled	Disabled	0
24	1	Permit	Disabled	Disabled	Disabled	Disabled	0

Aging Configuration

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

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

The Static MAC Table Configuration screen in Figure 4-110 appears.

Figure 4-110: Static MAC Table Configuration page screenshot

Static MAC Table Configuration for Switch 1

Delete	VLAN ID	MAC Address	Port Members																							
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<input type="checkbox"/>	1	00-30-4F-AA-BB-CC	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This page includes the following fields:

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

MAC Address Table Status

Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Figure 4-111: MAC Address Table Status

MAC Address Table for Switch 1

Start from VLAN 1 Trace with entries 00-00-00-00-00-00 20

Auto refresh Refresh Clear << >>

			Port Members																											
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	ST1	ST2	
Dynamic	1	00-00-74-5B-78-2B								✓																				
Dynamic	1	00-07-84-7A-5C-77								✓																				
Dynamic	1	00-01-8C-5E-19-CD								✓																				
Dynamic	1	00-03-1E-01-0E-79								✓																				
Dynamic	1	00-0A-78-91-42-03								✓																				
Dynamic	1	00-0C-6E-50-87-04								✓																				
Dynamic	1	00-0C-6E-72-87-7E								✓																				
Dynamic	1	00-07-6C-83-12-0D								✓																				
Dynamic	1	00-11-2F-34-37-9E								✓																				
Dynamic	1	00-11-2F-7F-D8-BE								✓																				
Dynamic	1	00-14-5E-16-1D-16								✓																				
Dynamic	1	00-14-5E-19-59-60								✓																				
Dynamic	1	00-14-5E-7F-57-FA								✓																				
Dynamic	1	00-14-5E-7C-53-CD								✓																				
Dynamic	1	00-14-8F-73-87-1D								✓																				
Dynamic	1	00-14-8F-73-87-80								✓																				
Dynamic	1	00-15-5E-10-DB-23								✓																				
Dynamic	1	00-15-5D-71-09-00								✓																				
Dynamic	1	00-15-5D-71-09-02								✓																				
Dynamic	1	00-15-5D-71-09-05								✓																				

Navigating the MAC Table

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

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

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

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

MAC Table Columns

Object	Description
Type	Indicates whether the entry is a static or dynamic entry.
VLAN	The VLAN ID of the entry.
MAC address	The MAC address of the entry.
Port Members	The ports that are members of the entry.

Buttons

Auto-refresh ☐ : Check this box to enable an automatic refresh of the page at regular intervals.

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

Clear : Flushes all dynamic entries.

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

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

Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the Managed Switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

<source MAC address, VLAN> pair for frames received on the port.

Note that you can also manually add secure addresses to the port using the Static Address Table. The selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

MAC Table Learning

Figure 4-112: Port Security Settings screenshot

Port Security

MAC Table Learning for Switch 1

	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

This page includes the following fields:

Object	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

LLDP

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in Figure 4-113 appears.

Figure 4-113: LLDP Configuration page screenshot

LLDP Configuration

LLDP Parameters

Tx Interval	<input type="text" value="10"/>	seconds
Tx Hold	<input type="text" value="3"/>	times
Tx Delay	<input type="text" value="2"/>	seconds
Tx Reinit	<input type="text" value="2"/>	seconds

LLDP Port Configuration for Switch 1

Port	Mode	Optional TLVs				
		Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
1	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Tx only <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Enabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Disabled <input type="button" value="v"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

LLDP Parameters

Object	Description
Tx Interval	<p>The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.</p> <p>Default: 30 seconds</p> <p>This attribute must comply with the following rule:</p> <p>$(\text{Transmission Interval} * \text{Hold Time Multiplier}) \leq 65536$, and $\text{Transmission Interval} \geq (4 * \text{Delay Interval})$</p>
Tx Hold	<p>Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.</p> <p>TTL in seconds is based on the following rule:</p> <p>$(\text{Transmission Interval} * \text{Holdtime Multiplier}) \leq 65536$.</p> <p>Therefore, the default TTL is $4 * 30 = 120$ seconds.</p>
Tx Delay	<p>If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.</p> <p>This attribute must comply with the rule:</p> <p>$(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$</p>
Tx Reinit	<p>When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.</p>

LLDP Port Configuration

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

Object	Description
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode.

Object	Description
	<p>Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.</p> <p>Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.</p> <p>Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.</p> <p>Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.</p>
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa	<p>Optional TLV: When checked the "system capability" is included in LLDP information transmitted.</p> <p>The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.</p>
Mgmt Addr	<p>Optional TLV: When checked the "management address" is included in LLDP information transmitted.</p> <p>The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address</p>

LLDP Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Neighbor screen in Figure 4-114 appears.

Figure 4-114: LLDP Neighbor Information page screenshot

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 7	463DE94C68556861	00-02-03-05-02-0A	ENM-KENT	Winbond W89C84B PCI Fast Ethernet Adapter - Packet Scheduler Miniport	Station Only(+)	10.1.1.17 (IPv4)

Auto-refresh ☐ Refresh

The columns hold the following information:

Object	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: <ul style="list-style-type: none"> 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only

Object	Description
	<p>9. Reserved</p> <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

LLDP Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refers to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-1154 appears.

Figure 4-115: LLDP Statistics page screenshot

Global Counters

Neighbor entries were last changed at 2009-10-15 Thu 05:21:29 +0000 (1124903 sec. ago)

Total Neighbors Entries Added

1

Total Neighbors Entries Deleted

0

Total Neighbors Entries Dropped

0

Total Neighbors Entries Aged Out

0

Auto-refresh

☐

Refresh

Clear

LLDP Statistics for Switch 1

Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Orig. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	10753	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0

Global Counters

Object	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added. It is also shows the time elapsed since last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

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

Network Diagnostics

Cable Diagnostics

This page is used for running the Cable Diagnostics. Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running cable diagnostic. Therefore, running cable diagnostic on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The ports belong to the currently selected stack unit, as reflected by the page header.

Figure 4-116: Cable Diagnostics page screenshot

Cable Diagnostics for Switch 1

Port: All Start

Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--
17	--	--	--	--	--	--	--	--
18	--	--	--	--	--	--	--	--
19	--	--	--	--	--	--	--	--
20	--	--	--	--	--	--	--	--
21	--	--	--	--	--	--	--	--
22	--	--	--	--	--	--	--	--
23	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--

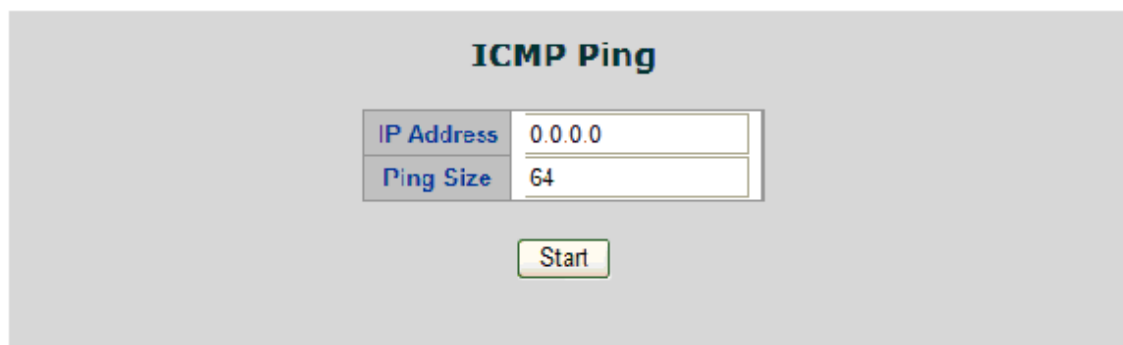
Object	Description
Port	The port where you are requesting Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

Ping

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

After you press the START button, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-116 appears.

Figure 4-117: ICMP Ping page screenshot



The screenshot shows a web interface for ICMP Ping. It features a title 'ICMP Ping' at the top. Below the title, there are two input fields: 'IP Address' with the value '0.0.0.0' and 'Ping Size' with the value '64'. Below these fields is a 'Start' button.

This page includes the following fields:

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

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

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

Stacking - GE-DSSG-244 / GE-DSSG-244-PoE

Using Stacking, it is possible to connect a number of switches together in a stack, which behaves as a single switch as seen from outside the stack.

Two types of stack topologies are supported:

- **Ring topology**
- **Chain topology (same as a disconnected ring)**

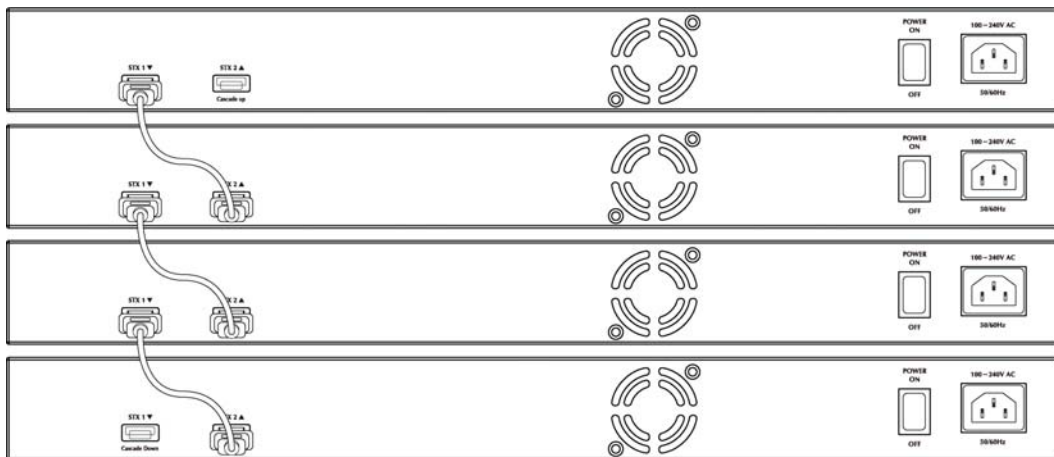
Multiple GE Security GE-DSSG-244 series devices may be connected together to constitute a ring or chain stack topology using the STX / 5Gbps ports as interconnect links. Dedicated stacking features built into GE-DSSG-244 makes all devices in the stack operate together as a single, much larger switch. Among the stacking features are:

- Hardware controlled stack wide learning and continuous automatic MAC table synchronization
- Shortest path forwarding, providing low latency and optimal use of stacking link bandwidth
- QoS consistency across stack
- Single point of management for simple stack administration
- Low Cost and Flexible HDMI-like Stacking cables
- Real Plug and Play connectivity

The following figure shows an example with five devices in a ring topology stack. Each device in the stack is, in a stack context, called a unit. The ports connecting the units are called stack ports, and the ports connecting to external hosts and switches are called front ports.

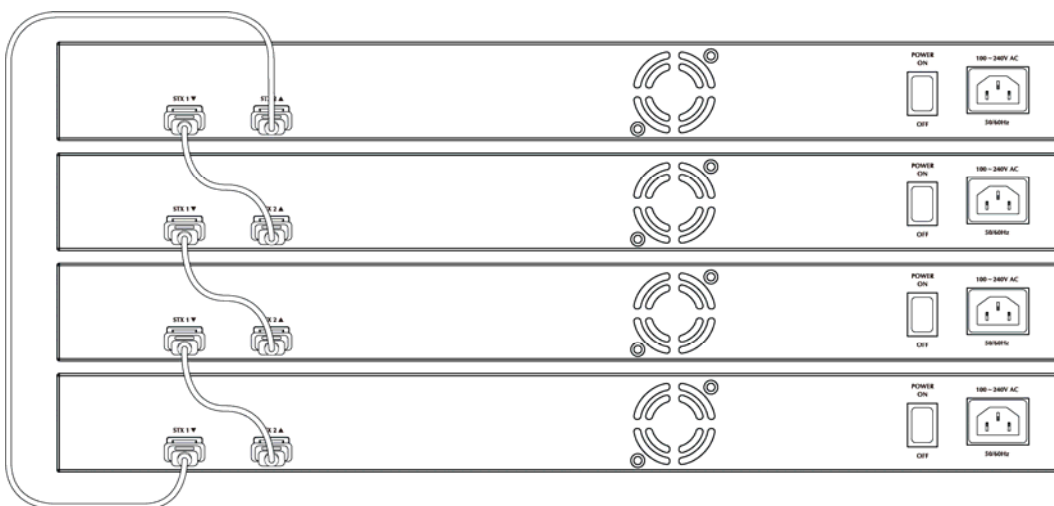
- **Chain Stack:** A chain of switches, that is, no redundant forwarding paths.

Figure 4-118: Chain Stack topology



- **Ring Stack:** A ring of switches, thereby providing redundant forwarding paths.

Figure 4-119: Ring Stack topology



- **Back-to-Back Stack:** Two switches interconnected on both stacking ports.

Figure 4-120: Back to back Stack topology



Stack

This section provides information for understand stacking architecture, include the below items:

- Switch IDs
 - Assigning and Swapping Switch IDs
 - Removing a Switch From the Stack
 - Replacing a Switch
 - General Switch ID Assignment Rules
- Master Election
- Stack Redundancy
- Shortest Path Forwarding

Switch IDs

The Switch ID (1-16) assigned to a GE-DSSG-244 series Switch.

- **Assigning and Swapping Switch IDs**

When a switch is added to the stack, a Switch ID is automatically assigned to the switch. The automatic SID assignment can be modified by choosing a different Switch ID on the Stack Configuration page. This method allows Switch IDs to be assigned so that it is easier for the user to remember the ID of each switch.

The Switch IDs of two switches can be swapped by simply interchanging the values in the Switch ID column.

NOTE: Changing Switch IDs does not result in any interruption of the stack operation.

- **Removing a Switch From the Stack**

When a switch is removed from the stack, the configuration for the switch is preserved, and the switch still appears on the Stack Configuration page. If the configuration of the switch is not to be transferred to another switch, then the configuration may be deleted by choosing Delete, followed by "Save".

- **Replacing a Switch**

If a switch is to be replaced with another switch (for example, replacing failing hardware), the following procedure must be used to assign the configuration of the failing switch to the new hardware:

1. Remove the failing switch from the stack. For example, assume that the failing switch had Switch ID 3.
2. Insert the new switch into the stack. The new switch is assigned an unused Switch ID.
3. To remove the automatic switch ID assignment, choose "Delete", followed by "Save". The new switch is then shown with Switch ID set to "-".
4. To assign the configuration of Switch ID 3 to the new hardware, simply choose 3 in the Switch ID column and click "Save".
5. The new hardware has now taken over the configuration of the failing hardware.

- **General Switch ID Assignment Rules**

When assigning Switch IDs to the devices in the stack, you must note the following:

1. Switches with assigned IDs can be changed to use any other switch ID (possibly by swapping Switch ID with another active switch).
2. When swapping two Switch IDs, the devices will retain their (own) configuration, except for the Switch ID.
3. Switches without an assigned Switch ID can only be assigned to any unused ID.
4. When assigning a Switch ID of an inactive switch to a new switch, the new switch will inherit the former's configuration (see "Replacing a Switch" above).
5. Deleting a switch will remove any configuration pertaining to it.
6. Deleting an active switch will leave it with an unassigned Switch ID until rebooted or manually assigning a Switch ID.

Master Election

Within a managed stack, one master switch (or just "master") must be elected. Any switch not being master is a slave switch (or just "slave").

To elect a master, the following criteria are evaluated sequentially:

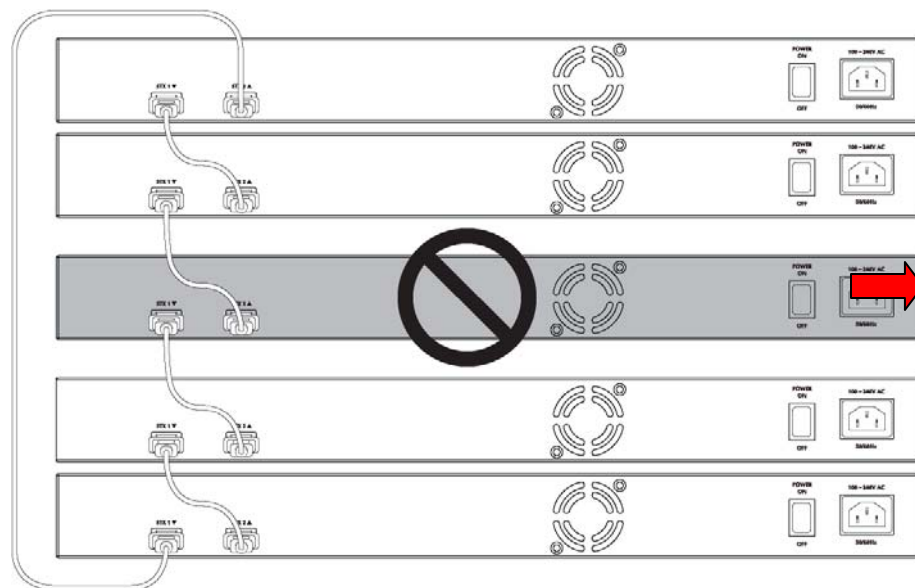
1. If any switch already claims to have been master for more than 30 seconds, then that switch will become master.
2. If multiple switches claim to have been master for more than 30 seconds, then the switch, which has been master for the longest period of time, will become master.
3. The switch with the smallest master priority.
4. The switch with the smallest MAC address.

The above algorithm ensures that once a master has been elected and has been master for more than 30 seconds, it will remain master. However in some cases the user may want to enforce a new master election.

Stack Redundancy

In the unlikely event that a GE-DSSG-244 series switch fails in a stack, stack integrity is maintained if the redundant cable is connected to the stack. The affected switch within the sack can be replaced or removed without disrupting normal operation. The broken link is bypassed and data transmission continues uninterrupted. The single management IP address for the stack is also preserved for uninterrupted management and monitoring.

Figure 4-121: Remove or Replace a switch from the stack

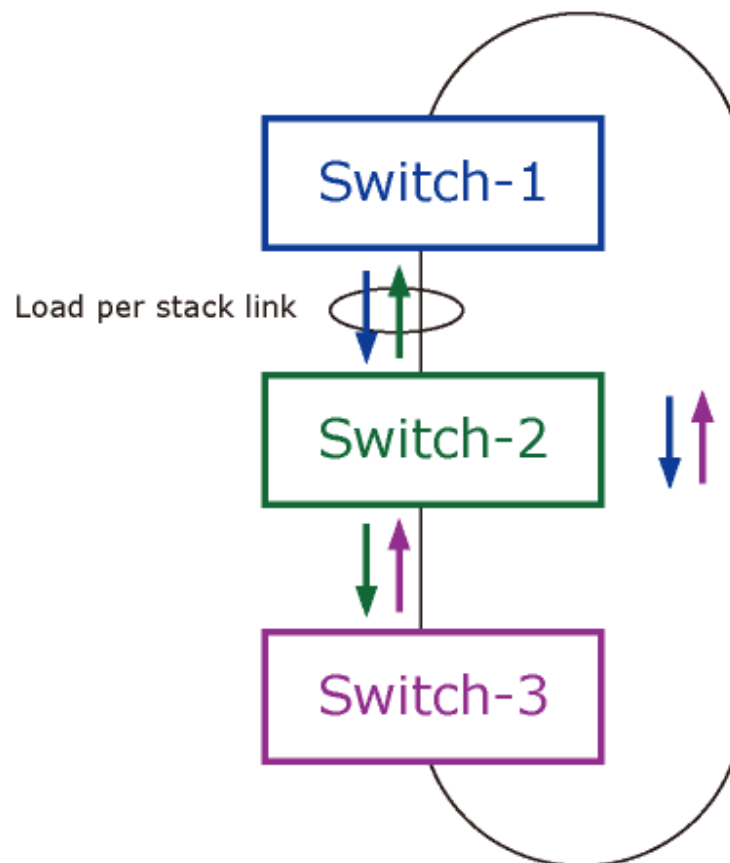


Shortest Path Forwarding

The GE-DSSG-244 series switch supports shortest path forwarding technology to optimal data flow across the stack. The advantage of shortest path forwarding as below:

- * **Automatic Loop Prevention** - Using Time To Live (TTL) information in the stack-header
- * **Utilize all stack links in the ring.**

Figure 4-122: True Ring Topology



Stack Configuration

This page is used to configure the stack, include assign Switch ID, master priority and display the current stack member information. The screen in Figure 4-123 appears.

Figure 4-123: Stack Configuration page screenshot

Delete	Stack Member	Switch ID	Master Capable	Priority	Description	Switch Type
<input type="checkbox"/>	00-30-41-76-26-93	1	Yes	3	GE-DSSG-244-PoE	GE Security GE-DSSG-244-PoE Managed Switch
<input type="checkbox"/>	00-30-41-76-c4-2b	2	Yes	3	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch
<input type="checkbox"/>	00-30-41-24-24-24	3	Yes	4	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch

☐ Start Master Election

This page includes the following fields:

Object	Description
Delete	Deletes this switch from the stack configuration.
Stack Member	The MAC address of the switch.
Switch ID	The Switch ID (1-16) assigned to a switch. For more information, see description of Switch IDs
Master Capable	Indicates whether a switch is capable of being master. An unmanaged switch, for example, will not be Master Capable.
Master Priority	The priority that the switch has in the master election process. The smaller the priority, the more likely the switch will become master during the master election process.
Switch Type	The product name of the switch.
Start Master Election	By checking this option, the "Save" operation will also start the master election process. This is done by clicking "Start Master Election", followed by "Save". This causes the first two criteria to be ignored, thereby basing master election only on master priority and MAC address. When master election is enforced, the first two criteria are ignored for a period of 10-15 seconds.

On the Stack State Monitor web page, this is shown by **Reelect** being set to "Yes" for one of the switches in the stack.

Stack Information

This page provides an overview of the stack topology, as detected by SPROUT.

- Stack Topology

The Stack Topology screen in Figure 4-124 appears.

Figure 4-124: Stack Information page screenshot - Stack Topology

Stack Topology	
Stack Topology	Chain
Stack Member Count	3
Last Topology Change	1970-01-01 Thu 00:02:28 +0000
Master Switch	00-30-4f-76-26-93
Last Master Change	-

This page includes the following fields:

Object	Description
Stack Topology	Specifies the type of topology for the stack: Chain: A chain of switches, that is, no redundant forwarding paths. Ring: A ring of switches, thereby providing redundant forwarding paths. Back-to-Back: Two switches interconnected on both stacking ports.
Stack Member Count	The number of switches in the stack.
Last Topology Change	The time of the last topology change in the stack.
Master Switch	The MAC address of the current stack master switch.
Last Master Change	The time of the last master change in the stack.

Stack List

For each switch in the stack, the following information is shown: The MAC address, Switch ID, product name and version, and master election state. The master election state is normally "No". Only when the user enforces a forced master election, the master election state takes the value "Yes". For details about the master election algorithm, see Stack Configuration. The Stack List screen in Figure 4-125 appears.

Figure 4-125: Stack Information page screenshot - Stack List

Stack List						
Stack Member	Switch ID	Product		Master		
		Name	Version	Priority	Time	Reelect
00-30-4f-76-26-93	1	GE Security GE-DSSG-244-PoE Managed Switch	v1.0b090925	3	0d 02:00:55	No
00-30-4f-76-c4-2b	2	GE Security GE-DSSG-244 Managed Switch	v1.0b090925	3	-	No
00-30-4f-24-24-24	3	GE Security GE-DSSG-244 Managed Switch	v1.0b090925	4	-	No

This page includes the following fields:

Object	Description
Delete	Deletes this switch from the stack configuration.
Stack Member	The MAC address of the switch.
Switch ID	The Switch ID (1-16) assigned to a switch. For more information, see description of Switch IDs
Master Capable	Indicates whether a switch is capable of being master. An unmanaged switch, for example, will not be Master Capable.
Master Priority	The priority that the switch has in the master election process. The smaller the priority, the more likely the switch will become master during the master election process.
Switch Type	The product name of the switch.
Start Master Election	By checking this option, the "Save" operation will also start the master election process. This is done by clicking "Start Master Election", followed by "Save". This causes the first two criteria to be ignored, thereby basing master election only on master priority and MAC address. When master election is enforced, the first two criteria are ignored for a period of 10-15 seconds.

Master Forwarding Table

As the heading suggests, the information in the table is as seen from the master view.

For each switch in the stack, the following information is shown:

- The MAC address, switch ID, distance information, and the primary forwarding path to the switch.
- For ring topology, a backup path is also provided.

Figure 4-126: Stack Information page screenshot - Master Forwarding Table

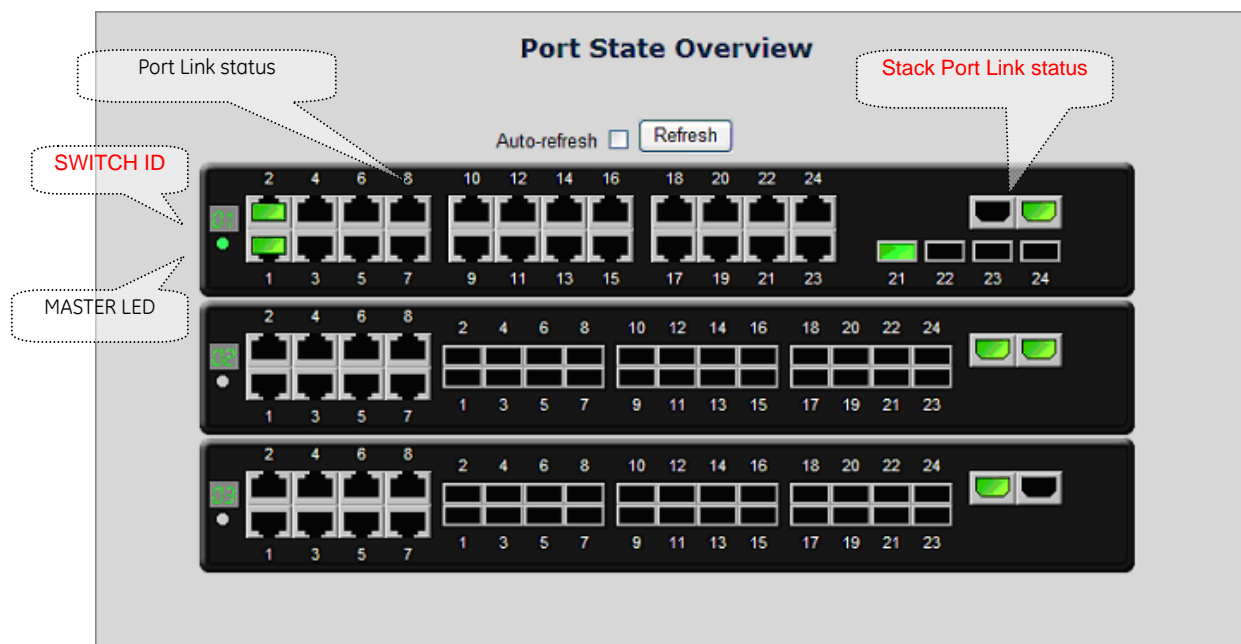
Master Forwarding Table					
Stack Member	Switch ID	Distance		Forwarding	
		Port 25	Port 26	Port 25	Port 26
00-30-4f-76-26-93	1	0	0	Local	Local
00-30-4f-76-c4-2b	2	-	1	-	Primary
00-30-4f-24-24-24	3	-	2	-	Primary

Auto-refresh ☐ Refresh

Stack Port State Overview

This page provides an overview of the current switch port states. Clicking on the image of a port opens the Port Statistics page. The port states are illustrated as follows:

Figure 4-127: Port State Overview page screenshot



Stack Example

Stacking function is convenient for administrator to manage multiple switches by single IP. Basically, you got to have min. 2 units. The GE-DSSG-244 series Switch supports auto stack configuration. Once the stack cable is connect to the stack port of each GE-DSSG-244 series switch and power on them, the stack is built automatically and the Switch ID is automatically assigned to the switch. It is also easy to add or delete stackable switch to the stack without service interruption. The key points of Stack management are:

- Identify the MASTER SWITCH
- Assign/re-assign Switch ID for each management purpose

Step 1: linking the switches by HDMI-like stack cable.

Step 2: Check the Master LED of each GE-DSSG-244 series switch to find out the Master Switch that is elected automatically by the stack operation.

Step 3: Use the Web browser such as IE 6.0 to login the Master Switch, the default IP address is 192.168.0.100.

Step 4: Choose "Stack \ Stack Configuration" from menu tree. You can see the Stack had established automatically. As the screen shows:

1. The Switch ID is automatically assigned to the switches
2. All switches with same Priority value "3".
3. The one that can't be deleted is the Stack master.

Figure 4-128: Stack Configuration

Delete	Stack Member	Switch ID	Master		Description	Switch Type
			Capable	Priority		
<input type="checkbox"/>	00-30-4f-76-26-93	1	Yes	3	GE-DSSG-244-PoE	GE Security GE-DSSG-244-PoE Managed Switch
<input type="checkbox"/>	00-30-4f-76-c4-2b	2	Yes	3	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch
<input type="checkbox"/>	00-30-4f-24-24-24	3	Yes	3	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch

☐ Start Master Election

Step 5: We wish to make the GE-DSSG-244 series switch with MAC "00-30-4f-76-c4-2b" / Switch ID=2 to become the Stack Master and swap the Switch ID to 1.

- Select the switch with ID=1 and assign a new ID for this unit, for example: ID=4

Figure 4-129: Assigning new ID for current master

Delete	Stack Member	Switch ID	Master		Description	Switch Type
			Capable	Priority		
<input type="checkbox"/>	00-30-4f-76-26-93	1	Yes	3	GE-DSSG-244-PoE	GE Security GE-DSSG-244-PoE Managed Switch
<input type="checkbox"/>	00-30-4f-76-c4-2b	2	Yes	3	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch
<input type="checkbox"/>	00-30-4f-24-24-24	3	Yes	3	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch

☐ Start Master Election

- Select the target switch and set up with lower priority "1", also re-assign the Switch ID=1 for it. After that click **Save**, click "Start Master Election" and save again.

Figure 4-130: Assigning a lower priority value for the target switch

Stack Configuration

Delete	Stack Member	Switch ID	Master		Description	Switch Type
			Capable	Priority		
<input type="checkbox"/>	00-30-4f-76-26-93	4	Yes	3	GE-DSSG-244-PoE	GE Security GE-DSSG-244-PoE Managed Switch
<input type="checkbox"/>	00-30-4f-76-c4-2b	1	Yes	1	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch
<input type="checkbox"/>	00-30-4f-24-24-24	3	Yes	2	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch

☐ Start Master Election

- Reflashing the web browser, the switch with MAC address "00-30-4f-76-26-93" now becomes the Stack Master.

Figure 4-131: The result after master election

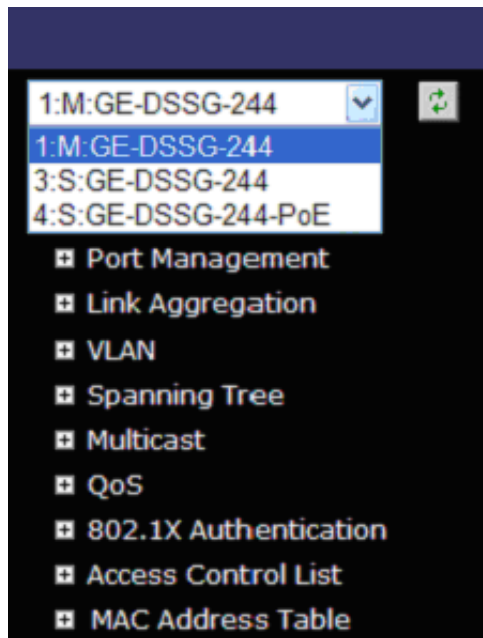
Stack Configuration

Delete	Stack Member	Switch ID	Master		Description	Switch Type
			Capable	Priority		
<input type="checkbox"/>	00-30-4f-76-c4-2b	1	Yes	1	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch
<input type="checkbox"/>	00-30-4f-24-24-24	3	Yes	3	GE-DSSG-244	GE Security GE-DSSG-244 Managed Switch
<input type="checkbox"/>	00-30-4f-76-26-93	4	Yes	3	GE-DSSG-244-PoE	GE Security GE-DSSG-244-PoE Managed Switch

☐ Start Master Election

Step 6: After the Stack Master and Members have been configured; any switch in the stack can be managed from the web agent by choosing the desired Member ID from the Switch drop down menu.

Figure 4-132: To manage the member switch



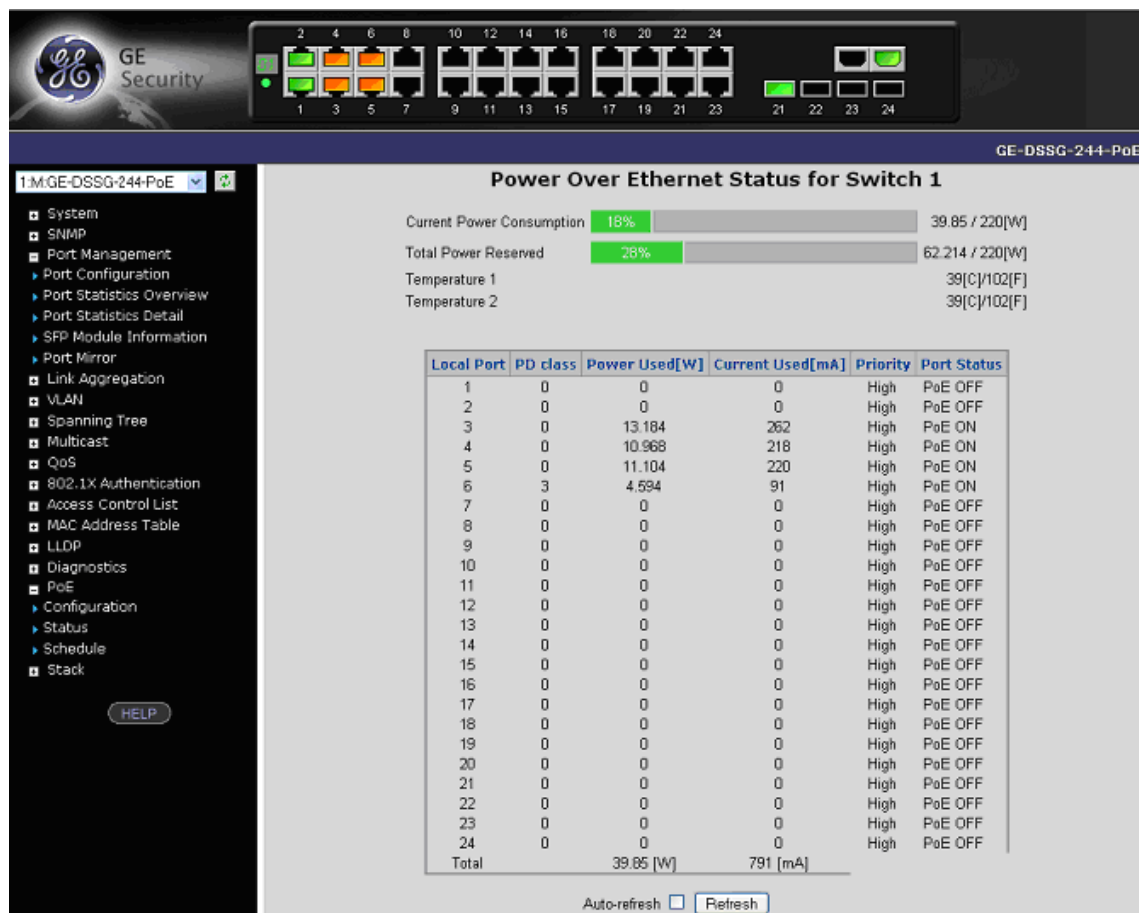
NOTE: Slave switch IP will be covered by Master one, and disappear temporarily. The slave IP address can be the same as Master IP address. Thus, if the master switch malfunctions, you can still access the other switch by same IP address.

NOTE: If you have difficulty on selecting another switch, you may be connecting to the slave switch's web, please close the browser window, use the "arp -d *" DOS command to clear the ARP table and then reopen the web.





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.

Figure 4-133: Power over Ethernet Status



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 Configuration

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.

Measuring voltage and current monitors the PSU input power consumption. 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, and maximum allowable power per port.

Reserved Power determined by

There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.

Classification mode

In this mode, each port automatic determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Three different port classes exist and one for 4, 7 and 15.4 Watts.

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 (or to 15.4Watts)
4	Not Allowed	Reserved for Future Use

NOTE: In this mode, the Maximum Power fields have no effect.

Allocation mode

In this mode, the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. The ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver.

NOTE: In this mode the port power is not turned on if the PD requests more power the available.

Auto mode

The Power Management function will automatically select the mode of operation, according to the following sequence:

- Port class, if available
- Power allocation, if available
- Port power consumption.

Consumption

In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

Priority mode

In this mode the user assign the priority to the ports/PD. When the total PoE power consumption request is over the allowed power supply limitation, the system shut down PoE ports by port priority setting.

Ethernet Port Configuration

This section allows the user to inspect and configure the current PoE port settings. The screen shown in Figure 4-134 appears.

Figure 4-134: Power over Ethernet Status

Power Over Ethernet Configuration for Switch 1

Power Management Mode Configuration

Mode
 Auto mode ▼

Power Supply Configuration

Power Supply [W]
 220

Ethernet Port Configuration

Port	PoE Enabled	Priority	Maximum Power [W]	Power Allocation[W]
1	✓	High ▼	15.4	15.4
2	✓	High ▼	15.4	15.4
3	✓	High ▼	15.4	15.4
4	✓	High ▼	15.4	15.4
5	✓	High ▼	15.4	15.4
6	✓	High ▼	15.4	15.4
7	✓	High ▼	15.4	15.4
8	✓	High ▼	15.4	15.4
9	✓	High ▼	15.4	15.4
10	✓	High ▼	15.4	15.4
11	✓	High ▼	15.4	15.4
12	✓	High ▼	15.4	15.4
13	✓	High ▼	15.4	15.4

This page includes the following fields:

Object	Description
Mode	<p>There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.</p> <p>Classification mode</p> <p>Allocation mode</p> <p>Auto mode</p> <p>Port class, if available</p> <p>Power allocation, if available</p> <p>Port power consumption.</p> <p>Consumption</p> <p>Priority mode</p> <p>The default PoE management mode is "Auto mode".</p>
Power Supply	<p>Set limit value of the total PoE port provided power to the PDs.</p> <p>For GE-DSSG-244-POE, the available max. value is 220.</p>
Local Port	This is the logical port number for this row.
PoE Enabled	The PoE Enabled represents whether the PoE is enable for the port.
Priority	<p>The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.</p> <p>The priority is used in the case where the remote devices requires uses more power than power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the lowest port number.</p>
Maximum Power	The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.
Power Allocation	<p>It can limit the port PoE supply watts. 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> <p>Note. The system PoE mode have to set to Allocation mode then it effect.</p>

NOTE: For GE-DSSG-244-POE, the total PoE power reservation from Port-1~24 is up to 220W.

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 4-4.

Table 4-4: Device class

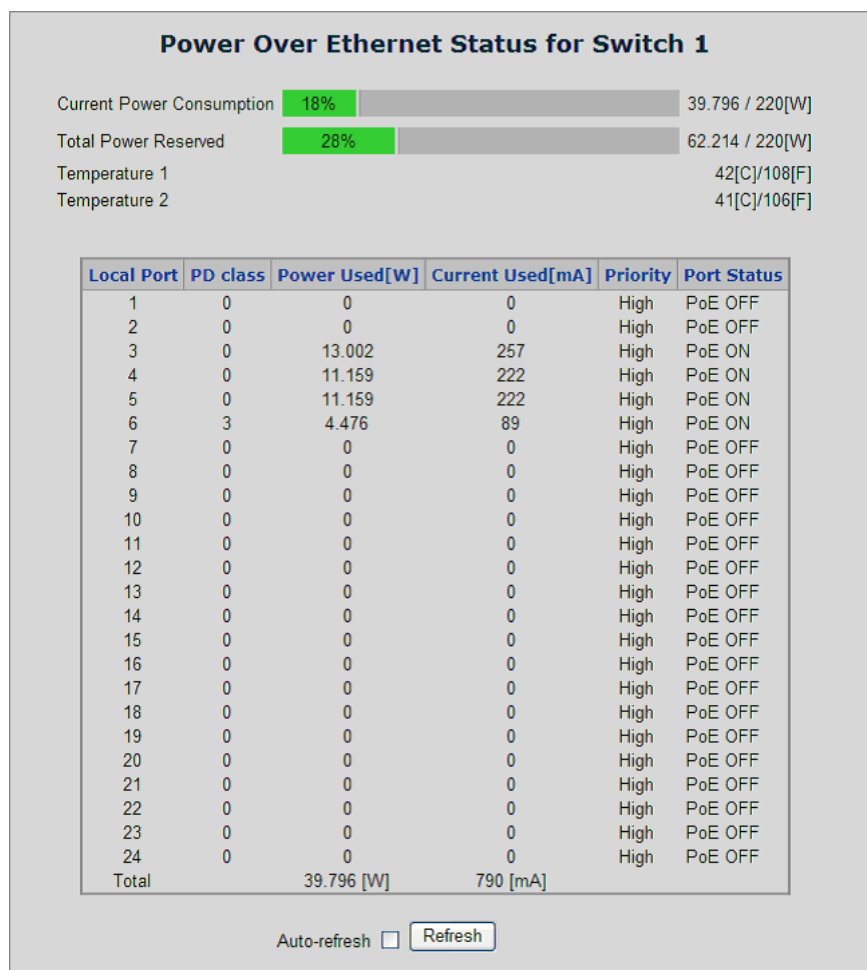
Class	Usage	Range of maximum power used by the PD
0	Default	0.44 to 12.95 Watts
1	Optional	0.44 to 3.84 Watts
2	Optional	3.84 to 6.49 Watts
3	Optional	6.49 to 12.95 Watts
4	Not Allowed	Reserved for Future Use

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

PoE Status

This page allows the user to inspect the total power consumption, total power reserved and current status for all PoE ports.

Figure 4-135: Power over Ethernet Status



This page includes the following fields:

Object	Description
Current Power Consumption	Show the total watts usage of PoE Switch.
Total Power Reserved	Shows how much the total power be reserved for all PDs.
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
Local Port	This is the logical port number for this row.

Object	Description
PD Class	<p>Display the class of the PD attached to the port, as established by the classification process.</p> <p>Class 0 is the default for PDs. 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 4-4.</p>
Power Reserved	The Power Reserved shows how much the power the PD has reserved.
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is using.
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status.
Total	Show the total watts usage of all PDs.

PoE Schedule

This section provides the user a way to configure a PoE schedule. The "PoE schedule" helps you to enable or disable PoE power feeding for PoE ports during specified time intervals and it is a powerful function to help SMB or Enterprise save power and money.

Figure 4-136: Power over Ethernet Status

Power Over Ethernet Schedulefor Switch 1

Current Time

1970-01-01 Thu 02:58:27 +0000

Mode

Enable

Port

Port 3

Schedule Day

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Day Start

09:00

Day End

20:00

Night Start

24:00

Night End

24:00

Save

Hour	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Mon	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Tue	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Wed	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Thu	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Fri	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Sat	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Refresh

This page includes the following fields:

Object	Description
Current Time	Display the current time of the System
Mode	Allow to enable or disable PoE Schedule function on selected port.
Port	Allow setting PoE schedule by specified port.
Schedule Day	Set to enable / disable PoE power providing by day.
Day Start	Allow selecting and setting which day time wants to start PoE power providing.
Day End	Allow selecting and setting which day time wants to stop PoE power providing.
Night Start	Allow selecting and setting which night time wants to start PoE power providing.
Night End	Allow selecting and setting which night time wants to stop PoE power providing.
Refresh	Press this button to refresh current Web page.

You need to select a target port manually to enable this function. The configuring tool could help you to set schedule quickly and easily.

For example, if user wants to set **[Port 3]** enables PoE power providing during AM 09:00 to PM 20:00, and only from Monday to Friday. It just needs to choice **3** at **Port** and select the check boxes from **Mon** to **Fri**, set Day Start Time to **9:00**, Day stop time to **18:00** and Night start time to **18:00**, Night stop time to **20:00**. Then click **"Save"**. The system will show "ON" for specified days and hours on the schedule table.

Figure 4-137: PoE Schedule configuration sample

Power Over Ethernet Schedule for Switch 1

Current Time

1970-01-01 Thu 03:32:45 +0000

Mode

Enable ▼

Port

Port 3 ▼

Schedule Day

☐ Sun
 ☒ Mon
 ☒ Tue
 ☒ Wed
 ☒ Thu
 ☒ Fri
 ☐ Sat

Day Start

09:00 ▼

Day End

18:00 ▼

Night Start

18:00 ▼

Night End

20:00 ▼

Hour	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Mon	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Tue	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Wed	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Thu	off	off	off	Now	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Fri	off	off	off	off	off	off	off	off	off	on	on	on	on	on	on	on	on	on	on	on	off	off	off	off
Sat	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Chapter 5

Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

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

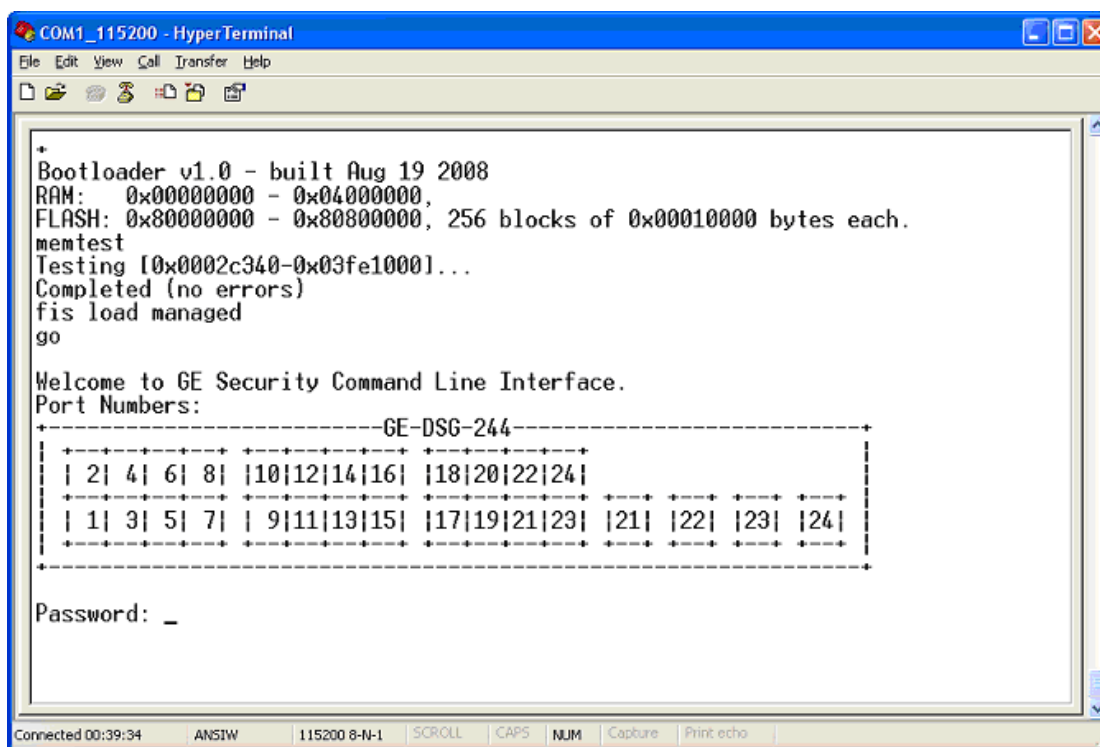
Logon to the Console

Once the terminal has connected to the device, power on the GE-DSG / GE-DSSG-244 series Managed Switch, the terminal will display that it is running testing procedures.

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

Password: admin

Figure 5-1: GE-DSG / GE-DSSG-244 series Managed Switch Console Login screen

**NOTE:**

1. For security reasons, please change and memorize the new password after this first setup.
2. Only enter commands in lowercase letter in the console interface.

Configure IP address

The GE-DSG / GE-DSSG-244 series Managed Switch is shipped with default IP address as following.

IP Address : 192.168.0.100

Subnet Mask : 255.255.255.0

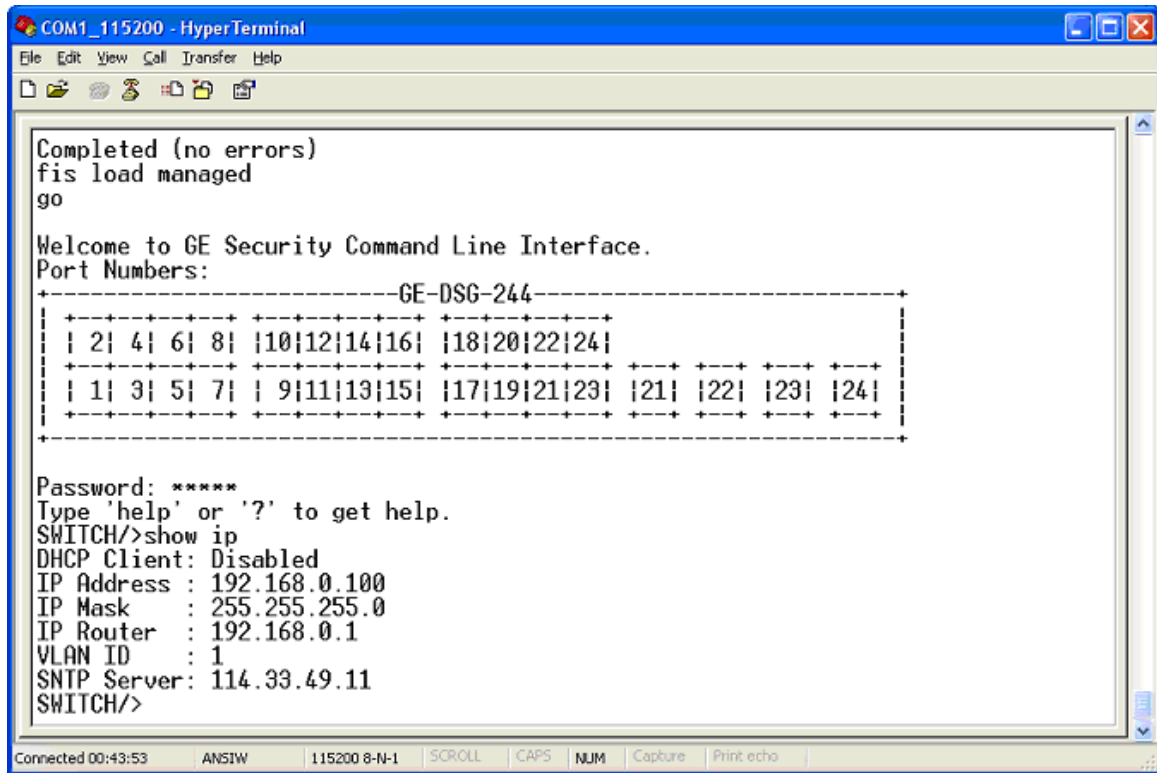
To check the current IP address or modify a new IP address for the Switch, please use the procedures as follow:

Show the current IP address

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

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

Figure 5-2: Show IP information screen



Configure IP address

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

Switch/> ip setup 192.168.1.100 255.255.255.0 192.168.1.1

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

IP: 192.168.1.100

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Figure 5-3: Set IP address screen

```

COM1_115200 - HyperTerminal
File Edit View Call Transfer Help

fis load managed
go

Welcome to GE Security Command Line Interface.
Port Numbers:
-----GE-DSG-244-----
+-----+
| 2| 4| 6| 8| 10|12|14|16| 18|20|22|24|
+-----+
| 1| 3| 5| 7| 9|11|13|15| 17|19|21|23| 21| 22| 23| 24|
+-----+

Password: *****
Type 'help' or '?' to get help.
SWITCH/>show ip
DHCP Client: Disabled
IP Address : 192.168.0.100
IP Mask : 255.255.255.0
IP Router : 192.168.0.1
VLAN ID : 1
SNTP Server: 114.33.49.11
SWITCH/>ip setup 192.168.1.100 255.255.255.0 192.168.1.1
SWITCH/>_

Connected 00:45:40 ANSIW 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```

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

If the IP is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of GE-DSG / GE-DSSG-244 series 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.

Telnet login

The Managed Switch also supports telnet for remote management. The switch asks for user name and password for remote login when using telnet, please use "admin" for password.

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

Figure 5-4: Telnet login screen

```

C:\ Telnet 192.168.0.100
Welcome to GE Security Command Line Interface.
Port Numbers:
+-----GE-DSG-244-----+
| +---+ +---+ +---+ +---+ +---+ +---+ +---+ +---+ |
| | 2| 4| 6| 8| |10|12|14|16| |18|20|22|24| |
| +---+ +---+ +---+ +---+ +---+ +---+ +---+ +---+ |
| | 1| 3| 5| 7| | 9|11|13|15| |17|19|21|23| |21| |22| |23| |24| |
| +---+ +---+ +---+ +---+ +---+ +---+ +---+ +---+ |
+-----+

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


Chapter 6

Command Line Mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

Command Groups

System	System settings and reset options
IP	IP configuration and Ping
Port	Port management
Aggr	Link Aggregation
LACP	Link Aggregation Control Protocol
RSTP	Rapid Spanning Tree Protocol
Dot1x	IEEE 802.1X port authentication
IGMP	Internet Group Management Protocol snooping
LLDP	Link Layer Discovery Protocol
MAC	MAC address table
VLAN	Virtual LAN
PVLAN	Private VLAN
QoS	Quality of Service
ACL	Access Control List
Mirror	Port mirroring
SNMP	Simple Network Management Protocol
Stack	Stack management
Firmware	Download of firmware via TFTP

System Command

System Configuration

Description:

Show system configuration.

Syntax:

System Configuration [all] [<port_list>]

Parameters:

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

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

Example:

To display system information:

```
Switch/>system configuration
System Name   : GE-DSSG-244
System Password: admin
CLI Prompt    : Switch
Timezone Offset: 0
MAC Address   : 00-30-4f-24-04-03
System Time   : 1970-01-01 03:13:21 +0000
System Uptime : 03:13:21

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

System Reboot

Description:

Reboot the system.

Syntax:

System Reboot

Example:

To reboot device without changing any of the settings:

```
Switch/>system reboot
```

System Restore Default**Description:**

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip: Keep IP configuration, default: Restore full configuration

Example:

To restore default value but not reset IP address:

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

System Name**Description:**

Set or show the system name.

Syntax:

System Name [<name>]

Parameters:

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

System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No blank or space characters are permitted as part of a name. The first character must be an alpha character, and the first or last character must not be a minus sign.

Default Setting:

GE-DSG-244

Example:

To set device title:

```
Switch/>>System name GE-DSG-244-LAB
```

System Prompt**Description:**

Set the CLI prompt string.

Syntax:

System Prompt <prompt>

Parameters:

<prompt>: CLI prompt string

Default Setting:

SWITCH

Example:

To change CLI title:

```
Switch/>>system prompt GE-DSSG-244  
GE-DSSG-244/>>
```

System Password**Description:**

Set or show the system password.

Syntax:

System Password [<password>]

Parameters:

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

Default Setting:

admin

Example:

To set password:

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

System SNTP**Description:**

Set or show the SNTP Time server address.

Syntax:

System SNTP [<ip_addr>]

Parameters:

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

Default Setting:

0.0.0.0

Example:

Set SNTP server:

```
SWITCH/>system sntp 220.130.158.52
```


System Timezone

Description:

Set or show the system timezone offset.

Syntax:

System Timezone [<offset>]

Parameters:

<offset>: Time zone offset in minutes (-720 to 720) relative to UTC

Default Setting:

0

Example:

To set timezone:

```
Switch/>system timezone 0
```

System Firmware Load

Description:

Load new firmware from TFTP server.

Syntax:

System Firmware Load <ip_server> <file_name>

Parameters:

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

<file_name>: Firmware file name

IP Configuration**Description:**

Show IP configuration.

Syntax:

IP Configuration

Example:

Show IP configuration:

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

IP DHCP**Description:**

Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable : Enable or renew DHCP client

disable: Disable DHCP client

Default Setting:

Disable

Example:

Disable DHCP server:

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

IP Setup

Description:

Set or show the IP setup.

Syntax:

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

Parameters:

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

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

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

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

Default Setting:

IP Address : 192.168.0.100

IP Mask : 255.255.255.0

IP Router : 192.168.0.1

VLAN ID : 1

Example:

Set IP address:

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

IP Ping**Description:**

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr> [<ping_length>]

Parameters:

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

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

Example:

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

Port Management Command

Port Configuration

Description:

Show port configuration.

Syntax:

Port Configuration [<port_list>]

Parameters:

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

Example:

Display port1~4 status:

```
SWITCH/>port configuration 1-4
```

Port	State	Mode	Flow Control	MaxFrame	Power	Excessive	Link
1	Enabled	Auto	Disabled	9600	Enabled	Discard	Down
2	Enabled	Auto	Disabled	9600	Enabled	Discard	Down
3	Enabled	Auto	Disabled	9600	Enabled	Discard	Down
4	Enabled	Auto	Disabled	9600	Enabled	Discard	100fdx

port state

Description:

Set or show the port administrative state.

Syntax:

Port State [<port_list>] [enable|disable]

Parameters:

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

enable : Enable port

disable : Disable port

(default: Show administrative mode)

Default Setting:

Enable

Example:

```
SWITCH/>port state 1 disable
```

Port Mode**Description:**

Set or show the port speed and duplex mode.

Syntax:

Port Mode [<port_list>] [10hdx|10fdx|100hdx|100fdx|1000fdx|auto]

Parameters:

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

10hdx : 10 Mbps, half duplex

10fdx : 10 Mbps, full duplex

100hdx : 100 Mbps, half duplex

100fdx : 100 Mbps, full duplex

1000fdx : 1 Gbps, full duplex

auto : Auto negotiation of speed and duplex

(default: Show configured and current mode)

Default Setting:

Auto

Example:

Set 10Mbps (half duplex) speed for port1

```
SWITCH/>port mode 1 10hdx
```

Port Flow Control

Description:

Set or show the port flow control mode.

Syntax:

Port Flow Control [<port_list>] [enable|disable]

Parameters:

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

enable : Enable flow control

disable : Disable flow control

(default: Show flow control mode)

Default Setting:

Disable

Example:

Enable flow control function for port1

```
SWITCH/>port flow control 1 enable
```

Port Maximum Frame

Description:

Set or show the port maximum frame size.

Syntax:

Port MaxFrame [<port_list>] [<max_frame>]

Parameters:

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

<max_frame>: Port maximum frame size (1518-9600), default: Show maximum frame size

Default Setting:

9600

Example:

Set 2048 frame size for port1

```
SWITCH/>port maxframe 1 2048
```

Port Power**Description:**

Set or show the port PHY power mode.

Syntax:

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:

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

enable : Enable all power control

disable: Disable all power control

actiphy: Enable ActiPHY power control

dynamic: Enable Dynamic power control

Default Setting:

Enable

Example:

Disable port power function for port1-4

```
SWITCH/>port power 1-4 disable
```

Port Excessive**Description:**

Set or show the port excessive collision mode.

Syntax:

Port Excessive [<port_list>] [discard|restart]

Parameters:

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

discard : Discard frame after 16 collisions

restart : Restart backoff algorithm after 16 collisions

(default: Show mode)

Default Setting:

Discard

Example:

SWITCH/>port excessive 1 restart

```
SWITCH/>port excessive 1 restart
```

Port Statistics**Description:**

Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>]

Parameters:

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

<command> : The command parameter takes the following values:

clear : Clear port statistics

packets : Show packet statistics

bytes : Show byte statistics

errors : Show error statistics

discards : Show discard statistics

filtered : Show filtered statistics

low : Show low priority statistics

normal : Show normal priority statistics

medium : Show medium priority statistics

high : Show high priority statistics

(default: Show all port statistics)

Port VeriPHY**Description:**

Run cable diagnostics.

Syntax:

Port VeriPHY [<port_list>]

Parameters:

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

Port Numbers**Description:**

Show port numbering.

Syntax:

Port Numbers

Mirror Configuration**Description:**

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

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

Mirror Port**Description:**

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

<port>|disable: Mirror port or 'disable', default: Show port

Default Setting:

Disable

Mirror SID

Description:

Set or show the mirror switch ID.

Syntax:

Mirror SID [<sid>]

Parameters:

<sid>: Switch ID (1-16)

Default Setting:

1

Example:

Set mirror SID 2 for switch

```
SWITCH/>mirror sid 2
```

Mirror Mode

Description:

Set or show the mirror mode.

Syntax:

Mirror Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

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

enable : Enable Rx and Tx mirroring

disable: Disable Mirroring

rx : Enable Rx mirroring

tx : Enable Tx mirroring

(default: Show mirror mode)

Default Setting:

Disable

Example:

Enable mirror mode for port20

```
SWITCH/>mirror mode 20 enable
```

Link Aggregation Command

Aggregation Configuration

Description:

Show link aggregation configuration.

Syntax:**Aggr Configuration****Example:**

```
SWITCH/>aggr configuration
Aggregation Mode:

SMAC : Enabled
DMAC : Disabled
IP   : Enabled
Port : Enabled
```

Aggregation Add

Description:

Add or modify link aggregation.

Syntax:

Aggr Add <port_list> [<aggr_id>]

Parameters:

<port_list>: Port list

<aggr_id> : Aggregation ID, global: 1-2, local: 3-14

Default Setting:

Disable

Example:

Add port 1~4 in Group1

```
SWITCH/>aggr add 1-4 1
```

Aggregation Delete**Description:**

Delete link aggregation.

Syntax:

Aggr Delete <aggr_id>

Parameters:

<aggr_id>: Aggregation ID, global: 1-2, local: 3-14

Example:

Delete Group2

```
SWITCH/>aggr delete 2
```

Aggregation Lookup**Description:**

Lookup link aggregation.

Syntax:

Aggr Lookup [<aggr_id>]

Parameters:

<aggr_id>: Aggregation ID, global: 1-2, local: 3-14

Example:

Show aggregation status

```
SWITCH/>aggr lookup 1
```

```
Aggr ID Name  Type  Ports
```

```
-----
```

```
1      GLAG1  Static  1-4
```

Aggregation Mode

Description:

Set or show the link aggregation traffic distribution mode.

Syntax:

Aggr Mode [smac|dmac|ip|port] [enable|disable]

Parameters:

smac	: Source MAC address
dmac	: Destination MAC address
ip	: Source and destination IP address
port	: Source and destination UDP/TCP port
enable	: Enable field in traffic distribution
disable	: Disable field in traffic distribution

Default Setting:

SMAC : Enabled

DMAC : Disabled

IP : Enabled

Port : Enabled

Example:

Disable SMAC mode

```
SWITCH/>Aggr mode smac disable
```

LACP Configuration

Description:

Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:

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

Example:

Show LACP configuration

```
SWITCH/>lacp configuration
```

Port	Mode	Key	Role
----	-----	----	-----
1	Disabled	Auto	Active
2	Disabled	Auto	Active
3	Disabled	Auto	Active
4	Disabled	Auto	Active
5	Disabled	Auto	Active
6	Disabled	Auto	Active
7	Disabled	Auto	Active
8	Disabled	Auto	Active
9	Disabled	Auto	Active
10	Disabled	Auto	Active
11	Disabled	Auto	Active
12	Disabled	Auto	Active
13	Disabled	Auto	Active
14	Disabled	Auto	Active
15	Disabled	Auto	Active
16	Disabled	Auto	Active
17	Disabled	Auto	Active
18	Disabled	Auto	Active
19	Disabled	Auto	Active
20	Disabled	Auto	Active
21	Disabled	Auto	Active
22	Disabled	Auto	Active
23	Disabled	Auto	Active
24	Disabled	Auto	Active

LACP Mode

Description:

Set or show LACP mode.

Syntax:

LACP Mode [<port_list>] [enable|disable]

Parameters:

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

enable : Enable LACP protocol

disable: Disable LACP protocol

(default: Show LACP mode)

Default Setting:

Disable

Example:

Enable LACP for port1~4

```
SWITCH/>lacp mode 1-4 enable
```

LACP Key

Description:

Set or show the LACP key.

Syntax:

LACP Key [<port_list>] [<key>]

Parameters:

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

<key> : LACP key (1-65535) or 'auto'

Default Setting:

Auto

Example:

Set key1 for port1~4

```
SWITCH/>lacp key 1-4 1
```

LACP Role**Description:**

Set or show the LACP role.

Syntax:

LACP Role [<port_list>] [active|passive]

Parameters:

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

active : Initiate LACP negotiation

passive: Listen for LACP packets

(default: Show LACP role)

Default Setting:

Active

Example:

Set passive for port1~4

```
SWITCH/>lacp role 1-4 passive
```

LACP Status**Description:**

Show LACP Status.

Syntax:

LACP Status [<port_list>]

Parameters:

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

Example:

Show LACP status of port1~4

```
SWITCH/>lacp status 1-4
```

Port	Mode	Key	Aggr ID	Partner System ID	Partner Port
1	Disabled	1	-	-	-
2	Disabled	1	-	-	-
3	Disabled	1	-	-	-
4	Disabled	1	-	-	-

LACP Statistics**Description:**

Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:

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

clear : Clear LACP statistics

Example:

Show LACP statistics of port1~4

```
SWITCH/>lacp statistics 1-4
```

Port	Rx Frames	Tx Frames	Rx Unknown	Rx Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0

VLAN Configuration Command

VLAN Configuration

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

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

Example:

Show VLAN status of port1

```
SWITCH/>vlan configuration 1

Mode : IEEE 802.1Q
Port PVID IngrFilter FrameType LinkType Q-in-Q Mode Eth type
-----
1 1 Disabled All UnTag Disable N/A

VID Ports
----
1 1-26
```

VLAN Mode

Description:

Set or show the VLAN Mode.

Syntax:

VLAN Mode [portbased|dot1q]

Parameters:

portbased : Port-Based VLAN Mode

dot1q : 802.1Q VLAN Mode

Default Setting:

Dot1q

Example:

Set VLAN mode in port base

```
SWITCH/>vlan mode portbased
```

VLAN PVID

Description:

Set or show the port VLAN ID.

Syntax:

VLAN PVID [<port_list>] [<vid>|none]

Parameters:

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

<vid>|none : Port VLAN ID (1-4095) or 'none', default: Show port VLAN ID

Default Setting:

1

Example:

Set PVID2 for port20

```
SWITCH/>vlan pvid 20 2
```

VLAN Frame Type

Description:

Set or show the port VLAN frame type.

Syntax:

VLAN FrameType [<port_list>] [all|tagged]

Parameters:

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

all : Allow tagged and untagged frames

tagged : Allow tagged frames only

(default: Show accepted frame types)

Default Setting:

All

Example:

Set port20 that allow tagged frames only

```
SWITCH/>vlan frametype 20 tagged
```

VLAN Ingress Filter**Description:**

Set or show the port VLAN ingress filter.

Syntax:

VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:

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

enable : Enable VLAN ingress filtering

disable : Disable VLAN ingress filtering

(default: Show VLAN ingress filtering)

Default Setting:

Disable

Example:

Enable VLAN ingress filtering for port20

```
SWITCH/>vlan ingressfilter 20 enable
```

VLAN Link Type**Description:**

Set or show the port VLAN link type.

Syntax:

VLAN LinkType [<port_list>] [untagged|tagged]

Parameters:

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

untagged : VLAN Link Type Tagged

tagged : VLAN Link Type Untagged

Default Setting:

Un-tagged

Example:

Enable tagged frame for port2

```
SWITCH/>vlan linktype 2 tagged
```

VLAN Q-in-Q Mode**Description:**

Set or show the port Q-in-Q mode.

Syntax:

VLAN Qinqmode [<port_list>] [disable|man|customer]

Parameters:

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

disable : Disable Q-in-Q VLAN Mode

man : Q-in-Q MAN Port Mode

customer : Q-in-Q Customer Port Mode

VLAN Ethernet Type**Description:**

Set or show out layer VLAN tag ether type in Q-in-Q VLAN mode.

Syntax:

VLAN Ethtype [<port_list>] [man|dot1q]

Parameters:

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

man : Set out layer VLAN tag ether type : MAN

dot1q : Set out layer VLAN tag ether type : 802.1Q

Default Setting:

N/A

Example:

```
SWITCH/>vlan ethtype 10 man
```

VLAN Add**Description:**

Add or modify VLAN entry.

Syntax:

VLAN Add <vid> [<port_list>]

Parameters:

<vid> : VLAN ID (1-4095)

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

Default Setting:

1

Example:

Add port17 to port24 in VLAN10

```
SWITCH/>vlan add 10 17-24
```


VLAN Delete

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>

Parameters:

<vid>: VLAN ID (1-4095)

Example:

Delete port17 to port24 in VLAN10

```
SWITCH/>vlan delete 10 17-24
```

VLAN Lookup

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>]

Parameters:

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

Example:

Show VLAN status

```
SWITCH/>vlan lookup
```

PVLAN Configuration

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

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

PVLAN Isolate

Description:

Set or show the port isolation mode.

Syntax:

PVLAN Isolate [<port_list>] [enable|disable]

Parameters:

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

enable : Enable port isolation

disable : Disable port isolation

(default: Show port isolation port list)

Default Setting:

Promiscuous

Example:

Enable isolate for port10

```
SWITCH/>pvlan isolate 10 enable
```

Spanning Tree Protocol Command

RSTP Configuration

Description:

Show RSTP configuration.

Syntax:

RSTP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Default Setting:

Disable

Example:

Show RSTP status of port1

```
SWITCH/>rstp configuration 1
System Priority : 32768
Max Age      : 20
Forward Delay : 15
Protocol Version: Normal

Port Mode    Path Cost  Priority  Edge    Point2point
-----
1  Disabled  Auto     128     Enabled  Auto
```

RSTP SysPrio

Description:

Set or show the RSTP system priority.

Syntax:

RSTP SysPrio [<sys_prio>]

Parameters:

<sys_prio>: RSTP system priority (0/4096/8192/.../57344/61440)

Default Setting:

32768

Example:

Set RSTP system priority value in 4096

```
SWITCH/>rstp sysprio 4096
```

RSTP Age**Description:**

Set or show the RSTP maximum age.

Syntax:

RSTP Age [<max_age>]

Parameters:

<max_age>: RSTP maximum age time (6-200)

Default Setting:

20

Example:

Set RSTP maximum age time in 200

```
SWITCH/>rstp age 200
```

RSTP Delay**Description:**

Set or show the RSTP forward delay.

Syntax:

RSTP Delay [<delay>]

Parameters:

<delay>: RSTP forward delay (4-30)

Default Setting:

15

Example:

Set RSTP forward delay value in 25

```
SWITCH/>rstp delay 25
```

RSTP Version

Description:

Set or show the RSTP protocol version.

Syntax:

RSTP Version [compatible|normal]

Parameters:

compatible: Compatible with STP

normal : RSTP

Default Setting:

Normal

Example:

Change RSTP version in compatible

```
SWITCH/>rstp version compatible
```

RSTP Mode

Description:

Set or show the RSTP mode.

Syntax:

RSTP Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

enable : Enable RSTP protocol

disable: Disable RSTP protocol

Default Setting:

Disable

Example:

Enable rstp mode for port1

```
SWITCH/>rstp mode 1 enable
```

RSTP Cost**Description:**

Set or show the RSTP path cost.

Syntax:

RSTP Cost [<port_list>] [<path_cost>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

<path_cost>: RSTP path cost (1-2000000000) or 'auto'

Default Setting:

Auto

Example:

Set RSTP cost value in 1 for port1

```
SWITCH/>rstp cost 1 1
```

RSTP Priority**Description:**

Set or show the RSTP priority.

Syntax:

RSTP Priority [<port_list>] [<priority>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

<priority> : RSTP priority (0/16/32/48/.../224/240)

Default Setting:

128

Example:

Set RSTP priority value in 16 for port1

```
SWITCH/>rstp priority 1 16
```

RSTP Edge**Description:**

Set or show the RSTP edge parameter.

Syntax:

RSTP Edge [<port_list>] [enable|disable]

Parameters:

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

enable : Enable RSTP edge

disable: Disable RSTP edge

Default Setting:

Enable

Example:

Disable RSTP edge parameter for port1

```
SWITCH/>rstp edge 1 disable
```

RSTP P2P**Description:**

Set or show the RSTP point2point parameter.

Syntax:

RSTP P2P [<port_list>] [enable|disable|auto]

Parameters:

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

enable : Enable RSTP point2point

disable: Disable RSTP point2point

auto : Automatic RSTP point2point detection

Default Setting:

Auto

Example:

Enable RSTP P2P mode for port1

```
SWITCH/>rstp p2p 1 enable
```

RSTP Status**Description:**

Show RSTP status.

Syntax:

RSTP Status [<port_list>]

Parameters:

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

Example:

Show RSTP status

```
SWITCH/>rstp status
```

```
=====
VLAN ID   : 3
Bridge ID  : 32771:00-30-4f-24-24-c1
Root ID    : 32771:00-30-4f-24-24-c1
Root Port  : -
Root Cost  : 0
Topology Flag: Steady
```

Port	Port Role	State	Path Cost	Edge	P2P	Neighb
1	Disabled	Disabled	1	No	Yes	RSTP

RSTP Statistics**Description:**

Show RSTP statistics.

Syntax:

RSTP Statistics [<port_list>]

Parameters:

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

RSTP mCheck**Description:**

Set the RSTP mCheck (Migration Check) variable for ports.

Syntax:

RSTP Mcheck [<port_list>]

Parameters:

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

Multicast Configuration Command

IGMP Configuration

Description:

Show IGMP snooping configuration.

Syntax:

IGMP Configuration [<port_list>]

Parameters:

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

Default Setting:

IGMP Mode: Disabled

Flooding : Disabled

Example:

Enable IGMP mode

```
SWITCH/>igmp mode enable
```

IGMP Mode

Description:

Set or show the IGMP snooping mode.

Syntax:

IGMP Mode [enable|disable]

Parameters:

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

Disabled

Example:

Enable IGMP mode

```
SWITCH/>igmp mode enable
```

IGMP State**Description:**

Set or show the IGMP snooping state for VLAN.

Syntax:

IGMP State [<vid>] [enable|disable]

Parameters:

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

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

VID State

---- -

1 Enabled

Example:

Enable IGMP mode

```
SWITCH/>igmp mode enable
```

IGMP State**Description:**

Set or show the IGMP snooping state for VLAN.

Syntax:

IGMP State [<vid>] [enable|disable]

Parameters:

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

enable : Enable IGMP snooping

disable: Disable IGMP snooping

(default: Show IGMP snooping mode)

Default Setting:

Enable

Example:

Disable VID 1

```
SWITCH/>igmp state 1 disable
```

IGMP Querier**Description:**

Set or show the IGMP snooping querier mode for VLAN.

Syntax:

IGMP Querier [<vid>] [enable|disable]

Parameters:

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

enable : Enable IGMP querier

disable : Disable IGMP querier

(default: Show IGMP querier mode)

Default Setting:

Disable

Example:

```
SWITCH/>igmp querier 1 enable
```

IGMP Fast Leave

Description:

Set or show the IGMP snooping fast leave port mode.

Syntax:

IGMP Fastleave [<port_list>] [enable|disable]

Parameters:

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

enable : Enable IGMP fast leave

disable : Disable IGMP fast leave

(default: Show IGMP fast leave mode)

Default Setting:

Disable

Example:

```
SWITCH/>igmp fastleave 1 enable
```

IGMP Router

Description:

Set or show the IGMP snooping router port mode.

Syntax:

IGMP Router [<port_list>] [enable|disable]

Parameters:

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

enable : Enable IGMP router port

disable : Disable IGMP router port

(default: Show IGMP router port mode)

Default Setting:

Disable

Example:

Enable IGMP snooping function for port1~4

```
SWITCH/>igmp router 1-4 enable
```

IGMP Flooding**Description:**

Set or show the IGMP snooping unregistered flood operation.

Syntax:

IGMP Flooding [enable|disable]

Parameters:

enable : Enable IGMP flooding

disable: Disable IGMP flooding

(default: Show IGMP flood mode)

Default Setting:

Disable

Example:

Enable IGMP flooding function

```
SWITCH/>igmp flooding enable
```

IGMP Groups**Description:**

Show IGMP groups.

Syntax:

IGMP Groups [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

IGMP Status

Description:

Show IGMP status.

Syntax:

IGMP Status [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

Default Setting:

Disable

Example:

Enable IGMP flooding function

```
SWITCH/>igmp status 1

Switch 1:
-----

  Querier  Rx    Tx    Rx    Rx    Rx    Rx
VID  Status  Queries  Queries  V1 Reports  V2 Reports  V3 Reports  V2 Leave
-----
1   IDLE    0      0      0      0      0      0
```

Quality of Service Command

QoS Configuration

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

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

QoS Classes

Description:

Set or show the number of traffic classes.

Syntax:

QoS Classes [<class>]

Parameters:

<class>: Number of traffic classes (1,2 or 4)

Default Setting:

4

Example:

Set QoS classes 2

```
SWITCH/>qos classes 2
```

QoS Default

Description:

Set or show the default port priority.

Syntax:

QoS Default [<port_list>] [<class>]

Parameters:

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

<class> : Traffic class low/normal/medium/high or 1/2/3/4

Default Setting:

Low

Example:

Set high priority for port5

```
SWITCH/>qos default 5 high
```

QoS Tag Priority**Description:**

Set or show the port VLAN tag priority.

Syntax:

QoS Tagprio [<port_list>] [<tag_prio>]

Parameters:

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

<tag_prio> : VLAN tag priority (0-7)

Default Setting:

0

Example:

Set priority7 for VLAN3

```
SWITCH/>qos tagprio 3 7
```

QoS QCL Port**Description:**

Set or show the port QCL ID.

Syntax:

QoS QCL Port [<port_list>] [<qcl_id>]

Parameters:

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

<qcl_id> : QCL ID

Default Setting:

1

Example:

Set QCL ID5 for port10

```
SWITCH/>qos qcl port 10 5
```

QoS QCL Add**Description:**

Add or modify QoS Control Entry (QCE).

If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used.

If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next QCE ID is not specified, the QCE will be placed last in the list.

Syntax:

QoS QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]

(etype <etype>) |

(vid <vid>) |

(port <udp_tcp_port>) |

(dscp <dscp>) |

(tos <tos_list>) |

(tag_prio <tag_prio_list>)

<class>

Parameters:

<qcl_id> : QCL ID

<qce_id> : QCE ID (1-24)

<qce_id_next> : Next QCE ID (1-24)

etype : Ethernet Type keyword

<etype> : Ethernet Type

vid : VLAN ID keyword

<vid> : VLAN ID (1-4095)

port : UDP/TCP port keyword

<udp_tcp_port> : Source or destination UDP/TCP port (0-65535)

dscp : IP DSCP keyword

<dscp> : IP DSCP (0-63)

tos : IP ToS keyword

<tos_list> : IP ToS list (0-7)

tag_prio : VLAN tag priority keyword

<tag_prio_list>: VLAN tag priority list (0-7)

<class> : Traffic class low/normal/medium/high or 1/2/3/4

QoS QCL Delete

Description:

Delete QCE.

Syntax:

QoS QCL Delete <qcl_id> <qce_id>

Parameters:

<qcl_id>: QCL ID

<qce_id>: QCE ID (1-24)

QoS QCL Lookup**Description:**

Lookup QCE.

Syntax:

QoS QCL Lookup [<qcl_id>] [<qce_id>]

Parameters:

<qcl_id>: QCL ID

<qce_id>: QCE ID (1-24)

QoS Mode**Description:**

Set or show the port egress scheduler mode.

Syntax:

QoS Mode [<port_list>] [strict|weighted]

Parameters:

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

strict : Strict mode

weighted: Weighted mode

(default: Show QoS mode)

Default Setting:

Strict

Example:

Set weighted mode for port15

```
SWITCH/>qos mode 15 weighted
```

QoS Weight**Description:**

Set or show the port egress scheduler weight.

Syntax:

QoS Weight [<port_list>] [<class>] [<weight>]

Parameters:

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

<class> : Traffic class low/normal/medium/high or 1/2/3/4

<weight> : Traffic class weight 1/2/4/8

QoS Rate Limiter**Description:**

Set or show the port rate limiter.

Syntax:

QoS Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

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

enable : Enable rate limiter

disable : Disable rate limiter

(default: Show rate limiter mode)

<bit_rate> : Rate in 1000 bits per second (500-1000000 kbps)

Default Setting:

Disabled, 500kbps

Example:

Set 1000kbps rate limiter for port17~24

```
SWITCH/>qos rate limiter 17-24 enable 1000
```

QoS Shaper**Description:**

Set or show the port shaper.

Syntax:

QoS Shaper [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

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

enable : Enable shaper

disable : Disable shaper

(default: Show shaper mode)

<bit_rate> : Rate in 1000 bits per second (500-1000000 kbps)

Default Setting:

Disabled, 500kbps

Example:

Set 1000kbps shaper for port 9~16

```
SWITCH/>qos shaper 9-16 enable 1000
```

QoS Unicast**Description:**

Set or show the unicast storm rate limiter.

Syntax:

QoS Storm Unicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable unicast storm control

disable : Disable unicast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable unicast storm rate limiter in 1kpps

```
SWITCH/>qos storm unicast enable 1k
```

QoS Multicast**Description:**

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable multicast storm control

disable : Disable multicast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable multicast storm rate limiter in 1kpps

```
SWITCH/>qos storm multicast enable 1k
```

QoS Broadcast**Description:**

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Broadcast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable broadcast storm control

disable : Disable broadcast storm control

<packet_rate>: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

Disabled, 1pps

Example:

Enable broadcast storm rate limiter in 1kpps

802.1x Port Access Control Command

Dot1x Configuration

Description:

Show 802.1X configuration.

Syntax:

Dot1x Configuration [<port_list>]

Parameters:

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

Example:

Show IEEE802.1x status of port1

```
SWITCH/>dot1x configuration 1
Mode      : Disabled
RADIUS Server : 0.0.0.0
RADIUS Secret :
Reauthentication: Disabled
Period     : 3600
Timeout    : 30
Age Period  : 300
Hold Time   : 10

Port  Admin State  Port State    Last Source  Last ID
-----
1    Authorized    802.1X Disabled  -            -
```

Dotx1 Mode

Description:

Set or show the 802.1X mode for the switch.

Syntax:

Dot1x Mode [enable|disable]

Parameters:

enable : Enable 802.1X

disable: Disable 802.1X

(default: Show 802.1X mode)

Default Setting:

Disable

Example:

Enable IEEE802.1x function for port1

```
SWITCH/>dot1x mode enable
```

Dot1x Status**Description:**

Set or show the 802.1X port state.

Syntax:

Dot1x State [<port_list>] [macbased|auto|authorized|unauthorized]

Parameters:

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

macbased : Switch performs 802.1X authentication on behalf of the client

auto : Port access requires 802.1X authentication

authorized : Port access is allowed

unauthorized: Port access is not allowed

(default: Show 802.1X state)

Default Setting:

Authorized

Example:

Change IEEE802.1x mode in auto.

```
SWITCH/>dot1x state 1 auto
```

Dot1x Server

Description:

Set or show the RADIUS server IP address.

Syntax:

Dot1x Server [<ip_addr>]

Parameters:

ip_addr: RADIUS server IP address (a.b.c.d) (default: Show IP address)

Default Setting:

0.0.0.0

Example:

Set RADIUS server IP address for switch. RADIUS server IP address is 192.168.0.254.

```
SWITCH/>dot1x server 192.168.0.254
```

Dot1x Secret

Description:

Set or show the secret shared with the RADIUS server.

Syntax:

Dot1x Secret [<shared_secret>]

Parameters:

<shared_secret>: Secret shared with external RADIUS server. To set an empty secret, use two quotes (""). To use spaces in secret, enquote the secret. Quotes in the secret are not allowed.

(default: Show shared secret)

Default Setting:

empty

Example:

Set authentication key "123abc@" in switch with the RADIUS server.

```
SWITCH/>dot1x secret 123abc@
```

Dot1x Authenticate**Description:**

Refresh (restart) 802.1X authentication process.

Syntax:

Dot1x Authenticate [<port_list>] [now]

Parameters:

<port_list>: Port list or 'all', default: All ports now: Force reauthentication immediately

Dot1x Re-authentication**Description:**

Set or show Reauthentication mode.

Syntax:

Dot1x Reauthentication [enable|disable]

Parameters:

enable : Enable reauthentication

disable: Disable reauthentication

(default: Show reauthentication mode)

Default Setting:

Disable

Example:

Enable re-authentication function

```
SWITCH/>dot1x reauthentication enable
```

Dot1x Period

Description:

Set or show the period between reauthentications.

Syntax:

Dot1x Period [<reauth_period>]

Parameters:

<reauth_period>: Period between reauthentications (1-3600 seconds)

(default: Show reauthentication period)

Default Setting:

3600

Example:

Set period re-authentication time in 3000 seconds

```
SWITCH/>dot1x period 3000
```

Dot1x Timeout

Description:

Set or show the time between EAPOL retransmissions.

Syntax:

Dot1x Timeout [<eapol_timeout>]

Parameters:

<eapol_timeout>: Time between EAPOL retransmissions (1-255 seconds)

(default: Show retransmission timeout)

Default Setting:

30

Example:

Set re-transmission time in 60 seconds

```
SWITCH/>dot1x timeout 60
```

Dot1x Statistics**Description:**

Show 802.1X statistics.

Syntax:**Dot1x Statistics** [<port_list>] [clear|eapol|radius]**Parameters:**

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

clear : Clear statistics

eapol : Show EAPOL statistics

radius : Show RADIUS statistics

(default: Show all statistics)

Dot1x Clients**Description:**

Set or show the maximum number of allowed clients for MAC-based ports.

Syntax:**Dot1x Clients** [<port_list>] [all|<client_cnt>]

Parameters:

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

all|<client_cnt>: MAC-based authentication: Set maximum number of clients allowed on a port.

all : Allow all new clients

<client_cnt>: A number ≥ 1

(default: Show current maximum)

Default Setting:

All

Dot1x Agetime**Description:**

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Dot1x Agetime [<age_time>]

Parameters:

<age_time>: Time between checks for activity on a MAC address that succeeded authentication

(default: Show age time)

Default Setting:

300

Example:

Set age time in 100 seconds

```
SWITCH/>dot1x agetime 100
```

Dot1x Holdtime**Description:**

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Dot1x Holdtime [<hold_time>]

Parameters:

<hold_time>: Hold time before MAC addresses that failed authentication expire
(default: Show hold time)

Default Setting:

10

Example:

Set hold time in 100 seconds

```
SWITCH/>dot1x holdtime 100
```


Access Control List Command

ACL Configuration

Description:

Show ACL Configuration.

Syntax:

ACL Configuration [<port_list>]

Parameters:

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

Default Setting:

300

Example:

Set age time in 100 seconds

```
SWITCH/>dot1x agetime 100
```

ACL Action

Description:

Set or show the ACL port default action.

Syntax:

ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>]
[<shutdown>]

Parameters:

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

permit : Permit forwarding (default)

deny : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy> : Port number for copy of frames or 'disable'

<logging> : System logging of frames: log|log_disable

<shutdown> : Shut down ingress port: shut|shut_disable

Default Setting:

Action: Permit

Rate Limiter: Disable

Port Copy: Disable

Loading: Disable

Shut down: Disable

Example:

????

```
SWITCH/>acl action 17-24 deny 1 24 log shut
```

ACL Policy**Description:**

Set or show the ACL port policy.

Syntax:

ACL Policy [<port_list>] [<policy>]

Parameters:

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

<policy> : Policy number (1-8)

Default Setting:

1

Example:

Set policy ID 8 for port 17-24

```
SWITCH/>acl policy 17-24 8
```

ACL Rate**Description:**

Set or show the ACL rate limiter.

Syntax:

ACL Rate [<rate_limiter_list>] [<packet_rate>]

Parameters:

<rate_limiter_list>: Rate limiter list (1-15), default: All rate limiters

<packet_rate> : Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

1

Example:

???

```
SWITCH/>acl rate 15 1024k
```

ACL Add**Description:**

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to Syntax:

ACL Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<sid>] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>])

<ace_id> : ACE ID (1-1024), default: Next available ID

<ace_id_next> : Next ACE ID (1-1024), default: Add ACE last

switch : Switch ACE keyword
 port : Port ACE keyword
 <port> : Port number
 policy : Policy ACE keyword
 <policy> : Policy number (1-8)
 <sid> : Switch ID (1-16) or 'any'
 <vid> : VLAN ID (1-4095) or 'any'
 <tag_prio> : VLAN tag priority (0-7) or 'any'
 <dmac_type> : DMAC type: any|unicast|multicast|broadcast
 etype : Ethernet Type keyword
 <etype> : Ethernet Type or 'any'
 <smac> : Source MAC address (xx-xx-xx-xx-xx-xx) or 'any'
 <dmac> : Destination MAC address (xx-xx-xx-xx-xx-xx) or 'any'
 arp : ARP keyword
 <sip> : Source IP address (a.b.c.d/n) or 'any'
 <dip> : Destination IP address (a.b.c.d/n) or 'any'
 <arp_opcode> : ARP operation code: any|arp|rarp|other
 <arp_flags> : ARP flags: request|smac|tmac|len|ip|ether [0|1|any]
 ip : IP keyword
 <protocol> : IP protocol number (0-255) or 'any'
 <ip_flags> : IP flags: ttl|options|fragment [0|1|any]
 icmp : ICMP keyword
 <icmp_type> : ICMP type number (0-255) or 'any'
 <icmp_code> : ICMP code number (0-255) or 'any'
 udp : UDP keyword
 <sport> : Source UDP/TCP port range (0-65535) or 'any'
 <dport> : Destination UDP/TCP port range (0-65535) or 'any'
 tcp : TCP keyword
 <tcp_flags> : TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]
 permit : Permit forwarding (default)
 deny : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'
<port_copy> : Port number for copy of frames or 'disable'
<logging> : System logging of frames: log|log_disable
<shutdown> : Shut down ingress port: shut|shut_disable

ACL Delete

Description:

Delete ACE.

Syntax:

ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-1024)

ACL Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

ACL Lookup [<ace_id>]

Parameters:

<ace_id>: ACE ID (1-1024)

ACL Clear

Description:

Clear all ACL counters.

Syntax:

ACL Clear

MAC Address Table Command

MAC Configuration

Description:

Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

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

Example:

Show port1 Mac state

```
SWITCH/>mac configuration 1
```

```
MAC Age Time: 300
```

```
Switch 1:
```

```
-----
```

```
Port Learning
```

```
-----
```

```
1    Auto
```

Mac Add

Description:

Add MAC address table entry.

Syntax:

MAC Add <mac_addr> <port_list> [<vid>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

<port_list>: Port list or 'all' or 'none'

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

Example:

Add Mac address 00-30-4F-01-01-02 in port1 and vid1

```
SWITCH/>mac add 00-30-4f-01-01-02 1 1
```

MAC Delete**Description:**

Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

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

Example:

Delete Mac address 00-30-4F-01-01-02 in vid1

```
SWITCH/>mac delete 00-30-4f-01-01-02 1
```

MAC Lookup**Description:**

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

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

Example:

Lookup state of Mac address 00-30-4F-01-01-02

```
SWITCH/>mac lookup 00-30-4f-01-01-02
```

MAC Age Time**Description:**

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-1000000), default: Show age time

Default Setting:

300

Example:

Set agetime value in 30

```
SWITCH/>mac agetime 30
```

MAC Learning**Description:**

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

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

auto : Automatic learning

disable: Disable learning

secure : Secure learning

(default: Show learn mode)

Default Setting:

Auto

Example:

Set secure learning mode in port1

```
SWITCH/>mac learning 1 secure
```

MAC Dump**Description:**

Show sorted list of MAC address entries.

Syntax:

MAC Dump [<mac_max>] [<mac_addr>] [<vid>]

Parameters:

<mac_max> : Maximum number of MAC addresses 1-8192, default: Show all addresses

<mac_addr>: First MAC address (xx-xx-xx-xx-xx-xx), default: MAC address zero

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

Example:

Show all of MAC table

```
SWITCH/>mac dump
```

MAC Statistics**Description:**

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

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

Example:

Set all of MAC statistics

```
SWITCH/>mac statistics
```

MAC Flush**Description:**

Flush all learned entries.

Syntax:

MAC Flush

LLDP Command

LLDP Configuration

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

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

LLDP Mode

Description:

Set or show LLDP mode.

Syntax:

LLDP Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

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

enable : Enable LLDP reception and transmission

disable: Disable LLDP

rx : Enable LLDP reception only

tx : Enable LLDP transmission only

(default: Show LLDP mode)

Default Setting:

Disable

Example:

Enable port1 LLDP function.

```
SWITCH/>>lldp mode 1 enable
```

LLDP Optional TLV**Description:**

Show / Set LLDP Optional TLVs.

Syntax:

LLDP Optional_TLV [<port_list>]
 [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Parameters:

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

port_descr : Description of the port

sysm_name : System name

sys_descr : Description of the system

sys_capa : System capabilities

mgmt_addr : Master's IP address

(default: Show optional TLV's configuration)

enable : Enables TLV

disable : Disable TLV

(default: Show optional TLV's configuration)

Default Setting:

Description of the port: Enable

System name: Enable

Description of the system: Enable

System capabilities: Enable

Master's IP address: Enable

Example:

Disable description of the port for port1

```
SWITCH/>lldp optional_tlv 1 port_descr disable
```

LLDP Interval

Description:

Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

<interval>: LLDP transmission interval (5-32768)

Default Setting:

30

Example:

Set transmission interval in 10

```
SWITCH/>lldp interval 10
```

LLDP Hold

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

<hold>: LLDP hold value (2-10)

Default Setting:

3

Example:

Set LLDP hold value in 10

```
SWITCH/>lldp hold 10
```

LLDP Delay**Description:**

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

<delay>: LLDP transmission delay (1-8192)

Default Setting:

2

Example:

Set LLDP delay value in 1

```
SWITCH/>lldp delay 1
```

LLDP Reinit**Description:**

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

<reinit>: LLDP reinit delay (1-10)

Default Setting:

2

Example:

Set LLDP reinit delay value in 3

```
SWITCH/>lldp reinit 3
```

LLDP Information

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

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

LLDP Statistics

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

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

clear : Clear LLDP statistics

Stack Management Command

Stack List

Description:

Show the list of switches in stack.

Syntax:

Stack List [detailed|productinfo]

Parameters:

detailed: Show detailed information

Stack List

Description:

Set the master election priority.

Syntax:

Stack Master Priority <sid>|local <mst_elect_prio>

Parameters:

<sid>|local : Switch ID (1-16) or local switch

<mst_elect_prio>: Master election priority: 1-4. 1 => Highest master probability

Example:

Set low priority for switch2

```
SWITCH/>stack master priority 2 4
```

Stack Master Reelect

Description:

Force master reelection (ignoring master time).

Syntax:

Stack Master Reelect

Stack Select

Description:

Set or show the selected switch ID.

Syntax:

Stack Select [<sid>|all]

Parameters:

<sid>: Switch ID (1-16), default: Show SID

Example:

Select switch2 to management switch2

```
SWITCH/>stack select 2
```

Stack SID Swap

Description:

Swap SID values used to identify two switches.

Syntax:

Stack SID Swap <sid> <sid>

Parameters:

<sid>: Switch ID (1-16)

Example:

Swap switch ID 1 and 2

```
SWITCH/>stack sid swap 2 1
```

Stack SID Delete**Description:**

Delete SID assignment and associated configuration.

Syntax:

Stack SID Delete <sid>

Parameters:

<sid>: Switch ID (1-16)

Stack SID Assign**Description:**

Assign SID and associated configuration to switch.

SID must be unassigned, switch must be present and switch must not already be assigned to a SID.

Syntax:

Stack SID Assign <sid> <mac_addr>

Parameters:

<sid> : Switch ID (1-16)

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

Example:

Assign SID2 for switch that use MAC address 00-30-4f-24-04-76

```
SWITCH/>stack sid assign 2 00-30-4f-24-04-76
```

Power over Ethernet Command

PoE Configuration

Description:

Show PoE configuration.

Syntax:

PoE Configuration

Example:

```
SWITCH/>poe configuration
```

Port	Mode	Priority	Max.Power[W]	PowerAlloc[W]
1	Enabled	High	15.4	15.4
2	Enabled	High	15.4	15.4
3	Enabled	High	15.4	15.4
4	Enabled	High	15.4	15.4
5	Enabled	High	15.4	15.4
6	Enabled	High	15.4	15.4
7	Enabled	High	15.4	15.4
8	Enabled	High	15.4	15.4
9	Enabled	High	15.4	15.4
10	Enabled	High	15.4	15.4
11	Enabled	High	15.4	15.4
12	Enabled	High	15.4	15.4
13	Enabled	High	15.4	15.4
14	Enabled	High	15.4	15.4
15	Enabled	High	15.4	15.4
16	Enabled	High	15.4	15.4
17	Enabled	High	15.4	15.4
18	Enabled	High	15.4	15.4
19	Enabled	High	15.4	15.4
20	Enabled	High	15.4	15.4
21	Enabled	High	15.4	15.4

```

22  Enabled High  15.4    15.4
23  Enabled High  15.4    15.4
24  Enabled High  15.4    15.4

```

Power Supply Max.

220 [W]

Power management mode

Power management mode : automode

PoE Mode

Description:

Set or show PoE mode.

Syntax:

PoE Mode [<port_list>] [enable|disable]

Parameters:

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

enable : Enables PoE

disable : Disable PoE

(default: Show PoE's mode)

PoE Priority

Description:

Show / Set PoE Priority.

Syntax:

PoE Priority [<port_list>] [low|high|critical]

Parameters:

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

low : Set priority to low

high : Set priority to high

critical : Set priority to critical

(default: Show PoE priority)

PoE Mgmt_mode**Description:**

Show / Set PoE management mode.

Syntax:

PoE Mgmt_mode [mgt_class|mgt_alloc|mgt_auto|mgt_consumption|mgt_priority]

Parameters:

mgt_class : handle power allocation according to PD class

mgt_alloc : power allocated according to values entered in power allocate

mgt_auto : automatic mode , according to the sequence:
class,allocation,consumption.

mgt_consumption : allocated according to PD actual need , with a maximum of 15.4
W per port

mgt_priority : max. port power determined by priority

(default: Show PoE power management mode)

Example:

```
SWITCH/> poe mgmt_mode

Power management mode
-----
Power management mode : automode
```

PoE Maximum_Power**Description:**

Set or show PoE maximum power per port (0-15.4, with one digit).

Syntax:

PoE Maximum_Power [<port_list>] [<port_power>]

Parameters:

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

<port_power>: PoE maximum power for the port (0-15.4)

PoE Alloc_Power**Description:**

PoE Alloc_Power [<port_list>] [<alloc_power>].

Syntax:

PoE Mgmt_mode [mgt_class|mgt_alloc|mgt_auto|mgt_consumption|mgt_priority]

Parameters:

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

<alloc_power>: PoE maximum power allocated for the port (0-15.4)

PoE Power_Supply**Description:**

Set or show the value of the power supply.

Syntax:

PoE Power_Supply [<supply_power>]

Parameters:

<supply_power>: PoE power for a power supply

PoE Status**Description:**

Show PoE status.

Syntax:**PoE Status****Example:**

```
SWITCH/> poe status
```

Port	Port Status	PD Class	Power Used [W]	Current Used [mA]
1	PoE ON	2	4.8	95
2	PoE OFF	0	0.0	0
3	PoE OFF	0	0.0	0
4	PoE OFF	0	0.0	0
5	PoE OFF	0	0.0	0
6	PoE OFF	0	0.0	0
7	PoE OFF	0	0.0	0
8	PoE OFF	0	0.0	0
9	PoE OFF	0	0.0	0
10	PoE OFF	0	0.0	0
11	PoE OFF	0	0.0	0
12	PoE OFF	0	0.0	0
13	PoE OFF	0	0.0	0
14	PoE OFF	0	0.0	0
15	PoE OFF	0	0.0	0
16	PoE OFF	0	0.0	0
17	PoE OFF	0	0.0	0
18	PoE OFF	0	0.0	0
19	PoE OFF	0	0.0	0
20	PoE OFF	0	0.0	0
21	PoE OFF	0	0.0	0
22	PoE OFF	0	0.0	0
23	PoE OFF	0	0.0	0

```
24 PoE OFF      0    0.0    0
Total           4.8    95

Current Power Consumption 4.8[W] (2%)
Total Power Reserved     7.268[W] (3%)
Temperature 1            37 (C) / 98 (F)
Temperature 2            43 (C) / 109 (F)
```


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

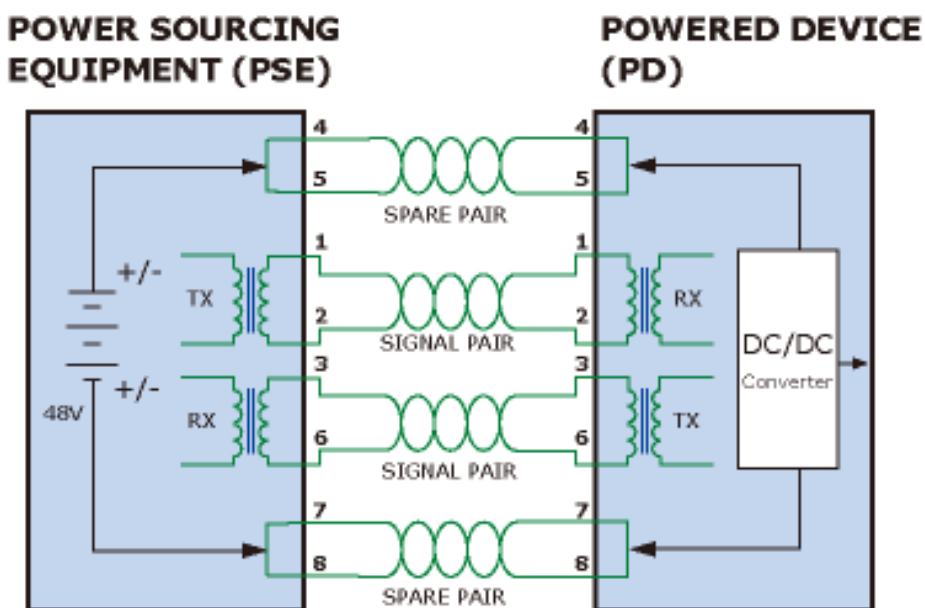
The specification of PoE typically requires two devices: the Powered Source Equipment (PSE) and the Powered Device (PD). The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of 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 8-2 and Figure 8-3:

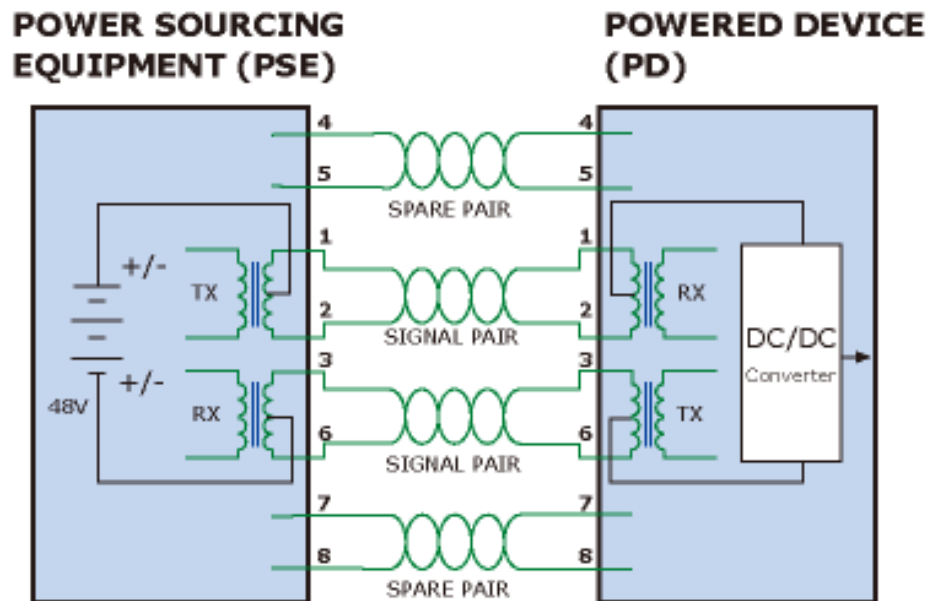
The spare pairs are used. Figure 8-2 shows the pair on pins 4 and 5 connected together and forming the positive supply, and the pair on pins 7 and 8 connected and forming the negative supply. (In fact, a late change to the spec allows either polarity to be used).

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 should you 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 KO signature resistor. Detection of this signature indicates that a valid PD is connected, and that provision of power to the device may commence.

The signature resistor lies in the PD's PoE front-end, isolated from the rest of 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 the 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 provisional startup.

Operation

During normal operation, the PSE provides 44-57 VDC, able to support a minimum of 15.4 watts power.

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 could 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 shuts down 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 resolve common problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

The Link LED is not lit

Solution:

Check the cable connection and remove duplex mode of the Ethernet Switch

Some stations cannot talk to other stations located on the other port

Solution:

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

Stacking not functioning

Solution:

1. Check that modules are installed correctly
2. GE Security HDMI-like Stacking cables not installed correctly (LEDs on front panel STX1 or STX2 do not light)
3. Check that the cables are inserted correctly
4. The stack cable is GE Security proprietary stack cable, the stack cable is cross-overed HDMI-like cable, and the normal HDMI cable can't be used for the GE-DSSG-244 series.

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-

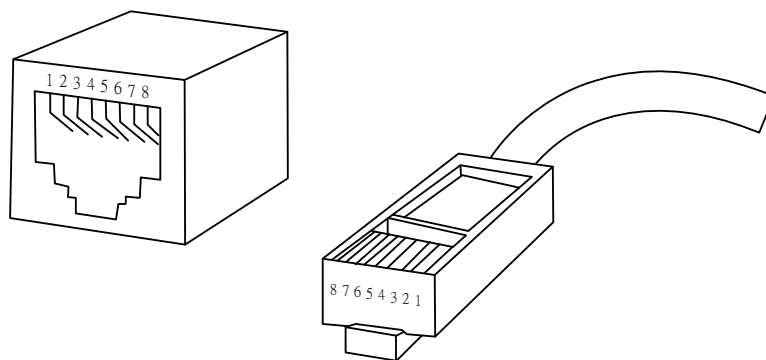
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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	

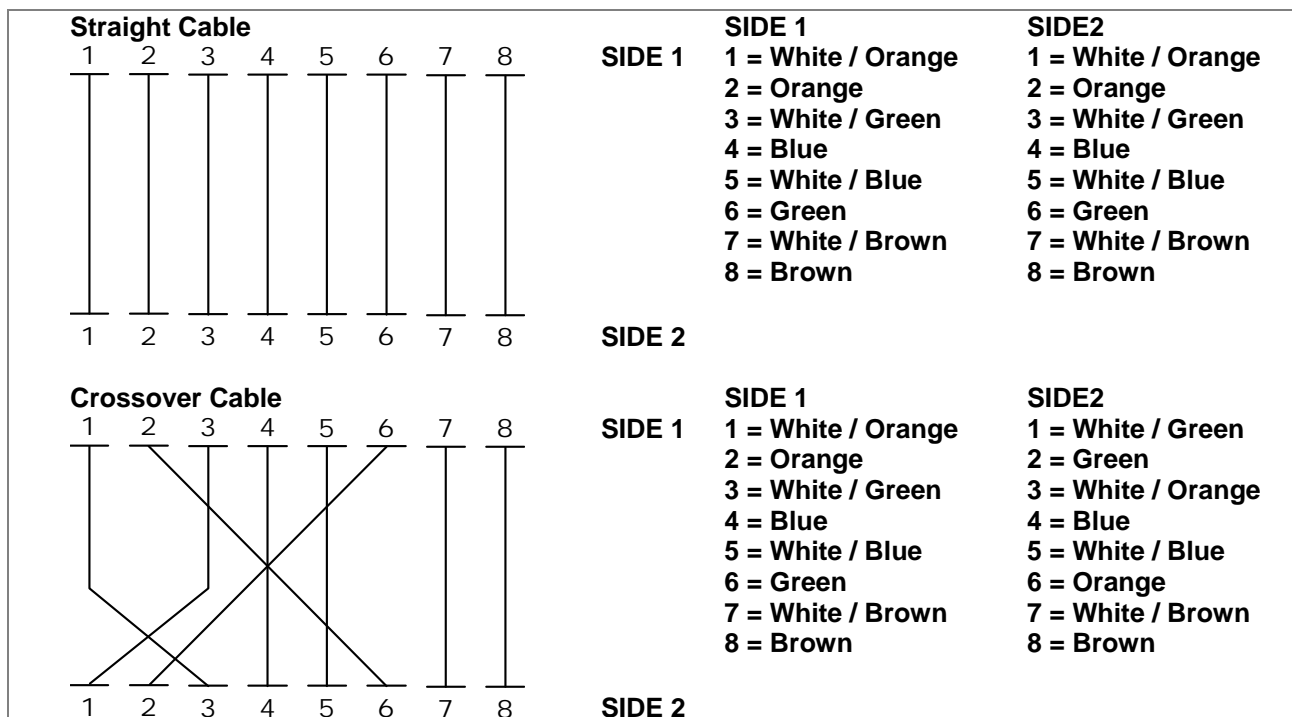
The standard cable, RJ-45 pin assignment



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 A-1: Straight-Through and Crossover Cable



Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

Appendix B

Glossary

Term	Definition
A	
ACE	<p>ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.</p> <p>There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.</p>
ACL	<p>ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.</p> <p>Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.</p> <p>ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.</p>
Aggregation	<p>Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.</p> <p>(Also Port Aggregation, Link Aggregation).</p>

Term	Definition
ARP	ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.
Auto-Negotiation	Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.
D	
DES	DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.
DHCP	DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network. DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.
DNS	DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.
DoS	DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.
Dotted Decimal Notation	Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Term	Definition
DSCP	DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.
E	
Ethernet Type	Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.
F	
FTP	FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.
Fast Leave	IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.
H	
HTTP	HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).
	HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.
	Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.
HTTPS	HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.
	HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

Term	Definition
I	
ICMP	ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.
IEEE 802.1X	IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.
IGMP	IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.
IGMP Querier	A router sends IGMP Query messages onto a particular link. This router is called the Querier.
IMAP	<p>IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.</p> <p>IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.</p> <p>The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.</p>

Term	Definition
IP	<p>IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.</p> <p>IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.</p> <p>The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.</p>
IPMC	IPMC is an acronym for IP MultiCast.
L	
LACP	LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.
LLDP	LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol, is used for network discovery, and works by having the units in the network exchanging information with their neighbors using LLDP frames.
M	
MAC Table	<p>Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.</p> <p>The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.</p>
MD5	MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.
Mirroring	<p>For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)</p> <p>Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.</p>

Term	Definition
N	
NetBIOS	<p>NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).</p> <p>The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.</p>
NFS	<p>NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.</p> <p>NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.</p>
O	
Optional TLVs.	<p>A LLDP frame contains multiple TLVs</p> <p>For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.</p>
P	
PING	<p>ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.</p> <p>Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.</p>
Policer	A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Term	Definition
POP3	<p>POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.</p> <p>POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.</p> <p>An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.</p> <p>POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.</p>
Private VLAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
Q	
QCE	<p>QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.</p> <p>There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.</p>
QCL	<p>QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.</p> <p>Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.</p>
QoS	<p>QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.</p> <p>A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.</p> <p>Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.</p>
R	
RARP	RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

Term	Definition
Router Port	<p>A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.</p> <p>RSTP</p> <p>In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.</p>
S	
SAMBA	<p>Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.</p> <p>Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.</p> <p>Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".</p>
SHA	<p>SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.</p>
Shaper	<p>A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.</p>
SMTP	<p>SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.</p>
SNMP	<p>SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.</p>
SNTP	<p>SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.</p>
SPROUT	<p>Stack Protocol using ROuting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.</p>

Term	Definition
STP	Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.
Switch ID	Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.
T	
Tag Priority	Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.
TCP	<p>TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.</p> <p>The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.</p> <p>The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.</p> <p>Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).</p>
TELNET	<p>TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.</p> <p>TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.</p>
TFTP	TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.
ToS	ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).
TLV	A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV (TLV is short for "Type Length Value").

Term	Definition
U	
UDP	<p>UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.</p> <p>UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.</p> <p>UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.</p> <p>Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).</p>
User Priority	User Priority is a 3-bit field storing the priority level for the 802.1Q frame.
V	
VLAN	<p>Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:</p> <p>VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.</p> <p>VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.</p> <p>Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.</p>
VLAN ID	VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.