GS1900 Series

GbE Smart Managed Switch

Version 1.0
Edition 2, 08/2013

User's Guide

Default Login Details	
IP Address	http://192.168.1.1 (In-band ports)
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Note: This guide is a reference for a series of products. Therefore some features or options in this guide may not be available in your product.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Note: It is recommended you use the Web Configurator to configure the Switch.

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

Contents Overview

Table of Contents

PART I
User's Guide

1

Getting to Know Your Switch

This chapter introduces the main features and applications of the Switch.

1.1 Introduction

The GS1900 series is a new generation Gigabit Ethernet (GbE) Web-Managed Switch.

This User's Guide covers the following models:

Table 1 GS1900 Series Comparison Table

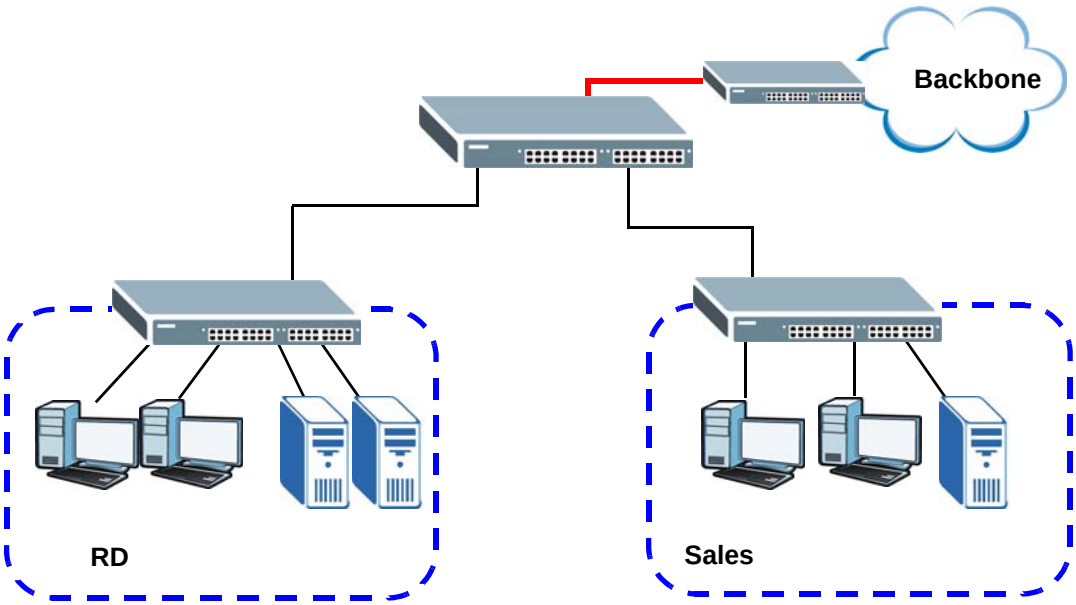
MODEL	GS1900-8	GS1900-8HP	GS1900-16	GS1900-24E	GS1900-24	GS1900-24HP	GS1900-48	GS1900-48HP
100/1000 Mbps Port	8	-	16	24	24	-	48	24
100/1000 Mbps PoE Port	-	8	-	-	-	24	-	24
1G SFP Slots Fiber	-	-	-	-	2	2	2	2
Desktop	v	v	v	v				
Wall-mount	v	v	v	v				
Rack-mount			v	v	v	v	v	v
Power ON/OFF Switch	v		v	v				

See the datasheet for a full list of firmware features available on the Switch.

1.1.1 Bridging Example

In this example the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch.

Figure 1 Bridging Application

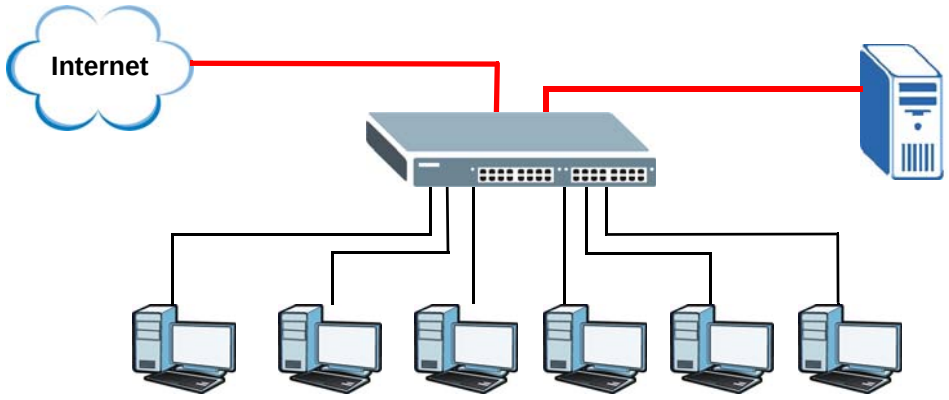


1.1.2 Gigabit Ethernet to the Desktop

The Switch is an ideal solution for small networks which demand high bandwidth for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch.

In this example, all computers can share high-speed applications on the server and access the Internet. To expand the network, simply add more networking devices such as switches, routers, computers, print servers and so on.

Figure 2 Gigabit to the Desktop



1.1.3 IEEE 802.1Q VLAN Application Example

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot

directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

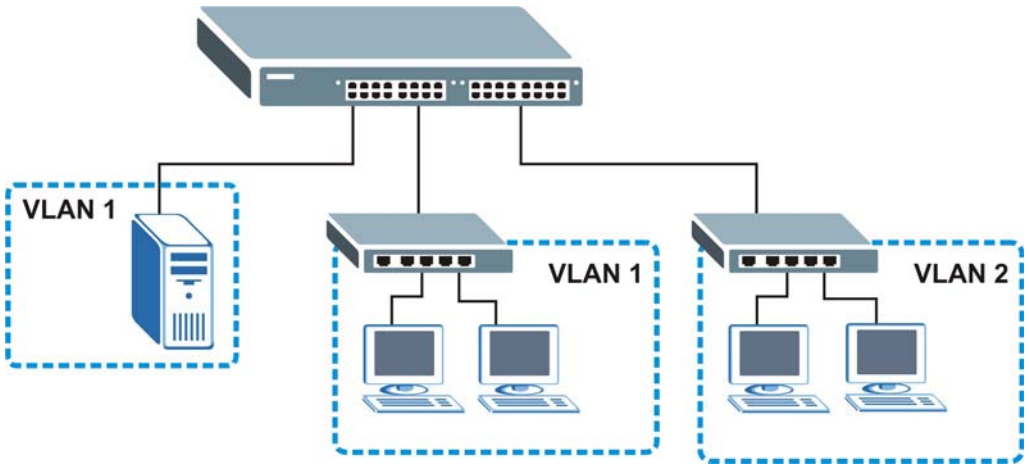
For more information on VLANs, refer to Chapter 8 on page 61.

1.1.3.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain, thus increasing network performance by reducing broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 3 Shared Server Using VLAN Example



1.1.4 IPv6 Support

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. At the time of writing, the Switch supports the following features.

- Static address assignment and stateless auto-configuration
- Neighbor Discovery Protocol (a protocol used to discover other IPv6 devices in a network)
- Remote Management using PING, SNMP, HTTP and TFTP services
- ICMPv6 to report errors encountered in packet processing and perform diagnostic functions, such as "PING"
- IPv4/IPv6 dual stack; the Switch can run IPv4 and IPv6 at the same time
- DHCPv6 client
- Multicast Listener Discovery (MLD) snooping

1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 31.
- TFTP. Use Trivial File Transfer Protocol for firmware upgrades and configuration backup/restore. See Section 31.1 on page 211, Section 31.3 on page 213, and Section 31.4 on page 215
- SNMP. The device can be configured by a SNMP manager. See Section 30.3 on page 196.

1.3 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.

2

Hardware Installation and Connection

This chapter shows you how to install and connect the Switch.

2.1 Freestanding Installation

1 Make sure the Switch is clean and dry.

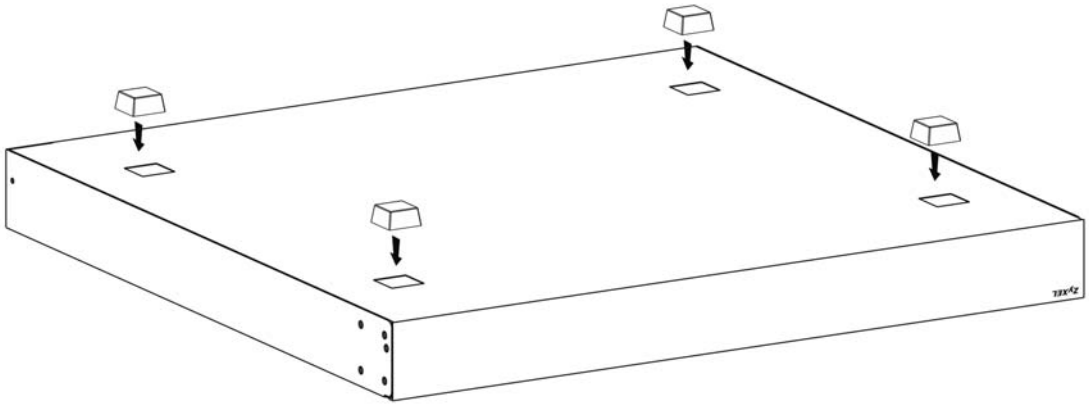
2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.

3 Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.

4 Remove the adhesive backing from the rubber feet.

5 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 4 Attaching Rubber Feet



Note: Do NOT block the ventilation holes. Leave space between devices when stacking.

Note: For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. This is especially important for enclosed rack installations.

2.2 Hardware Installation

See Table 1 on page 16 for a comparison of the hardware installation methods of each model:

Note: Ask an authorized technician to attach the Switch to the rack/wall.

Refer to Section 2.2.2 on page 22 for rack-mounting instructions. Take note of the following:

- The Switch should have a minimum 25 mm space around it for ventilation.
- The Switch should be placed on a desk that has a level surface and that is able to support the weight of the Switch.

To start using it, simply connect the power cables and turn on the Switch.

2.2.1 Wall Mounting

Do the following to attach your Switch to a wall.

See the following table for how far apart to place the screws.

Table 2 Distance between the centers of the holes for wall mounting

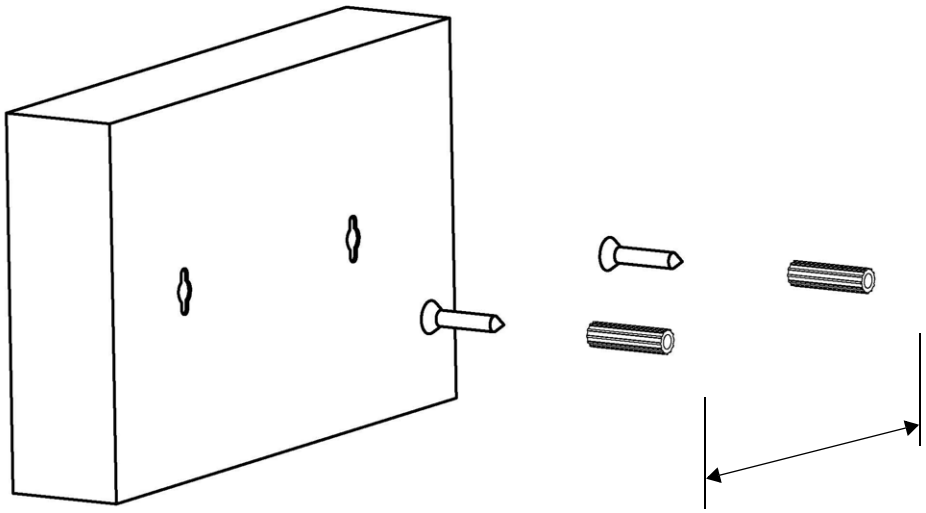
GS1900-8	GS1900-8HP	GS1900-16	GS1900-24E
176 mm	176 mm	148 mm	207 mm

Screw the two screws provided with your Switch into the wall (see the figure in step 2). Use screws with 6 mm ~ 8 mm (0.24" ~ 0.31") wide heads. Do not screw the screws all the way in to the wall; leave a small gap between the head of the screw and the wall.

The gap must be big enough for the screw heads to slide into the screw slots and the connection cables to run down the back of the Switch.

Note: Make sure the screws are securely fixed to the wall and strong enough to hold the weight of the Switch with the connection cables.

Align the holes on the back of the Switch with the screws on the wall. Hang the Switch on the screws.



The Switch should be wall-mounted horizontally. The Switch's side panels with ventilation slots should not be facing up or down as this position is less safe.

2.2.2 Rack Mounting

The Switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your Switch on a standard EIA rack using a rack-mounting kit.

Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

Failure to use the proper screws may damage the unit.

Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

Attaching the Mounting Brackets to the Switch

1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

Figure 5 Attaching the Mounting Brackets (GS1900-16 and GS1900-24E)

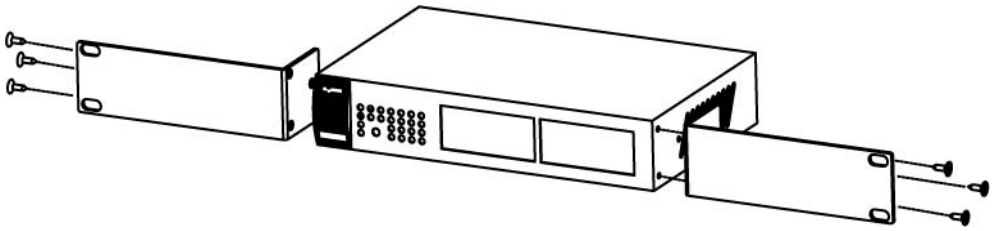
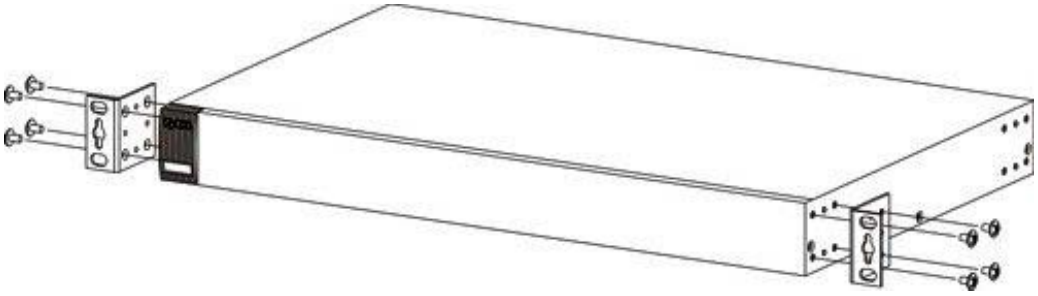


Figure 6 Attaching the Mounting Brackets (GS1900-24, GS1900-24HP, GS1900-48, GS1900-48HP)



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

4 You may now mount the Switch on a rack. Proceed to the next section.

2.2.2.1 Mounting the Switch on a Rack

1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 7 Mounting the Switch on a Rack (GS1900-16 and GS1900-24E)

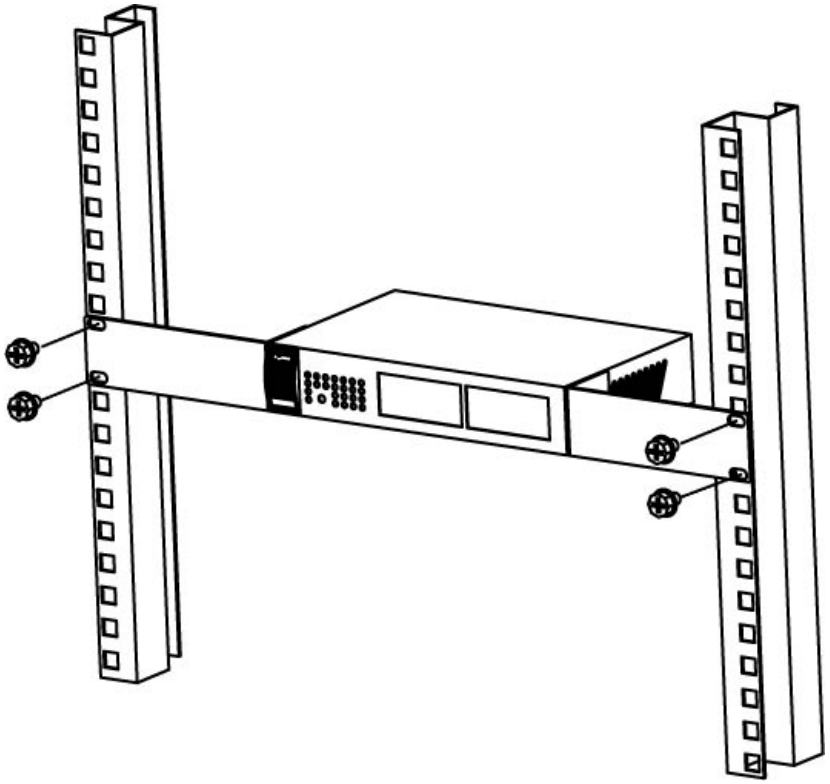
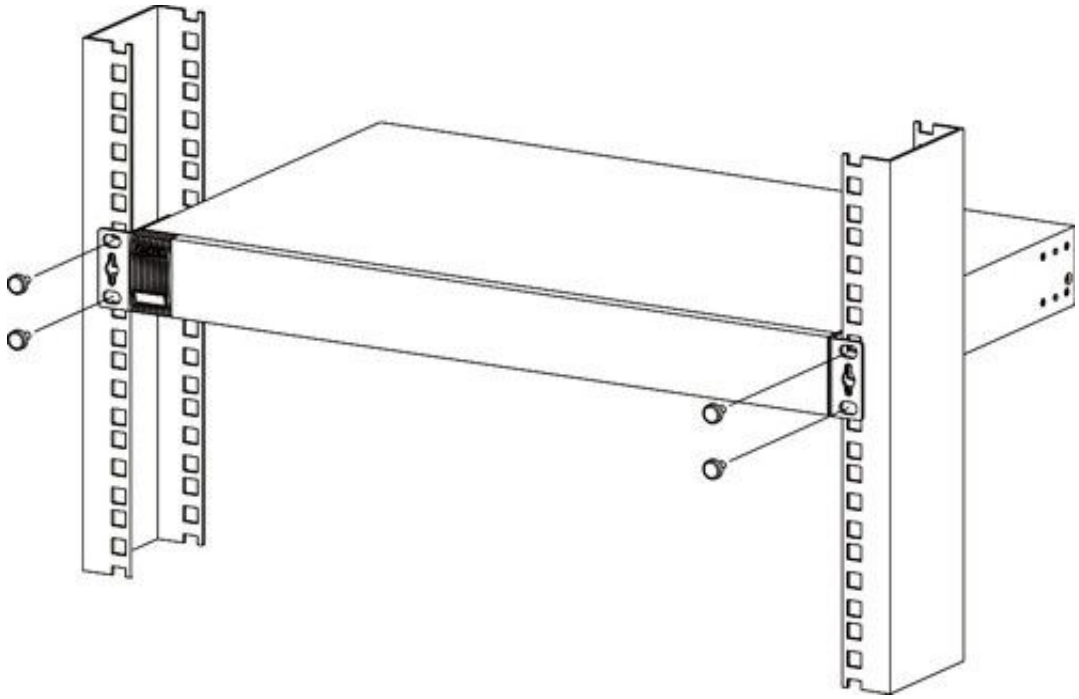


Figure 8 Mounting the Switch on a Rack (GS1900-24, GS1900-24HP, GS1900-48, GS1900-48HP)



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

3

Hardware Overview

This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

3.1 Front Panel Connections

The following figures show the front panels of the Switch.

Figure 9 Front Panel: GS1900-8

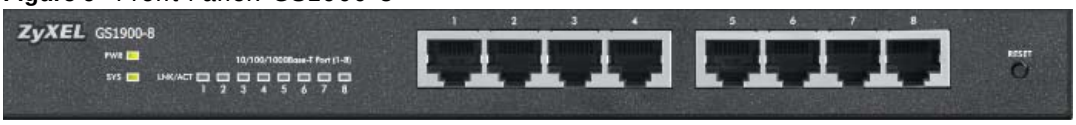


Figure 10 Front Panel: GS1900-8HP

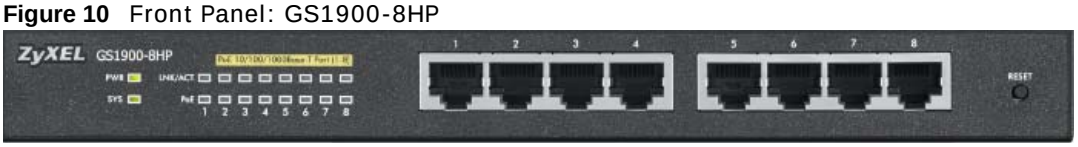


Figure 11 Front Panel: GS1900-16

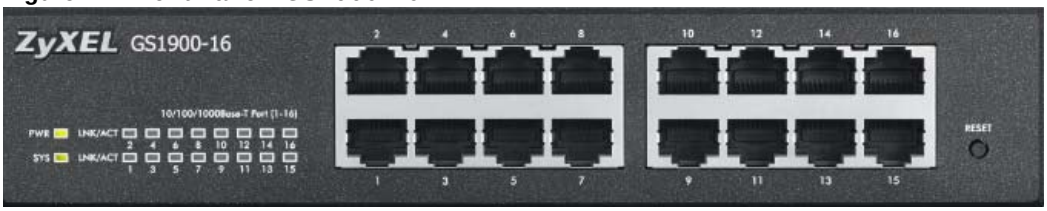


Figure 12 Front Panel: GS1900-24E

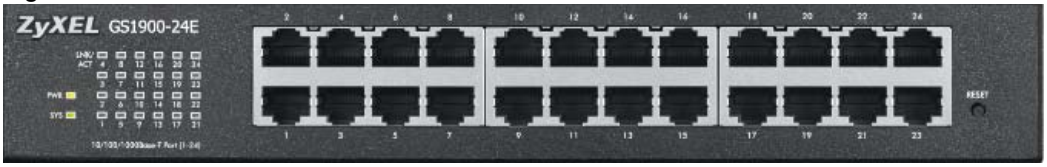
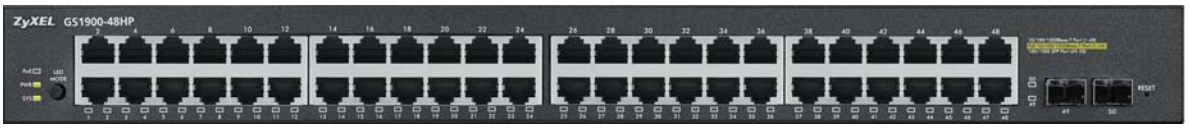


Figure 13 Front Panel: GS1900-24

Figure 14 Front Panel: GS1900-24HP

Figure 15 Front Panel: GS1900-48

Figure 16 Front Panel: GS1900-48HP



3.1.1 Ethernet Ports

The Switch has 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 10/100/1000 Mbps Gigabit Ethernet, the speed can be 10Mbps, 100 Mbps or 1000 Mbps. The duplex mode can be both half or full duplex at 100 Mbps and full duplex only at 1000 Mbps.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

3.1.1.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the Switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off

3.1.2 SFP Slots

These are slots for Small Form-Factor Pluggable (SFP) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the Switch. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-Factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

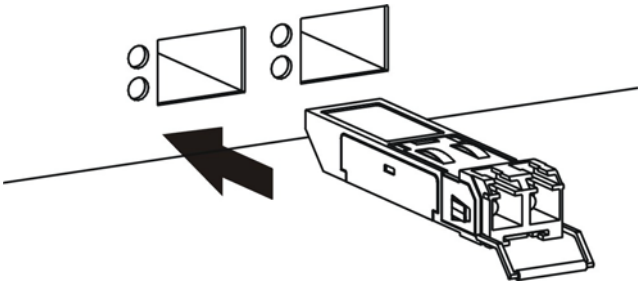
To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.2.1 Transceiver Installation

Use the following steps to install a transceiver.

1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

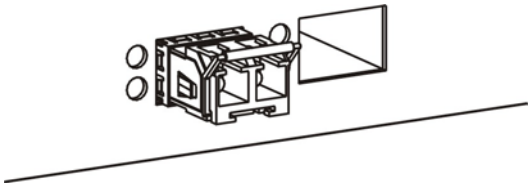
Figure 17 Transceiver Installation Example



2 Press the transceiver firmly until it clicks into place.

3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 18 Installed Transceiver

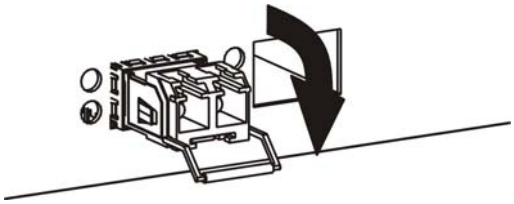


3.1.2.2 Transceiver Removal

Use the following steps to remove a transceiver.

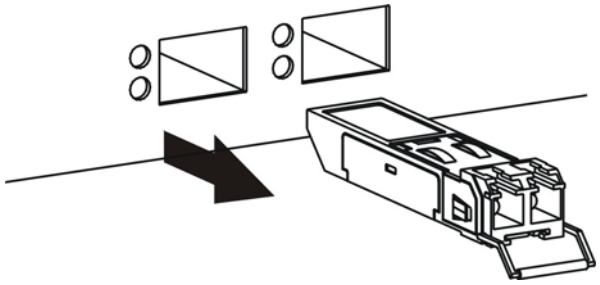
1 Open the transceiver's latch (latch styles vary).

Figure 19 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

Figure 20 Transceiver Removal Example



3.2 Rear Panel

The following figures show the rear panels of the Switch.

Figure 21 Rear Panel: GS1900-8

Figure 22 Rear Panel: GS1900-8HP

Figure 23 Rear Panel: GS1900-16

Figure 24 Rear Panel: GS1900-24E

Figure 25 Rear Panel: GS1900-24

Figure 26 Rear Panel: GS1900-24HP

Figure 27 Rear Panel: GS1900-48

Figure 28 Rear Panel: GS1900-48HP

3.2.1 Power Connection

Make sure you are using the correct power source and that no objects obstruct the airflow of the fans.

The Switch uses two power supply modules, one of which is redundant, so if one power module fails the system can operate on the remaining module.

Rear Panel Power Connection

Connect one end of the supplied power cord or power adaptor to the power receptacle on the back of the Switch and the other end to the appropriate power source.

For Switches with a power switch (see Table 1 on page 16), use the **POWER ON / OFF** switch to have the Switch power on or off.

Connecting the Power

Use the following procedures to connect the Switch to a power source after you have installed it in a rack.

Note: Use the included power cord for the AC power connection.

1 Connect the female end of the power cord to the AC power socket.

2 Connect the other end of the cord to a power outlet.

Disconnecting the Power

The power input connectors can be disconnected from the power source individually.

1 Disconnect the power cord from the power outlet.

2 Disconnect the power cord from the AC power socket.

3.3 LEDs

After you connect the power to the Switch, view the LEDs to ensure proper functioning of the Switch and as an aid in troubleshooting.

Table 3 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off or has failed.
SYS	Green	On	The system is on and functioning properly.
		Blinking	The system is rebooting and performing self-diagnostic tests.
		Off	The power is off or the system is not ready/malfunctioning.
Ethernet Ports			
LNK/ACT	Green	Blinking	The system is transmitting/receiving to/from a 100/1000 Mbps Ethernet network.
		On	The link to a 100/1000 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
PoE (see Section 1.1 on page 16)	Green	On	Power is supplied to all PoE Ethernet ports.
		Off	There is no power supply.
1G SFP Slots (Fiber Ports - see Section 1.1 on page 16)			
LNK/ACT	Green	Blinking	The system is transmitting/receiving to/from a 100/1000 Mbps Fiber network.
		On	The link to a 100/1000 Mbps Fiber network is up.
		Off	The link to a Fiber network is down.

4

The Web Configurator

4.1 Overview

The Switch **Web Configurator** allows easy management using an Internet browser.

In order to use the Web Configurator, you must:

- Use Internet Explorer 7.0 and later or Firefox 1.5 and later
- Allow pop-up windows
- Enable JavaScript (enabled by default)
- Enable Java permissions (enabled by default)
- Enable cookies

The recommended screen resolution is 1024 x 768 pixels and higher.

4.2 Access

1 Make sure your Switch hardware is properly connected. See the Quick Start Guide.

2 Browse to https://192.168.1.1. The **Login** screen appears.

Figure 29 The Login Screen

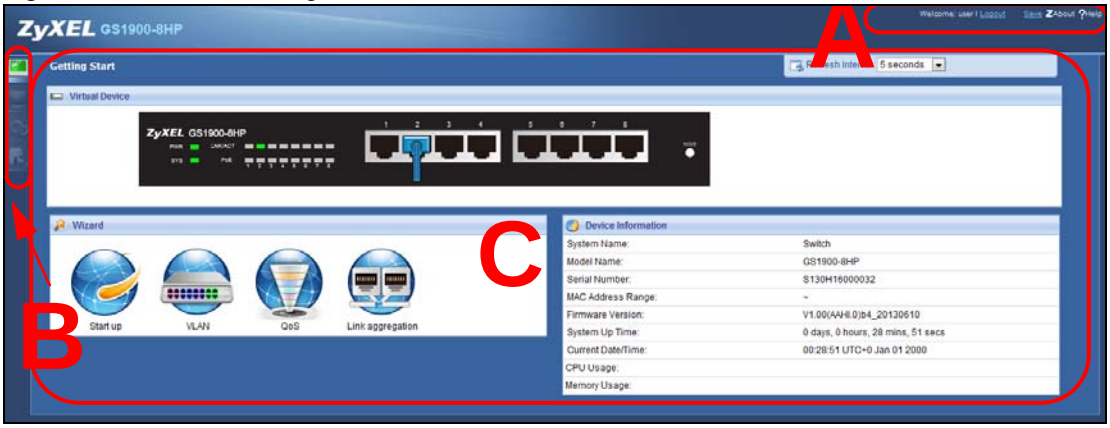
3 Enter the user name (default: “admin”) and password (default: “1234”).

4 Click **Login**. If you logged in using the default user name and password, getting start appears. The **Getting Start** screen appears every time you log in using the default user name and default password.

4.3 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Getting Start** screen. This guide uses the GS1900-8HP screens as an example. The screens may vary slightly for different models.

Figure 30 The Web Configurator's Main Screen



The Web Configurator's main screen is divided into these parts:

- **A** - Title Bar
- **B** - Navigation Panel
- **C** - Main Window

4.3.1 Title Bar

The title bar provides some useful links that always appear over the screens below, regardless of how deep into the Web Configurator you navigate.

Figure 31 Title Bar

The icons provide the following functions.

Table 4 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Logout	Click this to log out of the Web Configurator.
OK	Click **OK** to apply the changes.
Cancel	Click **Cancel** to discard the changes.
Save	Click this to apply your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.

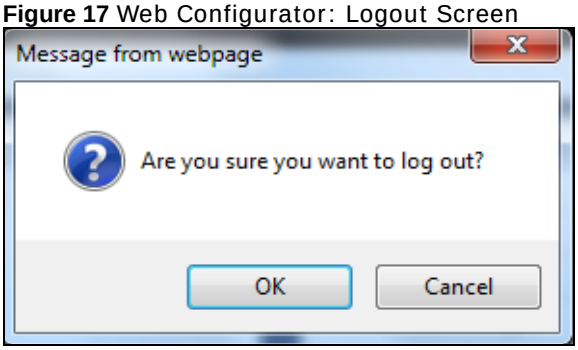
Table 4 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
About	Click this to display basic information about the Switch.
Help	Click this to open the help page for the current screen.

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Click **OK** and confirm at the pop-up screen to complete the task. Click **Cancel** and confirm at the pop-up screen to discard the changes.

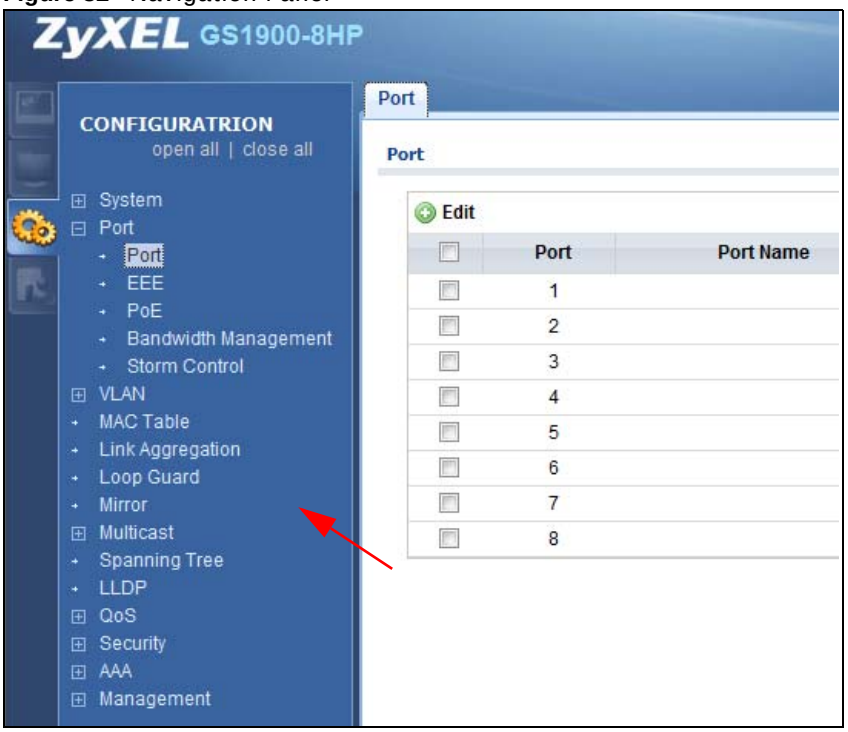
Figure 17 Web Configurator: Logout Screen



4.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Switch features. The following sections introduce the Switch's navigation panel menus and their screens.

Figure 32 Navigation Panel



Getting Start

Getting Start displays general device information, system status, system resource usage, and interface status.

For details on Getting Start features, see Chapter 5 on page 39.

Monitor Menu

The monitor menu screens display status and statistics information.

Table 5 Monitor Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
System		This link takes you to a screen where you can see general identification information for the Switch.
IP	IPv4	This link takes you to a screen where you can see an IPv4 interface and the IPv4 settings on the Switch.
	IPv6	This link takes you to a screen where you can see an IPv6 interface and the IPv6 settings on the Switch.
Information		This link takes you to a screen that displays general system information: system name, system location, and system contact.
Port		This link takes you to screens where you can see speed, flow control and priority settings for individual Switch ports.
Port	Status	Displays status settings for individual Switch ports.
	Port Counters	Displays interface, port 1 interface mib counters, port 1 etherlike mib counters, port 1 RMON mib counters settings for individual Switch ports.
	Bandwidth Utilization	Displays port bandwidth utilization settings for individual Switch ports.
PoE	Status	Displays POE status.
Bandwidth Management	Bandwidth Control	Displays egress global burst and port rate for individual Switch ports.
Storm Control		This link takes you to a screen that displays broadcast filters.
VLAN		This link takes you to screens where you can see port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also see a protocol based VLAN or a subnet based VLAN in these screens.
VLAN	VLAN	Displays VLAN settings.
	Port	Displays port settings.
	VLAN Port	Displays VLAN port settings.
Guest VLAN		Displays global and port settings.
Voice VLAN		Displays global and port settings.
MAC Table		This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of MAC address it is.
Link Aggregation		This link takes you to screen where you can view aggregate physical links to form one logical, higher-bandwidth link.
Loop Guard		This link takes you to a screen where you can view protection against network loops that occur on the edge of your network.
Multicast		This link takes you to screen where you can view various multicast features, IGMP snooping and create multicast VLANs.

Table 5 Monitor Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
IGMP	Vlan	Displays VLAN settings.
	Statistics	Displays statistics settings.
	Group	Displays group settings.
	Router	Displays router settings.
Spanning Tree		This link takes you to screens where you can view CIST, MST, STP preventing network loops.
	CIST	Displays CIST instance status.
	CIST Port	Displays CIST port status.
	MST	Displays MST instance status.
	MST Port	Displays MST port status.
	STP Statistics	Displays STP statistics.
LLDP		Displays statistics, remote information, and overloading.
	Statistics	Displays LLDP global and port statistics.
	Remote Information	Displays remote device information.
	Overloading	Displays port overloading information.
Security		Displays port security and 802.1X settings.
Port Security		Displays global and port settings.
802.1X	Port	Displays 802.1X port settings.
	Authenticated Hosts	Displays authenticated hosts table.
Management		Displays syslog and error disable.
Syslog		Displays logging filter select and show system log.
Error Disable		Displays global and port settings.

Configuration Menu

Use the configuration menu screens to configure the Switch's features.

Table 6 Configuration Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
System		This link takes you to a screen where you can configure general identification information and time settings for the Switch.
IP	IPv4	This link takes you to a screen where you can enable an IPv4 interface and configure the IPv4 settings on the Switch.
	IPv6	This link takes you to a screen where you can enable an IPv6 interface and configure the IPv6 settings on the Switch.
Time	System Time	Configure time of system.
	SNTP Server	Configure SNTP server settings.
Information		This link takes you to a screen that configures general system information: system name, system location, and system contact.
Port		This link takes you to screens where you can configure speed, flow control and priority settings for individual Switch ports.
Port		Configure port settings for individual Switch ports.
EEE		Configure EEE settings for individual Switch ports.

Table 6 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
PoE		This link takes you to a screen where you can configure the Switch to supply power over Ethernet.
Bandwidth Management	Bandwidth Control	Configure egress global burst and port rate.
Storm Control	Port	Configure port settings.
VLAN		This link takes you to screens where you can configure VLAN, guest VLAN, and voice VLAN settings.
VLAN	VLAN	Configure VLAN settings.
	Port	Configure port settings.
	VLAN Port	Configure VLAN port settings.
Guest VLAN	Global	Configure global settings.
	Port	Configure port settings.
Voice VLAN	Global	Configure global settings.
	OUI	Configure OUI settings.
	Port	Configure port settings.
MAC Table		This link takes you to a screen where you can configure the MAC address and VLAN ID of a device attach to a port. You can also configure what kind of MAC address it is.
	Static MAC	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
	Filtering MAC	This link takes you to a screen to set up filtering rules.
	Dynamic Age	Configure dynamic learned and MAC address information.
Link Aggregation		This link takes you to screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
	Global	Configure global settings.
	LAG Management	Configure LAG management settings.
	LAG Port	Configure LAG port settings.
	LACP Port	Configure LACP port settings.
Loop Guard		This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
	Global	Configure global settings.
	Port	Configure port settings.
Mirror		This link takes you to screens where you can copy traffic from one port or ports to another port. Thus, allowing you to examine the traffic from the first port without interference.
Multicast		This link takes you to screen where you can configure various multicast features, IGMP snooping and create multicast VLANs.
IGMP	Global	Configure global settings.
	Vlan	Configure Vlan settings.
	Router Port	Configure router port settings.
	Profile	Configure profile settings.
	Throttling	Configure throttling settings.
Spanning Tree		This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
	Global	Configure global settings.

Table 6 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
	STP Port	Configure STP port settings.
	CIST	Configure CIST settings.
	CIST Port	Configure CIST port settings.
	MST	Configure MST settings.
	MST Port	Configure MST port settings.
LLDP		Configure global, port, local information, MED network policy, and MED port settings.
	Global	Configure global settings.
	Port	Configure port settings.
	Local Information	Configure local information settings.
	MED Network Policy	Configure MED network policy settings.
	MED Port	Configure MED port settings.
QoS		Configure general and trust mode settings.
General	Port	Configure port settings.
	Queue	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
	CoS Mapping	Configure CoS mapping settings.
	DSCP Mapping	Configure DSCP mapping settings.
	IP Precedence Mapping	Configure IP precedence mapping settings.
Trust Mode	Global	Configure global settings.
	Port	Configure port settings.
Security		Configure port security, protected port, 802.1X and DoS settings.
Port Security	Global	Configure global settings.
	Port	Configure port settings.
Protected Port		Configure protected port settings.
802.1X	Global	Configure global settings.
	Port	Configure port settings.
	Protected Port	Configure protected port settings.
DoS	Global	Configure global settings.
	Port	Configure port settings.
AAA		This link takes you to a screen where you can view authentication, authorization and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
Auth Method		Configure auth method settings.
RADIUS		Configure RADIUS settings.
TACACS+		Configure TACACS+ settings.
Management		Configure syslog, SNMP, error disable, HTTP/HTTPS, users and remote access control.
Syslog	Global	Configure global settings.
	Local	Configure local settings.

Table 6 Configuration Menu Screens Summary (continued)

FOLDER OR LINK	TAB	FUNCTION
	Remote	Configure remote settings.
SNMP	Global	Configure global settings.
	Community	Configure community settings.
	Group	Configure group settings.
	User	Configure users settings.
	Trap	Configure trap settings.
	Trap Destination	Configure trap destination settings.
Error Disable		This link takes you to a screen where you can configure CPU protection and error disable recovery.
HTTP/HTTPS	HTTP	Configure HTTP settings.
	HTTPS	Configure HTTPS settings.
Users		Configure users settings.
Remote Access Control		This link takes you to a screen where you can configure global and profile settings.

Maintenance Menu

Use the maintenance menu screens to manage configuration and firmware files, run diagnostics, and reboot or shut down the Switch.

Table 7 Maintenance Menu Screens Summary

FOLDER OR LINK	TAB	FUNCTION
Firmware	Upload	Manage upload settings.
	Management	Manage dual image and images information.
Configuration	Backup	Manage backup configuration.
	Restore	Manage restore configuration.
	Management	Manage configuration settings.
	Factory Default	Restore factory defaults.
Diagnostics		This link takes you to screens where you can view system logs and can test port(s).
Port Test	Cable Diag	Manage cable diag and test results.
PING	IPv4	Manage ping test settings.
	IPv6	Manage IPv6 ping test settings.
Trace		Manage trace route settings.
Reboot		Reset the system.

5

Getting Start

5.1 Overview

Use the **Getting Start** screens to check status information about the Switch.

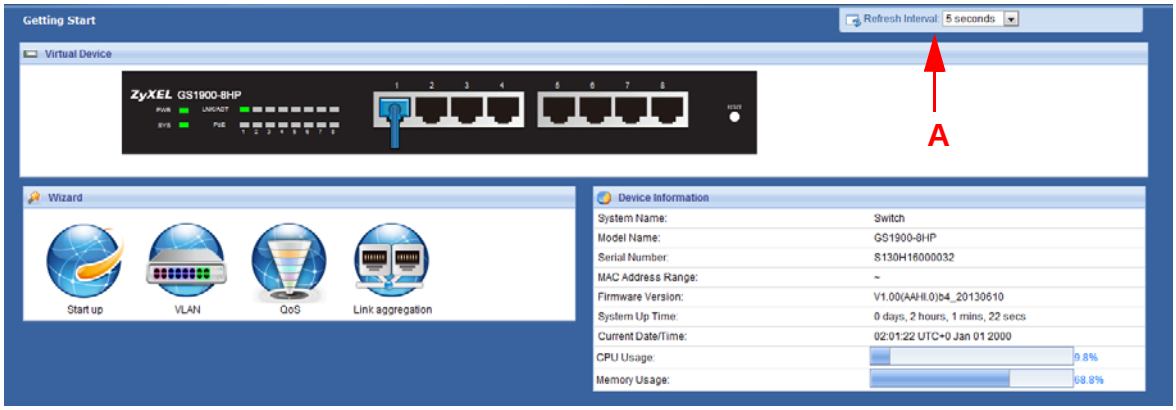
5.1.1 What You Can Do in this Chapter

- The main **Getting Start** screen (Section 5.2 on page 39) displays the Switch's general device information, system status, system resource usage, and interface status. You can also display other status screens for more information.

5.2 Getting Start

This screen is the first thing you see when you log into the Switch. It also appears every time you click the **Getting Start** icon in the navigation panel. The Getting Start displays general device information, system status, system resource usage, and interface status in widgets.

Figure 33 Getting Start



The following table describes the labels in this screen.

Table 8 Getting Start

LABEL	DESCRIPTION
Refresh Interval (A)	Use the drop-box to select: None, 5 seconds, 10 seconds, 15 seconds, 20 seconds, 25 seconds, or 30 seconds.
Virtual Device	Displays an image of the Switch.
Wizard	Displays the following links: Start up, VLAN, QoS, and link aggregation.
Device Information	
System Name	This field displays the name used to identify the Switch on any network.

Table 8 Getting Start (continued)

LABEL	DESCRIPTION
Model Name	This field displays the model name of this Switch.
Serial Number	This field displays the serial number of this Switch.
MAC Address Range	This field displays the MAC addresses used by the Switch. Each physical port or wireless radio has one MAC address. The first MAC address is assigned to the Ethernet LAN port, the second MAC address is assigned to the first radio, and so on.
Firmware Version	This field displays the version number and date of the firmware the Switch is currently running.
System Up Time	This field displays how long the Switch has been running since it last restarted or was turned on.
Current Date/ Time	This field displays the current date and time in the Switch. The format is hh:mm:ss yyyy-mm-dd .
CPU Usage	This field displays the Switch's recent CPU usage.
Memory Usage	This field displays the Switch's recent memory usage.

5.2.1 Wizard

Wizard displays start up, VLAN, QoS, and link aggregation.

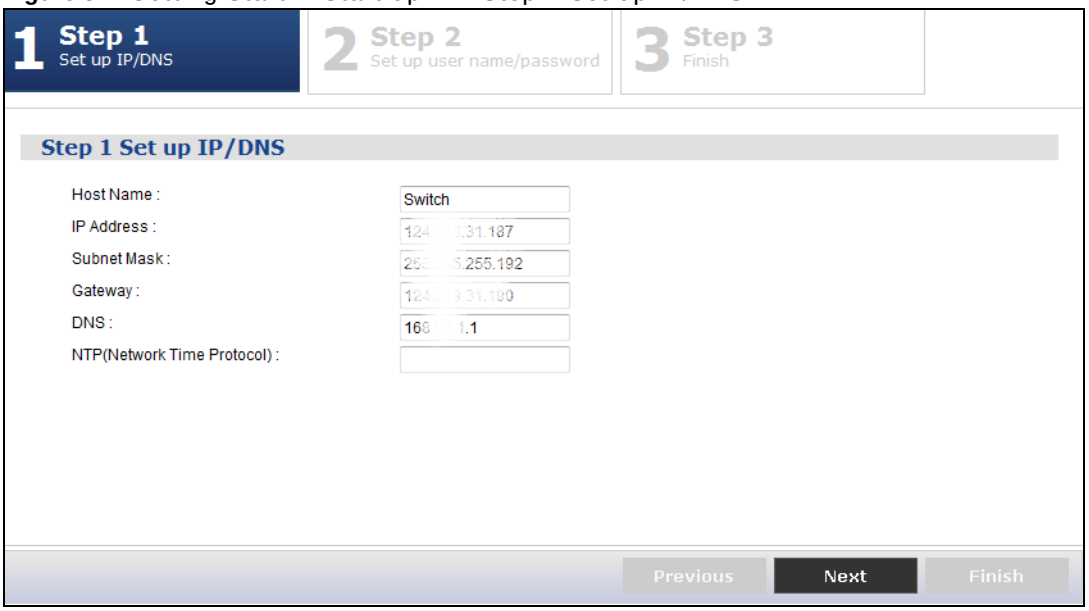
For details on Wizard features, see system Chapter 6 on page 51, VLAN Chapter 8 on page 61, QoS Chapter 27 on page 169, and link aggregation Chapter 10 on page 69.

Start up

In start up, you can set up IP/DNS, set up your username/password, and view finished results.

In order to set up your IP/DNS, please do the following. Click **Getting Start > Start up > 1 Step 1 Set up IP/DNS** to access this screen.

Figure 34 Getting Start > Start up > 1 Step 1 Set up IP/DNS



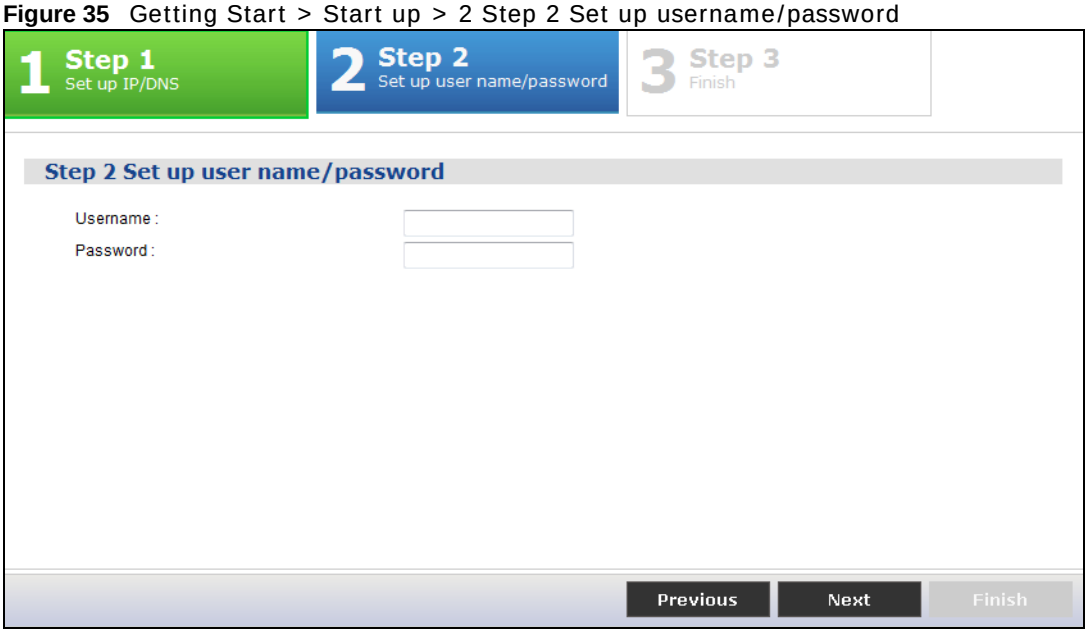
Each field is described in the following table.

Table 9 Getting Start > Start up > 1 Step 1 Set up IP/DNS

LABEL	DESCRIPTION
Host Name	This field displays a host name.
IP Address	The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.
Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
NTP(Network Time Protocol)	This field displays the NTP time servers from which the Switch gets the time and date.
Next	Click **Next** to show the next screen.

After clicking **Next,** the set up your username/password screen appears.

Figure 35 Getting Start > Start up > 2 Step 2 Set up username/password



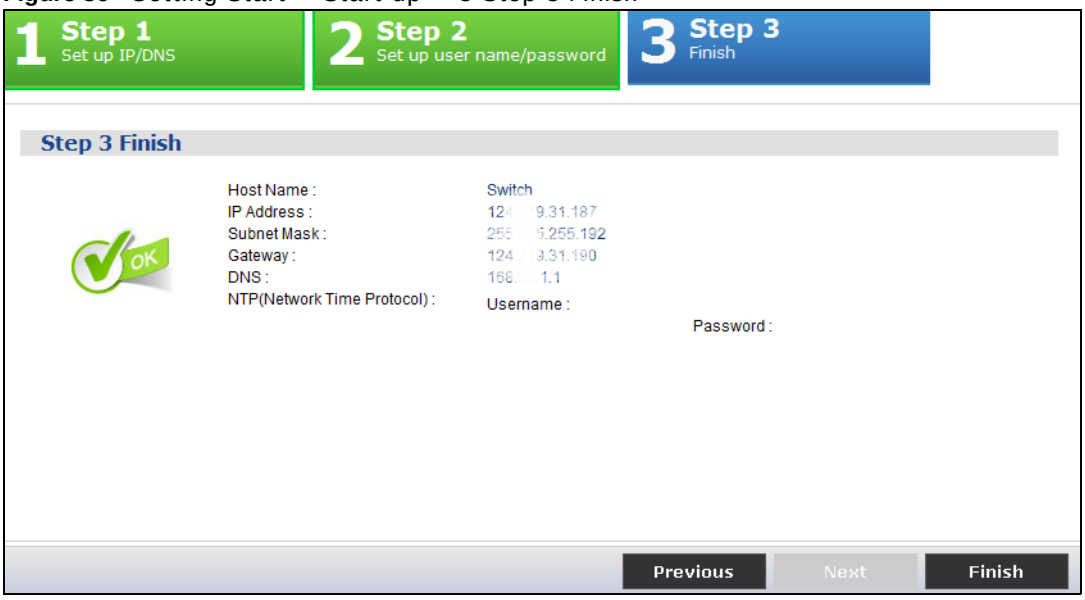
Each field is described in the following table.

Table 10 Getting Start > Start up > 2 Step 2 Set up username/password

LABEL	DESCRIPTION
Username	The default username is **admin** and associated default password is **1234**.
Password	The default username is **admin** and associated default password is **1234**.
Previous	Click **Previous** to show the previous screen.
Next	Click **Next** to show the next screen.

After clicking **Next,** the finish screen appears.

Figure 36 Getting Start > Start up > 3 Step 3 Finish



Each field is described in the following table.

Table 11 Getting Start > Start up > 3 Step 3 Finish

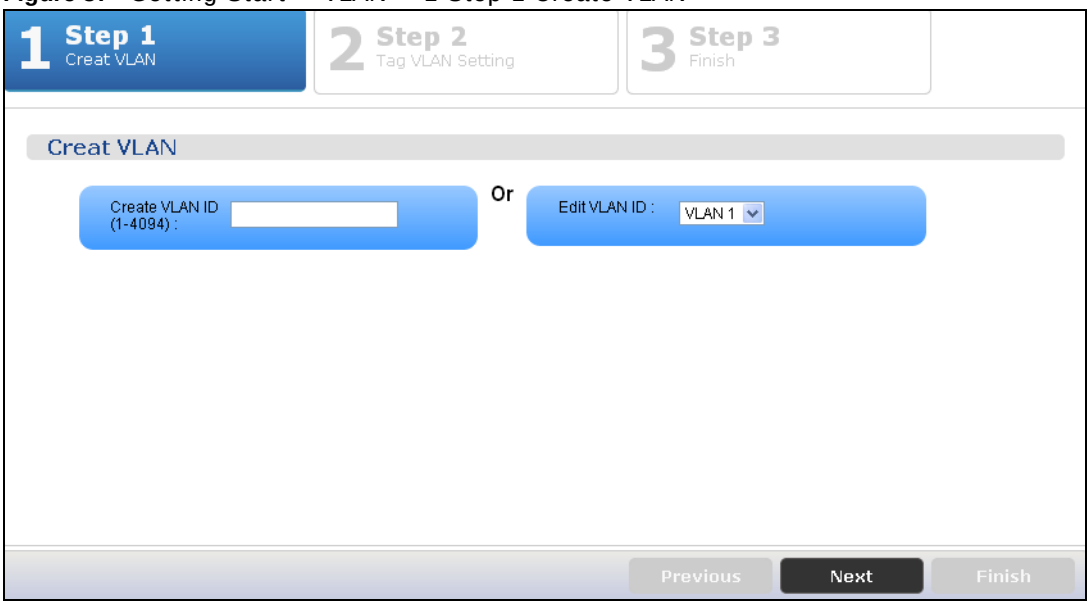
LABEL	DESCRIPTION
Host Name	This field displays a host name.
IP Address	The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.
Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
NTP(Network Time Protocol)	This field displays the NTP time servers from which the Switch gets the time and date.
Username	The default username is **admin** and associated default password is **1234**.
Password	The default username is **admin** and associated default password is **1234**.
Previous	Click **Previous** to show the previous screen.
Finish	Review the information and click **Finish** to create the task.

VLAN

In VLAN, you can create VLAN, tag VLAN setting, and view finished results.

In order to create VLAN, please do the following. Click **Getting Start > VLAN > 1 Step 1 Create VLAN** to access this screen.

Figure 37 Getting Start > VLAN > 1 Step 1 Create VLAN



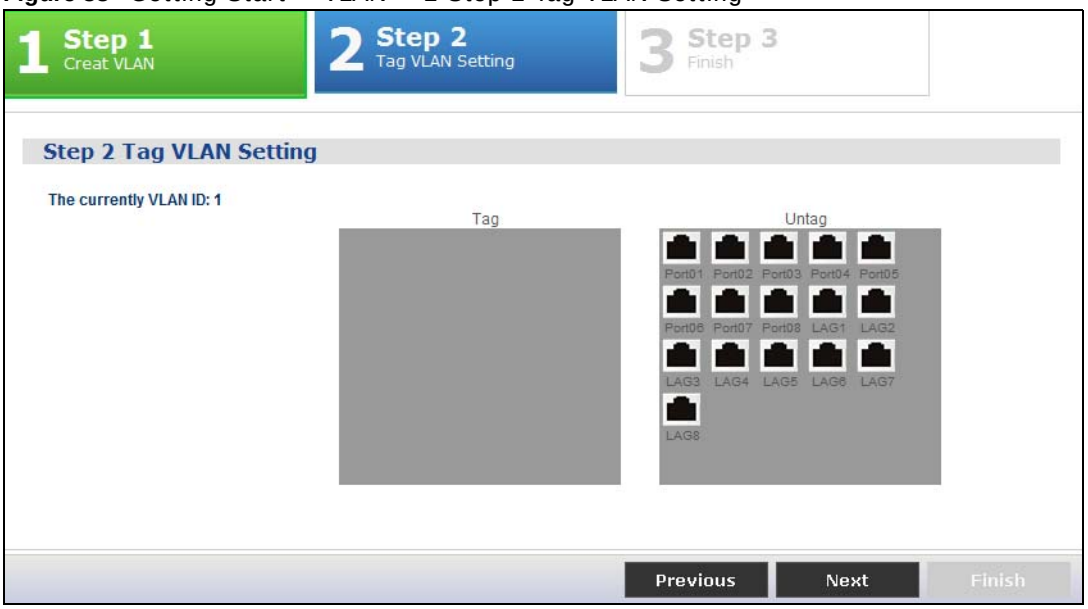
Each field is described in the following table.

Table 12 Getting Start > VLAN > 1 Step 1 Create VLAN

LABEL	DESCRIPTION
Create VLAN ID (1-4094)	Type a number between 1 and 4094 to create a VLAN ID.
Edit VLAN ID	Select from the drop-box a VLAN ID.
Next	Click **Next** to show the next screen.

After clicking Next, the tag VLAN setting screen appears.

Figure 38 Getting Start > VLAN > 2 Step 2 Tag VLAN Setting



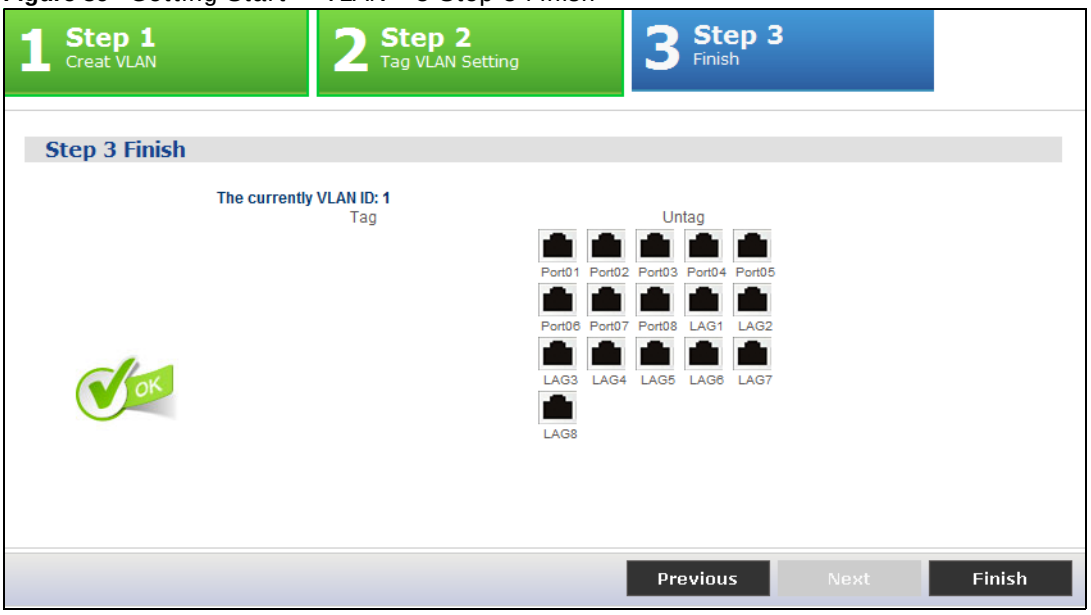
Each field is described in the following table.

Table 13 Getting Start > VLAN > 2 Step 2 Tag VLAN Setting

LABEL	DESCRIPTION
The currently VLAN ID	This field displays the VLAN identification number.
Tag	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
Untag	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
Previous	Click **Previous** to show the previous screen.
Next	Click **Next** to show the next screen.

After clicking **Next,** the finish screen appears.

Figure 39 Getting Start > VLAN> 3 Step 3 Finish



Each field is described in the following table.

Table 14 Getting Start > VLAN > 3 Step 3 Finish

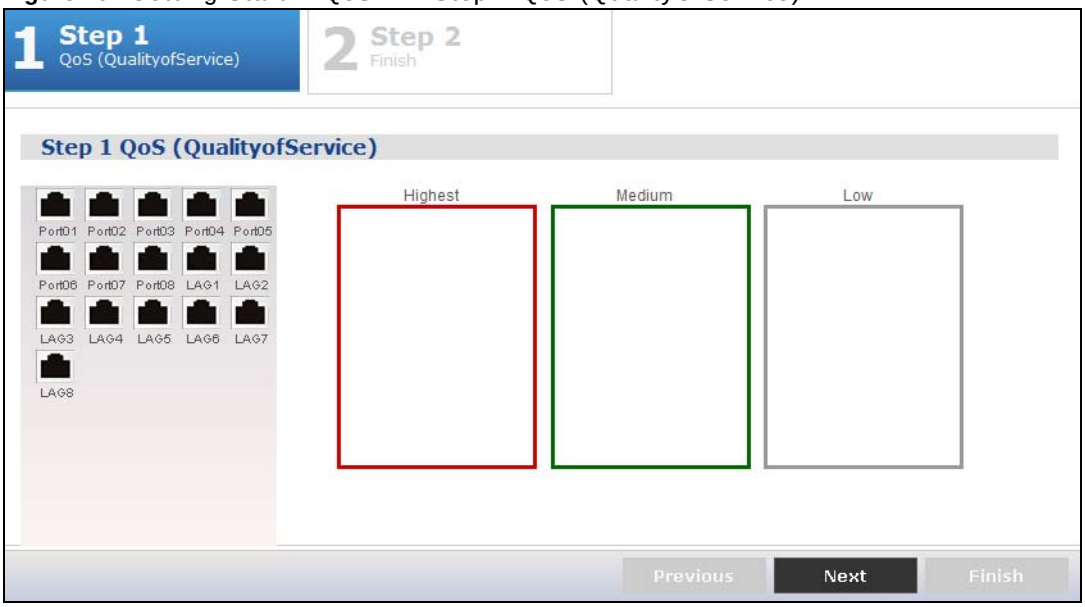
LABEL	DESCRIPTION
The currently VLAN ID	This field displays the VLAN identification number.
Tag	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
Untag	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
Previous	Click **Previous** to show the previous screen.
Finish	Review the information and click **Finish** to create the task.

QoS

In QoS, you can create QoS settings, and view finished results.

In order to create QoS settings, please do the following. Click **Getting Start > QoS > 1 Step 1 QoS (QualityOfService)** to access this screen.

Figure 40 Getting Start > QoS > 1 Step 1 QoS (QualityOfService)



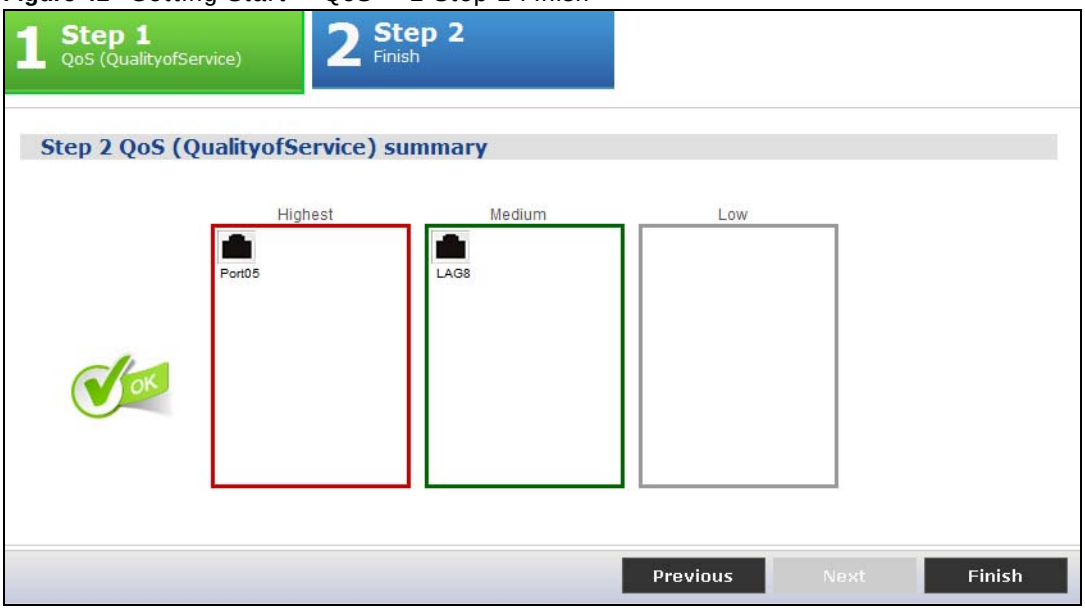
Each field is described in the following table.

Table 15 Getting Start > QoS > 1 Step 1 QoS (QualityOfService)

LABEL	DESCRIPTION
Highest	Click and drag icons located on the left to desired preference.
Medium	Click and drag icons located on the left to desired preference.
Low	Click and drag icons located on the left to desired preference.
Next	Click **Next** to show the next screen.

After clicking **Next,** the finish screen appears.

Figure 41 Getting Start > QoS > 2 Step 2 Finish



Each field is described in the following table.

Table 16 Getting Start > QoS > 2 Step 2 Finish

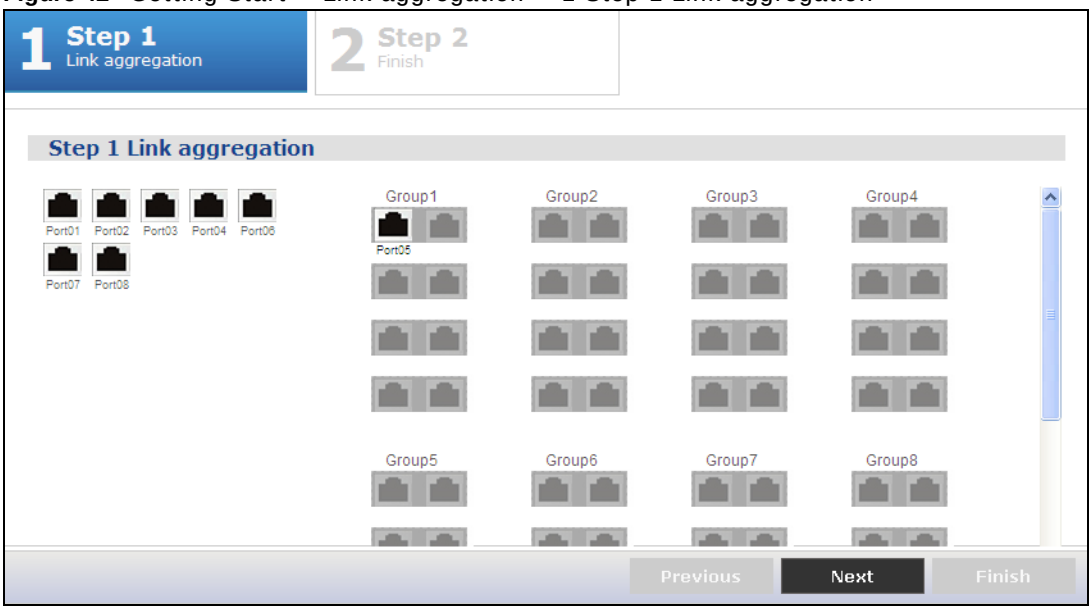
LABEL	DESCRIPTION
Highest	Displays summary results.
Medium	Displays summary results.
Low	Displays summary results.
Previous	Click **Previous** to show the previous screen.
Finish	Review the information and click **Finish** to create the task.

Link aggregation

In link aggregation, you can link aggregation and view finished results.

In order to create link aggregation settings, please do the following. Click **Getting Start > Link aggregation > 1 Step 1 Link aggregation** to access this screen.

Figure 42 Getting Start > Link aggregation > 1 Step 1 Link aggregation



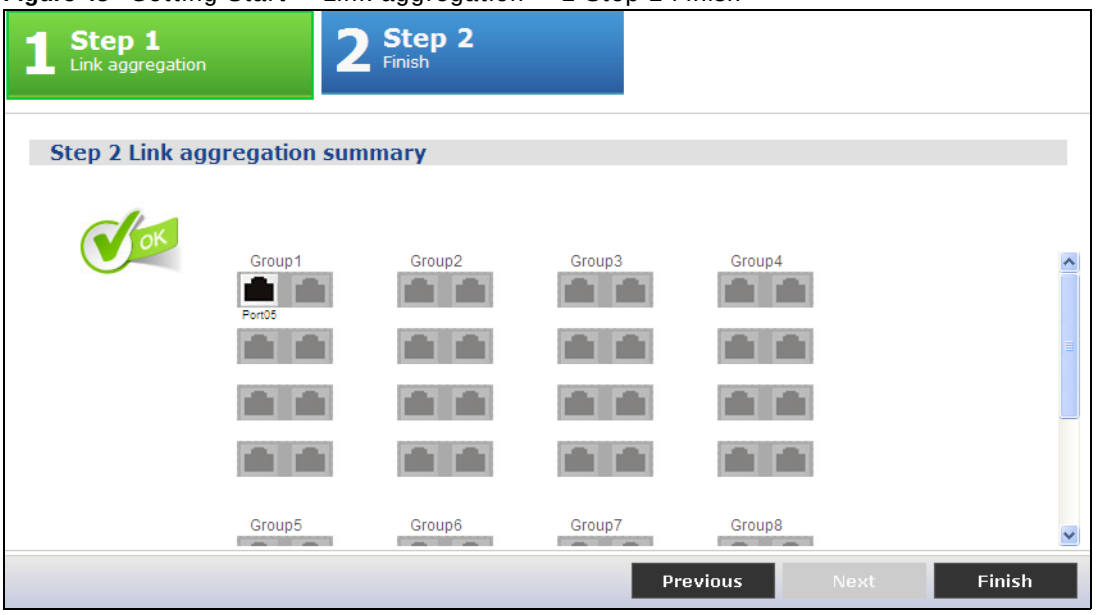
Each field is described in the following table.

Table 17 Getting Start > Link aggregation > 1 Step 1 Link aggregation

LABEL	DESCRIPTION
Group 1	Click and drag icons located on the left to desired preference.
Group 2	Click and drag icons located on the left to desired preference.
Group 3	Click and drag icons located on the left to desired preference.
Group 4	Click and drag icons located on the left to desired preference.
Group 5	Click and drag icons located on the left to desired preference.
Group 6	Click and drag icons located on the left to desired preference.
Group 7	Click and drag icons located on the left to desired preference.
Group 8	Click and drag icons located on the left to desired preference.
Next	Click **Next** to show the next screen.

After clicking **Next,** the finish screen appears.

Figure 43 Getting Start > Link aggregation > 2 Step 2 Finish



Each field is described in the following table.

Table 18 Getting Start > Link aggregation > 2 Step 2 Finish

LABEL	DESCRIPTION
Group 1	Displays summary results.
Group 2	Displays summary results.
Group 3	Displays summary results.
Group 4	Displays summary results.
Group 5	Displays summary results.
Group 6	Displays summary results.
Group 7	Displays summary results.
Group 8	Displays summary results.
Previous	Click **Previous** to show the previous screen.
Finish	Review the information and click **Finish** to create the task.

PART II
Technical Reference

The appendices provide general information. Some details may not apply to your Switch.

6

Monitor: System

6.1 Overview

This section provides information for **System** in **Monitor**. Use the **System** screens to view general Switch settings.

6.1.1 What You Can Do in this Chapter

- The **IP** screen (Section 6.2 on page 51) displays IPv4 and IPv6.
- The **Information** screen (Section 6.3 on page 53) displays the system information.

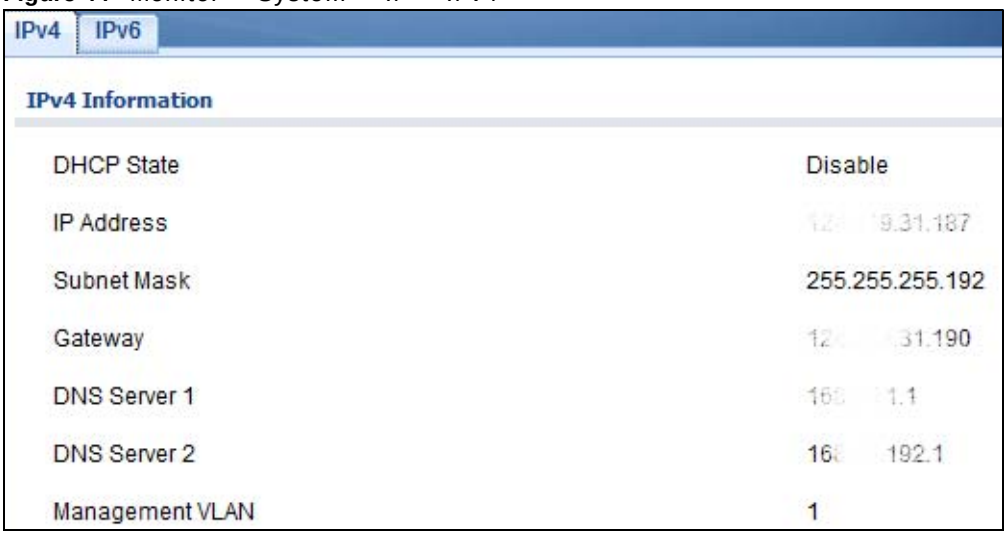
6.2 IP

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

6.2.1 IPv4

Use this screen to view the Switch's IPv4 information. Click **Monitor > System > IP > IPv4** to open this screen.

Figure 44 Monitor > System > IP > IPv4



The following table describes the labels in this screen.

Table 19 Monitor > System > IP > IPv4

LABEL	DESCRIPTION
DHCP State	This field displays the state of Dynamic Host Configuration Protocol RFC 2131 and RFC 2132 (DHCP).
IP Address	This field displays IP address of the Switch in the IP domain.
Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server 1	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. This field displays a domain name server IP address, enabling the use of a domain.
DNS Server 2	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. This field displays a domain name server IP address, enabling the use of a domain.
Management VLAN	This field displays the management VLAN.

6.2.2 IPv6

Use this screen to view the Switch's IPv6 information. Click **Monitor > System > IP > IPv6** to open this screen.

Figure 45 Monitor > System > IP > IPv6

The following table describes the labels in this screen.

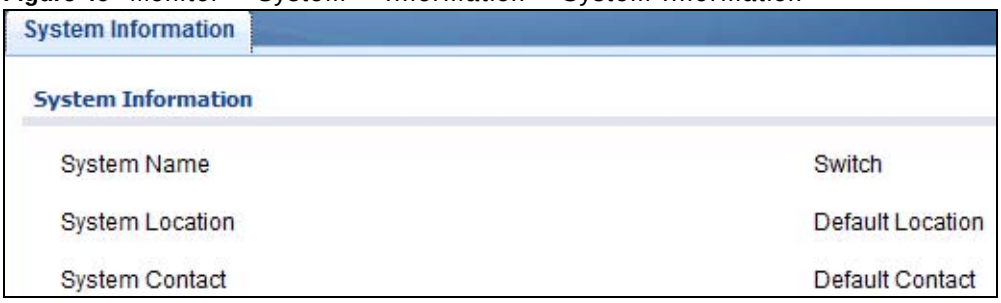
Table 20 Monitor > System > IP > IPv6

LABEL	DESCRIPTION
Auto Configuration	This field displays auto configuration.
IPv6 Address	This field displays IP address of the Switch in the IP domain.
IPv6 Gateway	This field displays the IP address of the default outgoing gateway.
DHCPv6 Client	This field displays the Switch's DHCP settings when it is acting as a DHCPv6 client.

6.3 Information

In the navigation panel, click **Monitor > System > Information > System Information** to display the screen as shown. You can view system information.

Figure 46 Monitor > System > Information > System Information



The following table describes the labels in this screen.

Table 21 Monitor > System > Information > System Information

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
System Location	This field displays the geographic location of the Switch for identification purposes.
System Contact	This field displays the person in charge of the Switch for identification purposes.

7

Monitor: Port

7.1 Overview

This section provides information for **Port** in **Monitor**. Use the **Port** screens to view general Switch port settings.

7.1.1 What You Can Do in this Chapter

- The **Port** screen (Section 7.2 on page 54) displays status, port counters, and bandwidth utilization.
- The **PoE** screen (Section 7.3 on page 58) displays PoE.
- The **Bandwidth Management** screen (Section 7.4 on page 59) displays bandwidth control.
- The **Storm Control** screen (Section 7.5 on page 60) displays port settings of the Switch.

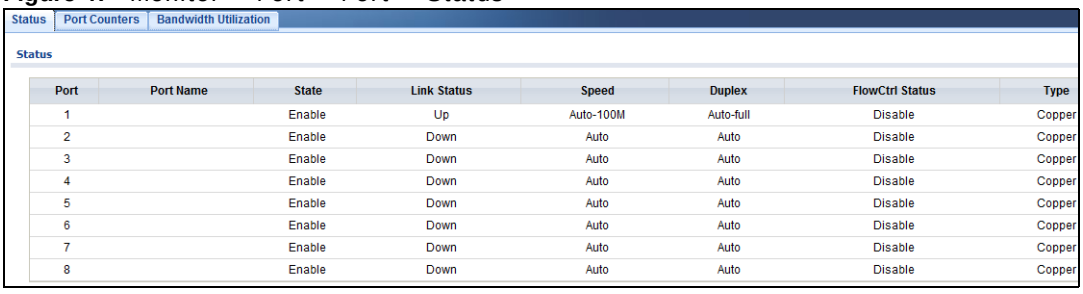
7.2 Port

Use this screen to view Switch port settings.

7.2.1 Status

Use this screen to view the Switch's port statistics. Click **Monitor > Port > Port > Status** to access this screen.

Figure 47 Monitor > Port > Port > Status



Each field is described in the following table.

Table 22 Monitor > Port > Port > Status

LABEL	DESCRIPTION
Port	This is the port index number.
Port Name	A descriptive name that identifies this port.

Table 22 Monitor > Port > Port > Status (continued)

LABEL	DESCRIPTION
State	This is port admin setting state.
Link Status	This field displays **Up** or **Down**. When port is linked, it displays **Up**; otherwise, **Down** is shown.
Speed	View the speed of the Ethernet connection on this port.
Duplex	View the duplex mode of the Ethernet connection on this port.
FlowCtrl Status	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.
Type	View the type on this port.

7.2.2 Port Counters

Use this screen to view the Switch's port counters settings. Click **Monitor > Port > Port > Port Counters** to access this screen.

Figure 48 Monitor > Port > Port > Port Counters

Each field is described in the following table.

Table 23 Monitor > Port > Port > Port Counters

LABEL	DESCRIPTION
Interface	
Port	This field displays the port.

Table 23 Monitor > Port > Port > Port Counters (continued)

LABEL	DESCRIPTION
Mode	This field displays the mode.
Port 1 Interface mib Counters	
ifInOctets	This field displays the ifInOctets.
ifInUcastPkts	This field displays the ifInUcastPkts.
ifInNUcastPkts	This field displays the ifInNUcastPkts..
ifInDiscards	This field displays the ifInDiscards.
ifOutOctets	This field displays the ifOutOctets.
ifOutUcastPkts	This field displays the ifOutUcastPkts.
ifOutNUcastPkts	This field displays the ifOutNUcastPkts.
ifOutDiscards	This field displays the ifOutDiscards.
ifInMulticastPkts	This field displays the ifInMulticastPkts.
ifInBroadcastPkts	This field displays the ifInBroadcastPkts.
ifOutMulticastPkts	This field displays the ifOutMulticastPkts.
ifOutBroadcastPkts	This field displays the ifOutBroadcastPkts.
Port 1 Etherlike mib Counters	
dot3StatsAlignmentErrors	This field displays the dot3StatsAlignmentErrors.
dot3StatsFCSErrors	This field displays the dot3StatsFCSErrors.
dot3StatsSingleCollisionFrames	This field displays the dot3StatsSingleCollisionFrames.
dot3StatsMultipleCollisionFrames	This field displays the dot3StatsMultipleCollisionFrames.
dot3StatsDeferredTransmissions	This field displays the dot3StatsDeferredTransmissions.
dot3StatsLateCollisions	This field displays the dot3StatsLateCollisions.
dot3StatsExcessiveCollisions	This field displays the dot3StatsExcessiveCollisions.
dot3StatsFrameTooLongs	This field displays the dot3StatsFrameTooLongs.
dot3StatsSymbolErrors	This field displays the dot3StatsSymbolErrors.
dot3ControlInUnkownOpcodes	This field displays the dot3ControlInUnkownOpcodes.
dot3lInPauseFrames	This field displays the dot3lInPauseFrames.
dot3lOutPauseFrames	This field displays the dot3lOutPauseFrames.
Port 1 RMON mib Counters	
etherStatsDropEvents	This field displays the etherStatsDropEvents.
etherStatsOctets	This field displays the etherStatsOctets.
etherStatsBroadcastPkts	This field displays the etherStatsBroadcastPkts.
etherStatsMulticastPkts	This field displays the etherStatsMulticastPkts.
etherStatsCRCAlignErrors	This field displays the etherStatsCRCAlignErrors.
etherStatsUnderSizePkts	This field displays the etherStatsUnderSizePkts.
etherStatsOverSizePkts	This field displays the etherStatsOverSizePkts.
etherStatsFragments	This field displays the etherStatsFragments.
etherStatsJabbers	This field displays the etherStatsJabbers.
etherStatsCollisions	This field displays the etherStatsCollisions.
etherStatsPkts64Octets	This field displays the etherStatsPkts64Octets.
etherStatsPkts65to127Octets	This field displays the etherStatsPkts65to127Octets.
etherStatsPkts128to255Octets	This field displays the etherStatsPkts128to255Octets.

Table 23 Monitor > Port > Port > Port Counters (continued)

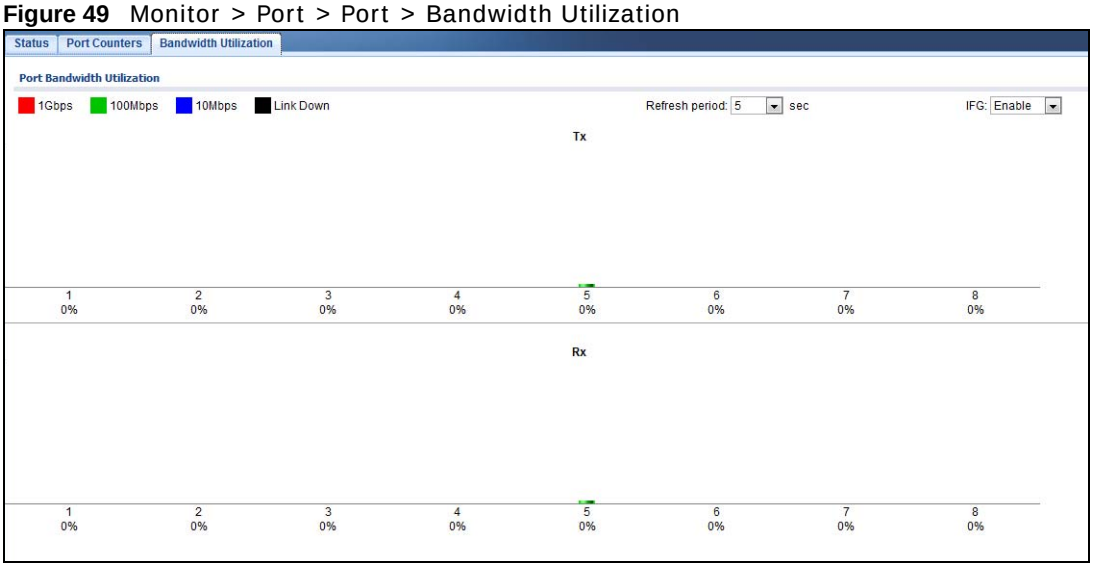
LABEL	DESCRIPTION
etherStatsPkts256to511Octets	This field displays the etherStatsPkts256to511Octets.
etherStatsPkts512to1023Octets	This field displays the etherStatsPkts512to1023Octets.
etherStatsPkts1024to1518Octets	This field displays the etherStatsPkts1024to1518Octets.

7.2.3 Bandwidth Utilization

Utilization is the percentage of a network's bandwidth that is currently being consumed by network traffic. Each vertical bar represents the highest utilization on a port, and can be either transmitted (Tx) traffic or received (Rx) traffic during the last time interval in seconds.

Use this screen to view the Switch's bandwidth utilization settings. Click **Monitor > Port > Port > Bandwidth Utilization** to access this screen.

Figure 49 Monitor > Port > Port > Bandwidth Utilization



Each field is described in the following table.

Table 24 Monitor > Port > Port > Bandwidth Utilization

LABEL	DESCRIPTION
Port Bandwidth Utilization	
1Gbps	This field displays the 1Gbps.
100Mbps	This field displays the 100Mbps.
10Mbps	This field displays the 10Mbps.
Link down	This field displays the link down.
Refresh period	This field displays the refresh period.
IFG	This field displays the IFG.
Tx	Transmitted (Tx) traffic during the last time interval in seconds.
Rx	Received (Rx) traffic during thetime interval in seconds.

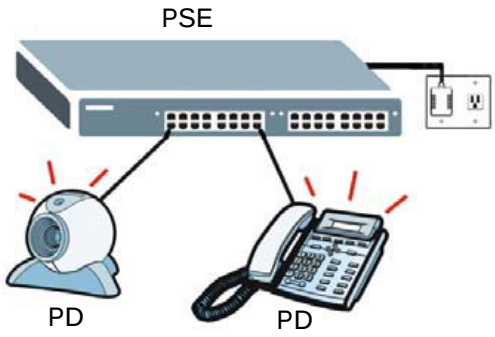
7.3 PoE

Note: The PoE function and the following screens are available for models ending in “HP” only.

The Switch supports both the IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3at High Power over Ethernet (PoE) standards. The Switch is Power Sourcing Equipment (PSE) because it provides a source of power via its Ethernet ports, and each device that receives power through an Ethernet port is a Powered Device (PD).

In the figure below, the IP camera and IP phone get their power directly from the Switch. Aside from minimizing the need for cables and wires, PoE removes the hassle of trying to find a nearby electric outlet to power up devices.

Figure 50 Powered Device Examples

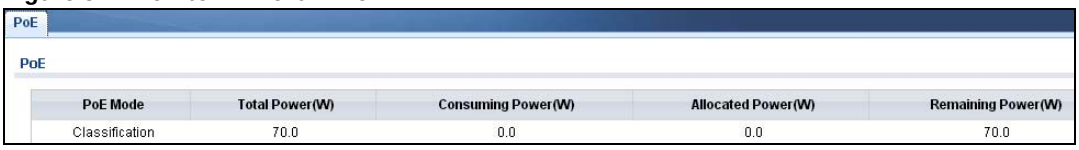


You can also set priorities so that the Switch is able to reserve and allocate power to certain PDs.

Note: The PoE devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

To view the current amount of power that PDs are receiving from the Switch, click **Monitor > Port > PoE**.

Figure 51 Monitor > Port > PoE



Each field is described in the following table.

Table 25 Monitor > Port > PoE

LABEL	DESCRIPTION
PoE Mode	This field displays the power management mode used by the Switch, whether it is in **Classification** or **Consumption** mode.
Total Power(W)	This field displays the total power the Switch can provide to the connected PoE-enabled devices on the PoE ports.
Consuming Power(W)	This field displays the total amount of power the Switch is currently supplying to the connected PoE-enabled devices.

Table 25 Monitor > Port > PoE

LABEL	DESCRIPTION
Allocated Power(W)	This field displays the total amount of power the Switch has reserved for PoE after negotiating with the connected PoE device(s). **Consuming Power (W)** can be less than or equal but not more than the **Allocated Power (W)**.
Remaining Power(W)	This field displays the amount of power the Switch can still provide for PoE. Note: The Switch must have at least 16 W of remaining power in order to supply power to a PoE device, even if the PoE device needs less than 16 W.

7.4 Bandwidth Management

This section shows you the maximum bandwidth using the **Bandwidth Management** screen. Bandwidth management shows themaximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

7.4.1 Bandwidth Control

Use this screen to view the Switch's bandwidth control in egress global burst and port rate.

An egress port is an outgoing port, that is, a port through which a data packet leaves for both ports. An ingress port is an incoming port, that is, a port through which a data packet enters.

Click **Monitor > Port > Bandwidth Management > Bandwidth Control** to access this screen.

Figure 52 Monitor > Port > Bandwidth Management > Bandwidth Control

Each field is described in the following table.

Table 26 Monitor > Port > Bandwidth Management > Bandwidth Control

LABEL	DESCRIPTION
Egress Global Burst	
Egress Global Burst	This field specifies the current egress burst size in bytes all ports.
Port Rate	View the maximum bandwidth allowed in kilobits per second (Kbps) for the traffic flow on a port.
Port	This field displays the port number.

Table 26 Monitor > Port > Bandwidth Management > Bandwidth Control (continued)

LABEL	DESCRIPTION
Ingress RateLimit (Kbps)	View the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Egress RateLimit (Kbps)	View the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.

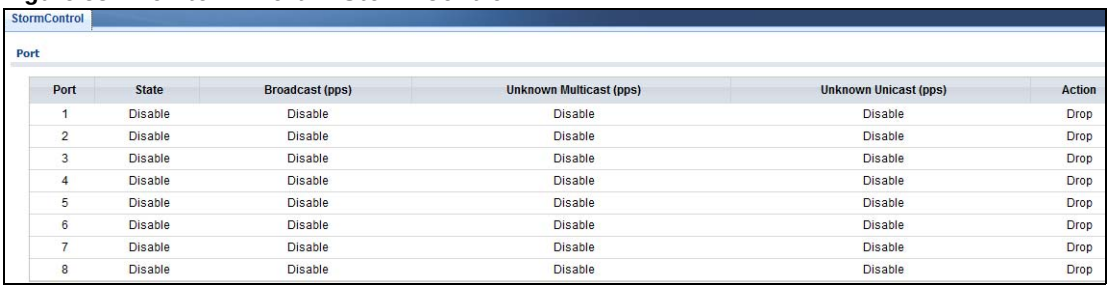
7.5 Storm Control

This section shows you the storm control feature.

Storm control limits the number of broadcast, multicast and unicast packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or unicast packets is reached per second, the subsequent packets are discarded. Enabling this feature reduces broadcast, multicast and/or unicast packets in your network. You can specify limits for each packet type on each port.

Click **Monitor > Port > Storm Control** to access this screen.

Figure 53 Monitor > Port > Storm Control



Each field is described in the following table.

Table 27 Monitor > Port > Storm Control

LABEL	DESCRIPTION
Port	
Port	This field displays the port number.
State	This field displays the state.
Broadcast (pps)	Displays how many broadcast packets the port receives (in pps).
Unknown Multicast (pps)	Displays how many unknown multicast packets the port receives (in pps).
Unknown Unicast (pps)	Displays how many unknown unicast packets the port receives (in pps).
Action	Displays the action the device takes when a limit is reached. The following options are available: • **Drop** - drop the packet. • **Shutdown** - shutdown the connection.

8

Monitor: VLAN

8.1 Overview

This section provides information for **VLAN** in **Monitor**.

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user on the same network.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

8.1.1 What You Can Do in this Chapter

- The **VLAN** screen (Section 8.2 on page 61) displays VLAN, port, and VLAN port settings.
- The **Guest VLAN** screen (Section 8.3 on page 64) displays the global and port settings of the Switch.
- The **Voice VLAN** screen (Section 8.4 on page 65) displays the global and port settings of the Switch.

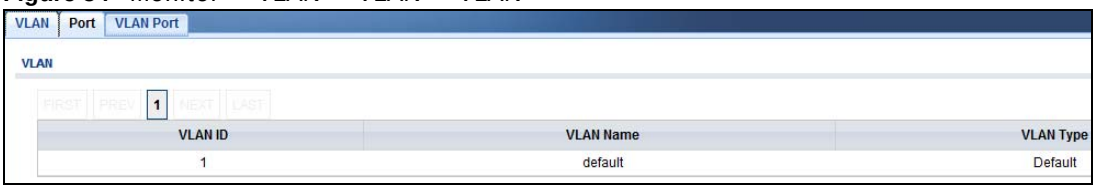
8.2 VLAN

Use this screen to view Switch VLAN settings.

8.2.1 VLAN

Use this screen to view the Switch's VLAN settings. Click **Monitor > VLAN > VLAN > VLAN** to access this screen.

Figure 54 Monitor > VLAN > VLAN > VLAN



Each field is described in the following table.

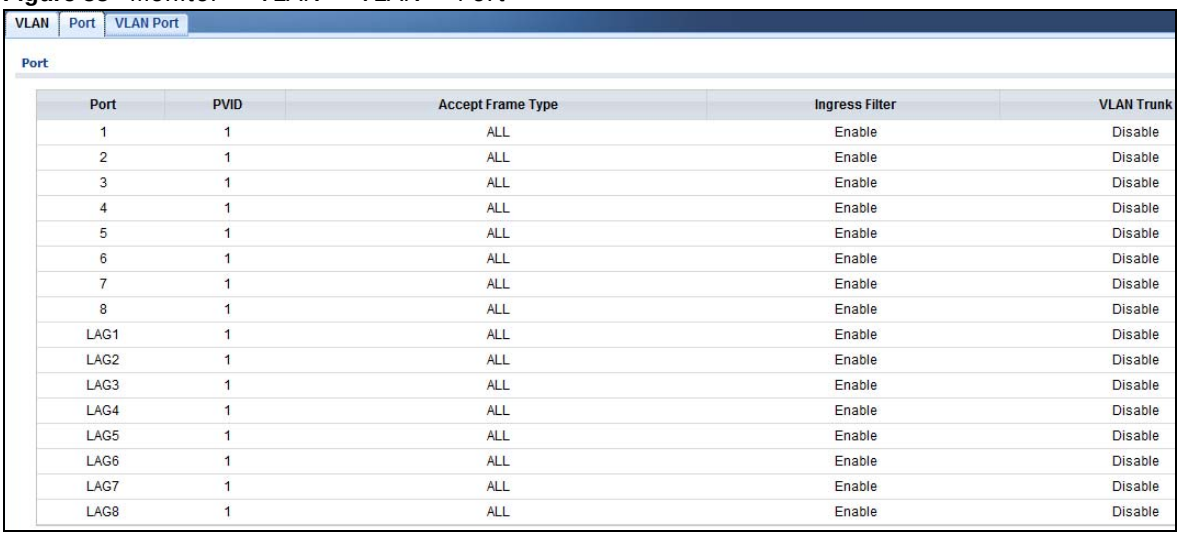
Table 28 Monitor > VLAN > VLAN > VLAN

LABEL	DESCRIPTION
VLAN	
VLAN ID	This is the VLAN identification number.
VLAN Name	Displays a descriptive name for the VLAN for identification purposes.
VLAN Type	Displays a type for the VLAN for identification purposes.

8.2.2 Port

Use this screen to view the Switch's port setting in VLAN. Click **Monitor > VLAN > VLAN > Port** to access this screen.

Figure 55 Monitor > VLAN > VLAN > Port



Each field is described in the following table.

Table 29 Monitor > VLAN > VLAN > Port

LABEL	DESCRIPTION
Port	
Port	This field displays the port number.
PVID	This is the port VLAN identification number. A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.

Table 29 Monitor > VLAN > VLAN > Port (continued)

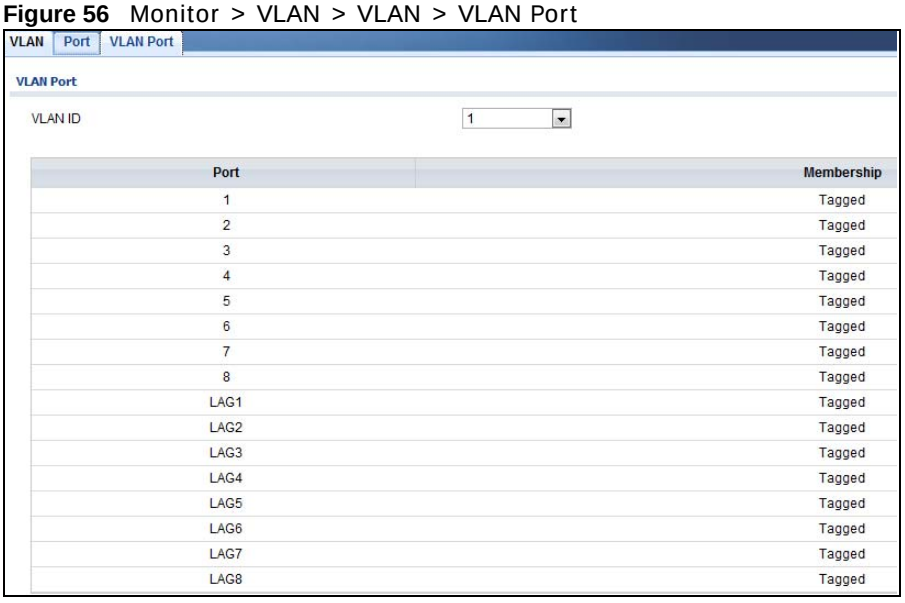
LABEL	DESCRIPTION
Accept Frame Type	This field displays the type that is accepted by the frame. Specifes the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**. **All** accepts all untagged or tagged frames on this port. This is the default setting. **Tag Only** accepts only tagged frames on this port. All untagged frames will be dropped. **Untag Only** accepts only untagged frames on this port. All tagged frames will be dropped.
Ingress Filter	If set, the Switch discards incoming frames for VLANs that do not have this port as a member.
VLAN Trunks	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.

8.2.3 VLAN Port

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port. Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports. Port-based VLANs are specific only to the Switch on which they were created.

Use this screen to view the Switch's VLAN port settings. Click **Monitor > VLAN > VLAN > VLAN Port** to access this screen.

Figure 56 Monitor > VLAN > VLAN > VLAN Port



Each field is described in the following table.

Table 30 Monitor > VLAN > VLAN > VLAN Port

LABEL	DESCRIPTION
VLAN Port	
VLAN ID	This is the VLAN identification number.

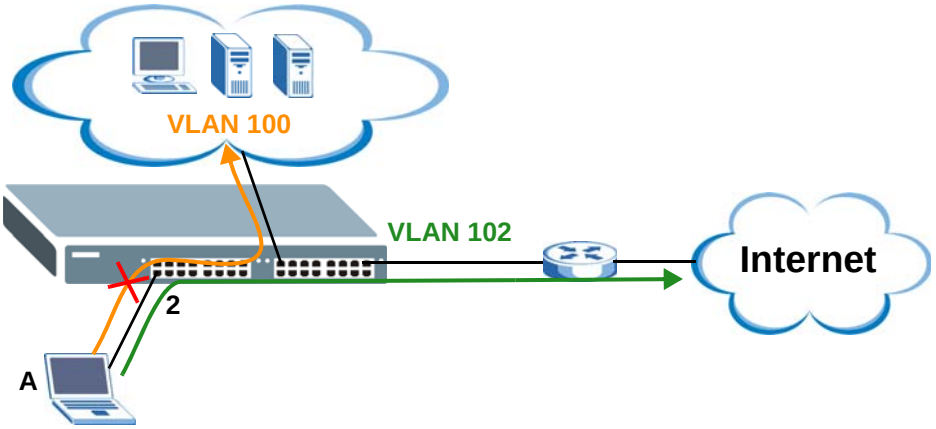
Table 30 Monitor > VLAN > VLAN > VLAN Port (continued)

LABEL	DESCRIPTION
Port	Displays the port index value.
Membership	Displays the status of the VLAN group: **Forbidden, Excluded, Tagged** or **Untagged.**

8.3 Guest VLAN

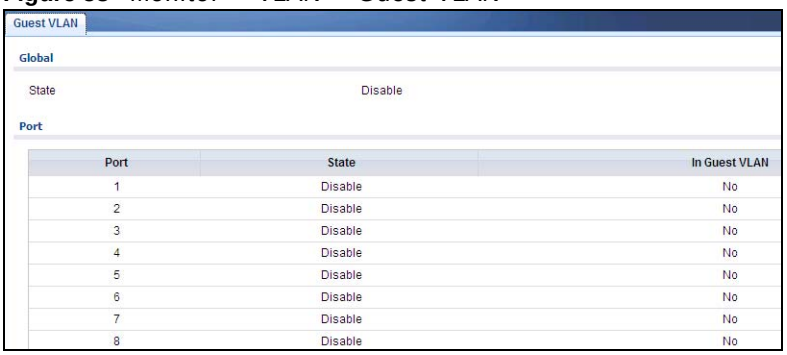
When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in the example), the user (**A** in the example) that is not IEEE 802.1x capable or fails to enter the correct username and password can still access the port, but traffic from the user is forwarded to the guest VLAN. That is, unauthenticated users can have access to limited network resources in the same guest VLAN, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 57 Guest VLAN Example



Use this screen to view the Switch's guest VLAN. Click **Monitor > VLAN > Guest VLAN** to access this screen.

Figure 58 Monitor > VLAN > Guest VLAN



Each field is described in the following table.

Table 31 Monitor > VLAN > Guest VLAN

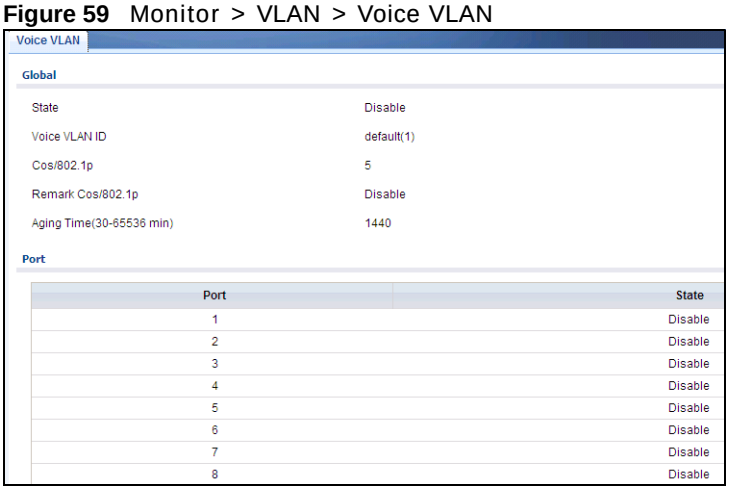
LABEL	DESCRIPTION
Global	
State	This field displays the state of global guest VLAN.
Port	
Port	This field displays a port number.
State	This field displays the state of a port.
In Guest VLAN	This field displays the status of the port, is the port is in guest VLAN or not.

8.4 Voice VLAN

Voice VLANs are VLANs configured specially for voice traffic. By adding the ports connected with voice devices to voice VLANs, you can have voice traffic transmitted within voice VLANs and perform QoS-related configuration for voice traffic as required, thus ensuring the transmission priority of voice traffic and voice quality.

Use this screen to view Switch global and port voice VLAN settings for voice traffic. Click **Monitor > VLAN > Voice VLAN** to access this screen.

Figure 59 Monitor > VLAN > Voice VLAN



Each field is described in the following table.

Table 32 Monitor > VLAN > Voice VLAN

LABEL	DESCRIPTION
Global	
State	This field displays the state of a port.
Voice VLAN ID	This is the voice VLAN identification number.
Cos/802.1p	This displays the packet's 802.1p priority field.
Remark Cos/802.1p	This field displays the state of the cos/802.1p.
Aging Time (30-65536 min)	Displays the time interval (from 30 to 65536) in minutes.
Port	

Table 32 Monitor > VLAN > Voice VLAN (continued)

LABEL	DESCRIPTION
Port	This field displays a port number.
State	This field displays the state of a port.

9

Monitor: MAC Table

9.1 Overview

This section provides information for **MAC Table** in **Monitor**.

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's **MAC Table**. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

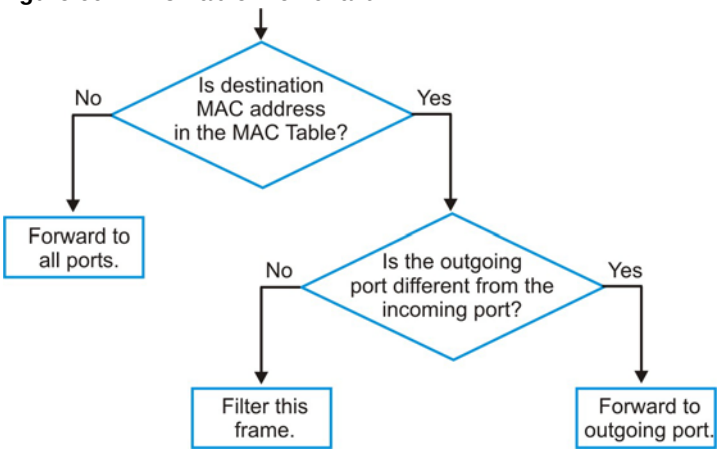
The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1 The Switch examines a received frame and learns the port from which this source MAC address came.

2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the **MAC Table**.

- If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
- If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
- If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 60 MAC Table Flowchart



This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of MAC address it is.

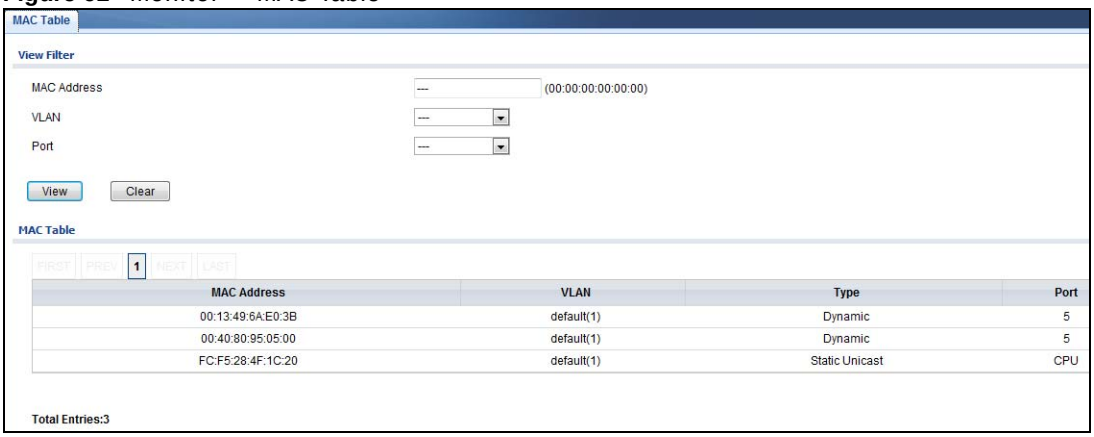
9.1.1 What You Can Do in this Chapter

- The **MAC Table** screen (Section 9.2 on page 68) displays view filter and MAC table of the Switch.

9.2 MAC Table

Use this screen to view filter static and MAC table settings. Click **Monitor > MAC Table** to access this screen.

Figure 61 Monitor > MAC Table



Each field is described in the following table.

Table 33 Monitor > MAC Table

LABEL	DESCRIPTION
View filter	
MAC Address	This is the MAC address of the device from which this incoming frame came.
VLAN	Displays a type for the VLAN for identification purposes.
Port	This is the port from which the above MAC address was learned.
View	This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of MAC address it is.
Clear	Click **Clear** to return the fields to the factory defaults.
MAC Table	
MAC Address	This is the MAC address of the device from which this incoming frame came.
VLAN	Displays a type for the VLAN for identification purposes.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).
Port	This is the port from which the above MAC address was learned.
Total Entries	Displays the number of total entries.

10

Monitor: Link Aggregation

10.1 Overview

This section provides information for **Link Aggregation** in **Monitor**.

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link. However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

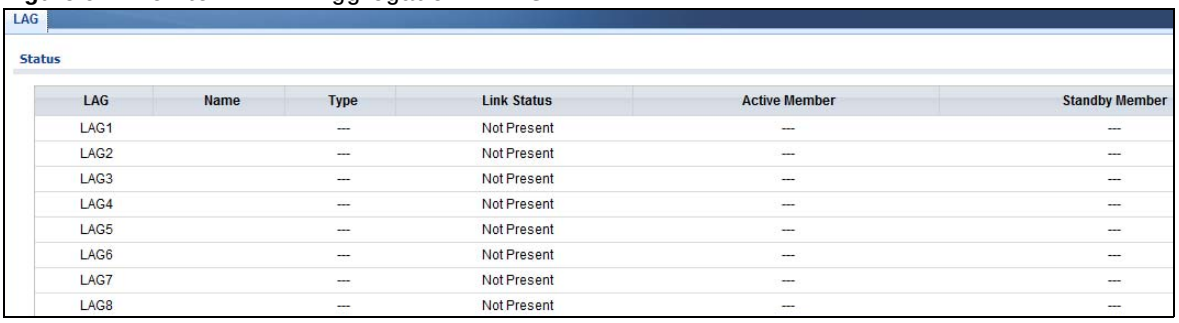
10.1.1 What You Can Do in this Chapter

- The **Link Aggregation** screen (Section 10.2 on page 69) displays link aggregation status.

10.2 Link Aggregation

Use the **Link Aggregation** screens to view Switch link aggregation status. Click **Monitor > Link Aggregation > LAG** to access this screen.

Figure 62 Monitor > Link Aggregation > LAG


LAG

Status

LAG	Name	Type	Link Status	Active Member	Standby Member
LAG1		---	Not Present	---	---
LAG2		---	Not Present	---	---
LAG3		---	Not Present	---	---
LAG4		---	Not Present	---	---
LAG5		---	Not Present	---	---
LAG6		---	Not Present	---	---
LAG7		---	Not Present	---	---
LAG8		---	Not Present	---	---

Each field is described in the following table.

Table 34 Monitor > Link Aggregation > LAG

LABEL	DESCRIPTION
LAG	Displays the link aggregation status index value.
Name	This field displays the name.
Type	This field displays the type.
Link Status	This field displays the status of the link.
Active Member	Displays if this member is an active member of a trunk.
Standby Member	Displays if this member is an standby member of a trunk.

11

Monitor: Loop Guard

11.1 Overview

This section provides information for **Loop Guard** in **Monitor**.

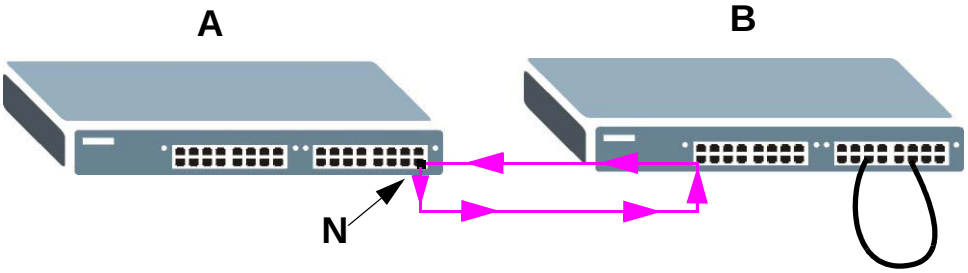
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

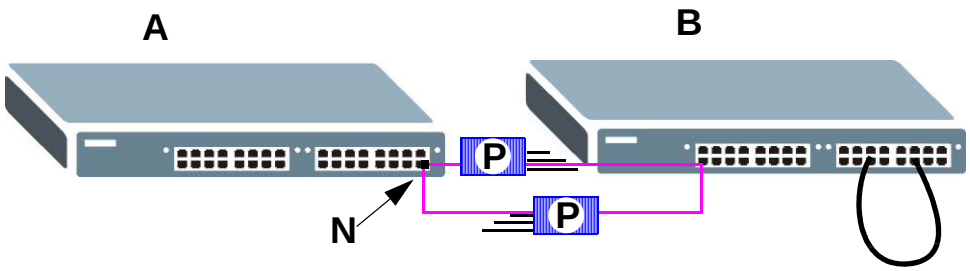
Figure 63 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

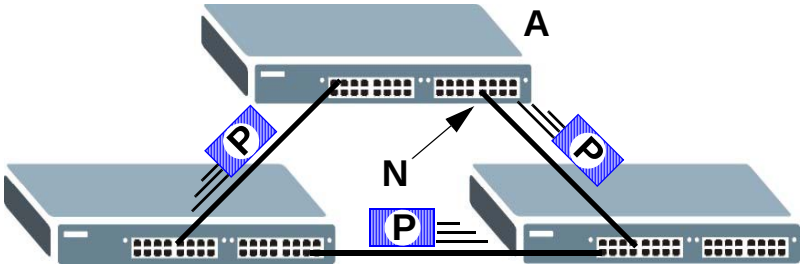
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 64 Loop Guard - Probe Packet



The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 65 Loop Guard - Network Loop



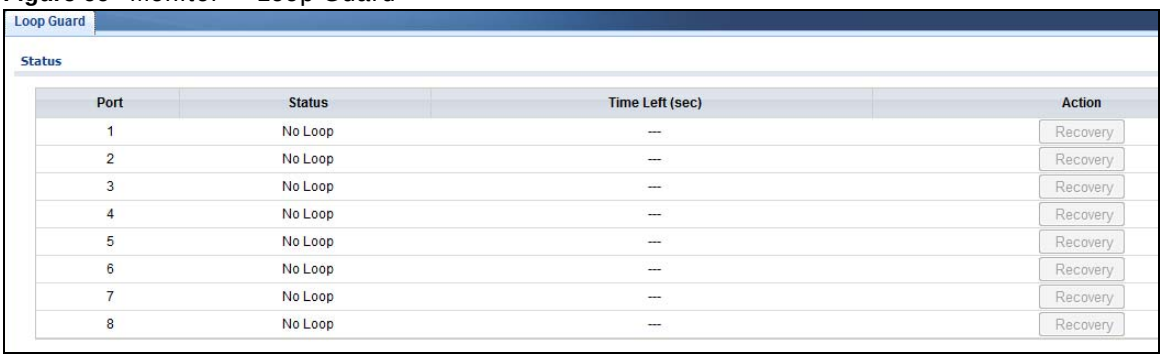
11.1.1 What You Can Do in this Chapter

- The **Loop Guard** screen (Section 11.2 on page 72) displays loop guard status.

11.2 Loop Guard

Use the **Loop Guard** screen to view Switch loop guard status. Click **Monitor > Loop Guard** to access this screen.

Figure 66 Monitor > Loop Guard



Each field is described in the following table.

Table 35 Monitor > Loop Guard

LABEL	DESCRIPTION
Loop Guard Status	
Port	This field displays a port number.
Status	This field displays the status.
Time Left (sec)	This field displays the amount of time left in seconds.
Action	This field displays the action.

12

Monitor: Multicast

12.1 Overview

This section provides information for **Multicast** in **Monitor**.

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in an IPv4 multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

12.1.1 What You Can Do in this Chapter

- The **IGMP** screen (Section 12.2 on page 74) displays Vlan, statistics, group, and router.

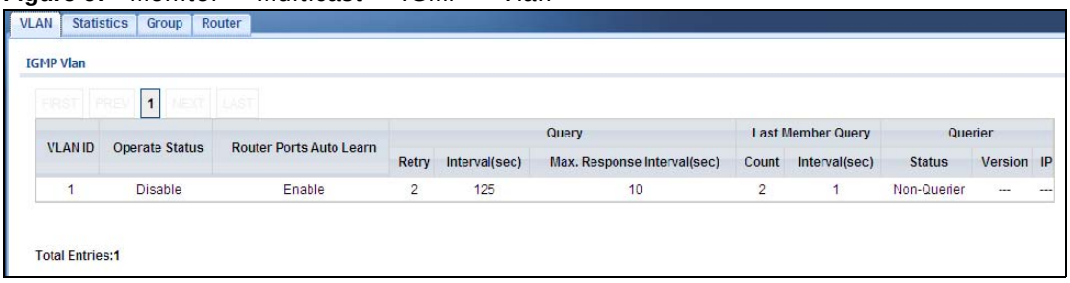
12.2 IGMP

Use this screen to view Switch various multicast features.

12.2.1 Vlan

Use this screen to view the Switch's IGMP vlan. Click **Monitor > Multicast > IGMP > Vlan** to access this screen.

Figure 67 Monitor > Multicast > IGMP > Vlan



Each field is described in the following table.

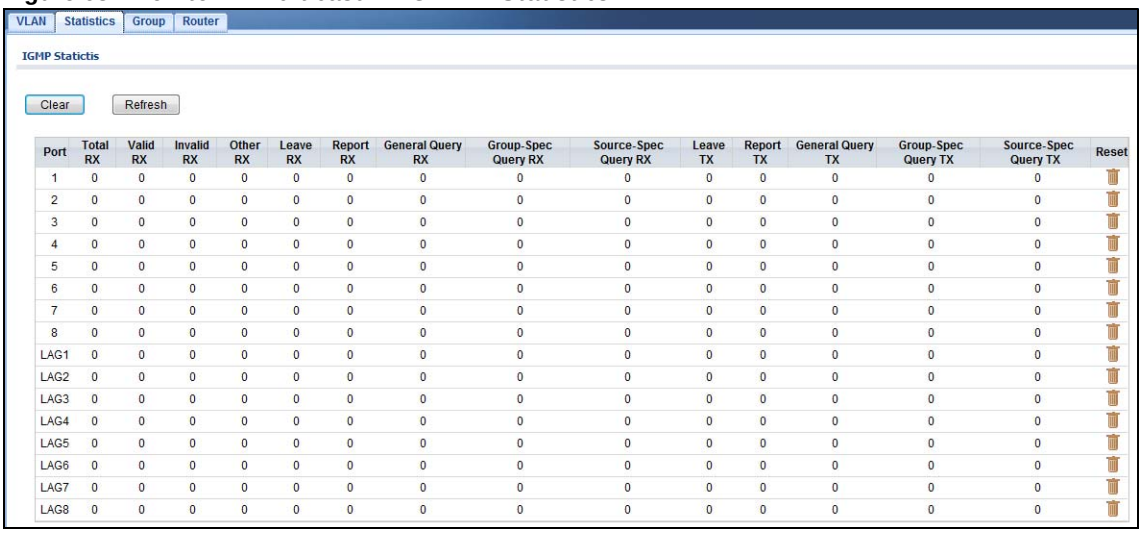
Table 36 Monitor > Multicast > IGMP > Vlan

LABEL	DESCRIPTION
VLAN ID	Displays the identification for the VLAN.
Operate Status	Displays the status of the operation.
Router Ports Auto Learn	Displays whether the router ports are auto learn or not.
Query	
Retry	Displays the number of retry.
Interval	Displays the number (in seconds) for the time interval.
Max. Reponse Interval(sec)	Displays the maximum reponse (in seconds) for the time interval.
Last Member Query	
Count	Displays the number of count.
Interval(sec)	Displays the in seconds for the time interval.
Querier	Allow sthe Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Status	This field displays the entry as querier or non-querier.
Version	This field displays the entry querier version.
IP	This field displays the the entry querier IP address.
Total Entries	This field displays the number of total entries.

12.2.2 Statistics

Use this screen to view the Switch's IGMP statistics. Click **Monitor > Multicast > IGMP > Statistics** to access this screen.

Figure 68 Monitor > Multicast > IGMP > Statistics



Each field is described in the following table.

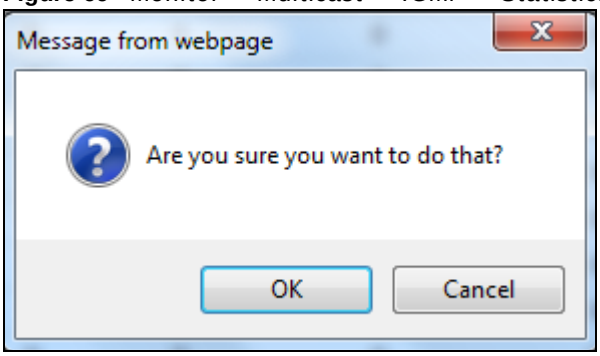
Table 37 Monitor > Multicast > IGMP > Statistics

LABEL	DESCRIPTION
Clear	Click **Clear** to reset the fields to the factory defaults.
Refresh	Click **Refresh** to reload the page.
Port	This field displays a port number.
Total RX	This field displays the total amount of RX.
Valid RX	This field displays the total amount of valid RX.
Invalid RX	This field displays the total amount of invalid RX.
Other RX	This field displays the total amount of other RX.
Leave RX	This field displays the total amount of leave RX.
Report RX	This field displays the total amount of report RX.
General Query RX	This field displays the total amount of general query RX.
Group-Spec Query RX	This field displays the total amount of group-spec query RX.
Source-Spec Query RX	This field displays the total amount of source-spec query RX.
Leave TX	This field displays the total amount of leave TX.
Report TX	This field displays the total amount of report TX.
General Query TX	This field displays the total amount of general query TX.
Group-Spec Query TX	This field displays the total amount of group-spec query TX.
Source-Spec Query TX	This field displays the total amount of source-spec query TX.
Source-Spec Query TX	This field displays the total amount of source-spec query TX.
Reset	Click **Reset** to modify settings.
OK	Click **OK** to apply the changes.
Cancel	Click **Cancel** to discard the changes.

In the Reset column, the **Reset** option allows you to delete a pre-existing rule.

Click **OK** and confirm at the pop-up screen to complete the task. Click **Cancel** and confirm at the pop-up screen to discard the changes.

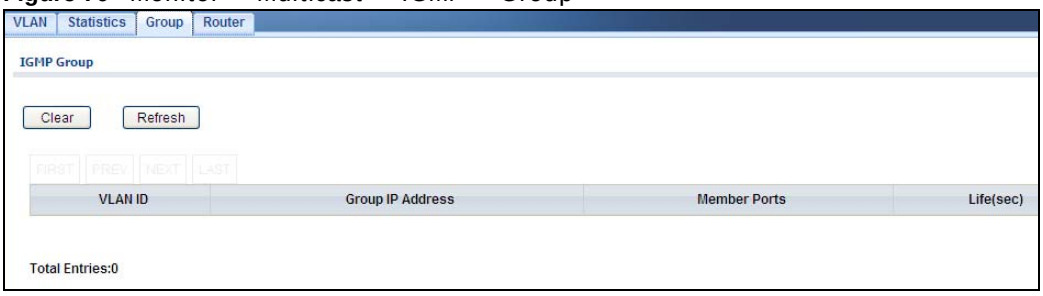
Figure 69 Monitor > Multicast > IGMP > Statistics > Reset



12.2.3 Group

Use this screen to view the Switch's IGMP group. Click **Monitor > Multicast > IGMP > Group** to access this screen.

Figure 70 Monitor > Multicast > IGMP > Group



Each field is described in the following table.

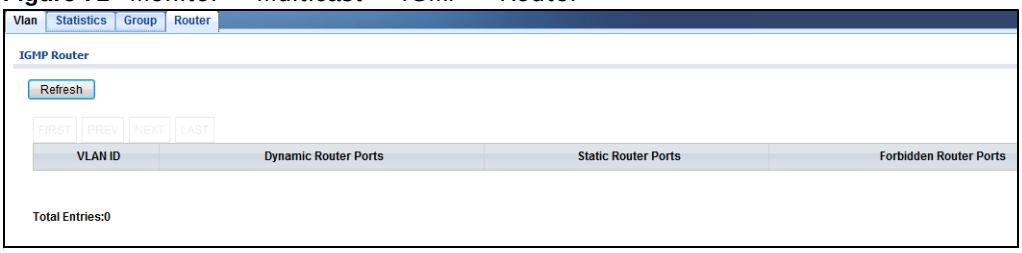
Table 38 Monitor > Multicast > IGMP > Group

LABEL	DESCRIPTION
Clear	Click **Clear** to delete the dynamic groups.
Refresh	Click **Refresh** to reload the page.
VLAN ID	Displays the identification for the VLAN.
Group IP Address	This field displays the group IP address.
Member Ports	This field displays the member ports.
Life(sec)	Displays life in seconds for the time interval.
Total Entries	This field displays the number of total entries.

12.2.4 Router

Use this screen to view the Switch's IGMP router. Click **Monitor > Multicast > IGMP > Router** to access this screen.

Figure 71 Monitor > Multicast > IGMP > Router



Each field is described in the following table.

Table 39 Monitor > Multicast > IGMP > Router

LABEL	DESCRIPTION
Refresh	Click **Refresh** to reload the page.
VLAN ID	Displays the identification for the VLAN.
Dynamic Router Ports	This field displays the dynamic router ports.
Static Router Ports	This field displays the static router ports.
Forbidden Router Ports	This field displays the forbidden router ports.
Total Entries	This field displays the number of total entries.

13

Monitor: Spanning Tree

13.1 Overview

This section provides information for **Spanning Tree** in **Monitor**.

The Switch supports Spanning Tree Protocol (STP), Common and Internal Spanning Tree (CIST), and Multiple Spanning Tree (MST).

13.1.1 What You Can Do in this Chapter

- The **Spanning Tree** screen (Section 13.2 on page 78) displays CIST, CIST port, MST, MST port, STP statistics.

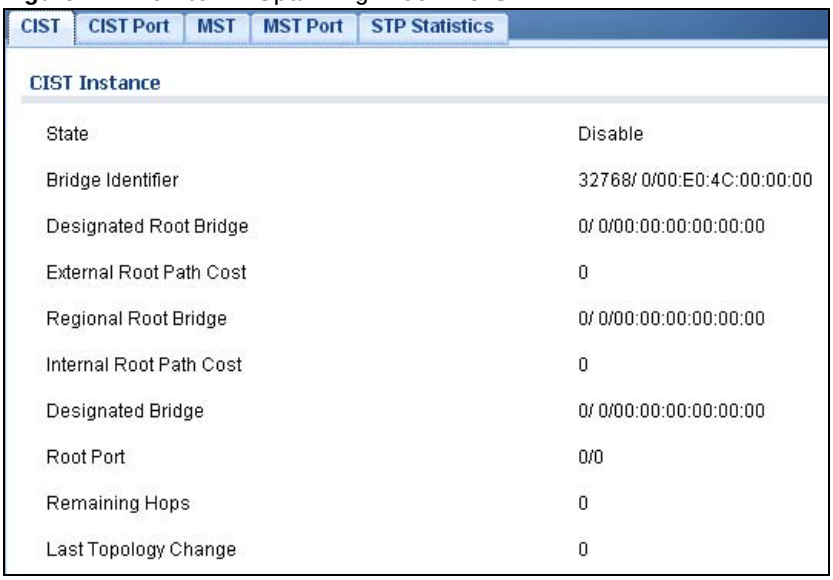
13.2 Spanning Tree

Use this screen to view Switch spanning tree settings.

13.2.1 CIST

Use this screen to view the Switch's spanning tree CIST instance. Click **Monitor > Spanning Tree > CIST** to access this screen.

Figure 72 Monitor > Spanning Tree > CIST



Each field is described in the following table.

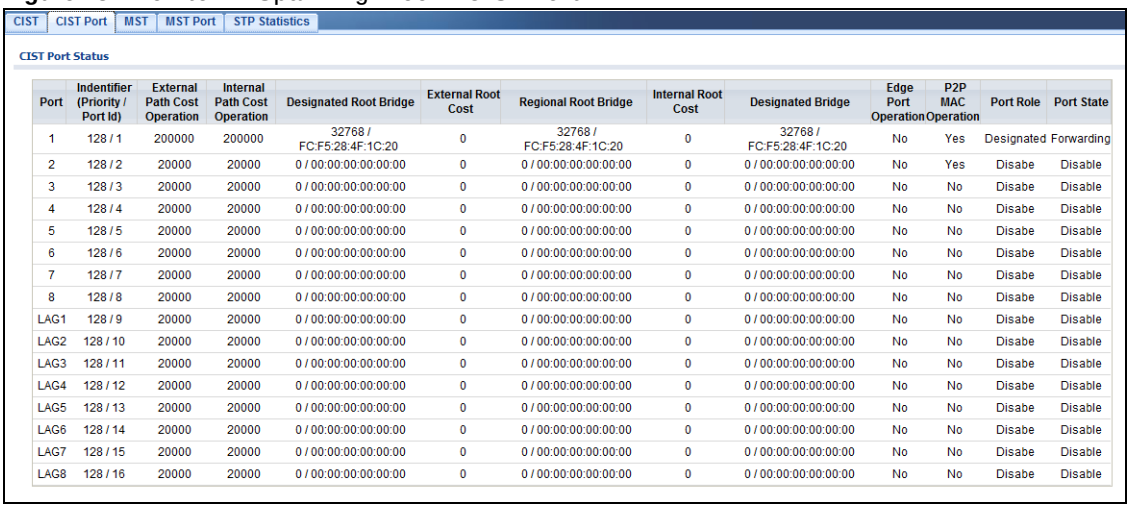
Table 40 Monitor > Spanning Tree > CIST

LABEL	DESCRIPTION
State	This field displays the state.
Bridge Indentifier	This is the unique identifier for this bridge, consisting of the bridge priority plus the MAC address.
Designate Root Bridge	Root bridge refers to the base of the spanning tree.
External Root Path Cost	The cost of the path from this bridge to the cist Root Bridge.
Regional Root Bridge	Root bridge refers to the base of the spanning tree.
Internal Root Path Cost	The cost of the path from this bridge to the internal Regional Root Bridge.
Designated Bridge	For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.
Root Port	On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.
Remanining Hops	This field displays the number of remanining hops.
Last Topology Change	Topology change information is directly propagated throughout the network from the device that generates the topology change.

13.2.2 CIST Port

Use this screen to view the Switch's spanning tree CIST port status. Click **Monitor > Spanning Tree > CIST Port** to access this screen.

Figure 73 Monitor > Spanning Tree > CIST Port



Each field is described in the following table.

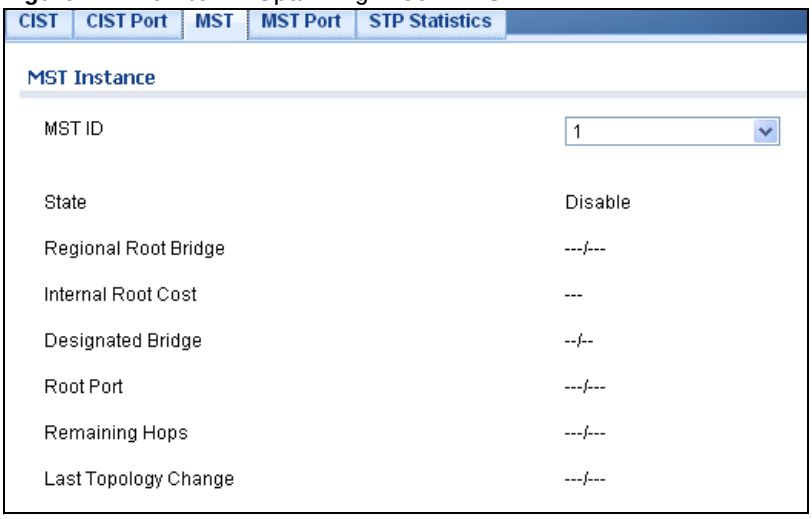
Table 41 Monitor > Spanning Tree > CIST Port

LABEL	DESCRIPTION
Port	This field displays the port number.
Indentifier (Priority / Port Id)	This field displays the identifier (in priority / port number).
External Path Cost Operation	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Internal Path Cost Operation	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Designate Root Bridge	Root bridge refers to the base of the spanning tree.
External Root Cost	This field displays the external root cost.
Regional Root Bridge	Root bridge refers to the base of the spanning tree.
Internal Root Cost	This field displays the internal root cost.
Designated Bridge	For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.
Edge Port Operation	An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes.
P2P MAC Operation	This field displays the state of the P2P MAC operation.
Port Role	This field displays the state of the port role.
Port State	This field displays the state of the port.

13.2.3 MST

Use this screen to view the Switch's spanning tree MST instance. Click **Monitor > Spanning Tree > MST** to access this screen.

Figure 74 Monitor > Spanning Tree > MST



Each field is described in the following table.

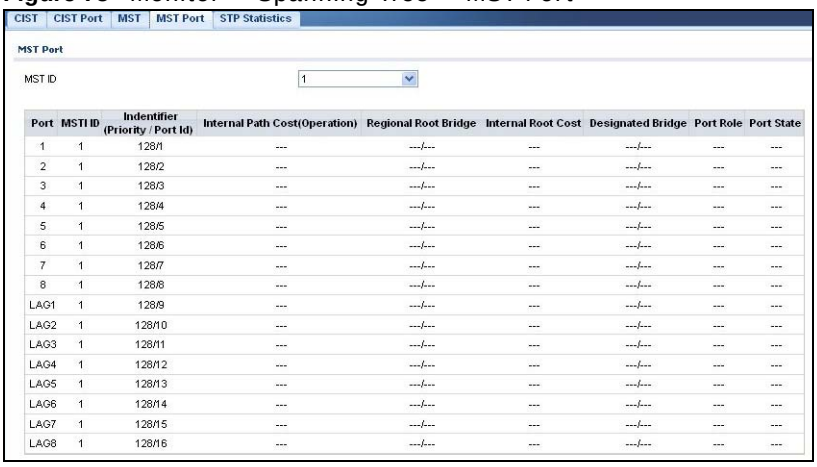
Table 42 Monitor > Spanning Tree > MST

LABEL	DESCRIPTION
MST ID	This is the unique identifier for this MST. Select a number from the drop-down menu to display results.
State	This field displays the state.
Regional Root Bridge	Root bridge refers to the base of the spanning tree.
Internal Root Cost	This field displays the internal root cost.
Designated Bridge	For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.
Root Port	On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.
Remanining Hops	This field displays the number of remanining hops.
Last Topology Change	Topology change information is directly propagated throughout the network from the device that generates the topology change.

13.2.4 MST Port

Use this screen to view the Switch's spanning tree MST port status. Click **Monitor > Spanning Tree > MST Port** to access this screen.

Figure 75 Monitor > Spanning Tree > MST Port



Each field is described in the following table.

Table 43 Monitor > Spanning Tree > MST Port

LABEL	DESCRIPTION
MST ID	This is the unique identifier for this MST. Select a number from the drop-down menu to display results.
Port	This field displays the port number.
MSTI ID	A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.

Table 43 Monitor > Spanning Tree > MST Port (continued)

LABEL	DESCRIPTION
Indentifier (Priority / Port Id)	This field displays the identifier (in priority / port number).
Internal Path Cost(Operation)	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost.
Regional Root Bridge	Root bridge refers to the base of the spanning tree.
Internal Root Cost	This field displays the internal root cost.
Designated Bridge	For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.
Port Role	This field displays the state of the port role.
Port State	This field displays the state of the port.

13.2.5 STP Statistics

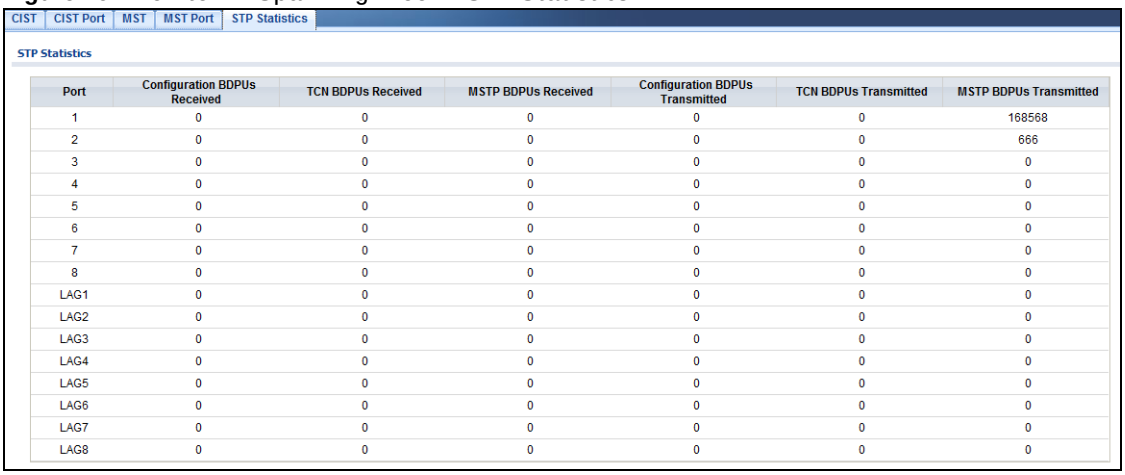
(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

Use this screen to view the Switch's spanning tree STP statistics. Click **Monitor > Spanning Tree > STP Statistics** to access this screen.

Figure 76 Monitor > Spanning Tree > STP Statistics



Each field is described in the following table.

Table 44 Monitor > Spanning Tree > STP Statistics

LABEL	DESCRIPTION
Port	This field displays the port number.
Configuration BDPUs Received	This field displays the configuration BDPUs received.
TCN BDPUs Received	This field displays the TCN BDPUs received.
MSTP BDPUs Received	This field displays the Multiple Spanning Tree Protocol (MSTP) BDPUs received.
Configuration BDPUs Transmitted	This field displays the configuration BDPUs transmitted.
TCN BDPUs Transmitted	This field displays the TCN BDPUs transmitted.
MSTP BDPUs Transmitted	This field displays the Multiple Spanning Tree Protocol (MSTP) BDPUs transmitted.

14

Monitor: LLDP

14.1 Overview

This section provides information for **LLDP** in **Monitor**.

Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.

14.1.1 What You Can Do in this Chapter

- The **LLDP** screen (Section 14.2 on page 84) displays statistics, remote information, and overloading.

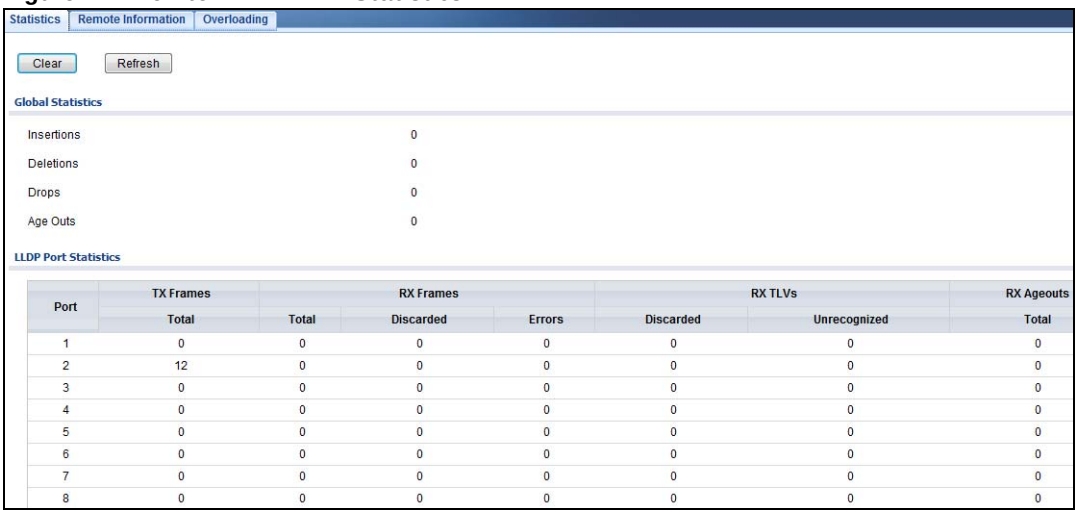
14.2 LLDP

This link takes you to a screen where you can view LLDP on the Switch. LLDP allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device.

14.2.1 Statistics

Use this screen to view the Switch's LLDP global and port statistics. Click **Monitor > LLDP > Statistics** to access this screen.

Figure 77 Monitor > LLDP > Statistics



Each field is described in the following table.

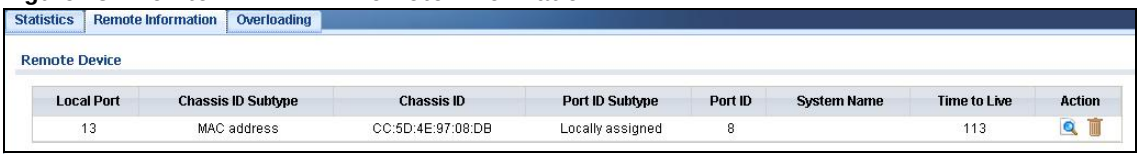
Table 45 Monitor > LLDP > Statistics

LABEL	DESCRIPTION
Clear	Click **Clear** to clear statistics.
Refresh	Click **Refresh** to reload the page.
Global Statistics	
Insertions	This field displays the number of insertions.
Deletions	This field displays the number of deletions.
Drops	This field displays the number of drops.
Age Outs	This field displays the number of age outs.
LLDP Port Statistics	
Port	This field displays the port number.
TX Frames Total	This field displays the total number of TX LLDP frames.
RX Frames Total	This field displays the total number of RX LLDP frames.
RX Frames Discarded	This field displays the number of discarded RX LLDP frames.
RX Frames Errors	This field displays the number of RX LLDP frames errors.
RX TLVs Discarded	This field displays the number of discarded RX LLDP TLVs.
RX TLVs Unrecongnized	This field displays the number of unrecongnized RX LLDP TLVs.
RX Ageouts Total	This field displays the total number of RX LLDP ageouts.

14.2.2 Remote Information

Use this screen to view the Switch's LLDP remote device information. Click **Monitor > LLDP > Remote Information** to access this screen.

Figure 78 Monitor > LLDP > Remote Information



Each field is described in the following table.

Table 46 Monitor > LLDP > Remote Information

LABEL	DESCRIPTION
Local Port	This field displays the local port.
Chassis ID Subtype	This field displays the chassis ID subtype.
Chassis ID	This field displays the chassis ID.
Port ID Subtype	This field displays the port ID subtype.
Port ID	This field displays the port ID.
System Name	This field displays the descriptive name of the Switch for identification purposes.
Time to Live	This field displays the live time of this entry.

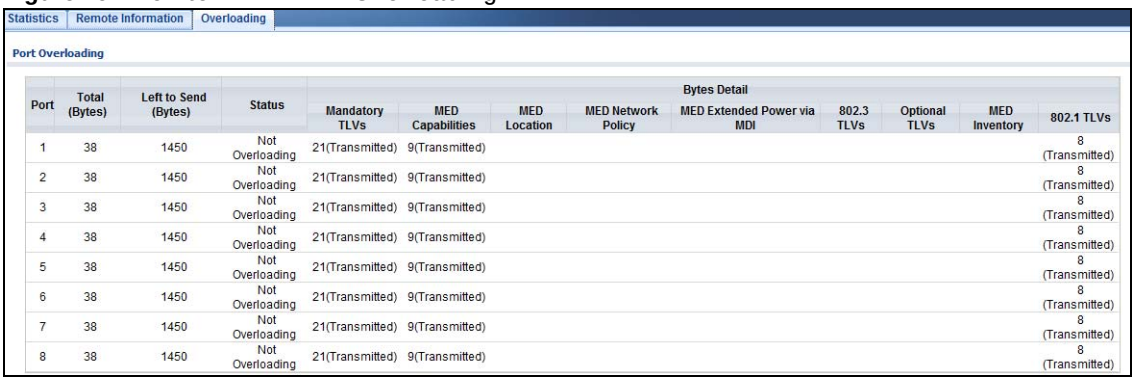
Table 46 Monitor > LLDP > Remote Information (continued)

LABEL	DESCRIPTION
Action	
Detail	Click **Detail** to show more information about this entry.
Delete	Click **Delete** to remove the entry.

14.2.3 Overloading

Use this screen to view the Switch's LLDP port overloading. Click **Monitor > LLDP > Overloading** to access this screen.

Figure 79 Monitor > LLDP > Overloading



Each field is described in the following table.

Table 47 Monitor > LLDP > Overloading

LABEL	DESCRIPTION
Port	This label shows the port you are viewing.
Total (Bytes)	This field displays the total in bytes.
Left to Send (Bytes)	This field displays what is left to send in bytes.
Status	This field displays whether the Switch is overloading or not.
Bytes Details	This field displays how many bytes used by TLVs
Mandatory TLVs	This field displays how many bytes used by mandatory TLVs.
MED Capabilities	This field displays how many bytes used by MED capabilities.
MED Location	This field displays how many bytes used by MED location.
MED Network Policy	This field displays how many bytes used by MED network policy.
MED Extended Power via MDI	This field displays how many bytes used by MED extended power via MDI.
802.3 TLVs	This field displays how many bytes used by 802.3 TLVs.
Optional TLVs	This field displays how many bytes used by optional TLVs.
MED Inventory	This field displays how many bytes used by MED inventory.
802.1 TLVs	This field displays how many bytes used by 802.1 TLVs.

15

Monitor: Security

15.1 Overview

This section provides information for **Security** in **Monitor**.

This link takes you to a screen where you can view the settings or traffic statistics which contain detailed information about specific activities.

15.1.1 What You Can Do in this Chapter

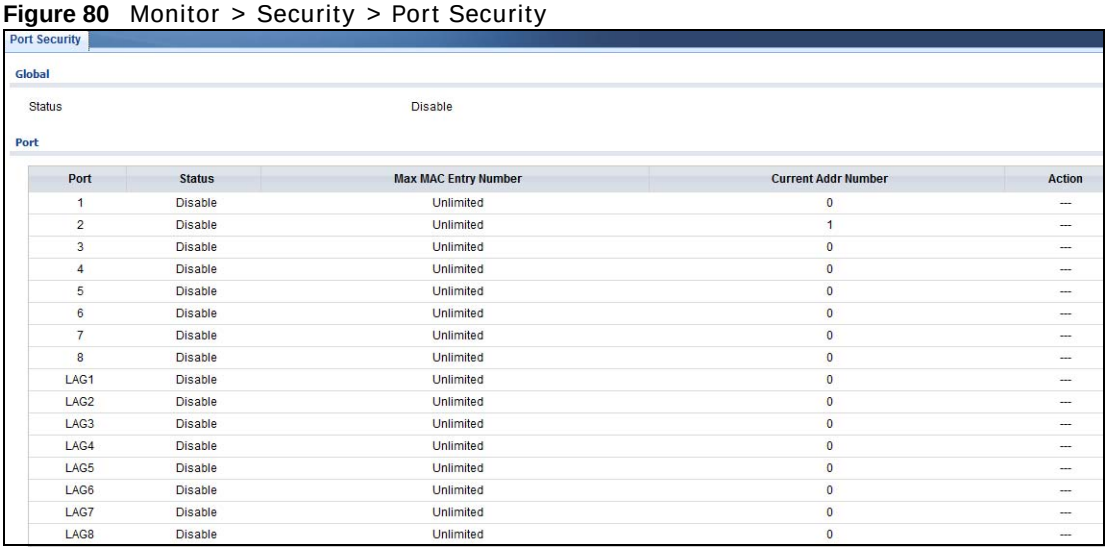
- The **Port Security** screen (Section 15.2 on page 87) displays global and port.
- The **802.1X** screen (Section 15.3 on page 88) displays port and authenticated hosts.

15.2 Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 8K MAC addresses in total with no limit on individual ports; system total MAC address entry is 8K. Static MAC address still can be configured when port security is enabled; the function of port security is concerned with dynamic mac address learn action. When total MAC address entry is 8k, static MAC can't be configured.

Use this screen to view Switch port security settings. Click **Monitor > Security > Port Security** to access this screen.

Figure 80 Monitor > Security > Port Security



Port	Status	Max MAC Entry Number	Current Addr Number	Action
1	Disable	Unlimited	0	---
2	Disable	Unlimited	1	---
3	Disable	Unlimited	0	---
4	Disable	Unlimited	0	---
5	Disable	Unlimited	0	---
6	Disable	Unlimited	0	---
7	Disable	Unlimited	0	---
8	Disable	Unlimited	0	---
LAG1	Disable	Unlimited	0	---
LAG2	Disable	Unlimited	0	---
LAG3	Disable	Unlimited	0	---
LAG4	Disable	Unlimited	0	---
LAG5	Disable	Unlimited	0	---
LAG6	Disable	Unlimited	0	---
LAG7	Disable	Unlimited	0	---
LAG8	Disable	Unlimited	0	---

Each field is described in the following table.

Table 48 Monitor > Security > Port Security

LABEL	DESCRIPTION
Global	
Status	This field displays the status of global control information.
Port	
Port	This field displays a port number.
Status	This field displays the status of port based control information.
Max MAC Entry Number	Displays the designated maximum number of allowed MAC entries. The maximum MAC entry number can be learned for individual ports.
Current Addr Number	This field displays the number of the current addr.
Action	This field displays the action(s) the Switch takes on the associated classified traffic flow.

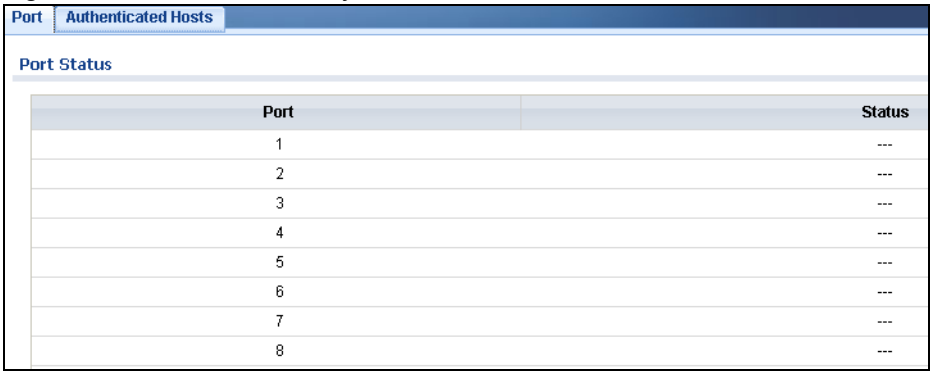
15.3 802.1X

Use this screen to view Switch 802.1x security settings.

15.3.1 Port

Use this screen to view the Switch's 802.1x port status. Click **Monitor > Security > 802.1X > Port** to access this screen.

Figure 81 Monitor > Security > 802.1x > Port



Each field is described in the following table.

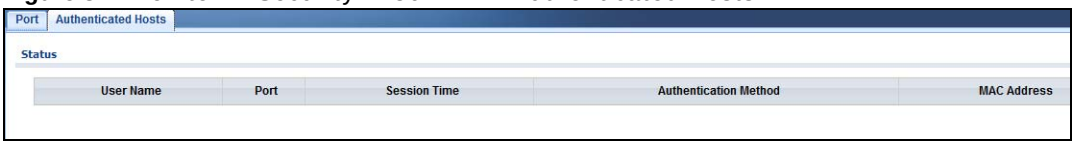
Table 49 Monitor > Security > 802.1x > Port

LABEL	DESCRIPTION
Port	This label shows the port you are viewing.
Status	This field displays status of the port.

15.3.2 Authenticated Hosts

Use this screen to view the Switch's 802.1x security authenticated host status. Click **Monitor > Security > 802.1X > Authenticated Hosts** to access this screen.

Figure 82 Monitor > Security > 802.1x > Authenticated Hosts



Each field is described in the following table.

Table 50 Monitor > Security > 802.1x > Authenticated Hosts

LABEL	DESCRIPTION
User Name	This field displays the name of a user.
Port	This label shows the port you are viewing.
Session Time	This label shows the session time.
Authentication Method	This label shows the authentication method.
MAC Address	This field displays the source MAC address in the binding.

16

Monitor: Management

16.1 Overview

This section provides information for **Management** in **Monitor**.

This chapter describes how to view management settings on the Switch.

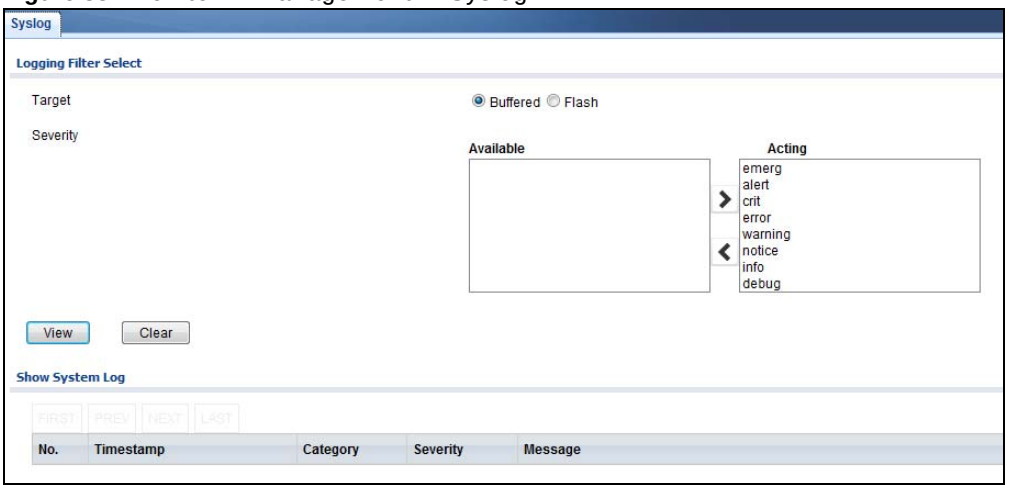
16.1.1 What You Can Do in this Chapter

- The **Syslog** screen (Section 16.2 on page 90) displays logging filter select and shows system log.
- The **Error Disable** screen (Section 16.3 on page 91) displays global and port.

16.2 Syslog

Use this screen to view Switch syslog management. Click **Monitor > Management > Syslog** to access this screen.

Figure 83 Monitor > Management > Syslog



Each field is described in the following table.

Table 51 Monitor > Management > Syslog

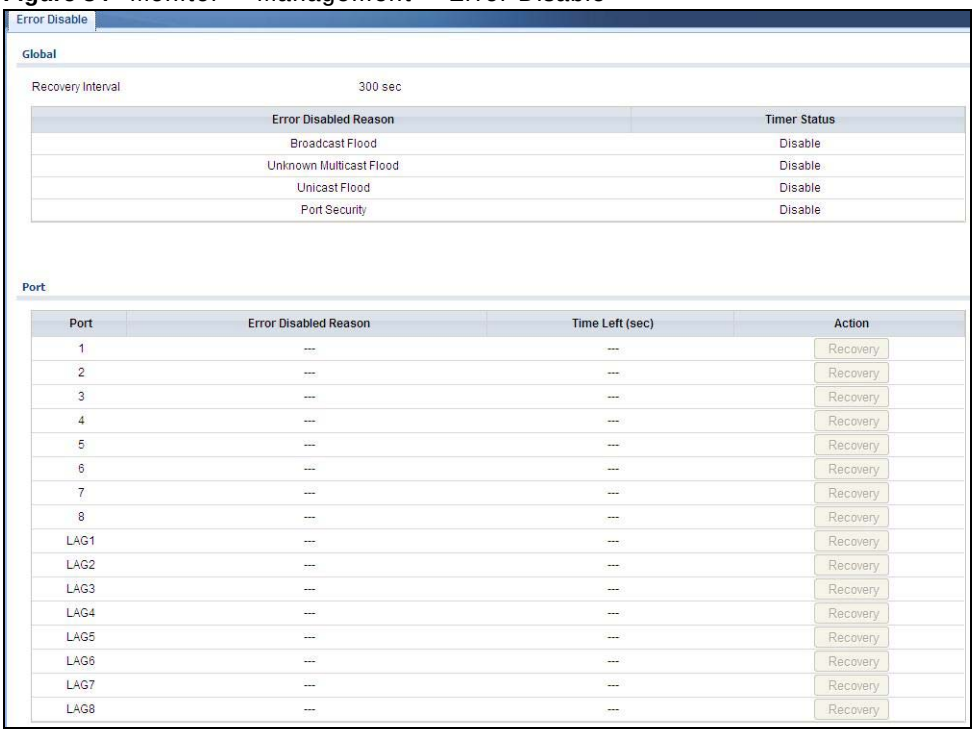
LABEL	DESCRIPTION
Logging Filter Select	
Target	Select **Buffered** or **Flash.** Buffered: Login saved to temporary memory. Flash: Login saved to permanent memory.
Severity	This field displays two options: Available and Acting. Severity type: crit, emerg, alert, error, warning, notice, info, and debug.
Available	Click **<** to move a severity type from the acting box to the available box. Click **>** to move a severity type to the acting box from the available box.
Acting	Click **<** to move a severity type from the acting box to the available box. Click **>** to move a severity type to the acting box from the available box.
>	Click **>** to move a severity type to the acting box from the available box.
<	Click **<** to move a severity type from the acting box to the available box.
View	Click **View** to display results**.**
Clear	Click **Clear** to clear results**.**
Show System Log	The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server
No.	This field displays the number you are viewing.
Timestamp	This field displays the timestamp.
Category	This field displays the category.
Severity	This field displays the severity.
Message	The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

16.3 Error Disable

This link takes you to a screen where you can view CPU protection and error disable recovery.

Use this screen to view Switch global and port error disable management. Click **Monitor > Management > Error Disable** to access this screen.

Figure 84 Monitor > Management > Error Disable



Each field is described in the following table.

Table 52 Monitor > Management > Error Disable

LABEL	DESCRIPTION
Global	
Recovery Interval	View the number of seconds (from 30 to 2592000) for the time interval of the recovery.
Error Disabled Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
Timer Status	Select this option to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Port	
Port	This field displays the port number.
Error Disabled Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
Time Left (sec)	This field displays the time left in seconds.
Action	This field displays the action.

17

Configuration: System

17.1 Overview

This section provides information for **System** in **Configuration.**

17.1.1 What You Can Do in this Chapter

- The IP screen (Section 17.2 on page 93) displays IPv4 and IPv6 settings.
- The Time screen (Section 17.3 on page 95) displays the system time and SNTP settings.
- The Information screen (Section 17.4 on page 96) displays the system information.

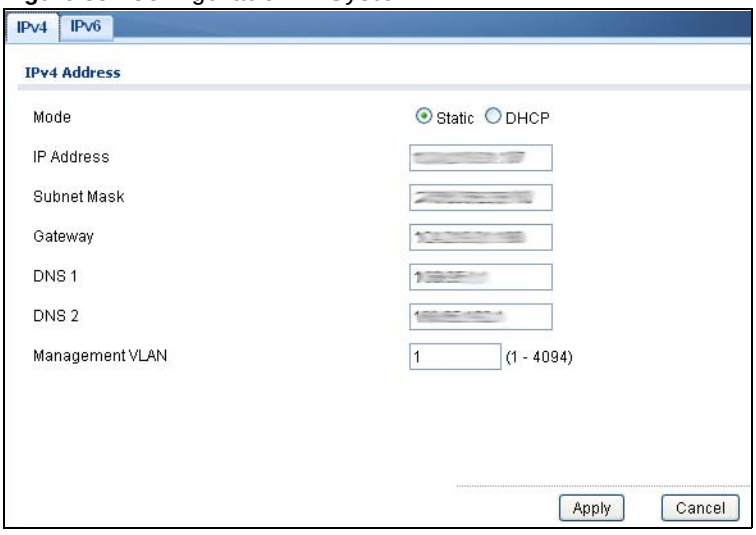
17.2 IP

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

17.2.1 The IPv4 Screen

Use this screen to view the IPv4 interface status and Switch's management IPv4 addresses. Click **Configuration > System > IP > IPv4** to open this screen.

Figure 85 Configuration > System > IP > IPv4



The following table describes the labels in this screen.

Table 53 Configuration > System > IP > IPv4

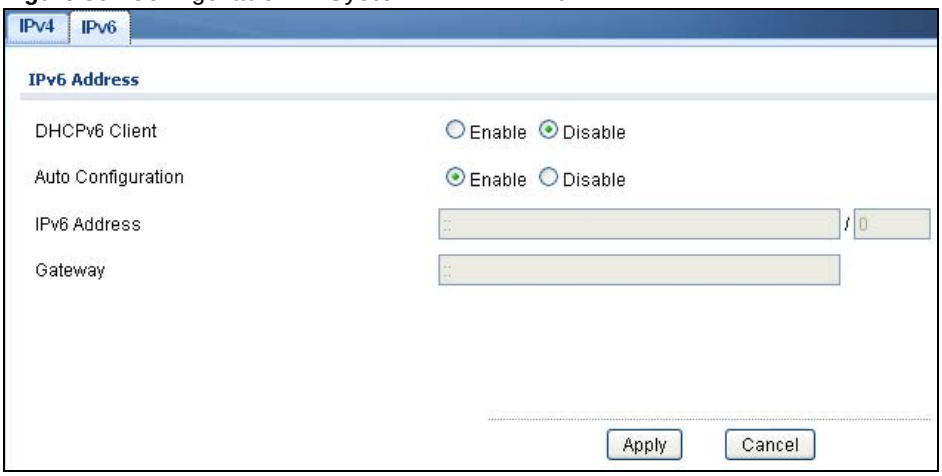
LABEL	DESCRIPTION
IPv4 Address	
Mode	Select Static to define the IPv4 network properties or DHCP to allow the device to define the properties.
IP Address	Enter the IP address of the Switch in the IP domain.
Subnet Mask	Enter the subnet mask of the Switch in the IP domain.
Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server 1	Enter the IP address for the primary domain name server. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa.
DNS Server 2	Enter the IP address for the secondary domain name server. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa.
Management VLAN	Enter the port number of the management VLAN.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

17.2.2 The IPv6 Screen

Use this screen to view the IPv6 interface status and Switch's management IPv6 addresses.

Click **Configuration** > **System** > **IP** > **IPv6** to open this screen.

Figure 86 Configuration > System > IP > IPv6



The following table describes the labels in this screen.

Table 54 Configuration > System > IP > IPv6

LABEL	DESCRIPTION
IPv6 Address	
DHCPv6 Client	Select **Enable** to allow the device to act as a DHCPv6 client or **Disable** to disallow it. This field displays the Switch's DHCP settings when it is acting as a DHCPv6 client.
Auto Configuration	Select **Enable** to allow the device to auto-configure the IPv6 properties or **Disable** to manually enter the properties.

Table 54 Configuration > System > IP > IPv6 (continued)

LABEL	DESCRIPTION
IPv6 Address	Enter the IPv6 address of the Switch in the IP domain.
Gateway	Enter the IPv6 address of the default outgoing gateway.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

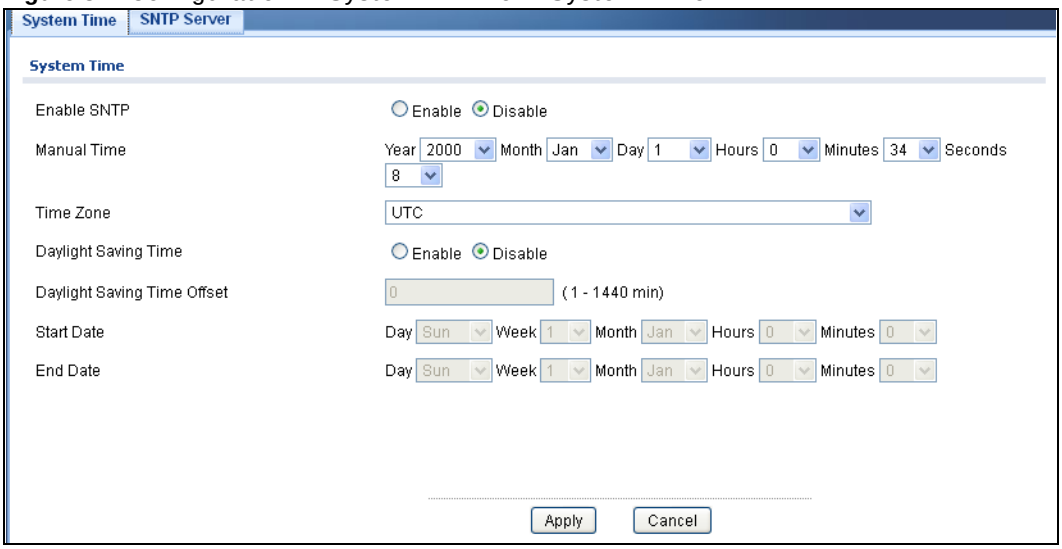
17.3 Time

The Time option is used to setup the system time and SNTP (Simple Network Time Protocol) server settings.

17.3.1 The System Time Screen

In the navigation panel, click **Configuration > System > Time** > **System Time** to display the screen as shown.

Figure 87 Configuration > System > Time > System Time



The following table describes the labels in this screen.

Table 55 Configuration > System > Time

LABEL	DESCRIPTION
System Time	
Enable SNTP	Select **Enable** to enable using a simple network time protocol (SNTP) server to manage the system time or **Disable** to manually manage system time.
Manual Time	Select the system date and time values from the dropdown lists.
Time Zone	Select the time zone from the dropdown list.
Daylight Saving Time	Select **Enable** to use Daylight Saving Time to offset the system time or **Disable** not adjust system time.

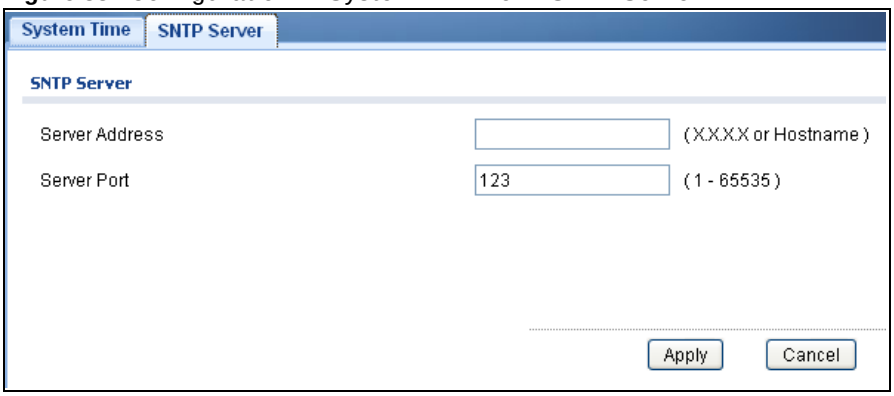
Table 55 Configuration > System > Time (continued)

LABEL	DESCRIPTION
Daylight Saving Time Offset	Enter the daylight saving time offset value in minutes.
Start Date	Select the start date of the daylight saving time period from the dropdown lists.
End Date	Select the end date of the daylight saving time period from the dropdown lists.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

17.3.2 The SNTP Server Screen

In the navigation panel, click **Configuration > System > Time > SNTP Server** to display the screen as shown.

Figure 88 Configuration > System > Time > SNTP Server



The following table describes the labels in this screen.

Table 56 Configuration > System > Time > SNTP Server

LABEL	DESCRIPTION
SNTP Server	
Server Address	Enter the address of the simple network time protocol (SNTP) server as an IP address (192.168.0.1) or as a URL (www.zyxel.com).
Server Port	Enter the port number of the SNTP server. The numeric value can be between 1 and 65535.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

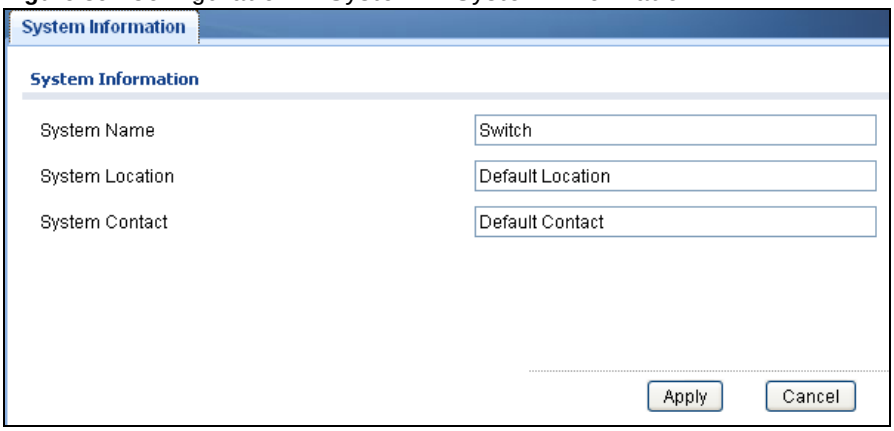
17.4 Information

The information option is used to set the following system information properties: system name, system location, and system contact information.

17.4.1 The System Information Screen

In the navigation panel, click **Configuration** > **System** > **System Information** to display the screen as shown. You can set the system name, system location, and system contact.

Figure 89 Configuration > System > System Information



The following table describes the labels in this screen.

Table 57 Configuration > System > System Information

LABEL	DESCRIPTION
System Information	
System Name	Enter the descriptive name of the Switch for identification purposes.
System Location	Enter the geographic location of the Switch for identification purposes.
System Contact	Enter the person in charge of the Switch for identification purposes.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

18

Configuration: Port

18.1 Overview

This section provides information for **Port** in **Configuration.**

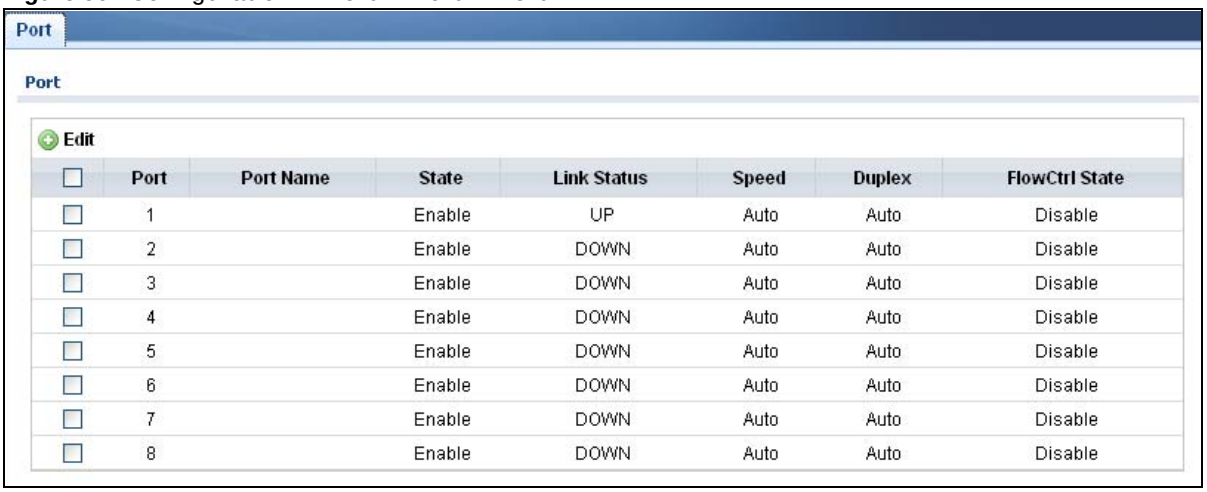
18.1.1 What You Can Do in this Chapter

- The Port screen (Section 18.2 on page 98) displays general port settings.
- The EEE screen (Section 18.3 on page 100) displays the port EEE settings.
- The PoE screen (Section 18.4 on page 101) displays the port PoE settings.
- The Bandwidth Management screen (Section 18.5 on page 105) displays the port ingress and egress settings.
- The Storm Control screen (Section 18.6 on page 107) displays the port storm control settings.

18.2 Port

Use this screen to view Switch port settings and select ports for configuration. Click **Configuration** > **Port** > **Port** > **Port** to open this screen.

Figure 90 Configuration > Port > Port > Port



The following table describes the labels in this screen.

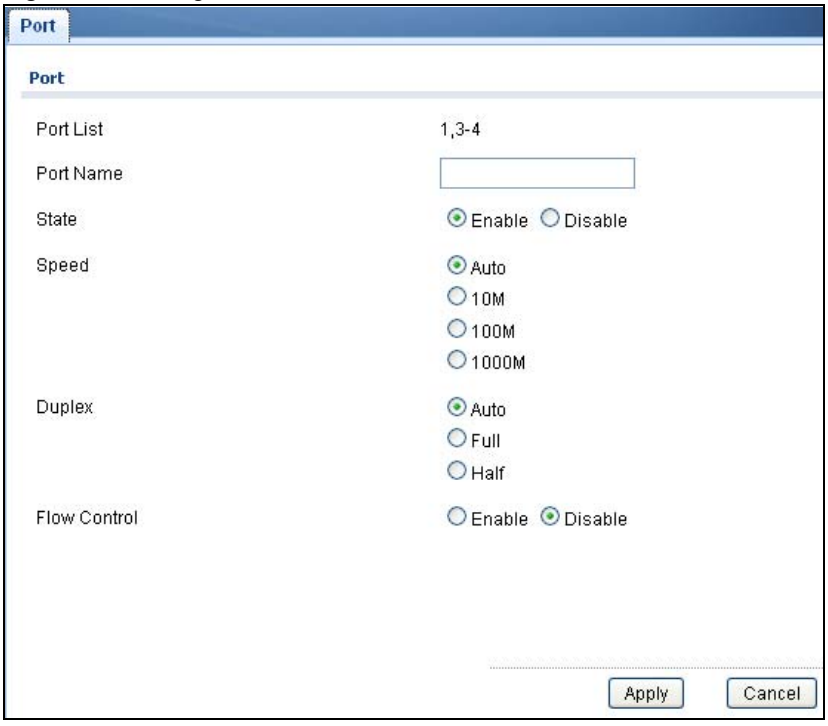
Table 58 Configuration > Port > Port > Port

LABEL	DESCRIPTION
Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index number.
Port Name	Displays a descriptive name that identifies this port. The length of the name can be up to 32 alpha-numerical characters. Note: Due to space limitations, the port name may be truncated in some web configurator screens.
State	Displays the port status as enabled or disabled.
Link Status	Displays the link status as up or down.
Speed	Displays the speed of the Ethernet connection on this port. The choices are **Auto**, **10M**, **100M**, and **1000M**.
Duplex	Displays the duplex mode of the Ethernet connection on this port. The choices are **auto**, **full**, or **half**.
FlowCtrl State	Displays the flow control state as enabled or disabled. A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.

18.2.1 The Port Edit Screen

Use this screen to configure Switch port settings. Click **Configuration** > **Port** > **Port** > **Edit** to open this screen.

Figure 91 Configuration > Port > Port > Edit



The following table describes the labels in this screen.

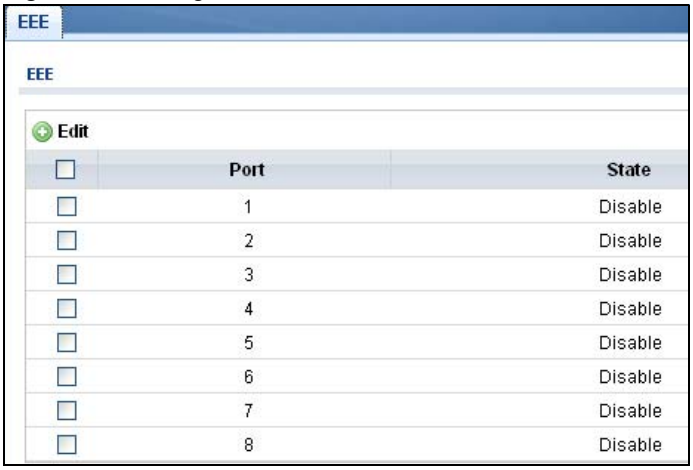
Table 59 Configuration > Port > Port > Edit

LABEL	DESCRIPTION
Port Edit	
Port List	Displays the list of port index numbers that are being configured.
Port Name	Enter a descriptive name that identifies this port. The length of the name can be up to 32 alpha-numerical characters. Note: Due to space limitations, the port name may be truncated in some web configurator screens.
State	Select **Enable** to enable the ports or **Disable** to disable them.
Speed	Select the speed of the Ethernet connection on this port. The choices are **Auto**, **10M**, **100M**, and **1000M**.
Duplex	Select the duplex mode of the Ethernet connection on this port. The choices are **Auto**, **Full**, or **Half**.
FlowCtrl State	Select **Enable** to allow the device to manage data flow or **Disable** to have no data flow management. A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

18.3 EEE

Use this screen to view Switch port Energy-Efficient Ethernet (EEE) settings and select ports for configuration. Click **Configuration** > **Port** > **EEE** > **EEE** to open this screen.

Figure 92 Configuration > Port > EEE > EEE



The following table describes the labels in this screen.

Table 60 Configuration > Port > EEE > EEE

LABEL	DESCRIPTION
EEE	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index number.
State	Displays the port status as enabled or disabled.

18.3.1 The EEE Edit Screen

Use this screen to configure Switch port EEE settings. Click **Configuration** > **Port** > **EEE** > **EEE** > **Edit** to open this screen.

Figure 93 Configuration > Port > EEE > EEE > Edit

The following table describes the labels in this screen.

Table 61 Configuration > Port > EEE > EEE > Edit

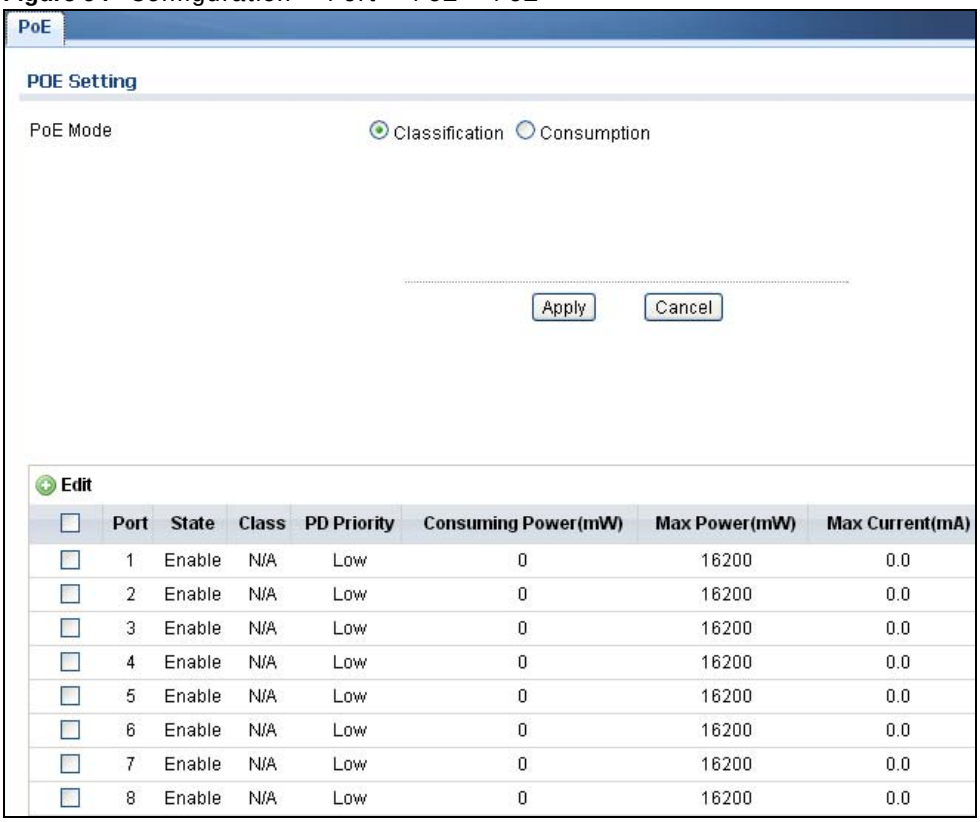
LABEL	DESCRIPTION
EEE	
Port List	Displays the list of port index numbers that are being configured.
State	Select **Enable** to designate the ports as EEE or **Disable** to not designate them as EEE.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

18.4 PoE

The Switch supports both the IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3at High Power over Ethernet (PoE) standards. The Switch is Power Sourcing Equipment (PSE) because it provides a source of power via its Ethernet ports, and each device that receives power through an Ethernet port is a Powered Device (PD).

Use this screen to view Switch port Power over Ethernet (PoE) settings and select ports for configuration. Click **Configuration** > **Port** > **PoE** > **PoE** to open this screen.

Figure 94 Configuration > Port > PoE > PoE



The following table describes the labels in this screen.

Table 62 Configuration > Port > PoE > PoE

LABEL	DESCRIPTION
PoE Setting	
PoE Mode	This field displays the power management mode used by the Switch, whether it is in **Classification** or **Consumption** mode.
Edit	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Port	Displays the port index number.
State	Displays which ports can receive power from the Switch. You can set this in the **Configuration** > **Port** > **PoE Edit** screen. • **Disable** - The PD connected to this port cannot get power. • **Enable** - The PD connected to this port can receive power.
Class	This shows the power classification of the PD. This is a number from 0 to 4, where each value represents a range of power (W) and current (mA) that the PD requires to function. The ranges are as follows. • **Class 0** - Default, 0.44 to 12.94 • **Class 1** - Optional, 0.44 to 3.84 • **Class 2** - Optional, 3.84 to 6.49 • **Class 3** - Optional, 6.49 to 12.95 • **Class 4** - Reserved (PSEs classify as Class 0) in a switch that supports IEEE 802.3af only. Optional, 12.95 to 25.50 in a switch that supports IEEE 802.3at.

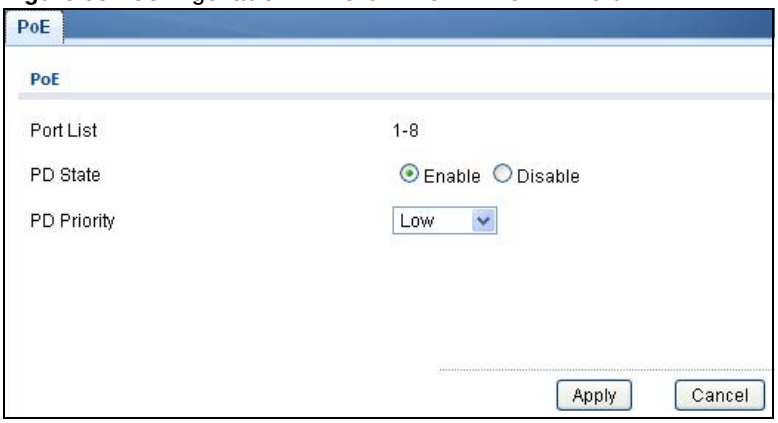
Table 62 Configuration > Port > PoE > PoE (continued)

LABEL	DESCRIPTION
PD Priority	When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority first. • **Critical** has the highest priority. • **High** has the Switch assign power to the port after all critical priority ports are served. • **Low** has the Switch assign power to the port after all critical and high priority ports are served
Consuming Power (mW)	Displays the current amount of power consumed by the PD from the Switch on this port.
Max Power (mW)	Displays the maximum amount of power the PD could use from the Switch on this port
Max Current (mA)	Displays the maximum amount of current drawn by the PD from the Switch on this port.

18.4.1 The PoE Edit Screen

Use this screen to configure Switch port PoE settings. Click **Configuration** > **Port** > **PoE** > **PoE** > **Edit** to open this screen.

Figure 95 Configuration > Port > PoE > PoE > Edit



The following table describes the labels in this screen.

Table 63 Configuration > Port > PoE > PoE> Edit

LABEL	DESCRIPTION
Port	
Port List	Displays the list of port index numbers that are being configured.
PD State	Select **Enable** to provide power to a PD connected to the port or **Disable** so the port cannot receive power from the Switch.

Table 63 Configuration > Port > PoE > PoE> Edit (continued)

LABEL	DESCRIPTION
PD Priority	This field is not available for the SFP or SFP+ ports. When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority. Select **Critical** to give the PD connected to this port the highest priority. Select **High** to set the Switch to assign the remaining power to the port after all critical priority ports are served. Select **Low** to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

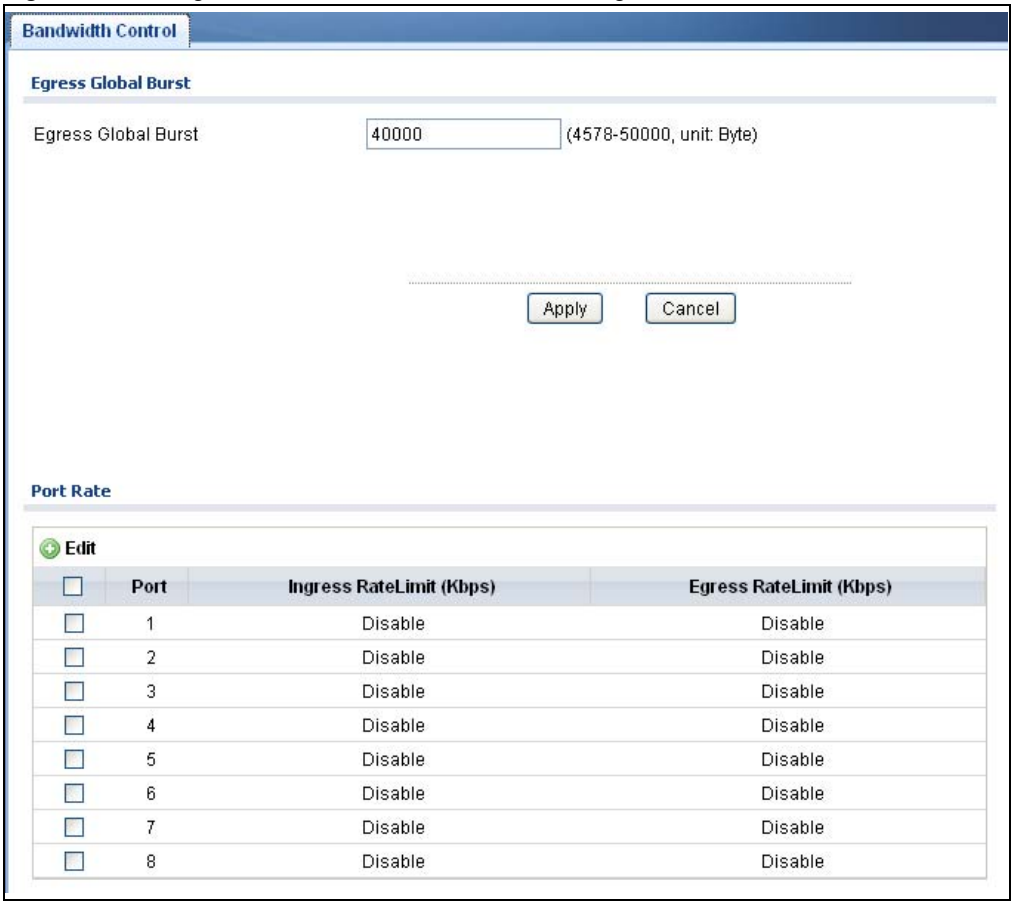
18.5 Bandwidth Management

Bandwidth management means defining a maximum allowable bandwidth for incoming and/or outgoing traffic flows on a port.

18.5.1 The Bandwidth Control Screen

Use this screen to view Egress Bandwidth Management settings and select ports for configuration. Click **Configuration** > **Port** > **Bandwidth Management** > **Bandwidth Control** to open this screen.

Figure 96 Configuration > Port > Bandwidth Management > Bandwidth Control



The following table describes the labels in this screen.

Table 64 Configuration > Port > Bandwidth Management > Bandwidth Control

LABEL	DESCRIPTION
Egress Global Burst	
Egress Global Burst	Specify the current egress burst size in bytes for all ports.
Port Rate	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.

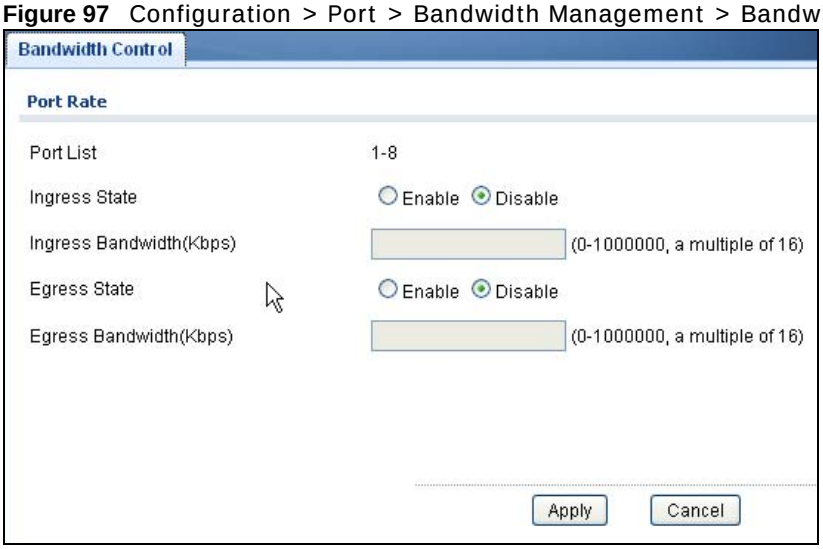
Table 64 Configuration > Port > Bandwidth Management > Bandwidth Control (continued)

LABEL	DESCRIPTION
Port	Displays the port index number.
Ingress Rate Limit (Kbps)	Displays the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Egress Rate Limit (Kbps)	Displays the maximum bandwidth allowed in kilobits per second (Kbps) for the outgoing traffic flow on a port.

18.5.2 The Port Rate Edit Screen

Use this screen to configure port rate Bandwidth Management settings. Click **Configuration** > **Port** > **Bandwidth Management** > **Bandwidth Control** > **Edit** to open this screen.

Figure 97 Configuration > Port > Bandwidth Management > Bandwidth Control > Edit



The following table describes the labels in this screen.

Table 65 Configuration > Port > Bandwidth Management > Bandwidth Control > Edit

LABEL	DESCRIPTION
Port Rate	
Port List	Displays the list of port index numbers that are being configured.
Ingress State	Select **Enable** to activate ingress peak rate limits on the port(s).
Ingress Bandwidth (Kbps)	Enter the maximum bandwidth allowed in kilobits per second (Kbps) for the outgoing traffic flow on a port.
Egress State	Select **Enable** to activate egress peak rate limits on the port(s).
Egress Bandwidth (Kbps)	Enter the maximum bandwidth allowed in kilobits per second (Kbps) for the outgoing traffic flow on a port.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

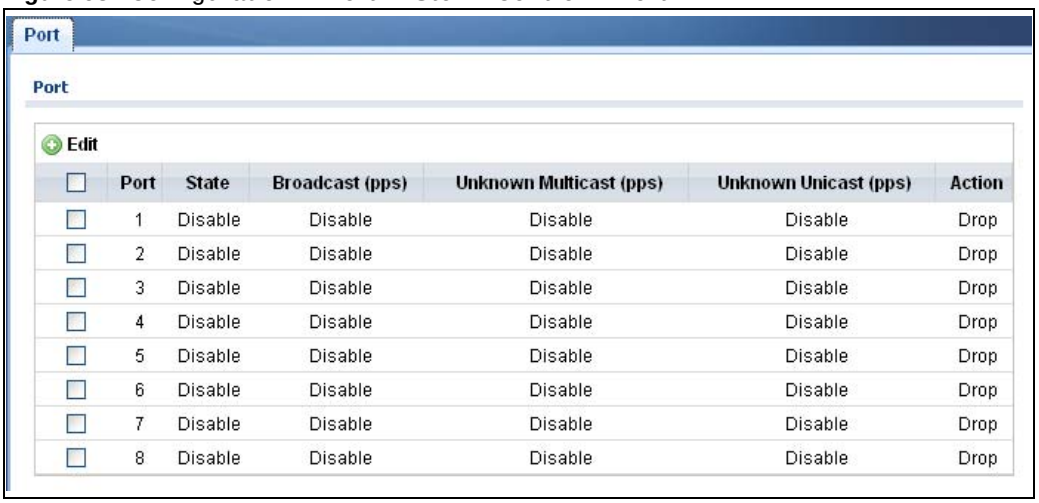
18.6 Storm Control

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

18.6.1 The Port Screen

Use this screen to view Storm Control settings for individual ports. Click **Configuration** > **Port** > **Storm Control** > **Port** to open this screen.

Figure 98 Configuration > Port > Storm Control > Port



The following table describes the labels in this screen.

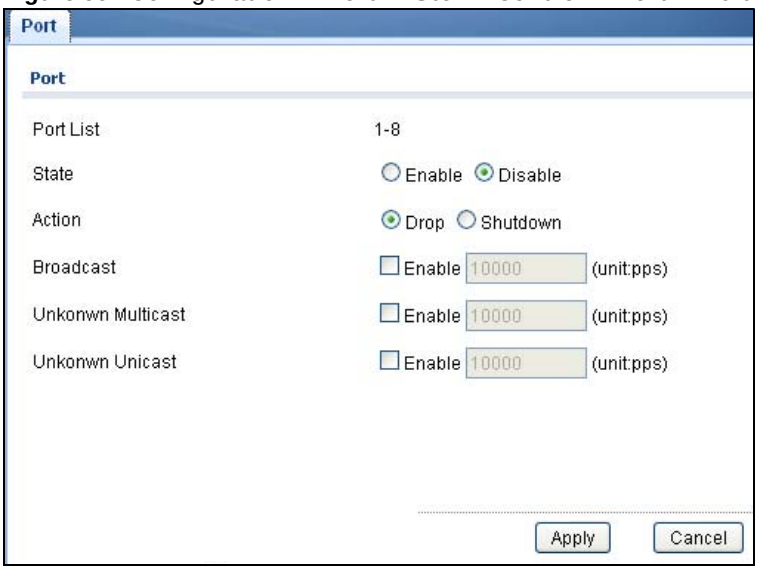
Table 66 Configuration > Port > Storm Control > Port

LABEL	DESCRIPTION
Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index number.
State	Displays whether the traffic storm control on the Switch is enabled or disabled.
Broadcast (pps)	Displays how many broadcast packets the port receives per second.
Unknown Multicast (pps)	Displays how many multicast packets the port receives per second.
Unknown Unicast (pps)	Displays how many unicast packets the port receives per second.
Action	Displays the action the device takes when a limit is reached. The following options are available: • **Drop** - drop the packet. • **Shutdown** - shutdown the connection.

18.6.2 The Port Edit Screen

Use this screen to configure Storm Control settings for individual ports. Click **Configuration** > **Port** > **Storm Control** > **Port** > **Edit** to open this screen.

Figure 99 Configuration > Port > Storm Control > Port > Edit



The following table describes the labels in this screen.

Table 67 Configuration > Port > Storm Control > Port > Edit

LABEL	DESCRIPTION
Port	
Port List	Displays the port list index number(s).
State	Select **Enable** to activate traffic storm control on the port(s).
Action	Determines the action the device takes when a limit is reached. The following options are available: • **Drop** - drop the packet when limit is reached. • **Shutdown** - shutdown the connection when a limit is reached.
Broadcast (pps)	Click the **Enable** checkbox to active the feature. Enter the maximum number of broadcast packets the port can receive per second.
Unknown Multicast (pps)	Click the **Enable** checkbox to active the feature. Enter the maximum number of multicast packets the port can receive per second.
Unknown Unicast (pps)	Click the **Enable** checkbox to active the feature. Enter the maximum number of unicast packets the port can receive per second.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19

Configuration: VLAN

19.1 Overview

This section provides information for **VLAN** in **Configuration.**

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user on the same network.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

19.1.1 What You Can Do in this Chapter

- The VLAN screen (Section 19.2 on page 110) displays VLAN, port, and VLAN port settings.
- The Guest VLAN screen (Section 19.3 on page 115) displays the global and port settings of the Switch.
- The Voice VLAN screen (Section 19.4 on page 117) displays the global, OUI, and port settings of the Switch.

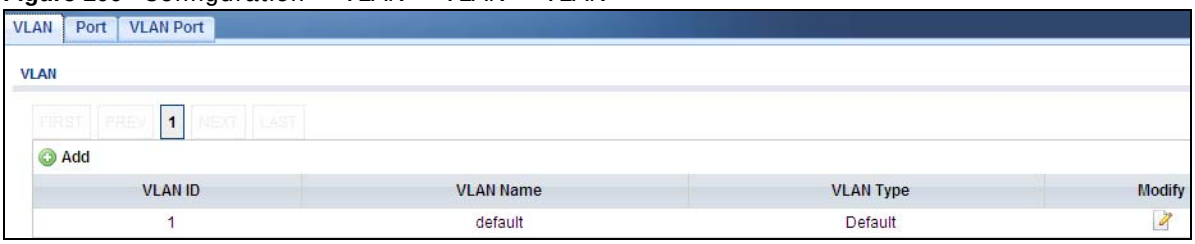
19.2 VLAN

Use this screen to view and configure VLAN settings.

19.2.1 The VLAN Screen

Use this screen to view VLAN settings. Click **Configuration** > **VLAN** > **VLAN** > **VLAN** to open this screen.

Figure 100 Configuration > VLAN > VLAN > VLAN



The following table describes the labels in this screen.

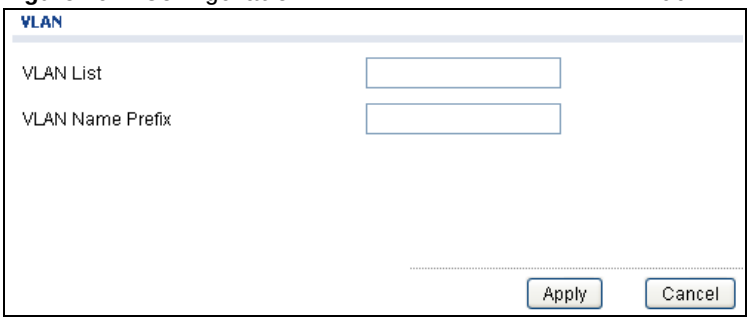
Table 68 Configuration > VLAN > VLAN > VLAN

LABEL	DESCRIPTION
Create VLAN	
Add	Click **Add** to create a new VLAN entry.
VLAN ID	Displays the VLAN ID number.
VLAN Name	Displays a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
VLAN Type	Displays **Default** or **Static**.
Modify	
Edit	Click **Edit** to make changes to the entry.

19.2.2 The VLAN Add Screen

Use this screen to add a VLAN. Click **Configuration** > **VLAN** > **VLAN** > **VLAN** > **Add** to open this screen.

Figure 101 Configuration > VLAN > VLAN > VLAN > Add



The following table describes the labels in this screen.

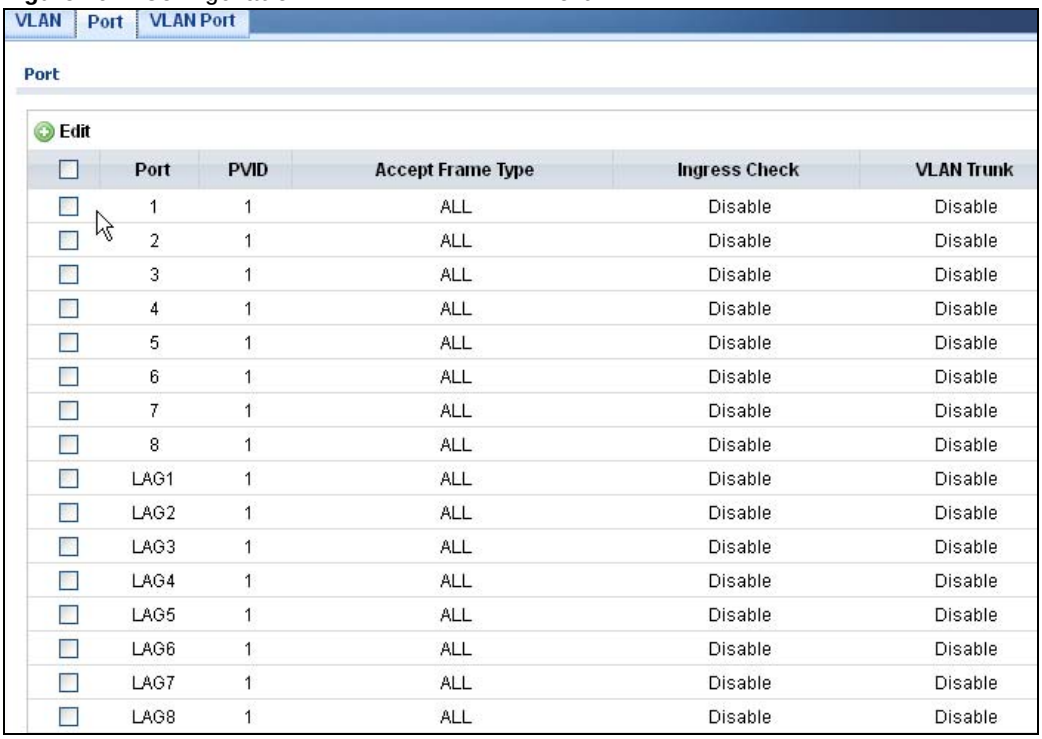
Table 69 Configuration > VLAN > VLAN > VLAN > Add

LABEL	DESCRIPTION
VLAN	
VLAN List	**Primary** private VLANs can associate with several (secondary) **Community** private VLANs and up to one (secondary) **Isolated** private VLAN. You only configure **VLAN Association List** for **Primary** private VLANs. Use a dash to associate consecutive VLANs and a comma (no spaces) to associate non-consecutive VLANs. For example, 51-53 includes 51, 52 and 53, but 51,53 does not include 52. Secondary private VLANs can only be associated with one primary private VLAN.
VLAN Name Prefix	Enter a prefix for the VLAN name.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19.2.3 The Port Screen

Use this screen to view port settings and select VLANs for configuration. Click **Configuration** > **VLAN** > **VLAN** > **Port** to open this screen.

Figure 102 Configuration > VLAN > VLAN > Port



The following table describes the labels in this screen.

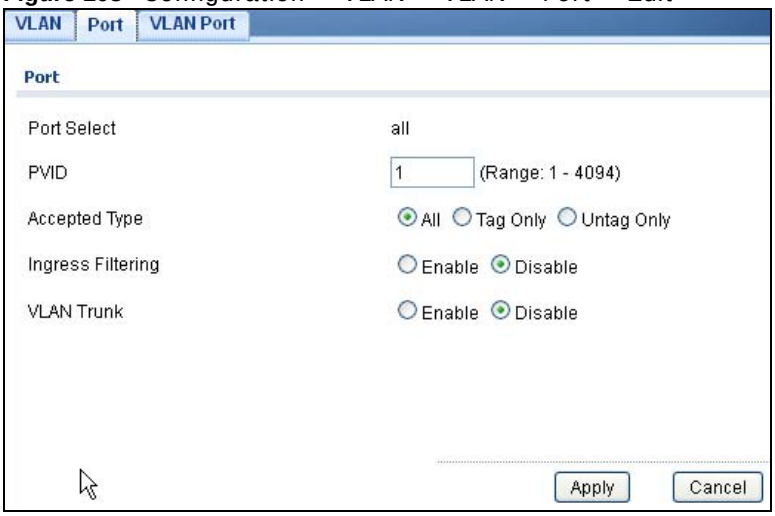
Table 70 Configuration > VLAN > VLAN > Port

LABEL	DESCRIPTION
Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index number.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Accept Frame Type	Specify the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set.
VLAN Trunk	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.

19.2.4 The Port Edit Screen

Use this screen to configure port settings. Click **Configuration** > **VLAN** > **VLAN** > **Port** > **Edit** to open this screen.

Figure 103 Configuration > VLAN > VLAN > Port > Edit



The following table describes the labels in this screen.

Table 71 Configuration > VLAN > VLAN > Port > Edit

LABEL	DESCRIPTION
Port	
Port Select	Displays the list of port index numbers that are being configured.
PVID	Enter a number between 1 and 4094 as the port VLAN ID.

Table 71 Configuration > VLAN > VLAN > Port > Edit (continued)

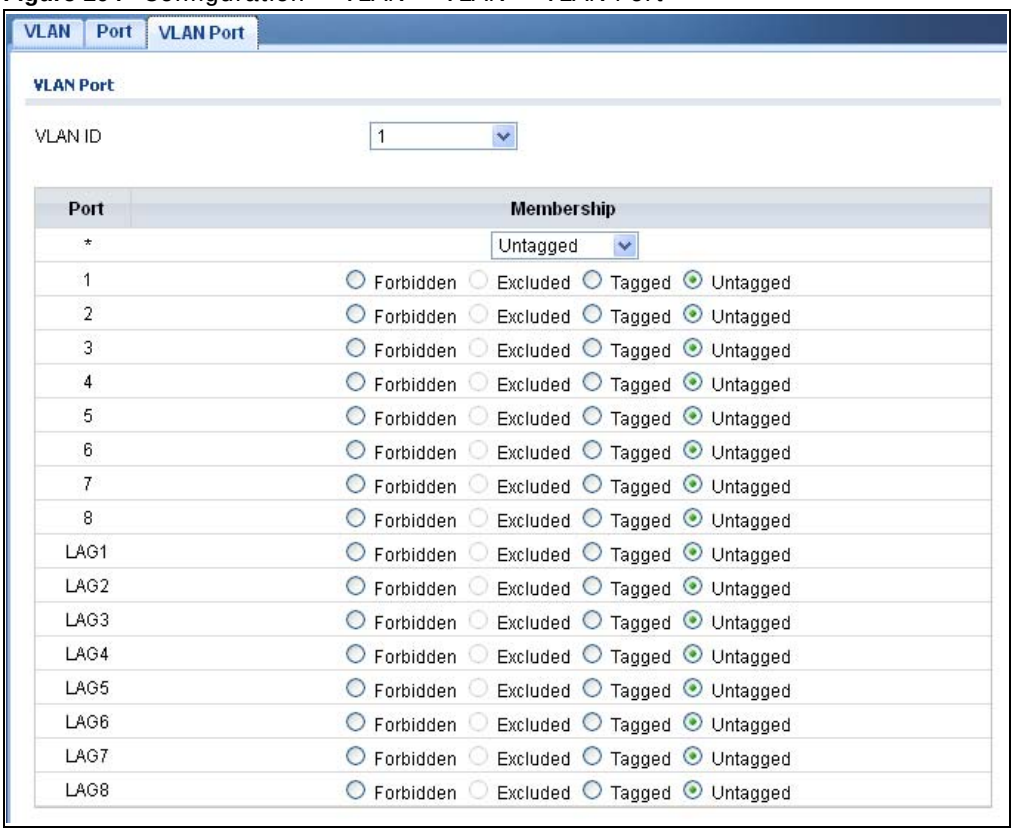
LABEL	DESCRIPTION
Accepted Type	Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped. Select **Untag Only** to accept only untagged frames on this port. All tagged frames will be dropped.
Ingress Filtering	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
VLAN Trunk	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19.2.5 The VLAN Port Screen

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port. Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports. Port-based VLANs are specific only to the Switch on which they were created.

Use this screen to view VLAN port settings. Click **Configuration** > **VLAN** > **VLAN** > **VLAN Port** to open this screen.

Figure 104 Configuration > VLAN > VLAN > VLAN Port



The following table describes the labels in this screen.

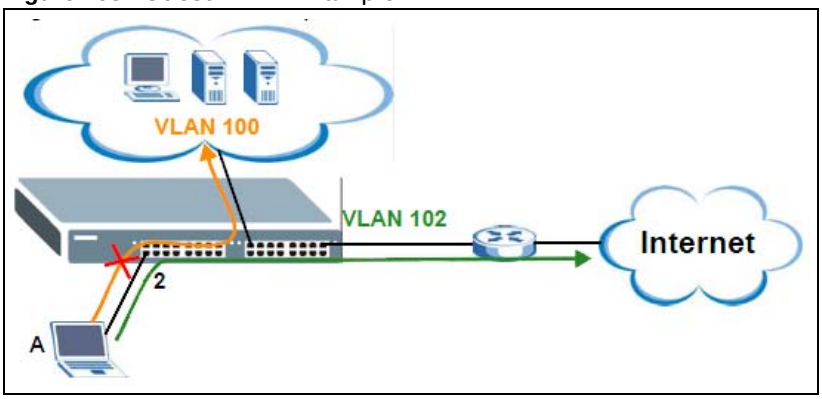
Table 72 Configuration > VLAN > VLAN > VLAN Port

LABEL	DESCRIPTION
VLAN Port	
VLAN ID	Select the ID of the VLAN you want to configure.
Port	Displays the port index value.
Membership	Select **Forbidden** if you want to prohibit the port from joining this VLAN group. Select **Excluded** to remove the port from the VLAN. Select **Tagged** to set the port TX tag status to tagged in the VLAN. Select **Untagged** to set the port TX tag status to untagged in the VLAN.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19.3 Guest VLAN

When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (102 in the example) on a port (2 in the example), the user (A in the example) that is not IEEE 802.1x capable or fails to enter the correct username and password can still access the port, but traffic from the user is forwarded to the guest VLAN. That is, unauthenticated users can have access to limited network resources in the same guest VLAN, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 105 Guest VLAN Example

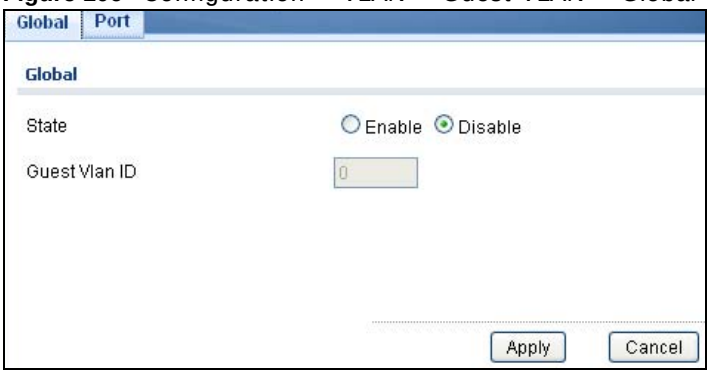


Use this screen to view and configure guest VLAN settings.

19.3.1 The Global Screen

Use this screen to configure the global Guest VLAN settings. Click **Configuration** > **VLAN** > **Guest VLAN** to open this screen.

Figure 106 Configuration > VLAN > Guest VLAN > Global



The following table describes the labels in this screen.

Table 73 Configuration > VLAN > Guest VLAN > Global

LABEL	DESCRIPTION
Global	
State	Select to enable the global Guest VLAN feature.

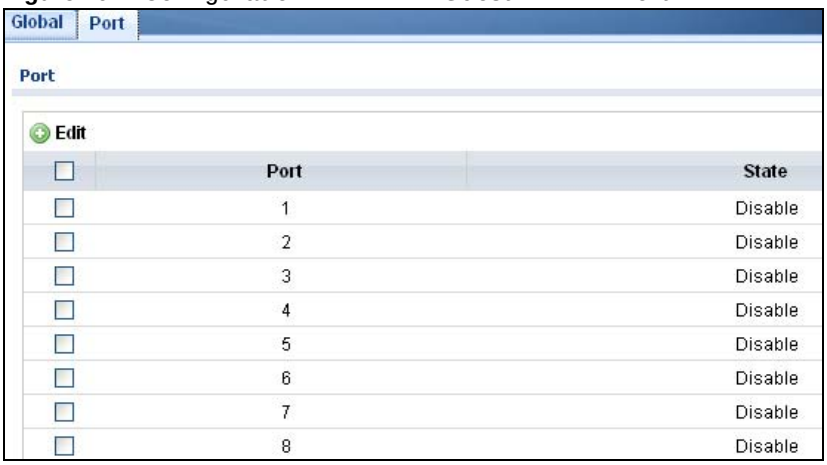
Table 73 Configuration > VLAN > Guest VLAN > Global (continued)

LABEL	DESCRIPTION
Guest VLAN ID	Enter the global guest VLAN ID.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19.3.2 The Port Screen

Use this screen to view the Guest VLAN port settings and select VLAN port(s) for configuration. Click **Configuration** > **VLAN** > **Guest VLAN** > **Port** to open this screen.

Figure 107 Configuration > VLAN > Guest VLAN > Port



The following table describes the labels in this screen.

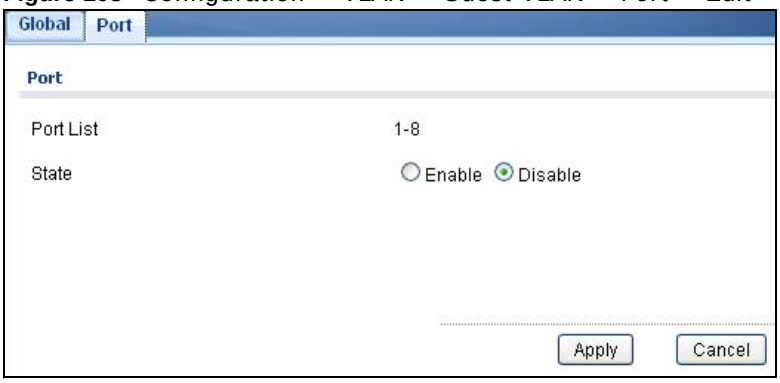
Table 74 Configuration > VLAN > Guest VLAN > Port

LABEL	DESCRIPTION
Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index number.
State	Display the state of the selected port.

19.3.3 The Port Edit Screen

Use this screen to configure the guest VLAN port EEE settings. Click **Configuration** > **VLAN** > **Guest VLAN** > **Port** > **Edit** to open this screen.

Figure 108 Configuration > VLAN > Guest VLAN > Port > Edit



The following table describes the labels in this screen.

Table 75 Configuration > VLAN > Guest VLAN > Port > Edit

LABEL	DESCRIPTION
Port	
Port List	Displays the list of port index numbers that are being configured.
State	Enable/Disable the guest VLAN feature.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19.4 Voice VLAN

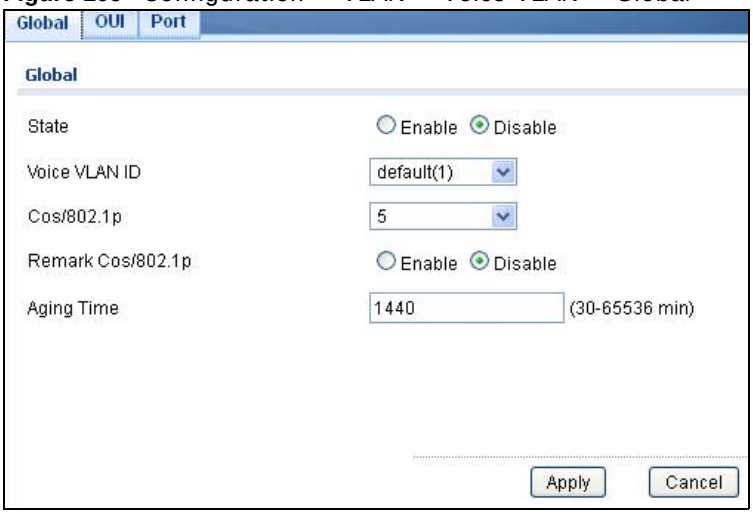
The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Use this screen to view and configure voice VLAN settings.

19.4.1 The Global Screen

Use this screen to configure the global Voice VLAN settings. Click **Configuration** > **VLAN** > **Voice VLAN** > **Global** to open this screen.

Figure 109 Configuration > VLAN > Voice VLAN > Global



The following table describes the labels in this screen.

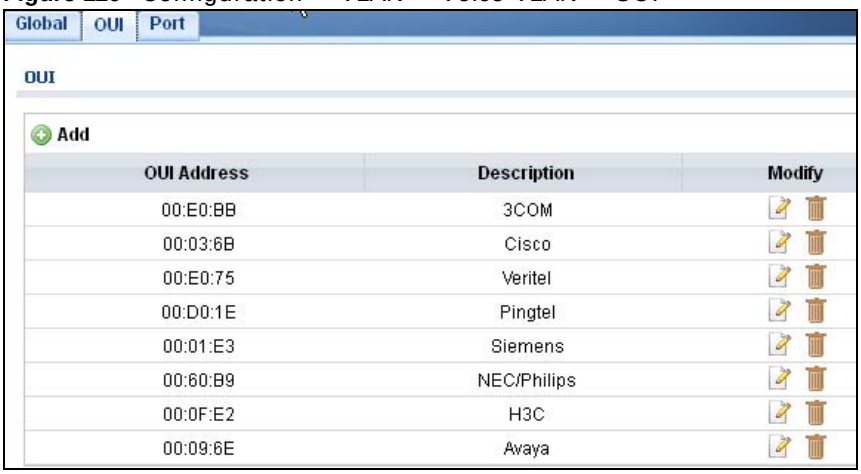
Table 76 Configuration > VLAN > Voice VLAN > Global

LABEL	DESCRIPTION
Global	
State	Select **Enable** to activate the global voice VLAN feature.
Voice VLAN ID	Enter the global voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
Cos/802.1p	Displays the 802.1p packet priority field.
Remark Cos/ 802.1p	Select to **Enable** the priority remark function for cos/802.1p.
Aging Time	Enter the voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19.4.2 The OUI Screen

Use this screen to view the OUI settings. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process. Click **Configuration** > **VLAN** > **Voice VLAN** > **OUI** to open this screen.

Figure 110 Configuration > VLAN > Voice VLAN > OUI



The following table describes the labels in this screen.

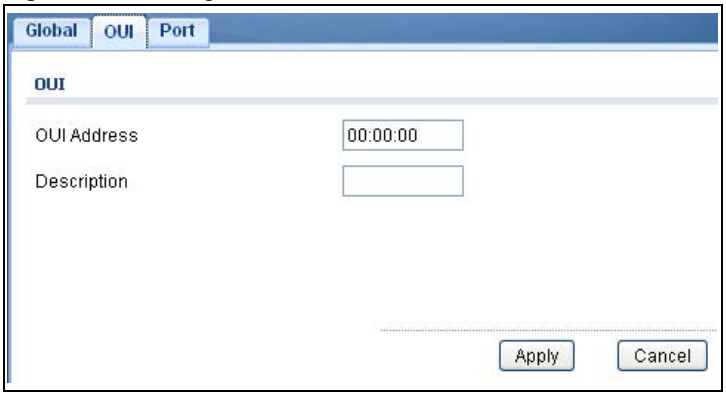
Table 77 Configuration > VLAN > Voice VLAN > OUI

LABEL	DESCRIPTION
OUI	
Add	Click **Add** to create a new OUI entry.
OUI Address	Displays an OUI address. A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	Displays a description of the OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

19.4.3 The OUI Add/Edit Screen

Use this screen to add/edit an OUI address. Click **Configuration** > **VLAN** > **Voice VLAN** > **OUI** > **Add/Edit** to open this screen.

Figure 111 Configuration > VLAN > Voice VLAN > OUI > Add/Edit



The following table describes the labels in this screen.

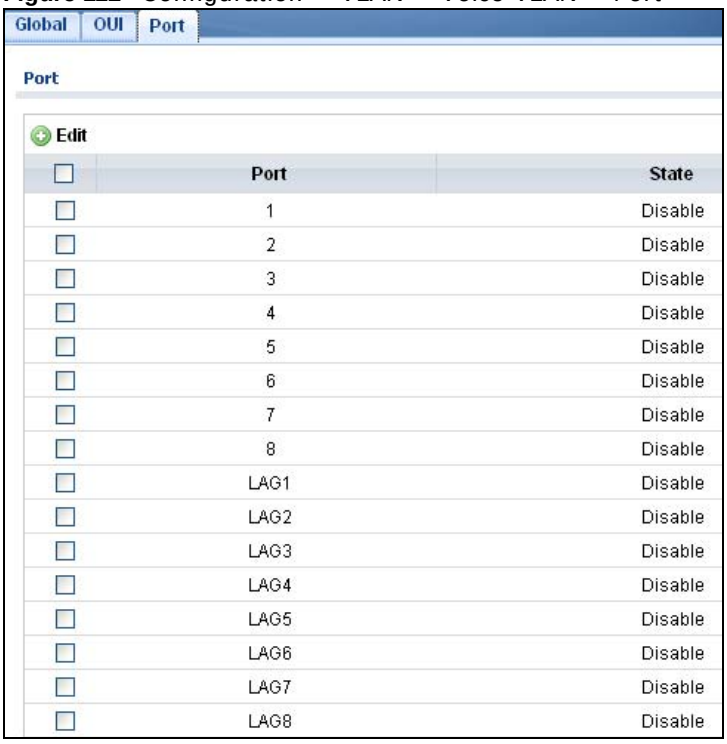
Table 78 Configuration > VLAN > Voice VLAN > OUI > Add/Edit

LABEL	DESCRIPTION
OUI	
OUI Address	Enter an OUI address. A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	Enter a description of the OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

19.4.4 The Port Screen

Use this screen to view the Voice VLAN port settings and select a port for configuration. Click **Configuration** > **VLAN** > **Voice VLAN** > **Port** to open this screen.

Figure 112 Configuration > VLAN > Voice VLAN > Port



The following table describes the labels in this screen.

Table 79 Configuration > VLAN > Voice VLAN > Port

LABEL	DESCRIPTION
Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.

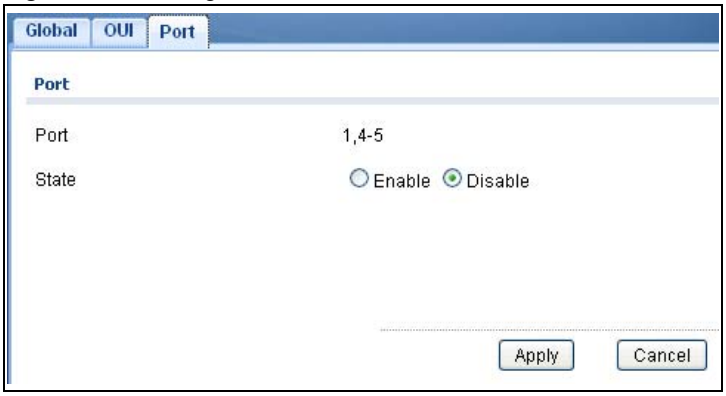
Table 79 Configuration > VLAN > Voice VLAN > Port (continued)

LABEL	DESCRIPTION
Port	Displays the port index value.
State	Displays the Voice VLAN port security mode state. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: • **Enabled**: Enable Voice VLAN security mode operation. • **Disabled**: Disable Voice VLAN security mode operation.

19.4.5 The Port Edit Screen

Use this screen to edit the port(s) security state. Click **Configuration** > **VLAN** > **Voice VLAN** > **Port** > **Add/Edit** to open this screen.

Figure 113 Configuration > VLAN > Voice VLAN > Port > Add/Edit



The following table describes the labels in this screen.

Table 80 Configuration > VLAN > Voice VLAN > Port > Add/Edit

LABEL	DESCRIPTION
Port	
Port	Displays the port(s) index value.
State	Select the Voice VLAN port security mode state. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: • **Enabled**: Enable Voice VLAN security mode operation. • **Disabled**: Disable Voice VLAN security mode operation.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

20

Configuration: MAC Table

20.1 Overview

This section provides information for **MAC Table** in **Configuration**.

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's **MAC Table**. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

20.1.1 What You Can Do in this Chapter

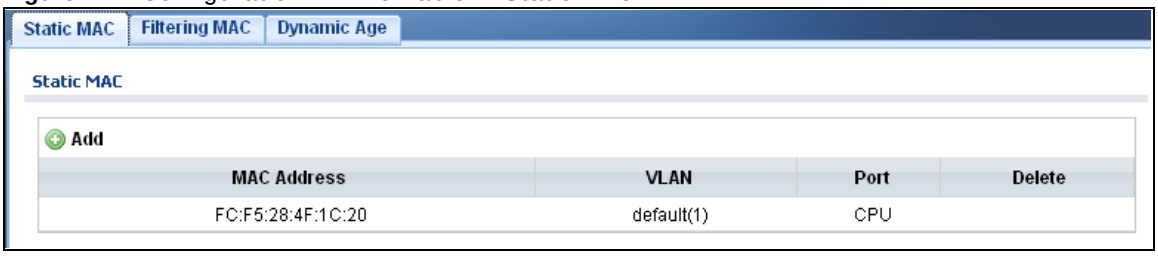
The MAC Table screen (Section 20.2 on page 122) displays Static MAC, Filtering MAC, and Dynamic MAC settings.

20.2 MAC Table

20.2.1 The Static MAC Screen

Use this screen to view Static MAC addresses settings. Click **Configuration > MAC Table** > **Static MAC** to open this screen.

Figure 114 Configuration > MAC Table > Static MAC



The following table describes the labels in this screen.

Table 81 Configuration > MAC Table > Static MAC

LABEL	DESCRIPTION
Static MAC	
Add	Click **Add** to create a new **Static MAC** entry.
MAC Address	Displays the object MAC address from which this incoming frame came.
VLAN	Displays the VLAN group to which this frame belongs.

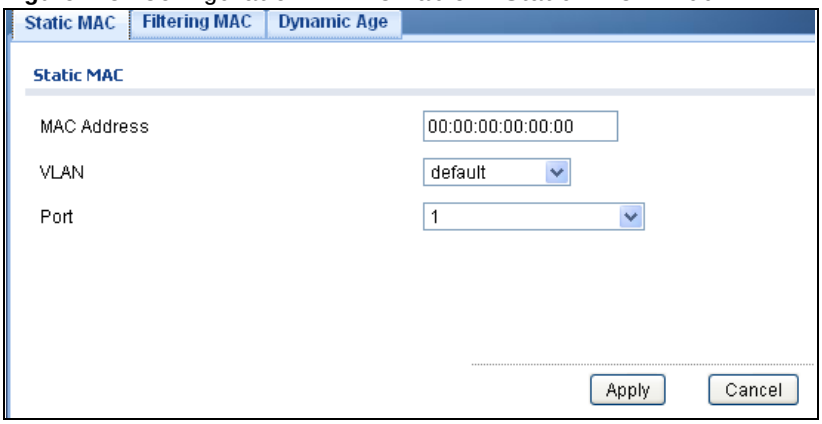
Table 81 Configuration > MAC Table > Static MAC (continued)

LABEL	DESCRIPTION
Port	Displays the port from which the above MAC address was learned.
Delete	Click **Delete** to remove the MAC address.

20.2.2 The Static MAC Add Screen

Use this screen to add new Static MAC addresses. Click **Configuration > MAC Table** > **Static MAC > Add** to open this screen.

Figure 115 Configuration > MAC Table > Static MAC > Add



The following table describes the labels in this screen.

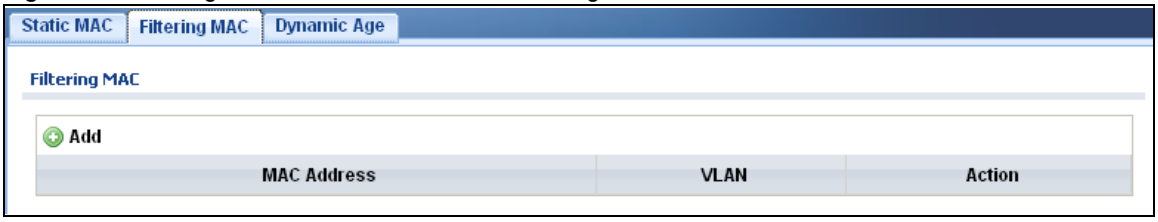
Table 82 Configuration > MAC Table > Static MAC > Add

LABEL	DESCRIPTION
Static MAC	
MAC Address	Enter the object MAC address.
VLAN	Select the VLAN group which to associate the MAC address.
Port	Select the port which to associate the above MAC address.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

20.2.3 The Filtering MAC Screen

Use this screen to view Filtering MAC addresses. Click **Configuration > MAC Table** > **Filtering MAC** to open this screen.

Figure 116 Configuration > MAC Table > Filtering MAC



The following table describes the labels in this screen.

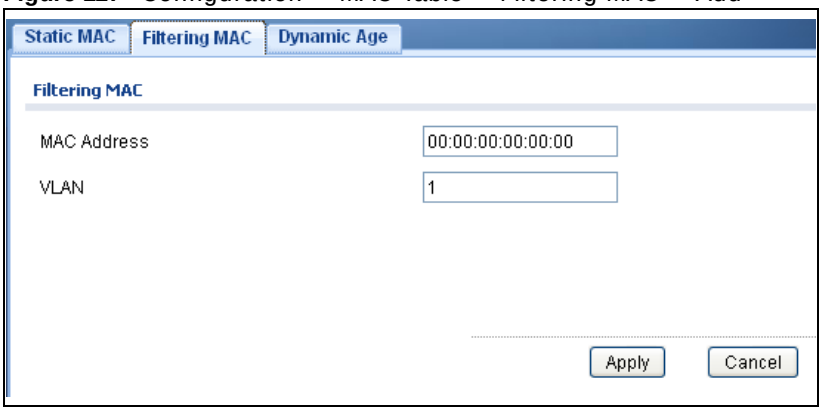
Table 83 Configuration > MAC Table > Filtering MAC

LABEL	DESCRIPTION
MAC Filtering	
Add	Click **Add** to create a new **Filtering MAC** entry.
MAC Address	Displays the filtering object MAC address from which this incoming frame came.
VLAN	Displays the VLAN group to which this frame belongs.
Action	
Delete	Click **Delete** to remove the entry.

20.2.4 The Filtering MAC Add Screen

Use this screen to add new Filtering MAC addresses. Click **Configuration > MAC Table > Filtering MAC** > **Add** to open this screen.

Figure 117 Configuration > MAC Table > Filtering MAC > Add



The following table describes the labels in this screen.

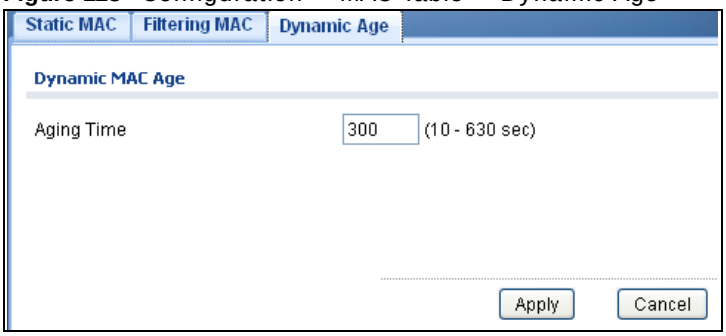
Table 84 Configuration > MAC Table > Filtering MAC > Add

LABEL	DESCRIPTION
Filtering MAC	
MAC Address	Enter the MAC address of the device.
VLAN	Select the VLAN group to associate the filtering object MAC address.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

20.2.5 The Dynamic Age Screen

Use this screen to enter the Dynamic MAC Age. The dynamic MAC age is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned). Click **Configuration > MAC Table > Dynamic Age** to open this screen.

Figure 118 Configuration > MAC Table > Dynamic Age



The following table describes the labels in this screen.

Table 85 Configuration > Dynamic Age

LABEL	DESCRIPTION
Dynamic MAC Age	
Aging Time	Enter the aging time of the MAC address. The value can be between 10 and 630 seconds.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

21

Configuration: Link Aggregation

21.1 Overview

This section provides information for **Link Aggregation** in **Configuration.**

This chapter shows you how to logically aggregate physical links to form one logical, higher bandwidth link.

21.1.1 What You Can Do in this Chapter

The Link Aggregation screen (Section 21.2 on page 126) displays global, LAG management, LAG port, and LACP port settings.

21.2 Link Aggregation

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

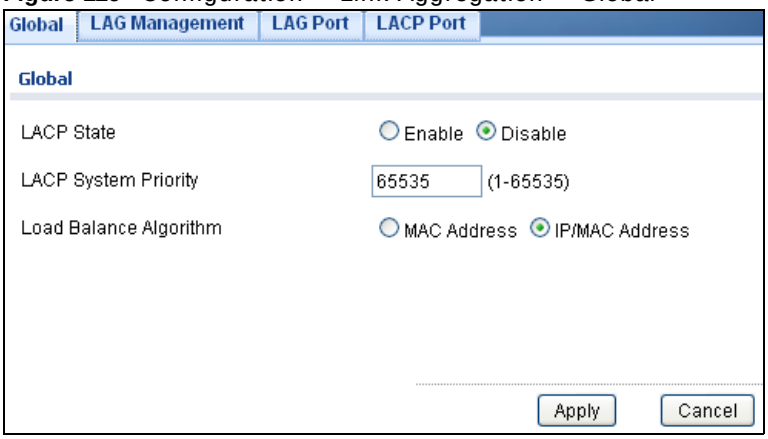
The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

21.2.1 The Global Screen

Use this screen to configure global Link Aggregation settings. Click **Configuration** > **Link Aggregation** > **Global** to open this screen.

Figure 119 Configuration > Link Aggregation > Global



The following table describes the labels in this screen.

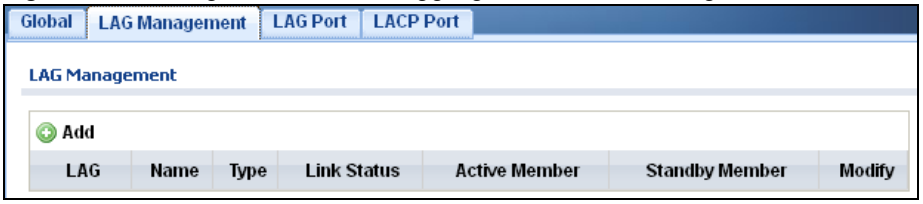
Table 86 Configuration > Link Aggregation > Global

LABEL	DESCRIPTION
Global	
LACP State	Select **Enable** to activate the link aggregation control protocol.
LACP System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Load Balance Algorithm	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **src-dst-IP + src-dst-mac** distribution type. If the Switch is behind a router, the packet's destination or source MAC address will be changed. In this case, set the Switch to distribute traffic based on its IP address to make sure port trunking can work properly. Select **src-dst-mac** to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select **src-dst-ip + src-dst-mac** to distribute traffic based on a combination of the packet's source and destination IP addresses.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

21.2.2 The LAG Management Screen

Use this screen to view LAG management settings. Click **Configuration** > **Link Aggregation** > **LAG Management** to open this screen.

Figure 120 Configuration > Link Aggregation > LAG Management



The following table describes the labels in this screen.

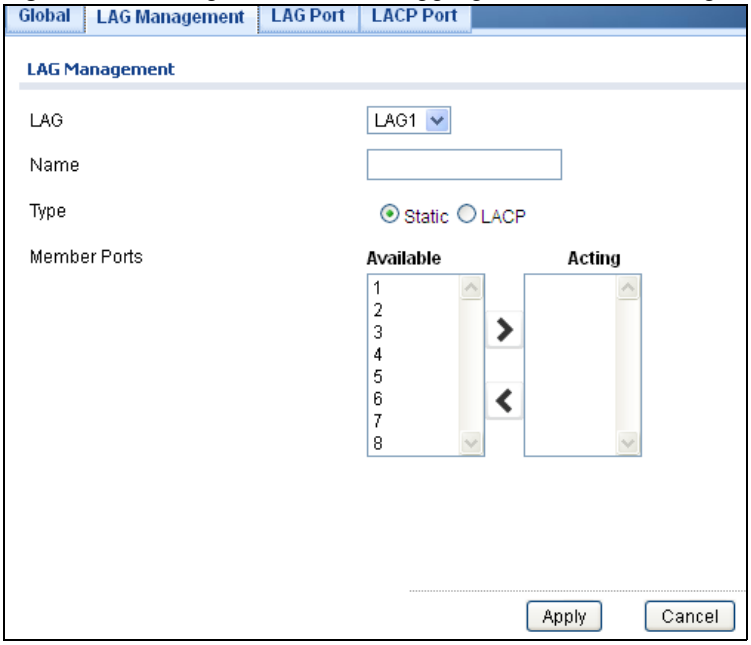
Table 87 Configuration > Link Aggregation > LAG Management

LABEL	DESCRIPTION
LAG Management	
Add	Click **Add** to create a new **LAG Management** entry.
LAG	Displays the link aggregation group (LAG), that is, one logical link containing multiple ports.
Name	Displays the name of the link aggregation group.
Type	This field displays how these ports were added to the trunk group. It displays: **Static** - if the ports are configured as static members of a trunk group. **LACP** - if the ports are configured to join a trunk group via LACP.
Link Status	Displays link status as either **Link up** or **Link down**.
Active Member	Displays if this member is an active member of a trunk.
Standby Member	Displays if this member is an standby member of a trunk.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

21.2.3 The LAG Add Screen

Use this screen to add a LAG. Click **Configuration** > **Link Aggregation** > **LAG Management** > **Add** to open this screen.

Figure 121 Configuration > Link Aggregation > LAG Management > Add



The following table describes the labels in this screen.

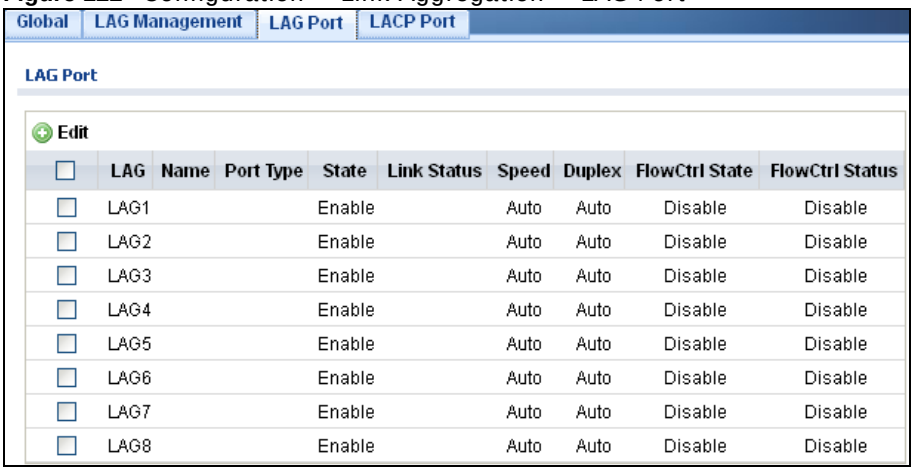
Table 88 Configuration > Link Aggregation > LAG Management > Add

LABEL	DESCRIPTION
LAG Management	
LAG	Select the link aggregation group (LAG).
Name	Enter the name of this entry.
Type	Select **Static** or **LACP**.
Member Ports	Select the member ports to be part of the LAG.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

21.2.4 The LAG Port Screen

Use this screen to view LAG port settings. Click **Configuration** > **Link Aggregation** > **LAG Port** to open this screen.

Figure 122 Configuration > Link Aggregation > LAG Port



The following table describes the labels in this screen.

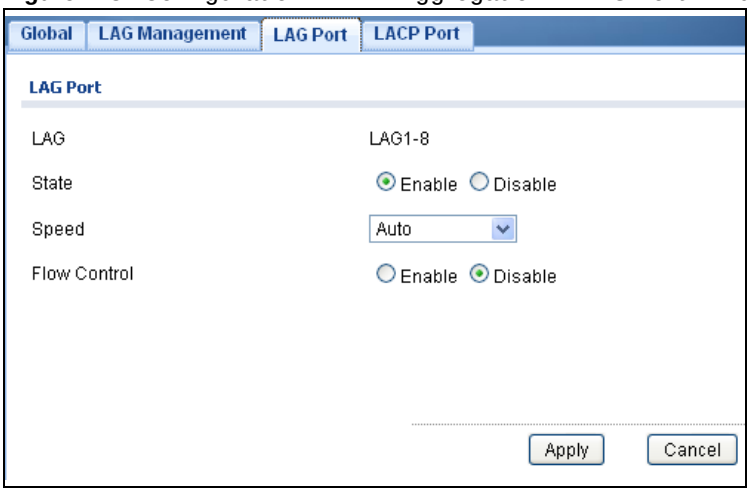
Table 89 Configuration > Link Aggregation > LAG Port

LABEL	DESCRIPTION
LAG Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
LAG	Displays the LAG index value.
Name	Displays the LAG name.
Port Type	Displays the port type.
State	Displays the state as **Enable**/**Disable**.
Speed	Displays the speed value as **Auto**, **Auto-10M**, **Auto-100M**, **Auto-1000M**, **Auto-10/100M**, **10M**, **100M**, or **1000M**.
Duplex	Displays the duplex value as **Full**, **Half**, or **Auto**.
FlowCtrl State	Displays whether flow control is **Enable**/**Disable**.
FlowCtrl Status	Displays whether flow control is in use (**Enable**) or not (**Disable**).

21.2.5 The LAG Port Edit Screen

Use this screen to edit a LAG port. Click **Configuration** > **Link Aggregation** > **LAG Port** > **Edit** to open this screen.

Figure 123 Configuration > Link Aggregation > LAG Port > Edit



The following table describes the labels in this screen.

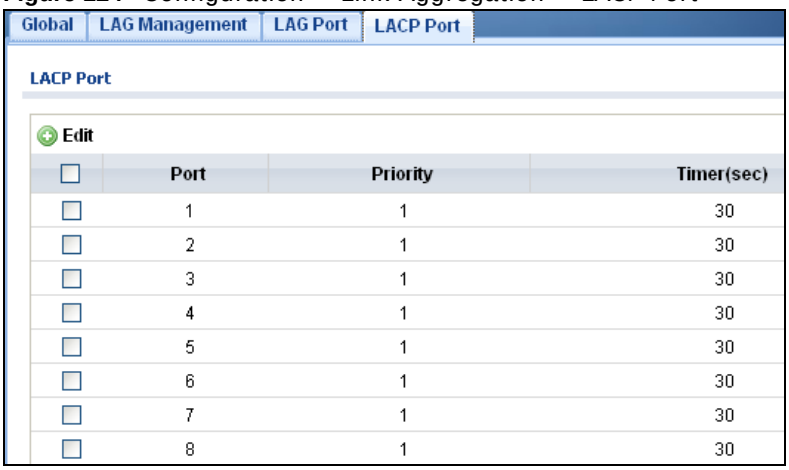
Table 90 Configuration > Link Aggregation > LAG Port > Edit

LABEL	DESCRIPTION
LAG Port Edit	
LAG	Displays the LAG index values.
State	Select the state to be **Enable** or **Disable**.
Speed	Displays the speed value as **Auto**, **Auto-10M**, **Auto-100M**, **Auto-1000M**, **Auto-10/100M**, **10M**, **100M**, or **1000M**.
Flow Control	Select **Enable** to use the flow control feature.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

21.2.6 The LACP Port Screen

Use this screen to view LACP Port settings. Click **Configuration** > **Link Aggregation** > **LACP Port** to open this screen.

Figure 124 Configuration > Link Aggregation > LACP Port



The following table describes the labels in this screen.

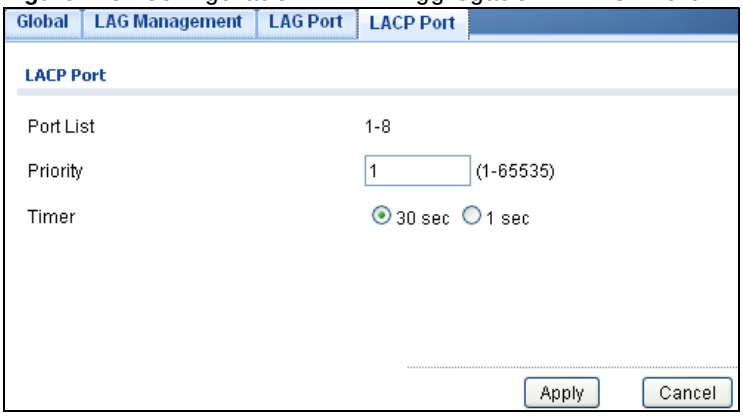
Table 91 Configuration > Link Aggregation > LACP Port

LABEL	DESCRIPTION
LACP Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index number.
Priority	Displays the priority value.
Timer (sec)	Displays the Timer value in seconds. Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible.

21.2.7 The LACP Port Edit Screen

Use this screen to edit a LACP Port. Click **Configuration** > **Link Aggregation** > **LACP Port** > **Edit** to open this screen.

Figure 125 Configuration > Link Aggregation > LACP Port > Edit



The following table describes the labels in this screen.

Table 92 Configuration > Link Aggregation > LACP Port > Edit

LABEL	DESCRIPTION
LACP Port	
Port List	Displays the list of port index numbers to be configured.
Priority	Enter a value for the port priority. The number can be between 1 and 65,535.
Timer	Select a timer value of either 1 second or 30 seconds.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

22

Configuration: Loop Guard

22.1 Overview

This section provides information for **Loop Guard** in **Configuration.**

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

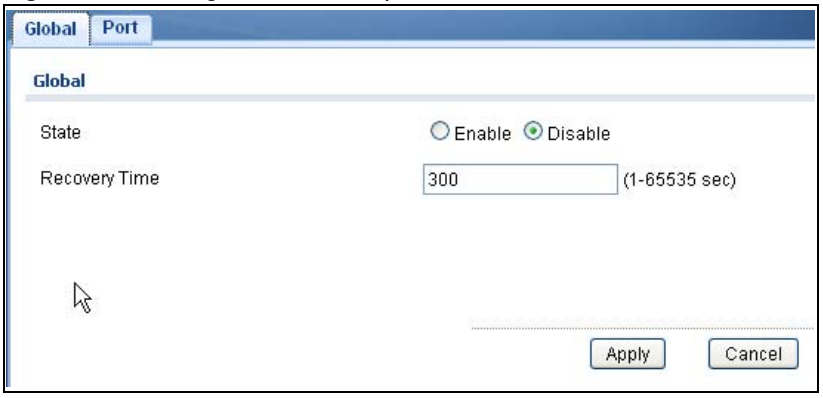
22.2 Loop Guard

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

22.2.1 The Global Screen

Use this screen to configure the global Loop Guard. Click **Configuration > Loop Guard** to open this screen.

Figure 126 Configuration > Loop Guard



The following table describes the labels in this screen.

Table 93 Configuration > Loop Guard

LABEL	DESCRIPTION
Global	
State	Select **Enable** to activate loop protection on this switch.

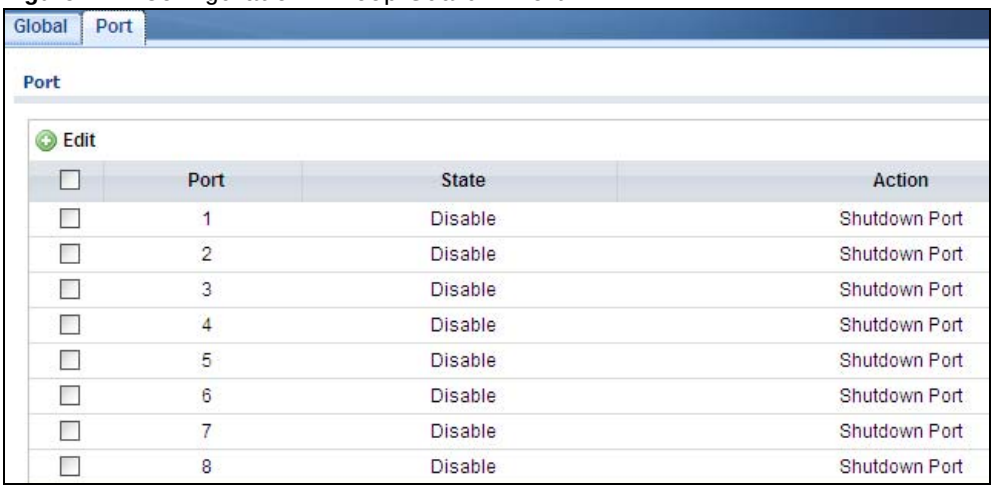
Table 93 Configuration > Loop Guard (continued)

LABEL	DESCRIPTION
Recovery Time	Enter the period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port).
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

22.2.2 The Loop Guard Port

Use this screen to view the Loop Guard Port. Click **Configuration** > **Loop Guard** > **Port** to open this screen.

Figure 127 Configuration > Loop Guard > Port



The following table describes the labels in this screen.

Table 94 Configuration > Loop Guard > Port

LABEL	DESCRIPTION
Port	
Edit	Click **Edit** to change the properties of the port.
Port	Displays the port index number.
State	Displays whether the port state is **Enable** or **Disable**.
Action	Displays the action to take by the Switch. The options are **Log**, **Shutdown Port**, and **Shutdown** and **Log**.

22.2.3 The Port Edit Screen

Use this screen to configure a Loop Guard port. Click **Configuration** > **Loop Guard** > **Port** > **Edit** to open this screen.

Figure 128 Configuration > Loop Guard > Port > Edit

The following table describes the labels in this screen.

Table 95 Configuration > Loop Guard > Port > Edit

LABEL	DESCRIPTION
Port	
Port List	Displays the list of port index numbers to be configured.
State	Select **Enable** to use the Admin Enabled feature.
Action	Select the action to take by the Switch.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

23

Configuration: Mirror

23.1 Overview

This section provides information for **Mirror** in **Configuration.**

23.2 Mirror

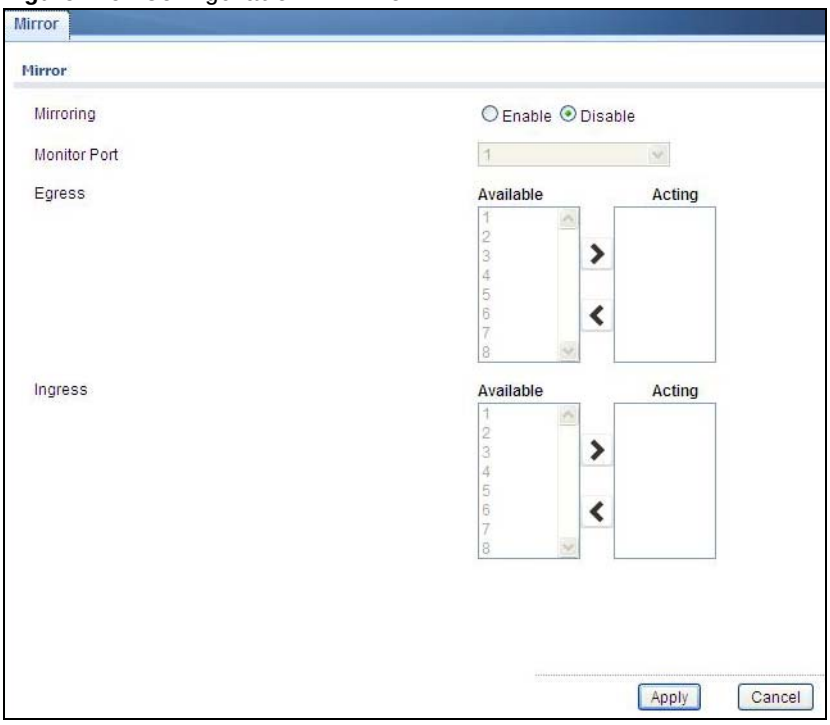
Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

The Switch supports local port mirroring.

23.2.1 The Mirror Screen

Use this screen to configure Mirroring. Click **Configuration > Mirror** to open this screen.

Figure 129 Configuration > Mirror



The following table describes the labels in this screen.

Table 96 Configuration > Mirror

LABEL	DESCRIPTION
Mirror	
Mirroring	Select **Enable** to activate port mirroring on the Switch or **Disable** to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Type the port number of the monitor port.
Egress	Specify the ports to mirror outgoing traffic.
Available	Click **<** to move a severity type from the acting box to the available box. Click **>** to move a severity type to the acting box from the available box.
Acting	Click **<** to move a severity type from the acting box to the available box. Click **>** to move a severity type to the acting box from the available box.
>	Click **>** to move a severity type to the acting box from the available box.
<	Click **<** to move a severity type from the acting box to the available box.
Ingress	Specify the ports to mirror incoming traffic.
Available	Click **<** to move a severity type from the acting box to the available box. Click **>** to move a severity type to the acting box from the available box.
Acting	Click **<** to move a severity type from the acting box to the available box. Click **>** to move a severity type to the acting box from the available box.
>	Click **>** to move a severity type to the acting box from the available box.
<	Click **<** to move a severity type from the acting box to the available box.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

24

Configuration: Multicast

24.1 Overview

This section provides information for **Multicast** in **Configuration.**

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

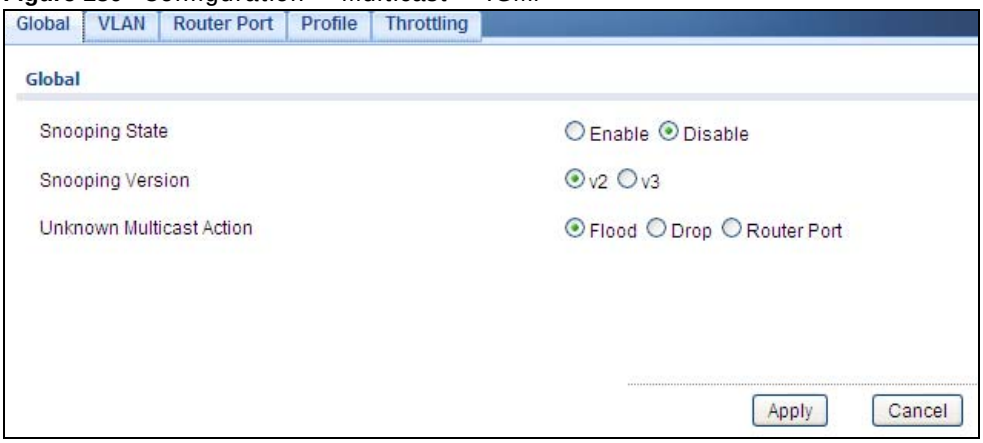
24.2 IGMP

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in an IPv4 multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

24.2.1 The Global Screen

Use this screen to view the **IGMP Global** settings. Click **Configuration > Multicast > IGMP** to open this screen.

Figure 130 Configuration > Multicast > IGMP



The following table describes the labels in this screen.

Table 97 Configuration > Multicast > IGMP

LABEL	DESCRIPTION
IGMP Global	
Snooping Status	Select **Enable** to turn on IGMP packet snooping or **Disable** to turn snooping off.

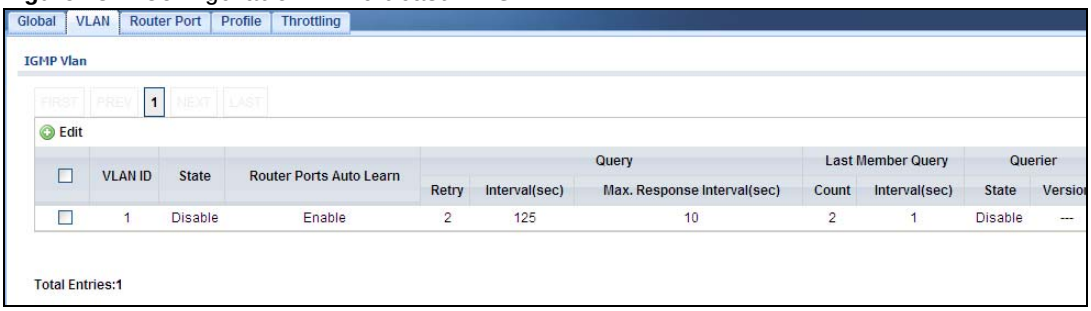
Table 97 Configuration > Multicast > IGMP (continued)

LABEL	DESCRIPTION
Snooping Version	Select **v2** or **v3** depending on the snooping version you require.
Unknown Multicast Action	Select to send the IPv4 unknown multicast frame to the router port. The following options are available: • **Flood** - select to send the frame(s) to all ports. • **Drop** - select to discard the frame(s). • **Router Port** - select to send the frame to router port.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

24.2.2 The VLAN Screen

Use this screen to view the **IGMP VLAN** settings. Click **Configuration > Multicast > IGMP > VLAN** to open this screen.

Figure 131 Configuration > Multicast > IGMP > VLAN



The following table describes the labels in this screen.

Table 98 Configuration > Multicast > IGMP > VLAN

LABEL	DESCRIPTION
IGMP VLAN	
Edit	Click **Edit** to change the properties of the IGMP VLAN entry.
VLAN ID	Displays the ID of a static VLAN; the valid range is between 1 and 4094.
Status	Display the status of the VLAN as enabled or disabled.
Router Ports Auto Learn	Displays the Switch learn multicast router port member status of any VLANs as enabled or disabled.
Query	
Retry	Displays the number of query retry times.
Interval (sec)	Displays the amount of time (in seconds) between general query messages sent by the router connected to the upstream port.
Max. Response Interval (sec)	Displays the amount of time (in seconds) the router connected to the upstream port waits for a response to an IGMP general query message.
Last Member Query	
Count	Displays the number of queries.
Interval (sec)	Displays the amount of time (in milliseconds) between the IGMP group-specific queries sent by an upstream port when an IGMP Done message is received.
Querier	

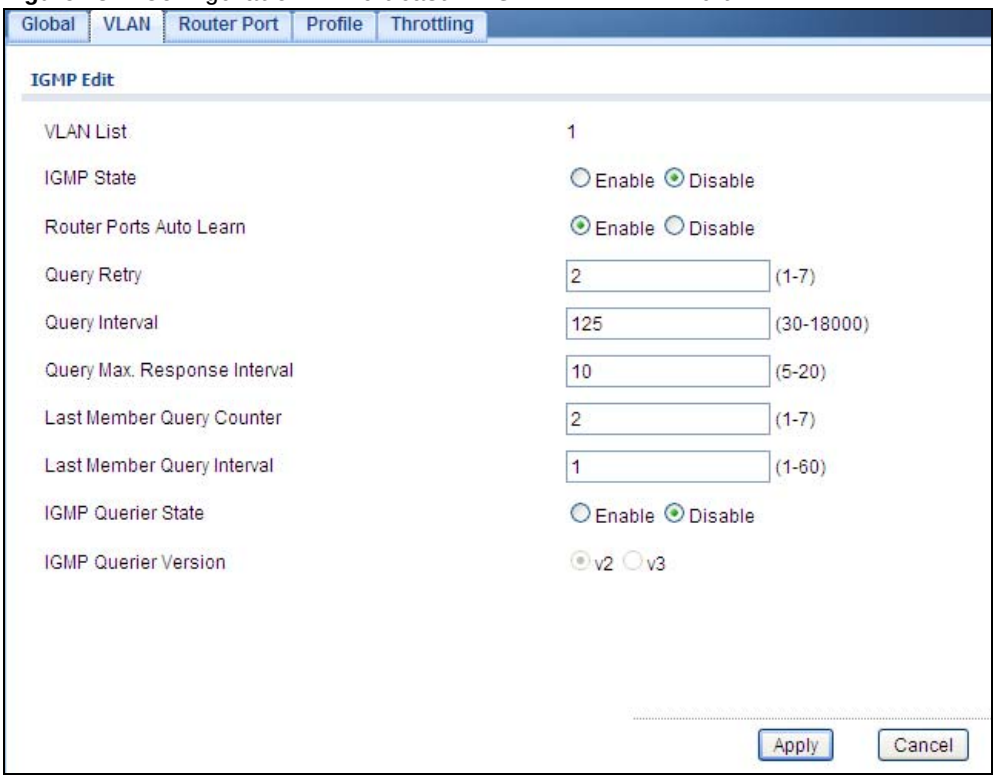
Table 98 Configuration > Multicast > IGMP > VLAN (continued)

LABEL	DESCRIPTION
State	Displays the switch current VLAN querier entry as **Enable** or **Disable**.
Version	Displays the switch current VLAN querier entry version.

24.2.3 The Edit IGMP Screen

Use this screen to configure the **IGMP VLAN** settings. Click **Configuration > Multicast > IGMP > VLAN** > **Edit** to open this screen.

Figure 132 Configuration > Multicast > IGMP > VLAN > Edit



The following table describes the labels in this screen.

Table 99 Configuration > Multicast > IGMP > VLAN > Modify

LABEL	DESCRIPTION
IGMP Edit	
VLAN List	Enter the ID of a static VLAN; the valid range is between 1 and 4094.
IGMP State	Select the status of the VLAN to **Enable** or **Disable** the function.
Router Ports Auto Learn	Select **Enabled** to have the Switch learn multicast router membership information of any VLANs automatically.
Query	
Retry	Enter the number of query retry times. The value can be between 1 and 7.
Interval (sec)	Enter the amount of time (in seconds) between general query messages sent by the router connected to the upstream port. The value can be between 30 and 18000.
Max. Response Interval (sec)	Enter the amount of time (in seconds) the router connected to the upstream port waits for a response to an IGMP general query message.

Table 99 Configuration > Multicast > IGMP > VLAN > Modify (continued)

LABEL	DESCRIPTION
Last Member Query	
Count	Enter the number of queries.
Interval (sec)	Enter the amount of time (in seconds) between the IGMP group-specific queries sent by an upstream port when an IGMP Done message is received.
Querier	
IGMP Querier State	Select the IGMP querier status to **Enable** or **Disable** the function.
IGMP Querier Version	Select the IGMP Querier version to **v2** or **v3**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

24.2.4 The Router Port Screen

Use this screen to view the **Router Port** settings. Click **Configuration > Multicast > IGMP > Router Port** to open this screen.

Figure 133 Configuration > Multicast > IGMP > Router Port

The following table describes the labels in this screen.

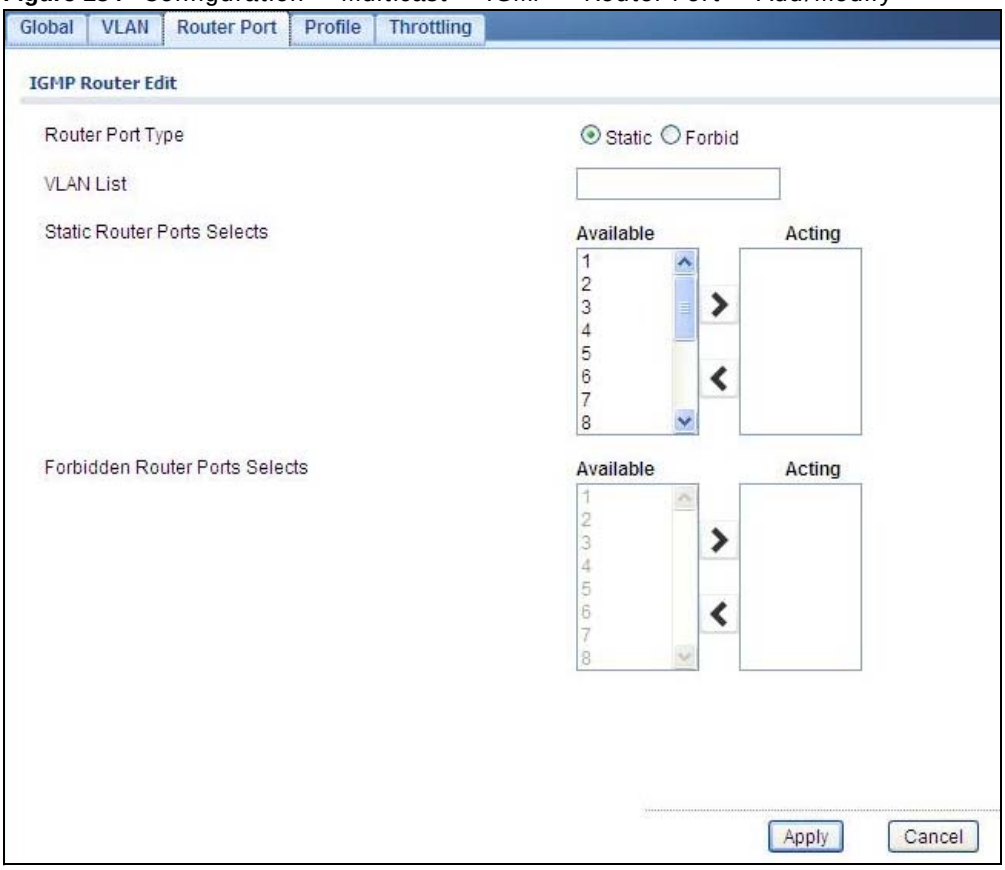
Table 100 Configuration > Multicast > IGMP > Router Port

LABEL	DESCRIPTION
Router Port	
Add	Click **Add** to create a new **Router Port** entry.
VLAN ID	Displays the ID of a static VLAN; the valid range is between 1 and 4094.
Static Router Ports	Displays the ports that are defined as static router ports.
Forbidden Router Ports	Displays the ports that are defined as forbidden router ports.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

24.2.5 The Add/Edit Router Port Screen

Use this screen to configure the **Router Port** settings. Click **Configuration > Multicast > IGMP > Router Port** > **Add/Modify** to open this screen.

Figure 134 Configuration > Multicast > IGMP > Router Port > Add/Modify



The following table describes the labels in this screen.

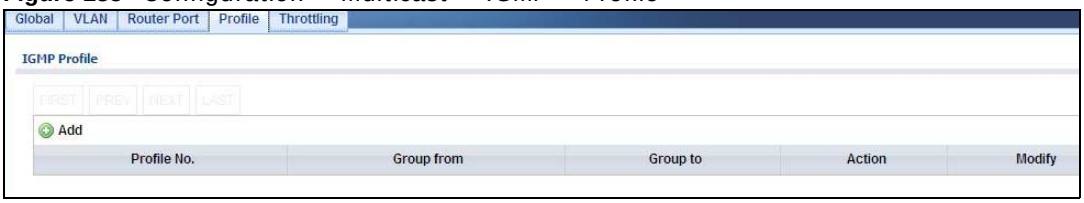
Table 101 Configuration > Multicast > IGMP > Router Port > Add/Modify

LABEL	DESCRIPTION
IGMP Router Edit	
Router Port Type	Select the router port(s) to be **Static** or **Forbidden**.
VLAN List	Enter the static VLAN IDs (valid range for each ID value is between 1 and 4094).
Static Router Ports Selects	Select the port(s) to be static router ports.
Forbidden Router Ports Selects	Select the port(s) to be forbidden router ports.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

24.2.6 The Profile Screen

Use this screen to view the **IGMP Profile** settings. Click **Configuration > Multicast > IGMP > Profile** to open this screen.

Figure 135 Configuration > Multicast > IGMP > Profile



The following table describes the labels in this screen.

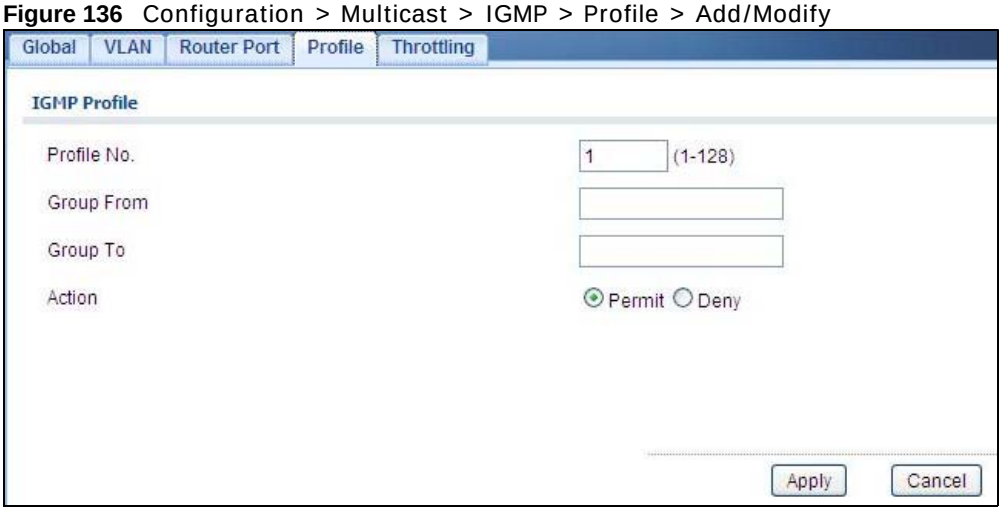
Table 102 Configuration > Multicast > IGMP > Profile

LABEL	DESCRIPTION
IGMP Profile	
Add	Click **Add** to create a new **IGMP Profile** entry.
Profile No.	Displays the **Profile No.**
Group from	Displays the profile start group IP address.
Group to	Displays the profile end group IP address.
Action	Displays the action of the profile as **Permit** or **Deny**.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

24.2.7 The Add/Edit Profile Screen

Use this screen to configure the **IGMP Profile** settings. Click **Configuration > Multicast > IGMP > Profile** > **Add/Modify** to open this screen.

Figure 136 Configuration > Multicast > IGMP > Profile > Add/Modify



The following table describes the labels in this screen.

Table 103 Configuration > Multicast > IGMP > Profile > Add/Modify

LABEL	DESCRIPTION
IGMP Profile	
Profile No.	Enter the **Profile No.**

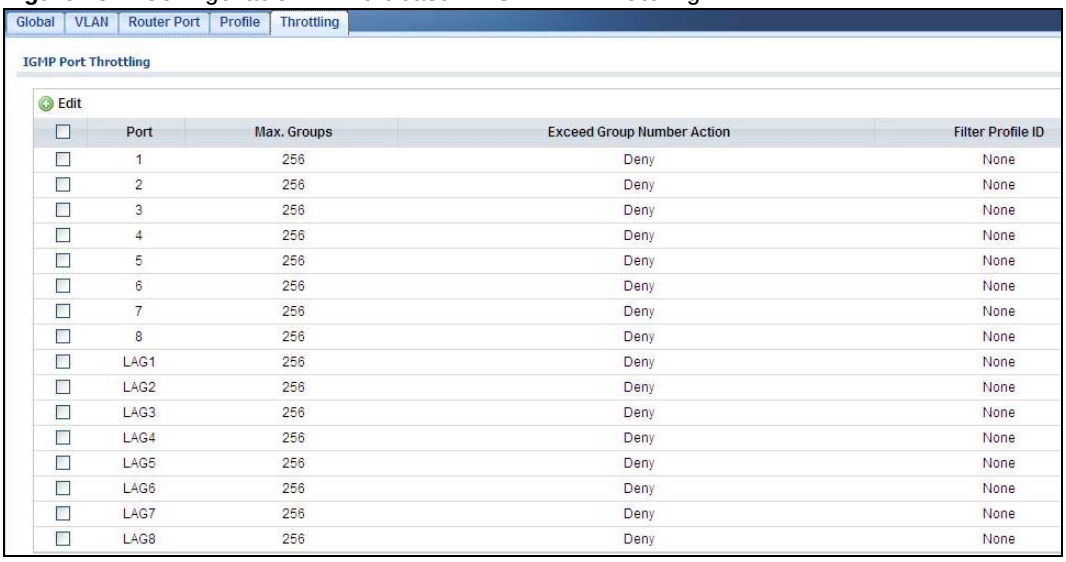
Table 103 Configuration > Multicast > IGMP > Profile > Add/Modify (continued)

LABEL	DESCRIPTION
Group from	Enter the profile start group IP address.
Group to	Enter the profile end group IP address.
Action	Select the action of the profile as to be **Permit** or **Deny**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

24.2.8 The Throttling Screen

Use this screen to view the **Throttling** settings. Click **Configuration > Multicast > IGMP > Throttling** to open this screen.

Figure 137 Configuration > Multicast > IGMP > Throttling



The following table describes the labels in this screen.

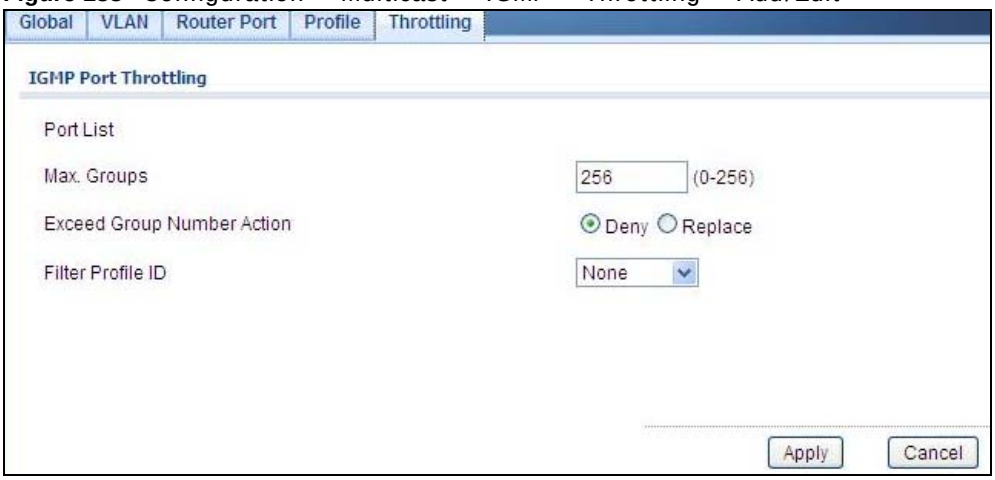
Table 104 Configuration > Multicast > IGMP > Throttling

LABEL	DESCRIPTION
IGMP Port Throttling	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index value.
Max. Groups	Displays the maximum number of groups.
Exceed Group Number Action	Displays the action taken by the groups as **Permit** or **Deny**.
Filter Profile ID	Displays the throttling filter profile ID.

24.2.9 The Add/Edit Throttling Screen

Use this screen to configure the **Throttling** settings. Click **Configuration > Multicast > IGMP > Throttling** > **Add/Edit** to open this screen.

Figure 138 Configuration > Multicast > IGMP > Throttling > Add/Edit



The following table describes the labels in this screen.

Table 105 Configuration > Multicast > IGMP > Throttling > Add/Edit

LABEL	DESCRIPTION
IGMP Port Throttling	
Port List	Enter the port index value(s).
Max. Groups	Enter the maximum number of groups. Enter a value between 0 and 256.
Exceed Group Number Action	Select the action taken by the groups to be **Deny** or **Replace**.
Filter Profile ID	Select the throttling filter profile ID from the dropdown list.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

25

Configuration: Spanning Tree

25.1 Overview

This section provides information for **Spanning Tree** in **Configuration.**

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

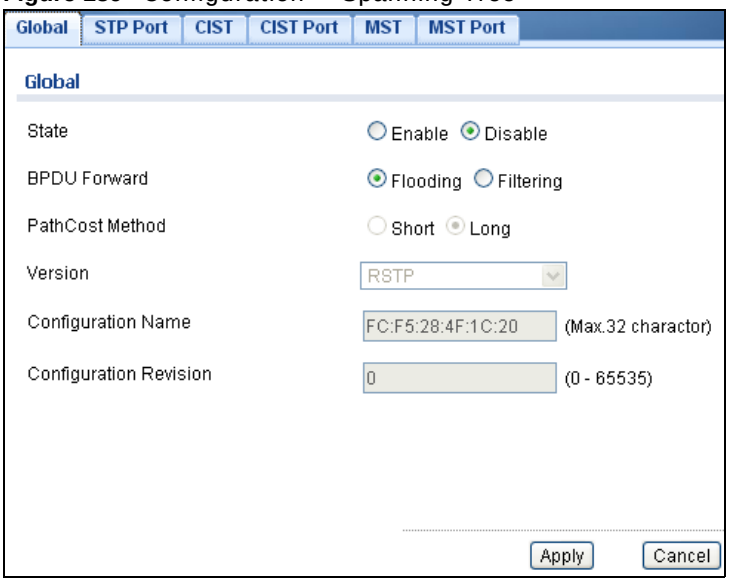
25.2 Spanning Tree

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.

25.2.1 The Global Screen

Use this screen to view the **Global** settings. Click **Configuration > Spanning Tree** to open this screen.

Figure 139 Configuration > Spanning Tree



The following table describes the labels in this screen.

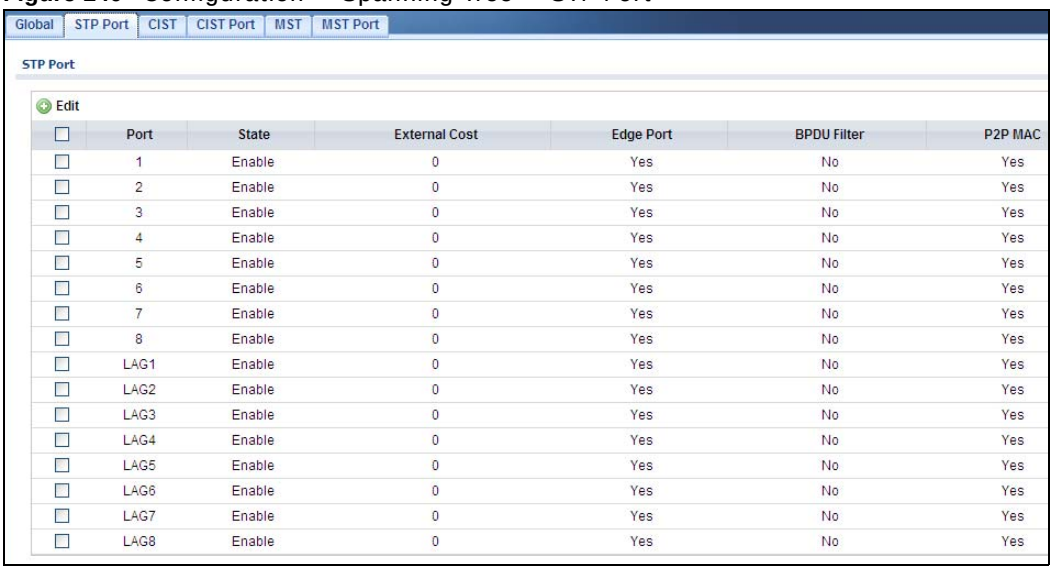
Table 106 Configuration > Spanning Tree

LABEL	DESCRIPTION
Global	
State	Select to **Enable** or **Disable** the Spanning-Tree function.
BPDU Forward	Select the bridge protocol data units forward (BPDU) option to be **Flooding** or **Filtering**.
Path Cost Method	Select **Short** or **Long** as a **Path Cost** method. Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended that you assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 40 on page 112 for more information.
Version	Select the type of spanning tree protocol to use. The following options are available: • **STP** • **RSTP** • **MSTP**
Configuration Name	Enter the name of the configuration in hexadecimal. The maximum number characters is 32.
Configuration Revision	Enter the revision number of configuration. The number can be between 0 and 65535.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

25.2.2 The STP Port Screen

Use this screen to view the **STP Port** settings. Click **Configuration > Spanning Tree > STP Port** to open this screen.

Figure 140 Configuration > Spanning Tree > STP Port



Port	State	External Cost	Edge Port	BPDU Filter	P2P MAC
1	Enable	0	Yes	No	Yes
2	Enable	0	Yes	No	Yes
3	Enable	0	Yes	No	Yes
4	Enable	0	Yes	No	Yes
5	Enable	0	Yes	No	Yes
6	Enable	0	Yes	No	Yes
7	Enable	0	Yes	No	Yes
8	Enable	0	Yes	No	Yes
LAG1	Enable	0	Yes	No	Yes
LAG2	Enable	0	Yes	No	Yes
LAG3	Enable	0	Yes	No	Yes
LAG4	Enable	0	Yes	No	Yes
LAG5	Enable	0	Yes	No	Yes
LAG6	Enable	0	Yes	No	Yes
LAG7	Enable	0	Yes	No	Yes
LAG8	Enable	0	Yes	No	Yes

The following table describes the labels in this screen.

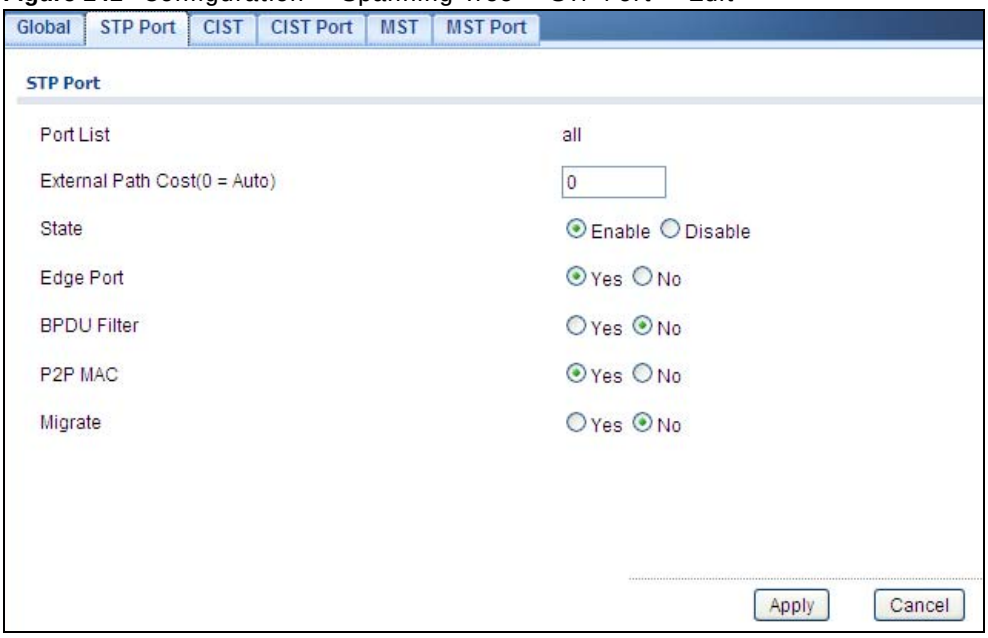
Table 107 Configuration > Spanning Tree > STP Port

LABEL	DESCRIPTION
STP Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the index number of the STP port.
State	Display the status of the STP port as enabled or disabled.
External Cost	Displays the external path cost.
Edge Port	Displays the edge port status as **Yes** or **No**.
BPDU Filter	Displays the BPDU filter status as **Yes** or **No**.
P2P MAC	Displays the P2P MAC status as **Yes** or **No**.

25.2.3 The STP Port Edit Screen

Use this screen to configure the **STP Port Edit** settings. Click **Configuration > Spanning Tree > STP Port > Edit** to open this screen.

Figure 141 Configuration > Spanning Tree > STP Port > Edit



The following table describes the labels in this screen.

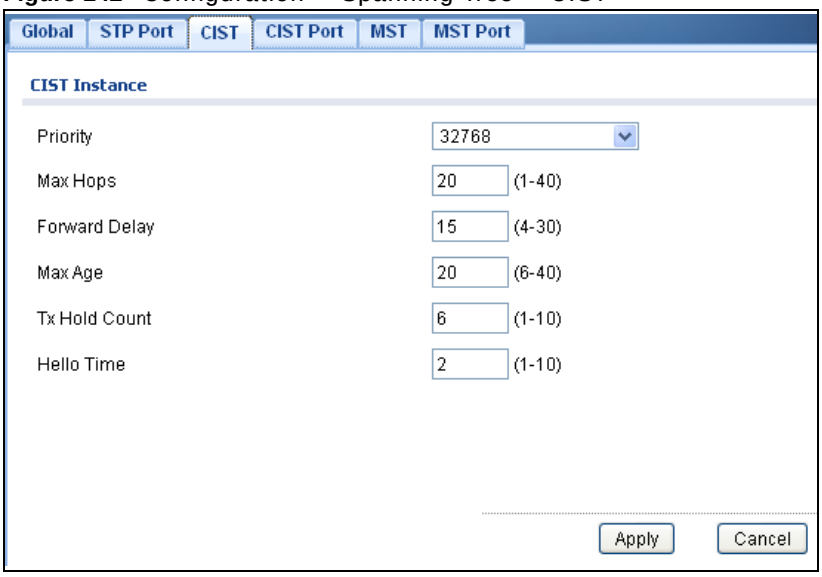
Table 108 Configuration > Spanning Tree > STP Port > Edit

LABEL	DESCRIPTION
STP Port	
Port List	Enter the index number of the STP port(s).
External Path Cost (0=Auto)	Enter the external path cost. Enter 0 for Auto.
State	Select the state of the STP port as enabled or disabled.
Edge Port	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
BPDU Filter	Select **Yes** to activate BPDU filter or **No** to deactivate it.
P2P MAC	Select **Yes** to activate P2P MAC or **No** to deactivate it.
Migrate	Select **Yes** to activate Migrate or **No** to deactivate it.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

25.2.4 The CIST Screen

Use this screen to view the **CIST** settings. Click **Configuration > Spanning Tree > CIST** to open this screen.

Figure 142 Configuration > Spanning Tree > CIST



The following table describes the labels in this screen.

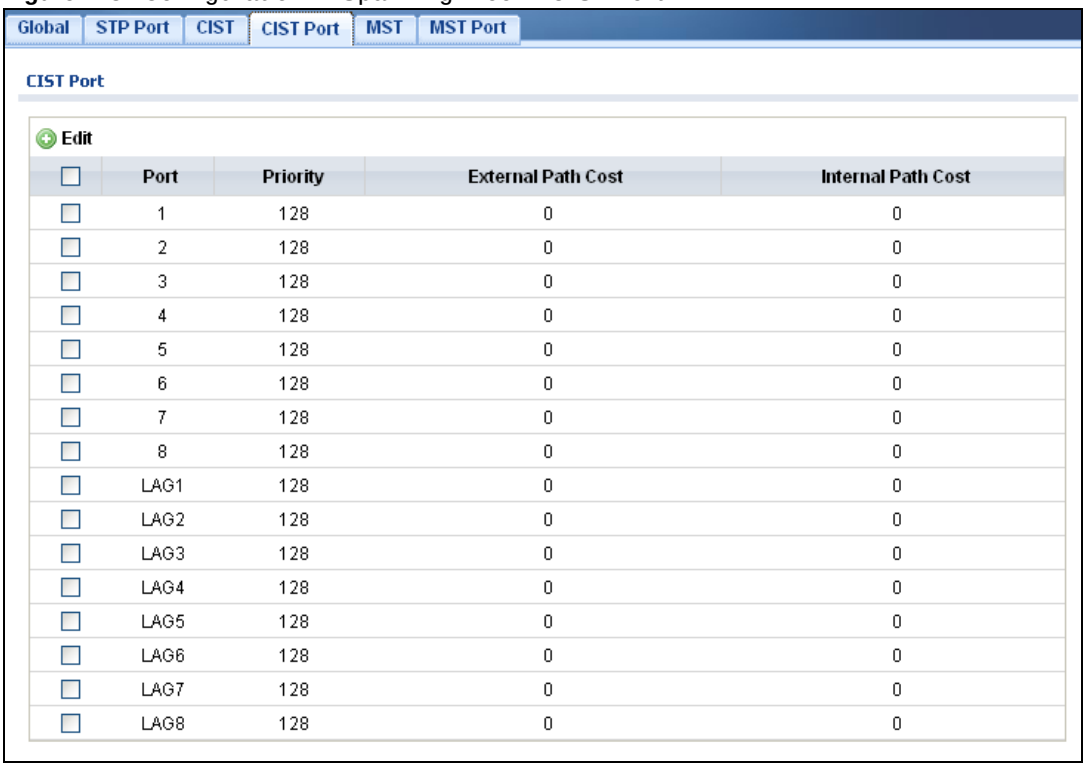
Table 109 Configuration > Spanning Tree > CIST

LABEL	DESCRIPTION
CIST Instance	
Priority	Configure priority of CIST bridge ID. Priority is part of bridge ID, used for CIST root bridge selection.
Max Hops	Enter a maximum number of hops value. The value can be between 1 and 40.
Forward Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Tx Hold Count	Enter a transmission hold count value. The value can be between 1 and 10.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

25.2.5 The CIST Port Screen

Use this screen to view the **CIST Port** settings. Click **Configuration > Spanning Tree > CIST Port** to open this screen.

Figure 143 Configuration > Spanning Tree > CIST Port



	Port	Priority	External Path Cost	Internal Path Cost
☐	1	128	0	0
☐	2	128	0	0
☐	3	128	0	0
☐	4	128	0	0
☐	5	128	0	0
☐	6	128	0	0
☐	7	128	0	0
☐	8	128	0	0
☐	LAG1	128	0	0
☐	LAG2	128	0	0
☐	LAG3	128	0	0
☐	LAG4	128	0	0
☐	LAG5	128	0	0
☐	LAG6	128	0	0
☐	LAG7	128	0	0
☐	LAG8	128	0	0

The following table describes the labels in this screen.

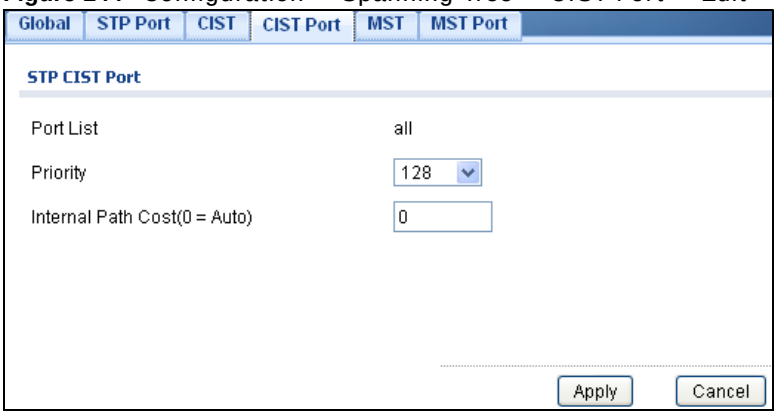
Table 110 Configuration > Spanning Tree > CIST Port

LABEL	DESCRIPTION
CIST Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the index number of the STP port.
Priority	Displays the priority for each port here.
External Path Cost	Displays the external path cost.
Internal Path Cost	Displays the internal path cost.

25.2.6 The CIST Port Edit Screen

Use this screen to configure the **CIST Port Edit** settings. Click **Configuration > Spanning Tree > CIST Port > Edit** to open this screen.

Figure 144 Configuration > Spanning Tree > CIST Port > Edit



The following table describes the labels in this screen.

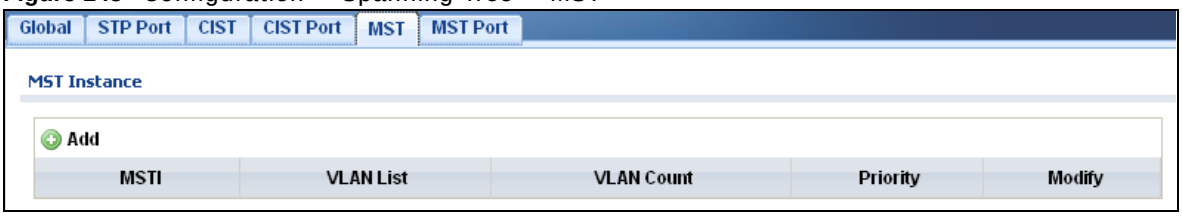
Table 111 Configuration > Spanning Tree > CIST Port > Edit

LABEL	DESCRIPTION
STP CIST Port	
Port List	Enter the index number of the STP port(s).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Internal Path Cost (0=Auto)	Enter the internal path cost. Enter 0 or Auto.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

25.2.7 The MST Screen

Use this screen to view the **MST** settings. Click **Configuration > Spanning Tree > MST** to open this screen.

Figure 145 Configuration > Spanning Tree > MST



The following table describes the labels in this screen.

Table 112 Configuration > Spanning Tree > MST

LABEL	DESCRIPTION
MST Instance	
Add	Click **Add** to create a new **MST Instance** entry.
MSTI	Displays the Multiple Spanning Tree Instance(s) (MSTI).
VLAN List	Display a list of MSTI VLANs.

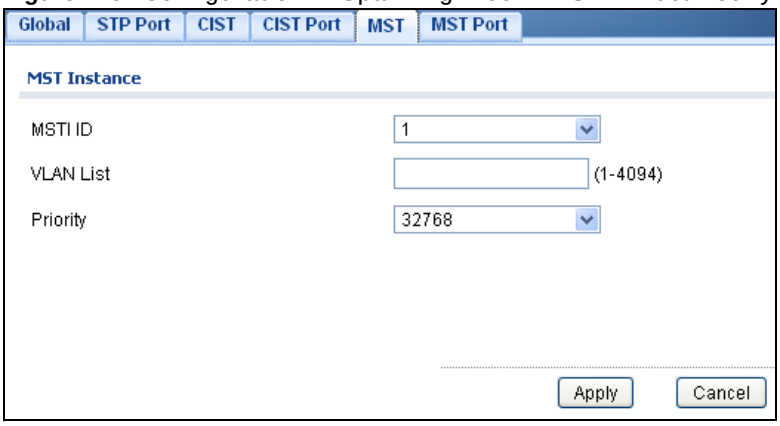
Table 112 Configuration > Spanning Tree > MST (continued)

LABEL	DESCRIPTION
VLAN Count	Displays the VLAN count.
Priority	Displays the priority for each port here.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

25.2.8 The Add/Modify MST Screen

Use this screen to configure the **MST** settings. Click **Configuration** > **Spanning Tree** > **MST** > **Add / Modify** to open this screen.

Figure 146 Configuration > Spanning Tree > MST > Add/Modify



The following table describes the labels in this screen.

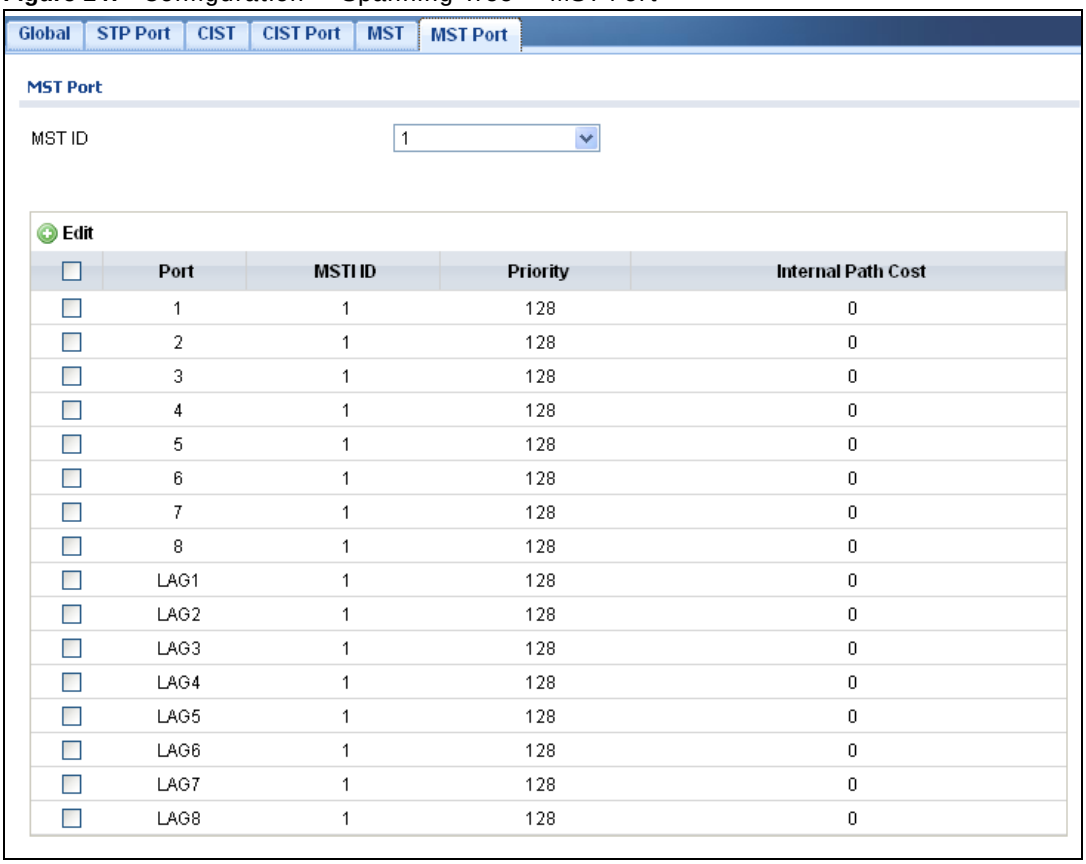
Table 113 Configuration > Spanning Tree > MST > Add/Modify

LABEL	DESCRIPTION
MST Instance	
MST ID	Displays the Multiple Spanning Tree Instance (MSTI) ID(s).
VLAN List	Display a list of MSTI VLANs.
Priority	Displays MSTI bridge ID priority value.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

25.2.9 The MST Port Screen

Use this screen to view the **MST Port** settings. Click **Configuration > Spanning Tree > MST Port** to open this screen.

Figure 147 Configuration > Spanning Tree > MST Port



The following table describes the labels in this screen.

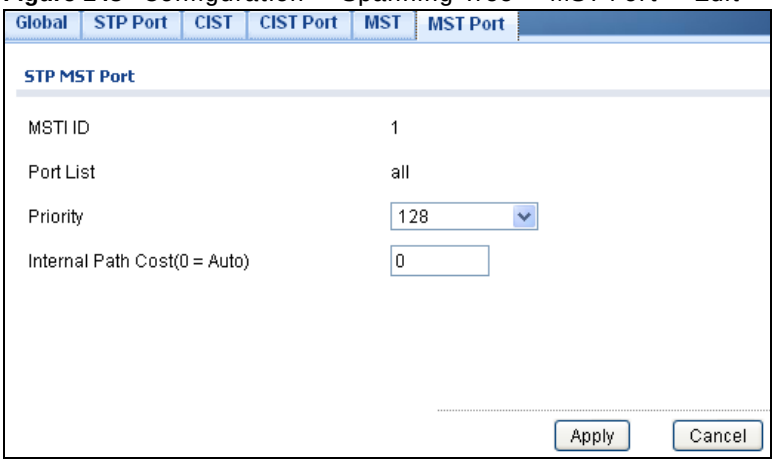
Table 114 Configuration > Spanning Tree > MST Port

LABEL	DESCRIPTION
MST Port	
MST ID	Select the MST port ID number from the dropdown list.
Edit	Select this check box to configure the properties of MST ID. Click the **Edit** button change the properties of the MST ID.
Port	Displays the index number of the MST port.
MSTI ID	Displays the index value of the MSTI.
Priority	Displays the priority for each port.
Internal Path Cost	Displays the internal path cost.

25.2.10 The MST Port Edit Screen

Use this screen to configure the **MST Port Edit** settings. Click **Configuration > Spanning Tree > MST Port > Edit** to open this screen.

Figure 148 Configuration > Spanning Tree > MST Port > Edit



The following table describes the labels in this screen.

Table 115 Configuration > Spanning Tree > MST Port > Edit

LABEL	DESCRIPTION
STP MST Port	
MST ID	Displays the MST ID number.
Port List	Enter the index number of the MTP port(s).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Internal Path Cost (0=Auto)	Enter the internal path cost. Enter 0 for Auto.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

26

Configuration: LLDP

26.1 Overview

This section provides information for **LLDP** in **Configuration.**

Use the **Link Layer Discovery Protocol (LLDP)** screens to configure LLDP Switch settings.

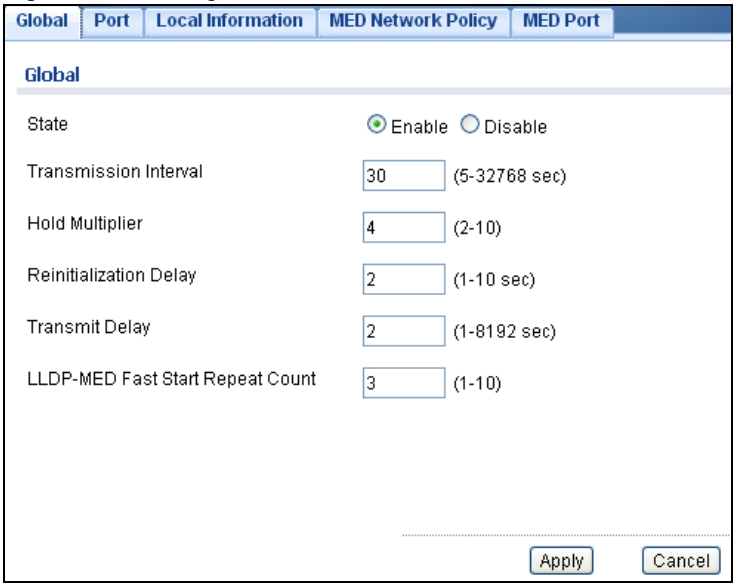
26.2 LLDP

This page allows the user to inspect and configure the current LLDP port settings.

26.2.1 The Global Screen

Use this screen to configure the **Global** settings. Click **Configuration > LLDP > Global** to open this screen.

Figure 149 Configuration > LLDP > Global



The following table describes the labels in this screen.

Table 116 Configuration > LLDP > Global

LABEL	DESCRIPTION
Global	
State	Select **Enable** to activate the global LLDP.

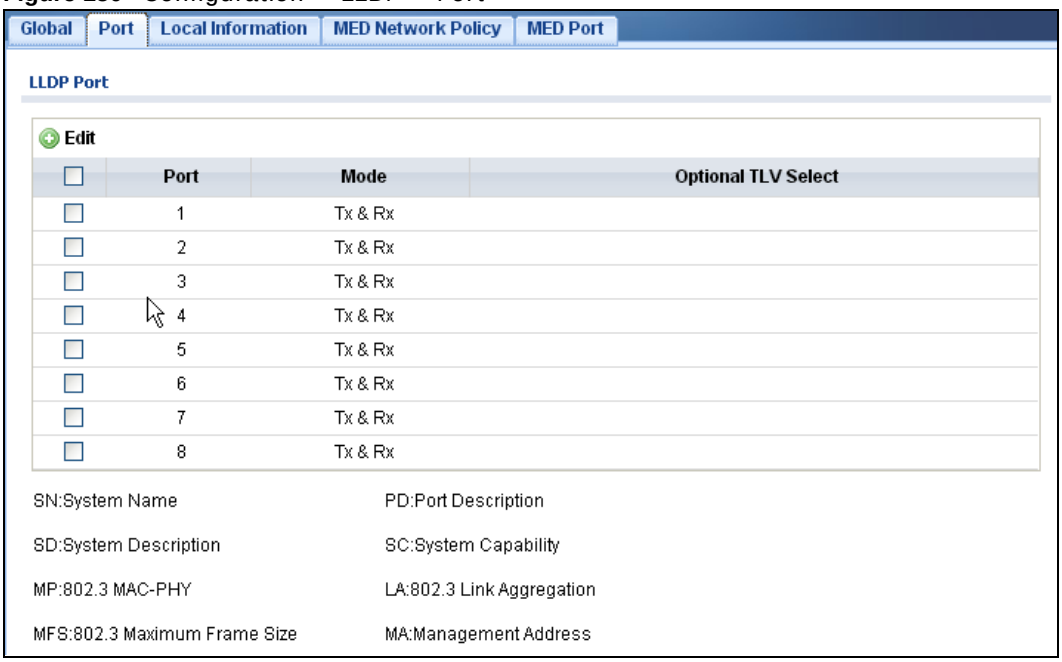
Table 116 Configuration > LLDP > Global (continued)

LABEL	DESCRIPTION
Transmission Interval	Enter the transmission interval value. The switch periodically transmits 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.
Hold Multiplier	Enter the hold multiplier value. 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.
Reinitialization Delay	Enter the reinitialization delay value. When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling 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.
Transmit Delay	Enter the transmission delay value. 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.
LLDP-MED Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

26.2.2 The Port Screen

Use this screen to view the **Port** settings. Click **Configuration > LLDP > Port** to open this screen.

Figure 150 Configuration > LLDP > Port



The following table describes the labels in this screen.

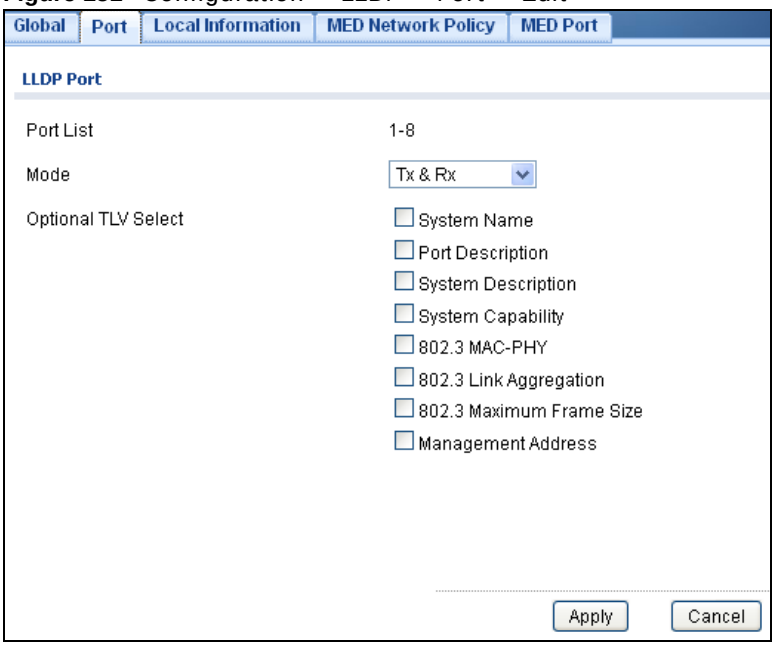
Table 117 Configuration > LLDP > Port

LABEL	DESCRIPTION
LLDP VLAN	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the index number of the LLDP port.
Mode	Displays the mode of the LLDP port as **Disable**, **Tx Only**, **Rx Only**, or **Tx & Rx**.
Optional TLV Select	Displays the TLV as one or more of the following options: • SN - System Name • PD - Port Description • SD - System Description • SC - System Capability • MP - 802.3 MAC-PHY • LA - 802.3 Link Aggregation • MFS - 802.3 Maximum Frame Size • MA - Management Address

26.2.3 The Port Edit Screen

Use this screen to configure the **Port Edit** settings. Click **Configuration > LLDP > Port > Edit** to open this screen.

Figure 151 Configuration > LLDP > Port > Edit



The following table describes the labels in this screen.

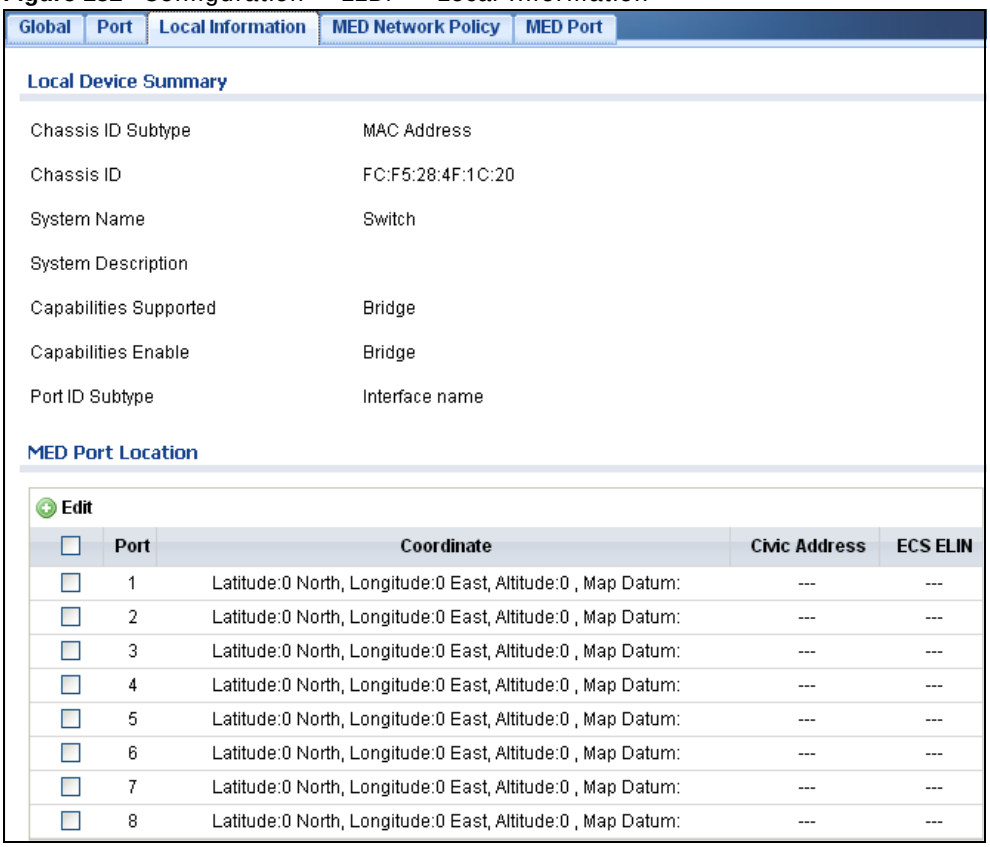
Table 118 Configuration > LLDP > Port > Edit

LABEL	DESCRIPTION
LLDP Port	
Port List	Displays the index number of the LLDP port(s).
Mode	Select the mode of the LLDP port as **Disable**, **Tx Only**, **Rx Only**, or **Tx & Rx**.
Optional TLV Select	Select the TLV as one or more of the following options: • **SN** - System Name • **PD** - Port Description • **SD** - System Description • **SC** - System Capability • **MP** - 802.3 MAC-PHY • **LA** - 802.3 Link Aggregation • **MFS** - 802.3 Maximum Frame Size • **MA** - Management Address
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

26.2.4 The Local Information Screen

Use this screen to view the **Local Information** settings. Click **Configuration > LLDP** > **Local Information** to open this screen.

Figure 152 Configuration > LLDP > Local Information



The following table describes the labels in this screen.

Table 119 Configuration > LLDP > Local Information

LABEL	DESCRIPTION
Local Device Summary	
Chassis ID Subtype	Displays the chassis ID subtype.
Chassis ID	The **Chassis ID** is the identification of the neighbor's LLDP frames.
System Name	**System Name** is the name advertised by the neighbor unit.
System Description	Displays the **System Description**.

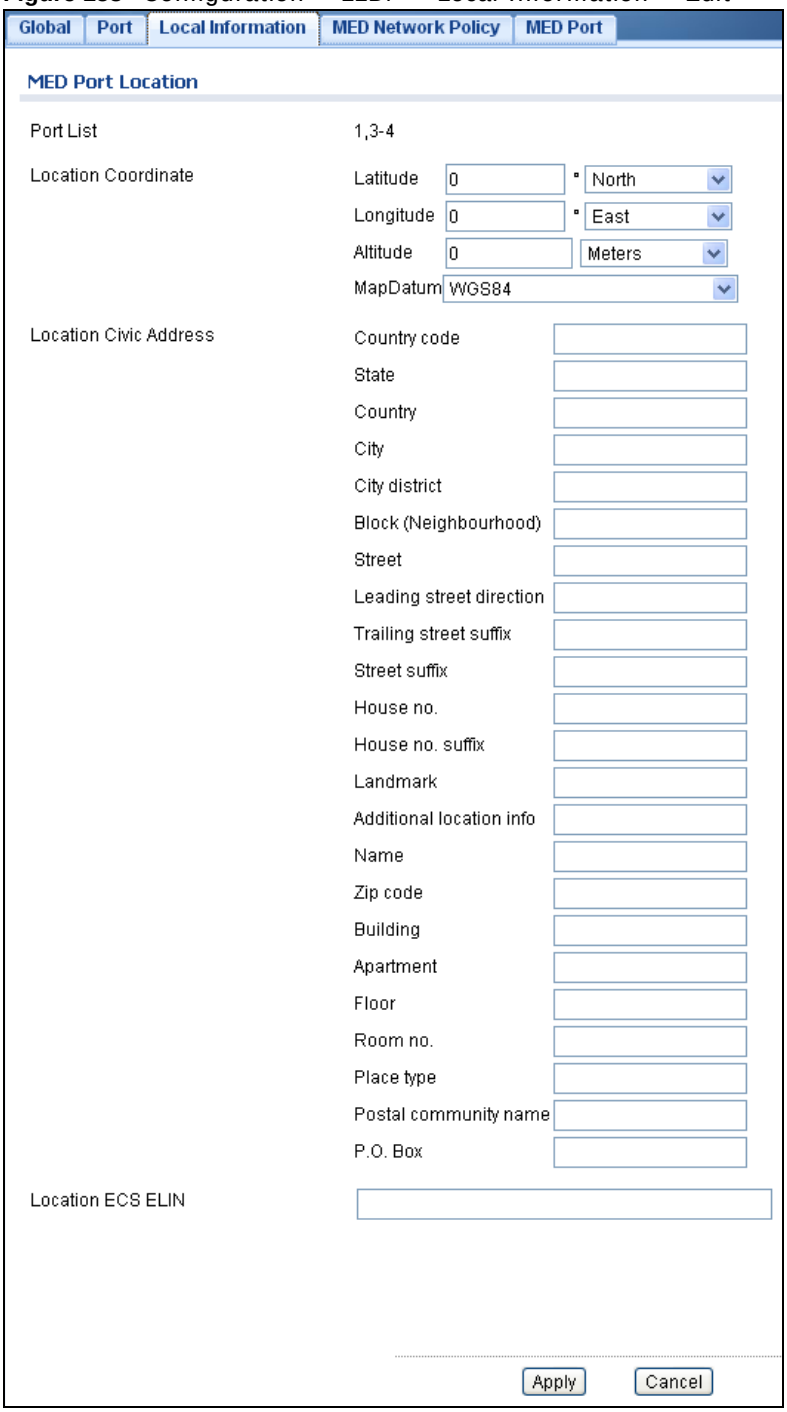
Table 119 Configuration > LLDP > Local Information (continued)

LABEL	DESCRIPTION
Capabilities Supported	**Capabilities Supported** describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Capabilities Enable	Displays which capability is enabled.
Port ID Subtype	Displays the **Port ID Subtype**.
MED Port Location	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the index number of the LLDP port(s).
Coordinate	Displays the location coordinate of the LLDP port(s).
Civic Address	Displays the location of the civic address(es) in hexadecimal.
ECS ELIN	Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA. Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

26.2.5 The Local Information Edit Screen

Use this screen to configure the **Port Edit** settings. Click **Configuration > LLDP > Local Information > Edit** to open this screen.

Figure 153 Configuration > LLDP > Local Information > Edit



The following table describes the labels in this screen.

Table 120 Configuration > LLDP > Local Information > Edit

LABEL	DESCRIPTION
MED Port Location	
Port List	Displays the index number of the LLDP port(s). The value is made of 16 pairs of hexadecimal characters.

Table 120 Configuration > LLDP > Local Information > Edit (continued)

LABEL	DESCRIPTION
Location Coordinates	
Latitude	**Latitude** SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either **North** of the equator or **South** of the equator.
Longitude	**Longitude** SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian.
Altitude	**Altitude** SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). **Meters:** Representing meters of Altitude defined by the vertical datum specified. **Floors:** Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The **Map Datum** is used for the coordinates given in these options: **WGS84:** (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. **NAD83/NAVD88:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). **NAD83/MLLW:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.
Location Civic Address	IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). • **Country code:** The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US. • **State:** National subdivisions (state, canton, region, province, prefecture). • **County:** County, parish, gun (Japan), district. • **City:** City, township, shi (Japan) - Example: Copenhagen. • **City district:** City division, borough, city district, ward, chou (Japan). • **Block (Neighborhood):** Neighborhood, block. • **Street:** Street - Example: Poppelvej. • **Leading street direction:** Leading street direction - Example: N. • **Trailing street suffix:** Trailing street suffix - Example: SW. • **Street suffix:** Street suffix - Example: Ave, Platz. • **House no.:** House number - Example: 21. • **House no. suffix:** House number suffix - Example: A, 1/2. • **Landmark:** Landmark or vanity address - Example: Columbia University. • **Additional location info:** Additional location info - Example: South Wing. • **Name:** Name (residence and office occupant) - Example: Flemming Jahn. • **Zip code:** Postal/zip code - Example: 2791. • **Building:** Building (structure) - Example: Low Library. • **Apartment:** Unit (Apartment, suite) - Example: Apt 42. • **Floor:** Floor - Example: 4. • **Room no.:** Room number - Example: 450F. • **Place type:** Place type - Example: Office. • **Postal community name:** Postal community name - Example: Leonia. • **P.O. Box:** Post office box (P.O. BOX) - Example: 12345.

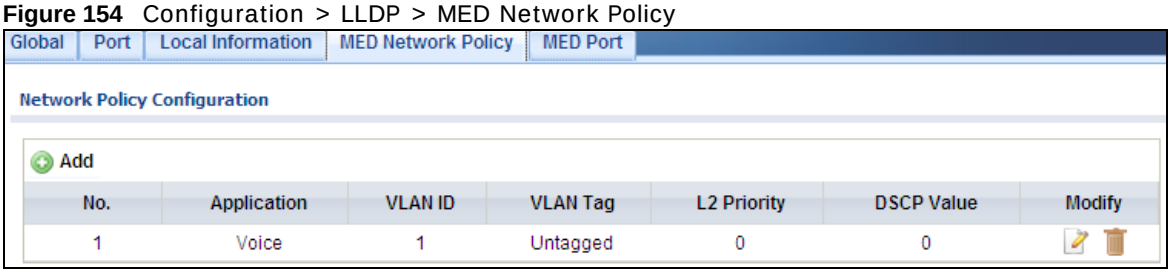
Table 120 Configuration > LLDP > Local Information > Edit (continued)

LABEL	DESCRIPTION
Location ECS ELIN	Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA. Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

26.2.6 The MED Network Policy Screen

Use this screen to view the **MED Network Policy** settings. Click **Configuration > LLDP** > **MED Network Policy** to open this screen.

Figure 154 Configuration > LLDP > MED Network Policy



The following table describes the labels in this screen.

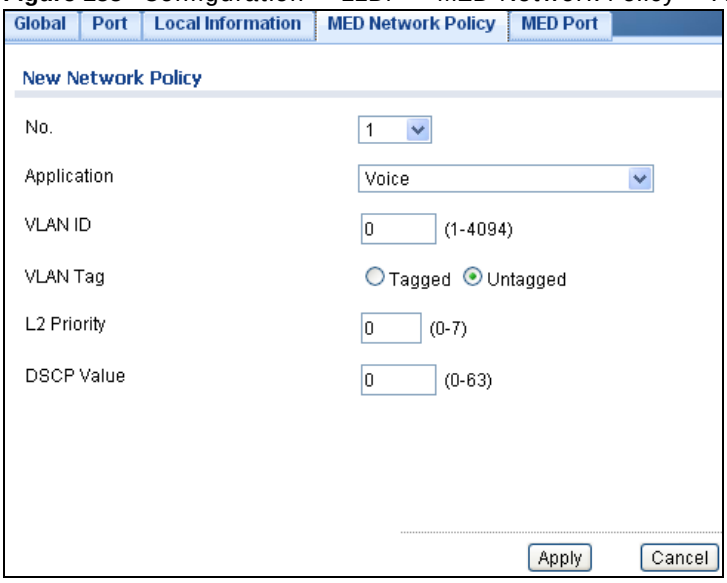
Table 121 Configuration > LLDP > MED Network Policy

LABEL	DESCRIPTION
Network Policy Configuration	
Add	Click **Add** to create a new **Network Policy Configuration** entry.
No.	Displays index of network policy.
Application	Displays the **Application type** indicating the primary function of the application(s).
VLAN ID	Displays the VLAN ID (VID) for the port as defined in IEEE 802.1Q-2003.
VLAN Tag	Displays the **VLAN Tag** value as **Tagged** or **Untagged**.
L2 Priority	Displays the L2 priority layer value.
DSCP Value	Displays the **DSCP Value**.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

26.2.7 The MED Network Policy Add/Edit Screen

Use this screen to configure the **Port Edit** settings. Click **Configuration > LLDP > MED Network Policy > Add/Edit** to open this screen.

Figure 155 Configuration > LLDP > MED Network Policy > Add/Edit



The following table describes the labels in this screen.

Table 122 Configuration > LLDP > MED Network Policy > Edit

LABEL	DESCRIPTION
MED Port Location Edit	
No.	Select the index of network policy
Application	Select the **Application** type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. 1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. **Voice Signalling** - for use in network topologies that require a different policy for the voice signalling than for the voice media. 3. **Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. **Guest Voice Signalling** - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. 5. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. 6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. **Video Signalling** - for use in network topologies that require a separate policy for the video signalling than for the video media.

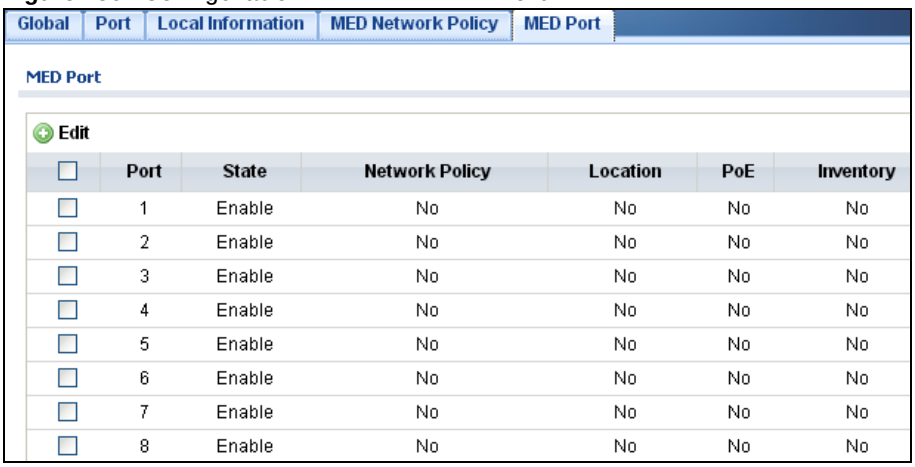
Table 122 Configuration > LLDP > MED Network Policy > Edit (continued)

LABEL	DESCRIPTION
VLAN ID	Enter the **VLAN ID** (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
VLAN Tag	**TAG** is indicative of whether the specified application type is using a tagged or an untagged VLAN. Select **Tagged** or **Untagged**. **Untagged:** The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. **Tagged:** The device is using the IEEE 802.1Q tagged frame format.
L2 Priority	**Priority** is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
DSCP Value	**DSCP** is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

26.2.8 The MED Port Screen

Use this screen to view the **MED Port** settings. Click **Configuration > LLDP** > **MED Port** to open this screen.

Figure 156 Configuration > LLDP > MED Port



The following table describes the labels in this screen.

Table 123 Configuration > LLDP > MED Port

LABEL	DESCRIPTION
MED Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the **MED Port** value.
State	Displays the state of the MED port as **Enable** or **Disable**.
Network Policy	Displays the **Network Policy** value.

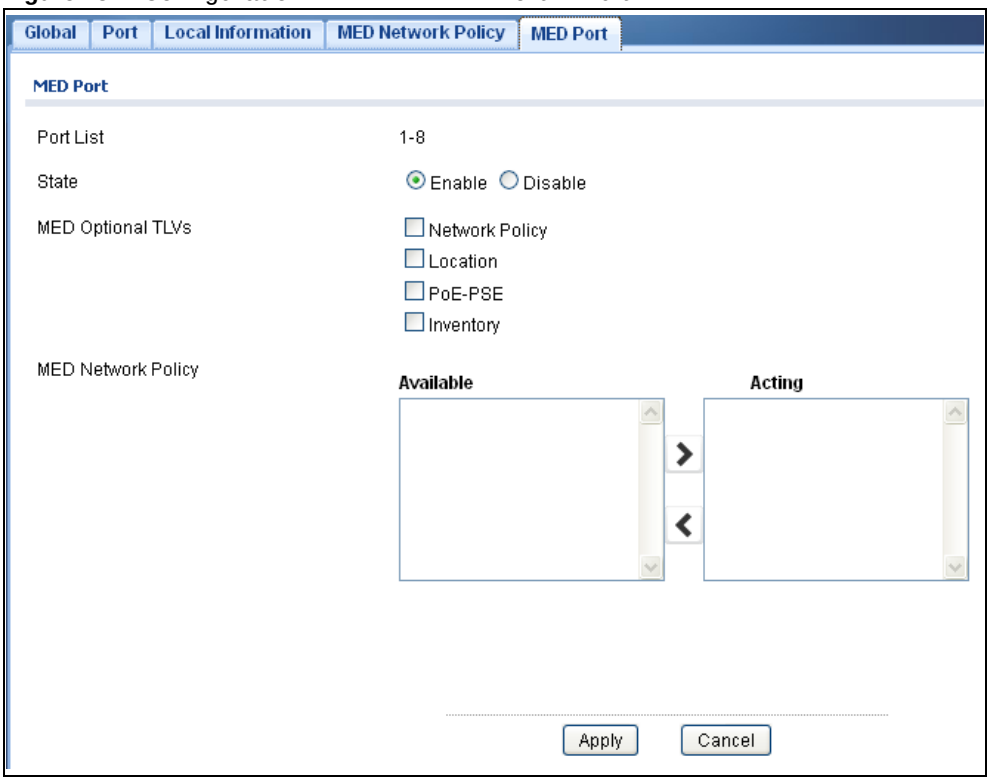
Table 123 Configuration > LLDP > MED Port (continued)

LABEL	DESCRIPTION
Location	Displays the **Location** value.
PoE	Displays the **PoE** value.
Inventory	Displays the **Inventory** value.

26.2.9 The MED Port Add/Edit Screen

Use this screen to configure the **MED Port Edit** settings. Click **Configuration > LLDP > MED Port > Edit** to open this screen.

Figure 157 Configuration > LLDP > MED Port > Edit



The following table describes the labels in this screen.

Table 124 Configuration > LLDP > MED Port > Edit

LABEL	DESCRIPTION
MED Port	
Port List	Displays the **Port List**.
State	Select **Enable** to activate the MED Port feature.
MED Optional TLVs	Select one or more of the MED Optional TLVs: • **Network Policy** • **Location** • **PoE PSE** • **Inventory**
MED Network Policy	Select one or more of the **MED Network Policies** in **Available** and move them to **Acting** to activate.

Table 124 Configuration > LLDP > MED Port > Edit (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

27

Configuration: QoS

27.1 Overview

This section provides information for **QoS** (Quality of Service) in **Configuration.**

27.2 General

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

27.2.1 The Port Screen

Use this screen to view the **Port** settings. Click **Configuration > QoS > General** to open this screen.

Figure 158 Configuration > QoS > General

Port | Queue | CoS Mapping | DSCP Mapping | IP Precedence Mapping

QoS Port

Edit

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
1	0	Disable	Disable	Disable
2	0	Disable	Disable	Disable
3	0	Disable	Disable	Disable
4	0	Disable	Disable	Disable
5	0	Disable	Disable	Disable
6	0	Disable	Disable	Disable
7	0	Disable	Disable	Disable
8	0	Disable	Disable	Disable
LAG1	0	Disable	Disable	Disable
LAG2	0	Disable	Disable	Disable
LAG3	0	Disable	Disable	Disable
LAG4	0	Disable	Disable	Disable
LAG5	0	Disable	Disable	Disable
LAG6	0	Disable	Disable	Disable
LAG7	0	Disable	Disable	Disable
LAG8	0	Disable	Disable	Disable

The following table describes the labels in this screen.

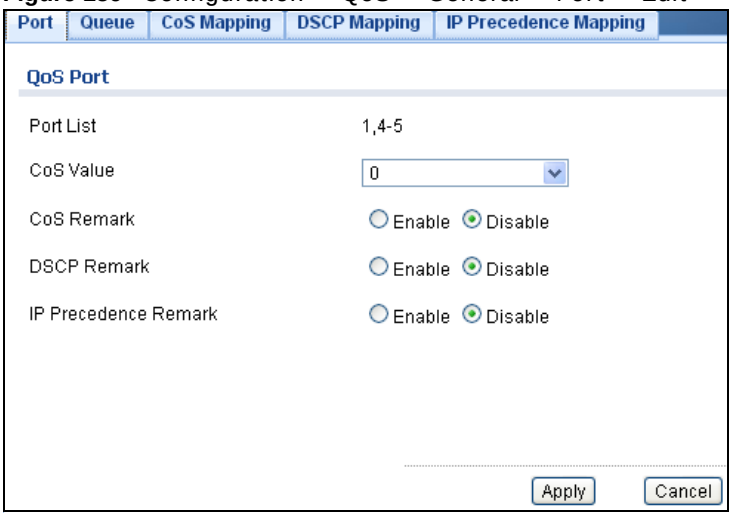
Table 125 Configuration > QoS > General

LABEL	DESCRIPTION
QoS Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the QoS port list.
CoS Value	Displays the CoS value, range: 0 - 7.
Remark CoS	Displays if this function is disabled or enabled.
Remark DSCP	Displays if this function is disabled or enabled.
Remark IP Precedence	Displays if this function is disabled or enabled.

27.2.2 The Port Edit Screen

Use this screen to configure the **Port Edit** settings. Click **Configuration > QoS > General** > **Port > Edit** to open this screen.

Figure 159 Configuration > QoS > General > Port > Edit



The following table describes the labels in this screen.

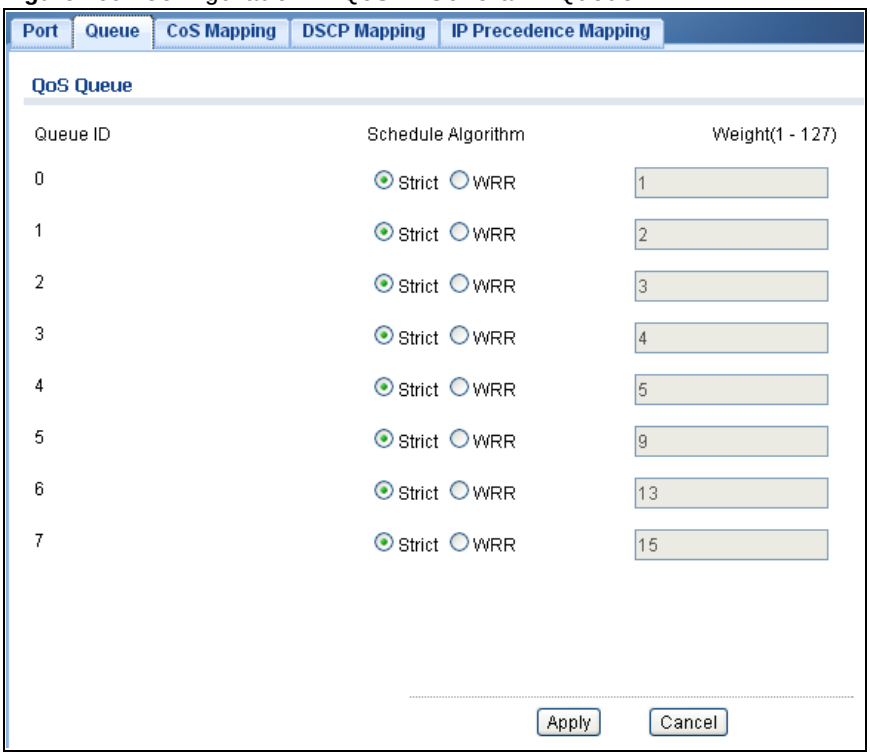
Table 126 Configuration > QoS > General > Port > Edit

LABEL	DESCRIPTION
QoS Port	
Port List	Displays the index number of the QoS port(s).
CoS Value	Select the **CoS Value** from the dropdown list.
CoS Remark	Select Enable to activate **CoS Remark**.
DSCP Remark	Select Enable to activate **DSCP Remark**.
IP Precedence Remark	Select Enable to activate **IP Precedence Remark**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

27.2.3 The Queue Screen

Use this screen to view the **Queue** settings. Click **Configuration > QoS > General** > **Queue** to open this screen.

Figure 160 Configuration > QoS > General > Queue



The following table describes the labels in this screen.

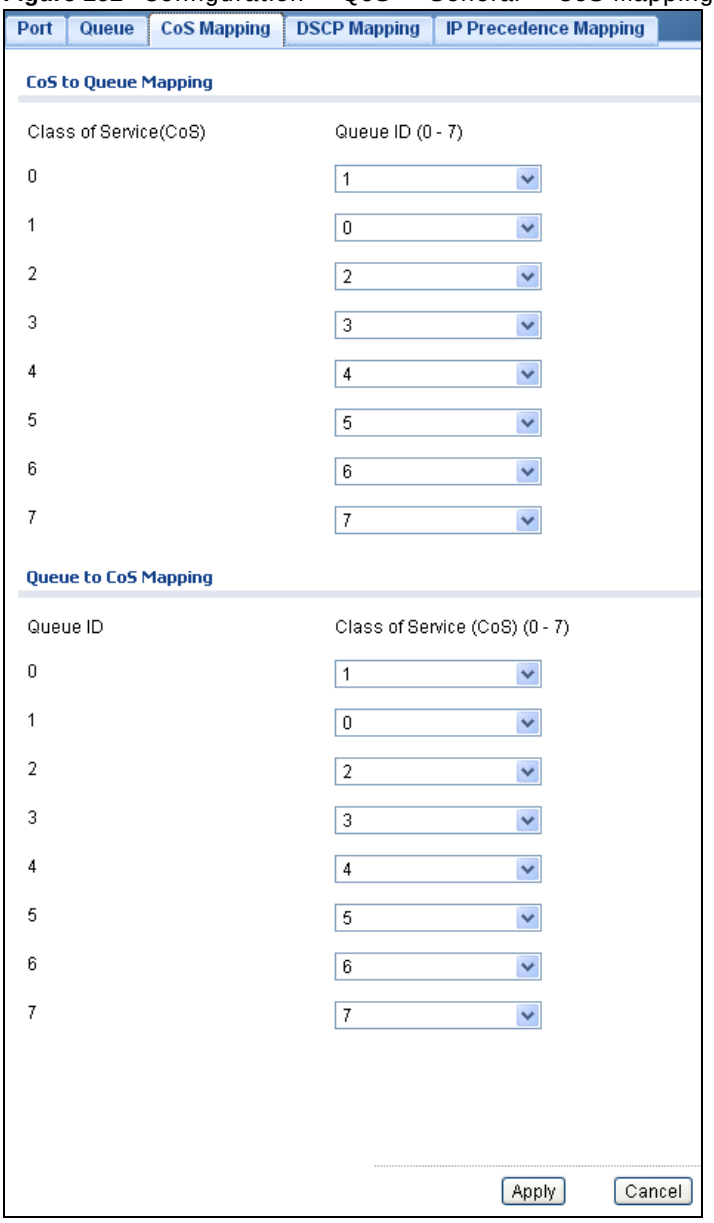
Table 127 Configuration > QoS > General > Queue

LABEL	DESCRIPTION
QoS Queue	
Queue ID	Displays the **Queue ID** value.
Schedule Algorithm	Select the **Schedule Algorithm** as **Strict** or **WRR**.
Weight (1-127)	Enter the weight of the QoS item.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

27.2.4 The CoS Mapping Screen

Use this screen to configure the **Cos Mapping** settings. Click **Configuration** > **QoS** > **General** > **CoS Mapping** to open this screen.

Figure 161 Configuration > QoS > General > CoS Mapping



The following table describes the labels in this screen.

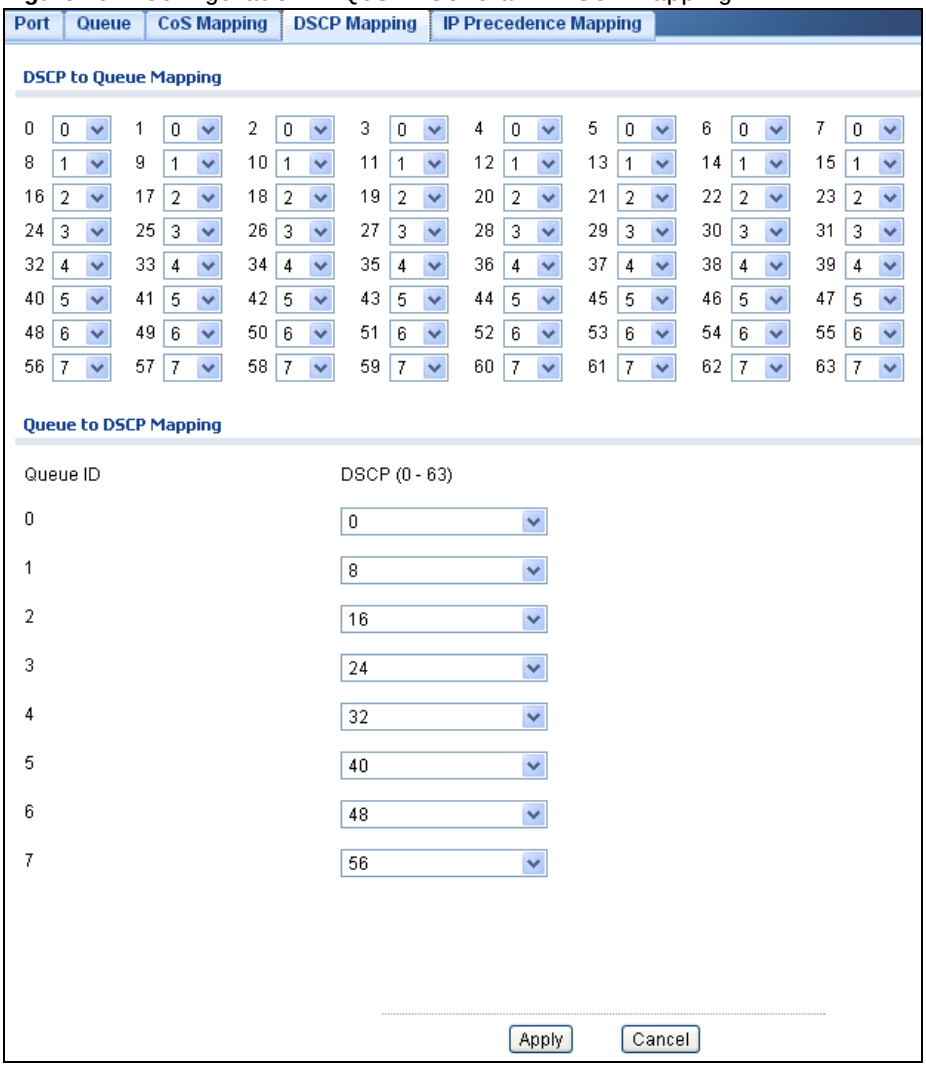
Table 128 Configuration > QoS > General > CoS Mapping

LABEL	DESCRIPTION
CoS to Queue Mapping	
Class of Service (CoS)	Displays a listing of the CoS, range: 0 - 7.
Queue ID (0-7)	Click the drop-down menu to map the CoS to a specific Queue ID.
Queue to CoS Mapping	
Queue ID	Displays a listing of the Queue ID, range: 0 - 7.
Class of Service (CoS) (0-7)	Click the drop-down menu to map the Queue ID to a specific CoS.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

27.2.5 The DSCP Mapping Screen

Use this screen to configure the **DSCP Mapping** settings. Click **Configuration** > **QoS** > **General** > **DSCP Mapping** to open this screen.

Figure 162 Configuration > QoS > General > DSCP Mapping



The following table describes the labels in this screen.

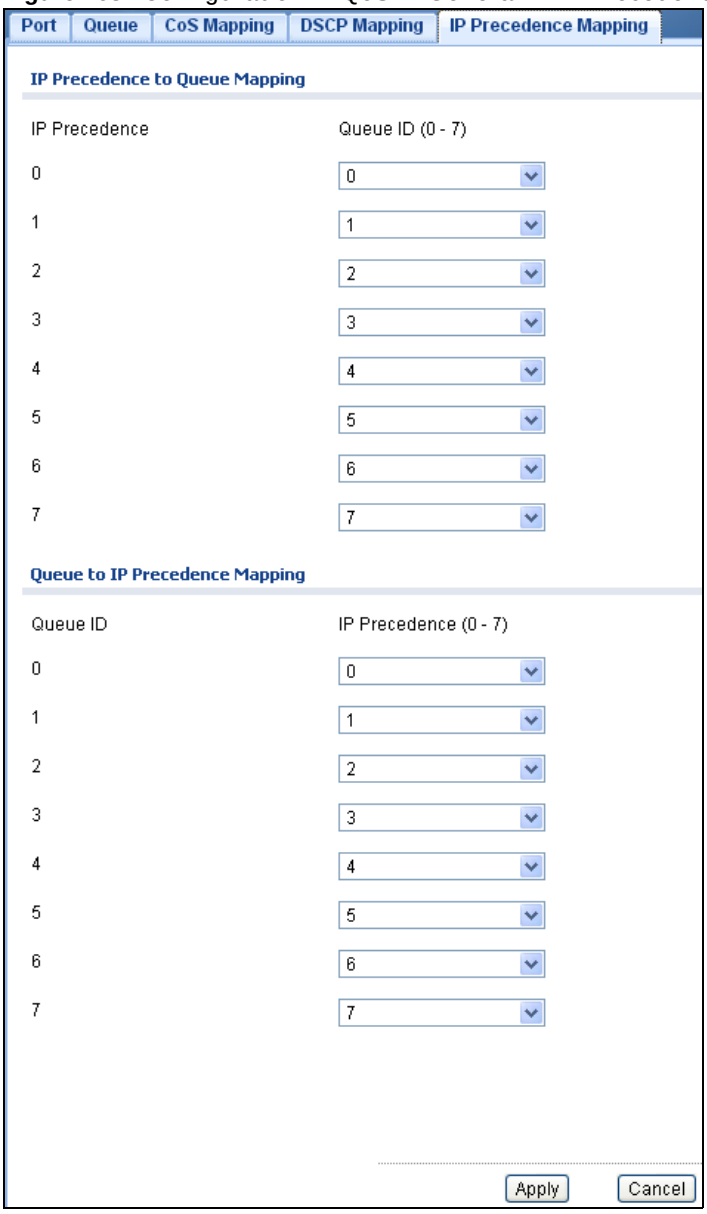
Table 129 Configuration > QoS > General > DSCP Mapping

LABEL	DESCRIPTION
DSCP to Queue Mapping	
Queue ID	Displays the DSCP **Queue ID** value.
Queue to DSCP Mapping	
DSCP (0-63)	Select the DSCP mapping value from the dropdown list.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

27.2.6 The IP Precedence Mapping Screen

Use this screen to configure the **IP Precedence Mapping** settings. Click **Configuration** > **QoS** > **General > IP Precedence Mapping** to open this screen.

Figure 163 Configuration > QoS > General > IP Precedence Mapping



The following table describes the labels in this screen.

Table 130 Configuration > QoS > General > IP Precedence Mapping

LABEL	DESCRIPTION
IP Precedence to Queue Mapping	
IP Precedence	Displays a listing of IP Precedence, range: 0 - 7.
Queue ID (0-7)	Click the drop-down menu to map an IP Precedence designation to a specific Queue ID (0 - 7).

Table 130 Configuration > QoS > General > IP Precedence Mapping (continued)

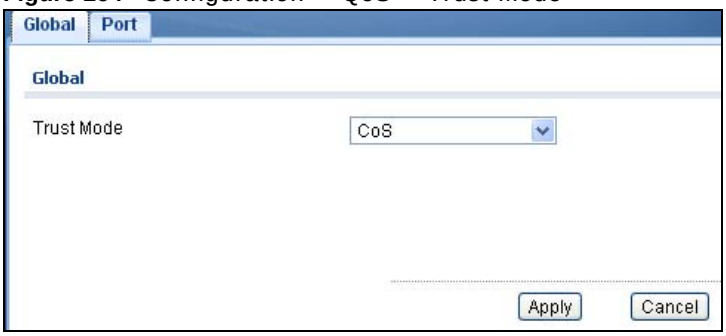
LABEL	DESCRIPTION
Queue to IP Precedence Mapping	
Queue ID	Displays a listing of Queue ID, range: 0 - 7.
IP Precedence (0-7)	Click the drop-down menu to map a Queue ID to a specific IP precedence.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

27.3 Trust Mode

27.3.1 The Global Screen

Use this screen to view the **Global** settings. Click **Configuration > QoS** > **Trust Mode** to open this screen.

Figure 164 Configuration > QoS > Trust Mode



The following table describes the labels in this screen.

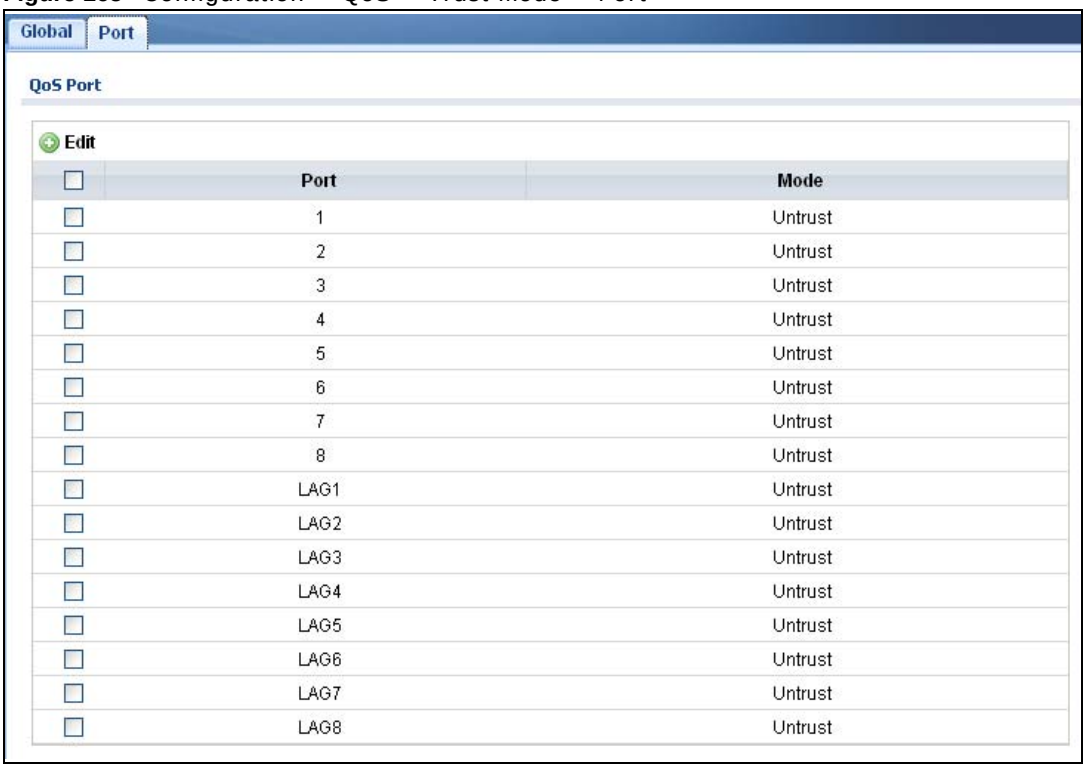
Table 131 Configuration > QoS > Trust Mode

LABEL	DESCRIPTION
Global	
Trust Mode	Select the **Trust Mode** from the dropdown list.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

27.3.2 The Port Screen

Use this screen to view the **Port** settings. Click **Configuration > QoS** > **Trust Mode > Port** to open this screen.

Figure 165 Configuration > QoS > Trust Mode > Port



The following table describes the labels in this screen.

Table 132 Configuration > QoS > Trust Mode > Port

LABEL	DESCRIPTION
QoS Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index value.
Mode	Displays the Trust status as **Trust** or **Untrust**.

27.3.3 The Trust Mode Edit Screen

Use this screen to configure the **Trust Mode** settings. Click **Configuration > QoS > Trust Mode > Port** > **Edit** to open this screen.

Figure 166 Configuration > QoS > Trust Mode > Port > Edit

The following table describes the labels in this screen.

Table 133 Configuration > QoS > Trust Mode > Port > Edit

LABEL	DESCRIPTION
QoS Port Trust Edit	
Port List	Displays the port index value(s).
Mode	Select the **Trust Mode** for the QoS port list as **Trust** or **Untrust**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28

Configuration: Security

28.1 Overview

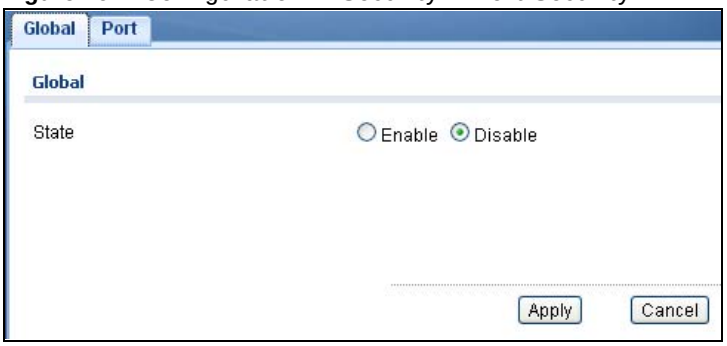
This section provides information for **Security** in **Configuration.**

28.2 Port Security

28.2.1 The Global Screen

Use this screen to view the **Global** settings. Click **Configuration > Security** > **Port Security** to open this screen.

Figure 167 Configuration > Security > Port Security



The following table describes the labels in this screen.

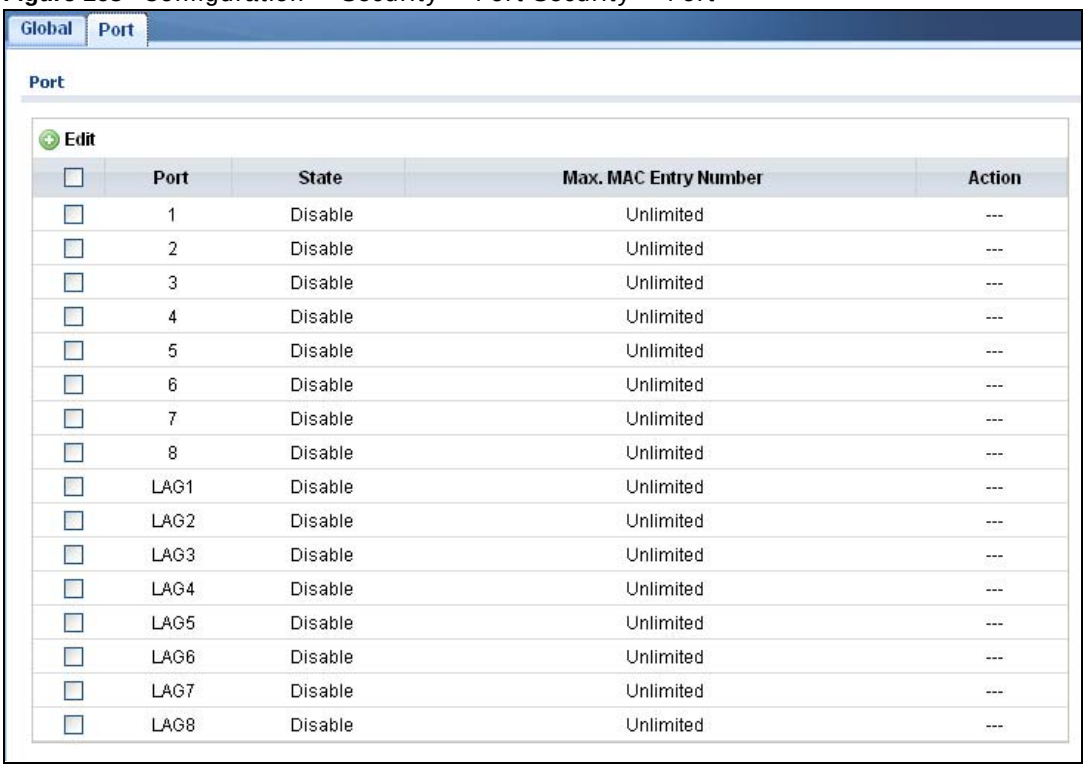
Table 134 Configuration > Security > Port Security

LABEL	DESCRIPTION
Global	
State	Select the global security setting to be enabled or disabled.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28.2.2 The Port Screen

Use this screen to view the **Port** settings. Click **Configuration > Security** > **Port Security > Port** to open this screen.

Figure 168 Configuration > Security > Port Security > Port



The following table describes the labels in this screen.

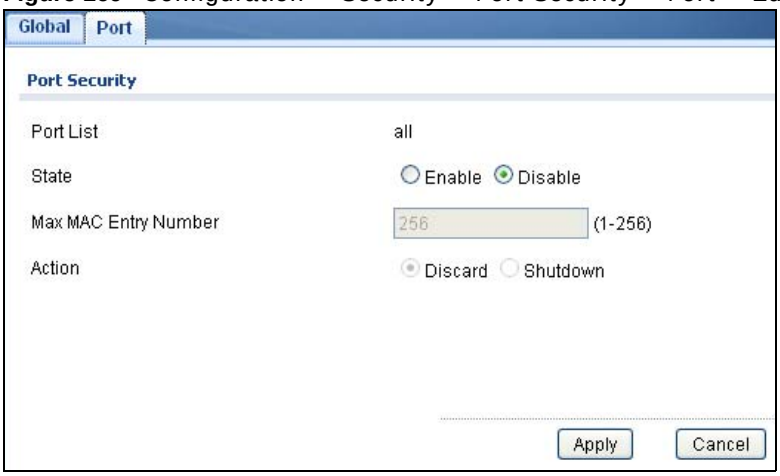
Table 135 Configuration > Security > Port Security > Port

LABEL	DESCRIPTION
Port	
Edit	Click **Edit** change the properties of the port.
Port	Displays the port index value.
State	Displays the Trust status as **Enable**/**Disable**.
Max. MAC Entry Number	Displays the designated maximum number of allowed MAC entries. The maximum MAC entry number can be learned for individual ports.
Action	Displays the **Action** as **Discard** or **Shutdown**.

28.2.3 The Port Edit Screen

Use this screen to configure the **Port** settings. Click **Configuration > Security** > **Port Security > Port > Edit** to open this screen.

Figure 169 Configuration > Security > Port Security > Port > Edit



The following table describes the labels in this screen.

Table 136 Configuration > Security > Port Security > Port > Edit

LABEL	DESCRIPTION
Port Security Edit	
Edit	Click **Edit** change the properties of the port.
Port List	Displays the port index value.
State	Select **Enable** or **Disable** for the Trust status.
Max. MAC Entry Number	Enter the maximum MAC entry number (maximum MAC entry number can be learned for individual ports).
Action	Select the **Action** as **Discard** or **Shutdown**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28.3 Protected Port

28.3.1 The Protected Port Screen

Use this screen to view the **Port** settings. Click **Configuration** > **Security** > **Protected Port** to open this screen.

Figure 170 Configuration > Security > Protected Port

The following table describes the labels in this screen.

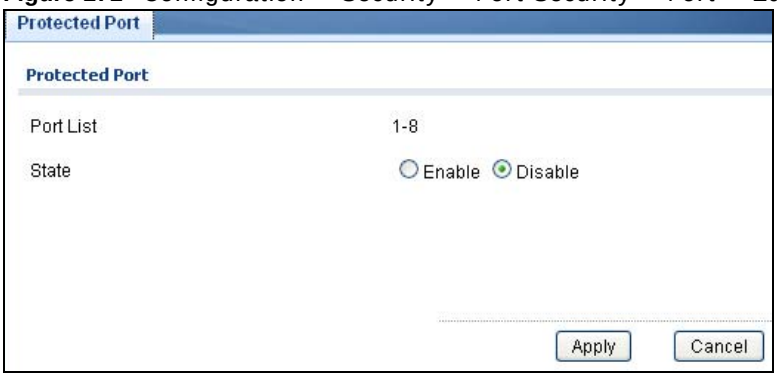
Table 137 Configuration > Security > Protected Port

LABEL	DESCRIPTION
Protected Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index value.
State	Displays the Trust status as **Enable**/**Disable**.

28.3.2 The Protected Port Edit Screen

Use this screen to configure the **Port** settings. Click **Configuration > Security** > **Port Security > Port > Edit** to open this screen.

Figure 171 Configuration > Security > Port Security > Port > Edit



The following table describes the labels in this screen.

Table 138 Configuration > Security > Port Security > Port > Edit

LABEL	DESCRIPTION
Protected Port	
Port List	Displays the port list index value(s).

Table 138 Configuration > Security > Port Security > Port > Edit (continued)

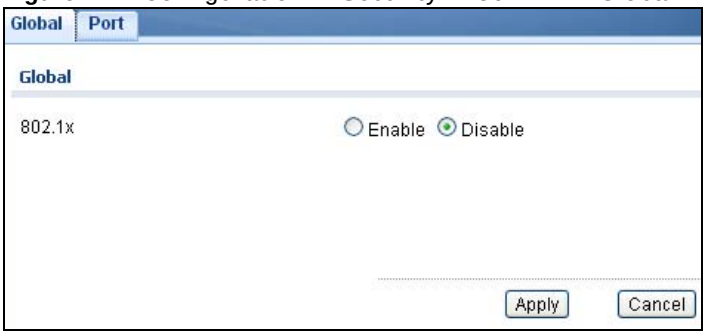
LABEL	DESCRIPTION
State	Select **Enable** or **Disable** for the **Protected Port** status.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28.4 802.1X

28.4.1 The Global Screen

Use this screen to view the **Global** settings. Click **Configuration > Security** > **802.1X** > **Global** to open this screen.

Figure 172 Configuration > Security > 802.1X > Global



The following table describes the labels in this screen.

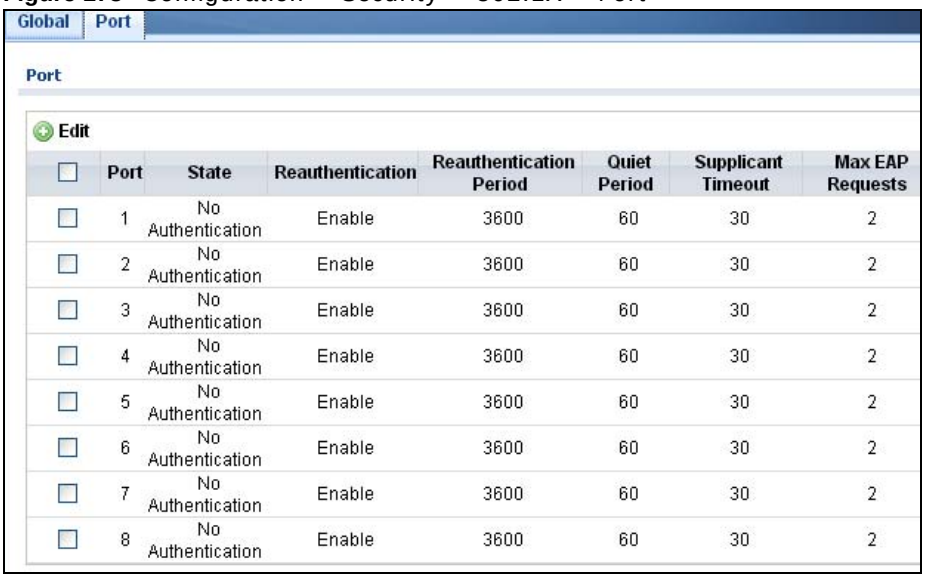
Table 139 Configuration > Security > 802.1X > Global

LABEL	DESCRIPTION
Global	
802.1X	Select the 802.1X security setting to be enabled or disabled.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28.4.2 The Port Screen

Use this screen to view the **Port** settings. Click **Configuration > Security** > **802.1X > Port** to open this screen.

Figure 173 Configuration > Security > 802.1X > Port



Port	State	Reauthentication	Reauthentication Period	Quiet Period	Supplicant Timeout	Max EAP Requests
1	No Authentication	Enable	3600	60	30	2
2	No Authentication	Enable	3600	60	30	2
3	No Authentication	Enable	3600	60	30	2
4	No Authentication	Enable	3600	60	30	2
5	No Authentication	Enable	3600	60	30	2
6	No Authentication	Enable	3600	60	30	2
7	No Authentication	Enable	3600	60	30	2
8	No Authentication	Enable	3600	60	30	2

The following table describes the labels in this screen.

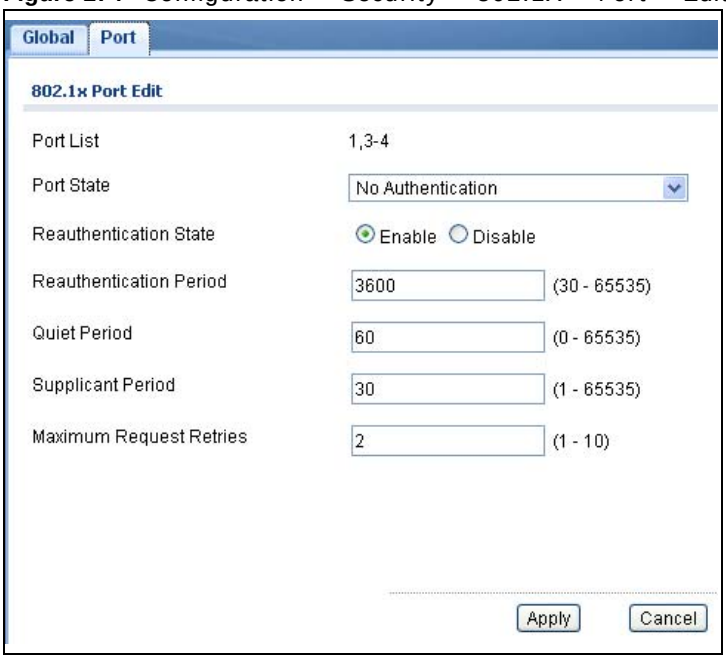
Table 140 Configuration > Security > 802.1X > Port

LABEL	DESCRIPTION
Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.
Port	Displays the port index value.
State	Displays the Trust status as enabled or disabled.
Reauthentication	Displays if Reauthentication function is enabled. If enabled, the subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Period	Displays the Reauthentication period for the function: the period of time ften a client has to re-enter his or her username and password to stay connected to the port.
Quiet Period	Display the time out period to transmit request after receiving a rejection from the sever.
Supplicant Time out	Display the time out period to transmit a request when the client does not responsed.
Max EAP Requests	Enter the maximum number of request retries.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28.4.3 The Port Edit Screen

Use this screen to configure the **Port** settings. Click **Configuration > Security** > **802.1X > Port > Edit** to open this screen.

Figure 174 Configuration > Security > 802.1X > Port > Edit



The following table describes the labels in this screen.

Table 141 Configuration > Security > 802.1X > Port > Edit

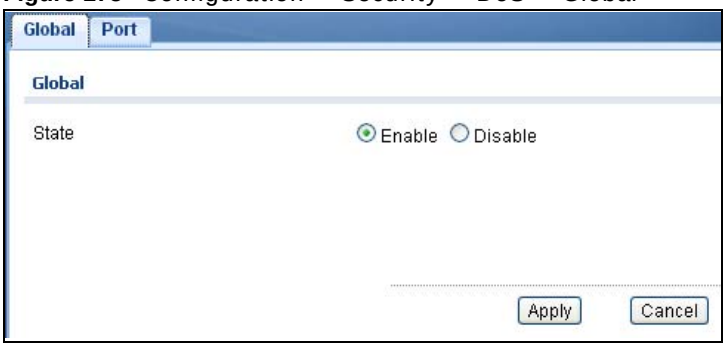
LABEL	DESCRIPTION
802.1X Port Edit	
Port List	Displays the port index value.
Port State	Displays the Trust status as enabled or disabled.
Reauthentication State	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port. Select **Enable** to activate feature.
Reauthentication Period	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Quiet Period	Display the time out period to transmit request after receiving a rejection from the sever.
Supplicant Period	Display the time out period to transmit a request when the client does not responsed.
Maximum Request Retries	Enter the maximum number of request retries.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28.5 DoS

28.5.1 The Global Screen

Use this screen to view the **Global** settings. Click **Configuration > Security** > **DoS** > **Global** to open this screen.

Figure 175 Configuration > Security > DoS > Global



The following table describes the labels in this screen.

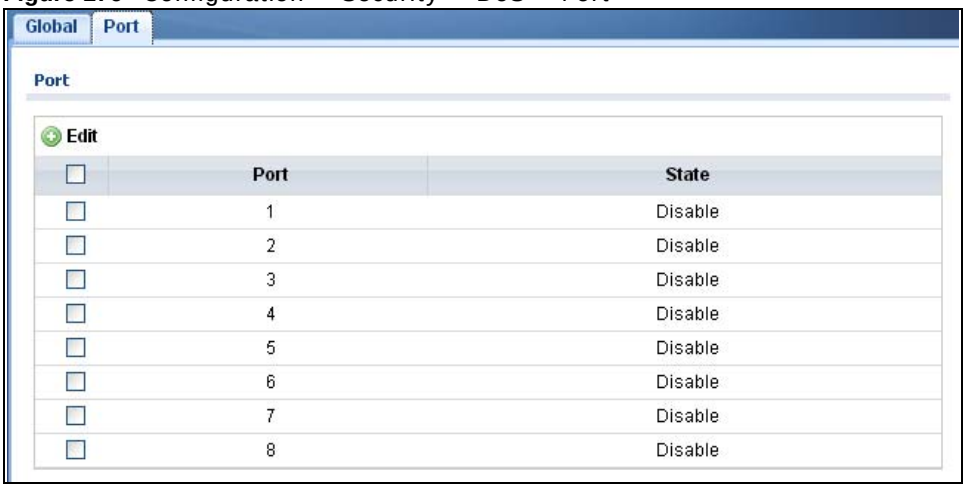
Table 142 Configuration > Security > DoS > Global

LABEL	DESCRIPTION
Global	
State	Select the DoS security setting to be enabled or disabled.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

28.5.2 The Port Screen

Use this screen to view the **Port** settings. Click **Configuration > Security** > **DoS > Port** to open this screen.

Figure 176 Configuration > Security > DoS > Port



The following table describes the labels in this screen.

Table 143 Configuration > Security > DoS > Port

LABEL	DESCRIPTION
Port	
Edit	Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port.

Table 143 Configuration > Security > DoS > Port

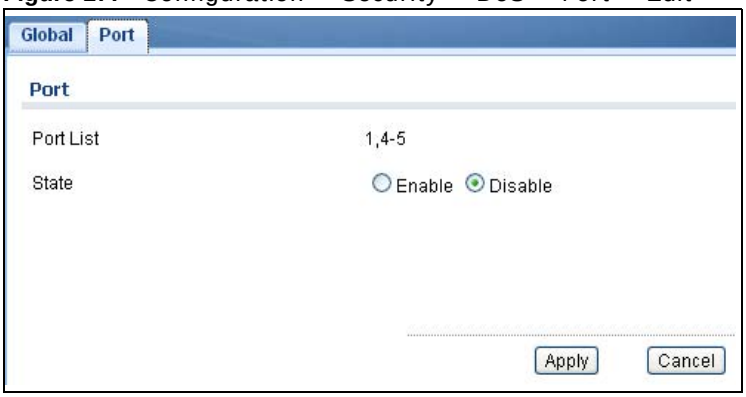
LABEL	DESCRIPTION
Port	Displays the port index value.
State	Displays the port's DoS feature as **Enable** or **Disable**.

28.5.3 The Port Edit Screen

Use this screen to configure the **Port** settings.

Click **Configuration > Security** > **DoS > Port > Edit** to open this screen.

Figure 177 Configuration > Security > DoS > Port > Edit



The following table describes the labels in this screen.

Table 144 Configuration > Security > DoS > Port > Edit

LABEL	DESCRIPTION
Port	
Port List	Displays the port index value.
State	Select **Enable** to activate the port's DoS feature.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

29

Configuration: AAA

29.1 Overview

This section provides information for **AAA** in **Configuration.**

Use the **AAA** screens to configure authentication, authorization and accounting settings on the Switch.

29.2 Auth Method

Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users.

29.2.1 The Auth Method Screen

Use this screen to view the **Auth Method** settings. Click **Configuration** > **AAA** > **Auth Method** to open this screen.

Figure 178 Configuration > AAA > Auth Method

The following table describes the labels in this screen.

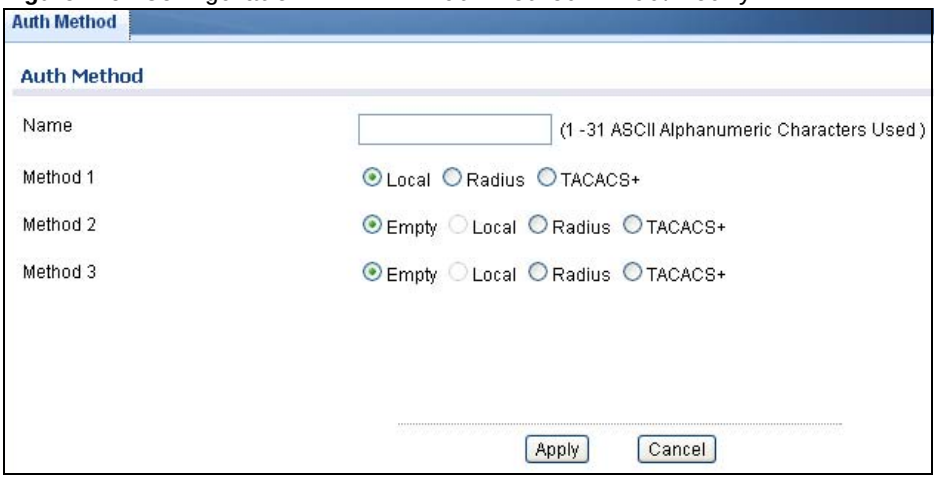
Table 145 Configuration > AAA > Auth Method

LABEL	DESCRIPTION
Auth Method	
Add	Click **Add** to create a new **Auth Method** entry.
Name	Displays the authentication method name. The name can be between 1 and 31 ASCII Alphanumeric Characters.
Method List	Displays the list of authentication methods as being **Local** or **Radius** or **TACACS+**.
Modify	Click the **Modify** button to change the configuration settings for a VLAN entry.

29.2.2 The Auth Method Add/Modify Screen

Use this screen to configure the **Auth Method** settings. Click **Configuration** > **AAA** > **Auth Method** > **Add/Modify** to open this screen.

Figure 179 Configuration > AAA > Auth Method > Add/Modify



The following table describes the labels in this screen.

Table 146 Configuration > AAA > Auth Method > Add/Modify

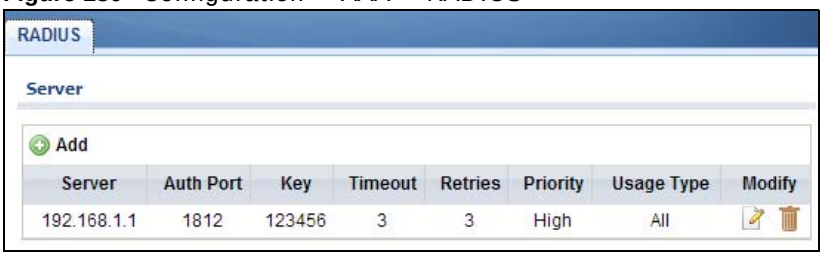
LABEL	DESCRIPTION
Auth Method	
Name	Enter the authentication method name. The name can be between 1 and 31 ASCII Alphanumeric Characters.
Method 1	Select the first authentication method as being **Local**, **Radius**, or **TACACS+**.
Method 2	Select the second authentication method as being **Empty**, **Local**, **Radius**, or **TACACS+**.
Method 3	Select the third authentication method as being **Empty**, **Local**, **Radius**, or **TACACS+**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

29.3 RADIUS

29.3.1 The RADIUS Screen

Use this screen to configure the **RADIUS** settings. Click **Configuration** > **AAA** > **RADIUS** to open this screen.

Figure 180 Configuration > AAA > RADIUS



The following table describes the labels in this screen.

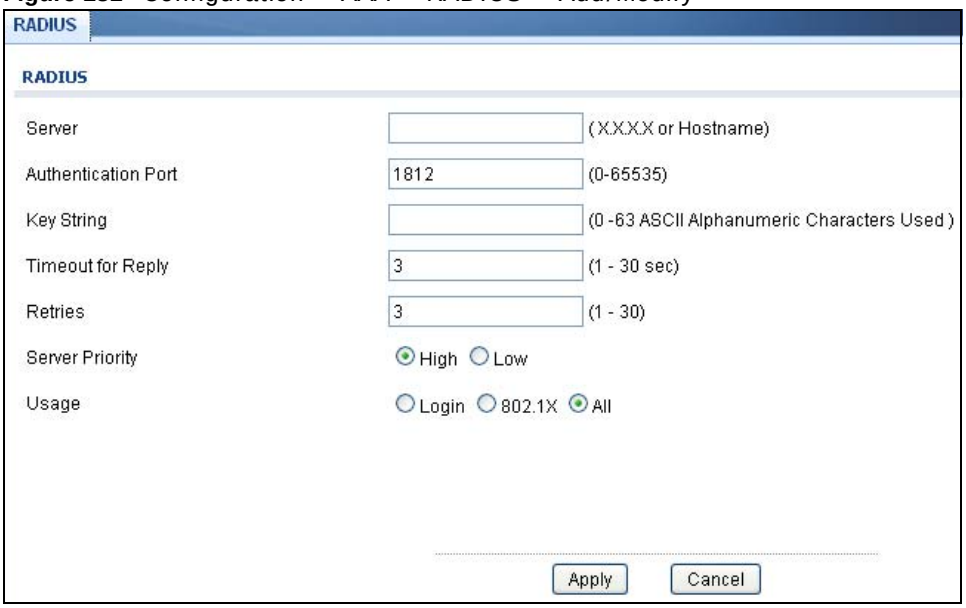
Table 147 Configuration > AAA > RADIUS

LABEL	DESCRIPTION
Server	
Add	Click **Add** to create a new **Server** entry.
Server	Displays the server name(s) as an IP address or a domain name.
Auth Port	Displays the authentication port number(s) as a value between 0 and 65535.
Key	Displays the authentication key.
Time out	Displays the number of time outs for replies. The value can be between 1 and 30 seconds.
Retries	Displays the number of retries. The value can be between 1 and 30.
Priority	Displays the server priority as **High** or **Low**.
Usage Type	Displays the server usage type as **Login**, **802.1X**, or **All**.
Modify	
Edit	Click to **Edit** modify the entry.
Modify	Click **Delete** to delete the entry.

29.3.2 The RADIUS Add/Modify Screen

Use this screen to configure the **RADIUS** settings. Click **Configuration** > **AAA** > **RADIUS** > **Add/Modify** to open this screen.

Figure 181 Configuration > AAA > RADIUS > Add/Modify



The following table describes the labels in this screen.

Table 148 Configuration > AAA > RADIUS > Add/Modify

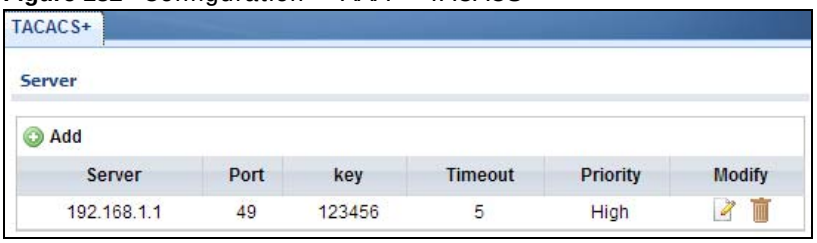
LABEL	DESCRIPTION
RADIUS	
Server	Enter the server name(s) as an IP address or a domain name.
Authentication Port	Enter the authentication port number(s) as a value between 0 and 65535.
Key String	Enter the authentication key string: 0 - 63 ASCII Alphanumeric Characters.
Timeout for Reply	Enter the number of time outs for replies. The value can be between 1 and 30 seconds.
Retries	Enter the number of retries. The value can be between 1 and 30.
Server Priority	Select the server priority as **High** or **Low**.
Usage	Select the server usage type as **Login**, **802.1X**, or **All**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

29.4 TACACS+

29.4.1 The TACACS+ Screen

Use this screen to configure the **TACACS+** settings. Click **Configuration** > **AAA** > **TACACS+** to open this screen.

Figure 182 Configuration > AAA > TACACS+



The following table describes the labels in this screen.

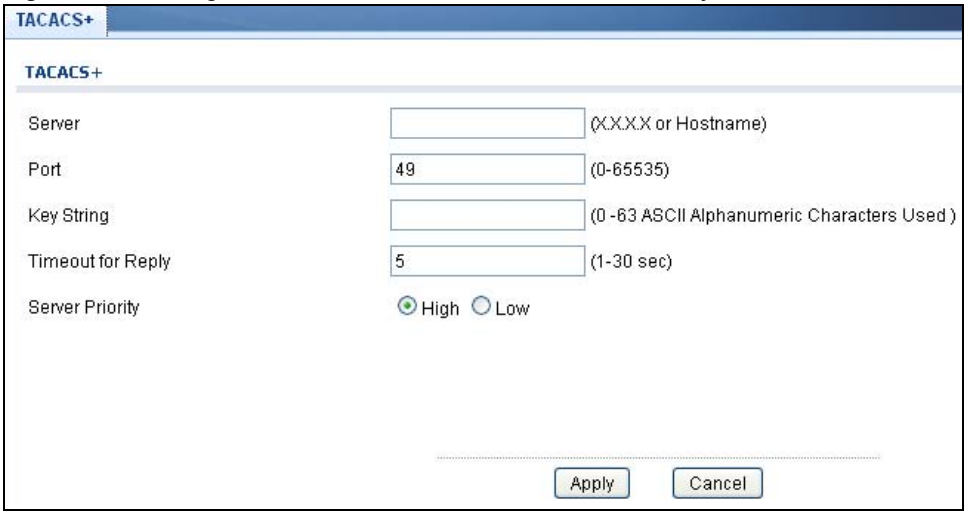
Table 149 Configuration > AAA > TACACS+

LABEL	DESCRIPTION
Server	
Add	Click **Add** to create a new **Server** entry.
Server	Displays the server name(s) as an IP address or a domain name.
Port	Displays the port number(s) as a value between 0 and 65535.
Key	Displays the authentication key.
Timeout	Displays the number of time outs for replies. The value can be between 1 and 30 seconds.
Priority	Displays the priority as **High** or **Low**.
Modify	
Edit	Click to **Edit** modify the entry.
Modify	Click **Delete** to delete the entry.

29.4.2 The TACACS+ Add/Modify Screen

Use this screen to configure the **TACACS+** settings. Click **Configuration** > **AAA** > **TACACS+** > **Add / Modify** to open this screen.

Figure 183 Configuration > AAA > TACACS+ > Add/Modify



The following table describes the labels in this screen.

Table 150 Configuration > AAA > TACACS+ > Add/Modify

LABEL	DESCRIPTION
TACACS+	
Server	Enter the server name(s) as an IP address or a domain name.
Port	Enter the port number(s) as a value between 0 and 65535.
Key String	Enter the authentication key string: 0 - 63 ASCII alphanumeric characters.
Timeout for Reply	Enter the number of time outs for replies. The value can be between 1 and 30 seconds.
Priority	Select the server priority as **High** or **Low**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30

Configuration: Management

30.1 Overview

This section provides information for **Management** in **Configuration.**

Use the **Management** screens to configure settings on the Switch. The following submenus are accessed from this section: **Syslog**, **SNMP**, **Error Disable**, **HTTP/HTTPS**, **Users**, **Remote Access Control**.

30.2 Syslog

30.2.1 The Global Screen

Use this screen to view the **Global** settings. Click **Configuration** > **Management** > **Syslog** to open this screen.

Figure 184 Configuration > Management > Syslog

The following table describes the labels in this screen.

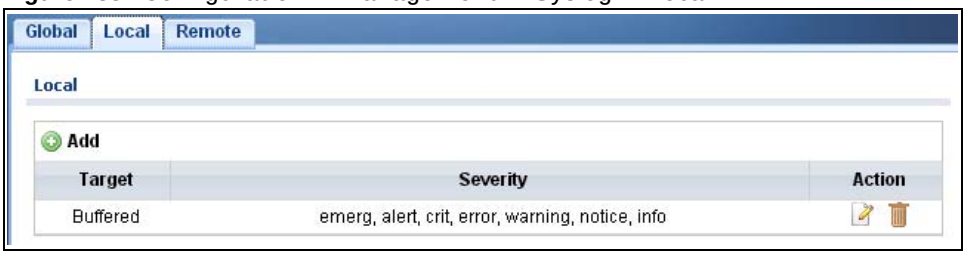
Table 151 Configuration > Management > Syslog

LABEL	DESCRIPTION
Global	
State	Select the global logging setting to be enabled or disabled.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.2.2 The Local Screen

Use this screen to view the **Local** settings. Click **Configuration** > **Management** > **Syslog** > **Local** to open this screen.

Figure 185 Configuration > Management > Syslog > Local



The following table describes the labels in this screen.

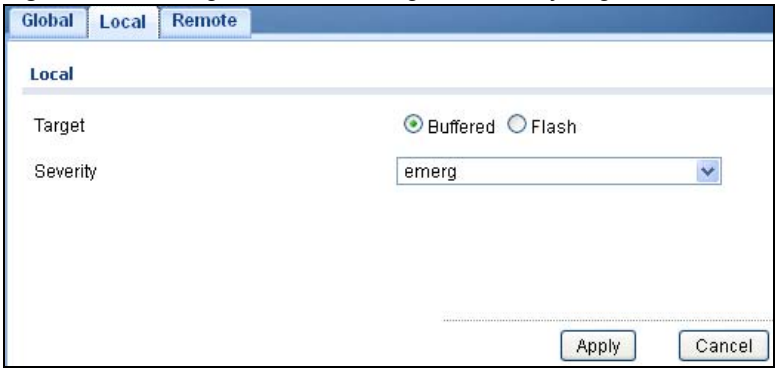
Table 152 Configuration > Management > Syslog > Local

LABEL	DESCRIPTION
Local	
Add	Click **Add** to create a new **Local** entry.
Target	Displays the local storage target for logging messages. The options are **Buffered** or **Flash**.
Severity	Displays the severity level of messages to be written to logs.
Action	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

30.2.3 The Local Add/Modify Screen

Use this screen to configure the **Local** settings. Click **Configuration** > **Management** > **Syslog** > **Local** > **Add/Modify** to open this screen.

Figure 186 Configuration > Management > Syslog > Local > Add/Modify



The following table describes the labels in this screen.

Table 153 Configuration > Management > Syslog > Local > Add/Modify

LABEL	DESCRIPTION
Local Add	
Target	Select the local storage target for logging messages. The options are **Buffered** or **Flash**.

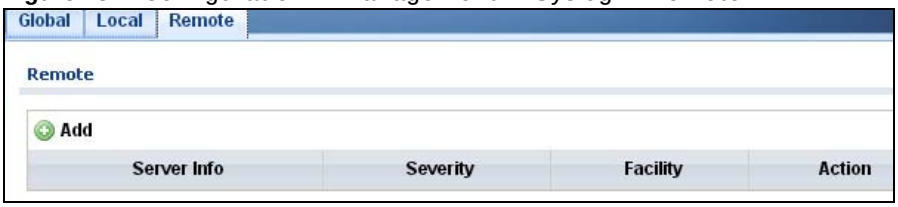
Table 153 Configuration > Management > Syslog > Local > Add/Modify (continued)

LABEL	DESCRIPTION
Severity	Select the severity level of messages to be written to logs.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.2.4 The Remote Screen

Use this screen to view the **Remote** settings. Click **Configuration** > **Management** > **Syslog** > **Remote** to open this screen.

Figure 187 Configuration > Management > Syslog > Remote



The following table describes the labels in this screen.

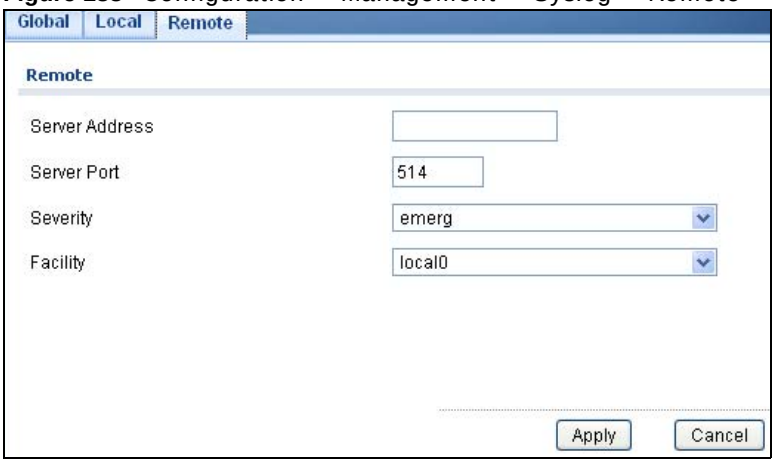
Table 154 Configuration > Management > Syslog > Remote

LABEL	DESCRIPTION
Local	
Add	Click **Add** to create a new **Remote** entry.
Server Info	Displays the server information which includes the server IP address and port number.
Severity	Displays the severity level of messages to be written to logs.
Facility	Displays the facility designation of the remote entry.
Action	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

30.2.5 The Remote Add/Modify Screen

Use this screen to configure the **Remote** settings. Click **Configuration** > **Management** > **Syslog** > **Remote** > **Add/Modify** to open this screen.

Figure 188 Configuration > Management > Syslog > Remote > Add/Modify



The following table describes the labels in this screen.

Table 155 Configuration > Management > Syslog > Remote > Add/Modify

LABEL	DESCRIPTION
Remote	
Server Address	Enter a server IP address or domain name.
Server Port	Enter a server port number.
Severity	Select the severity level of messages to be written to logs.
Facility	Select the facility from the dropdown list.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

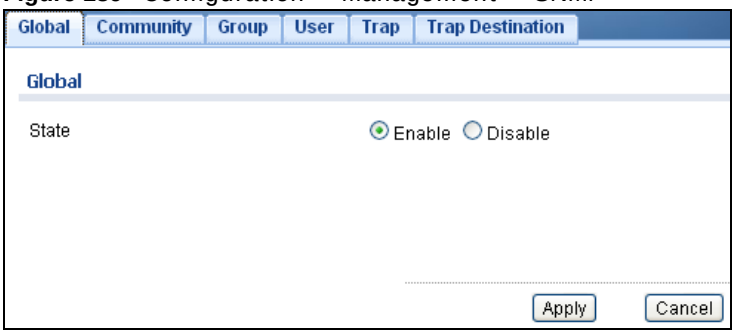
30.3 SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version 1 (SNMPv1), SNMP version 2c or Table 170 Access Control Overview Console Port SSH Telnet FTP Web SNMP One session Share up to nine sessions One session Up to five accounts No limit Chapter 42 Access Control 338 GS3700/ XGS3700 Series User's Guide SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

30.3.1 The Global Screen

Use this screen to view the **Global** settings. Click **Configuration** > **Management** > **SNMP** to open this screen.

Figure 189 Configuration > Management > SNMP



The following table describes the labels in this screen.

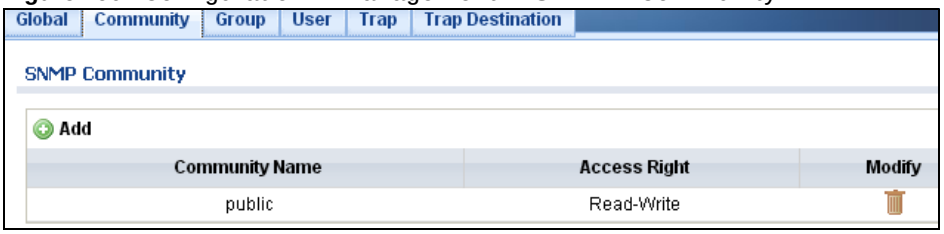
Table 156 Configuration > Management > SNMP

LABEL	DESCRIPTION
Global	
State	Select the global SNMP setting to be enabled or disabled.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.3.2 The Community Screen

Use this screen to view the **Community** settings. Click **Configuration** > **Management** > **SNMP** > **Community** to open this screen.

Figure 190 Configuration > Management > SNMP > Community



The following table describes the labels in this screen.

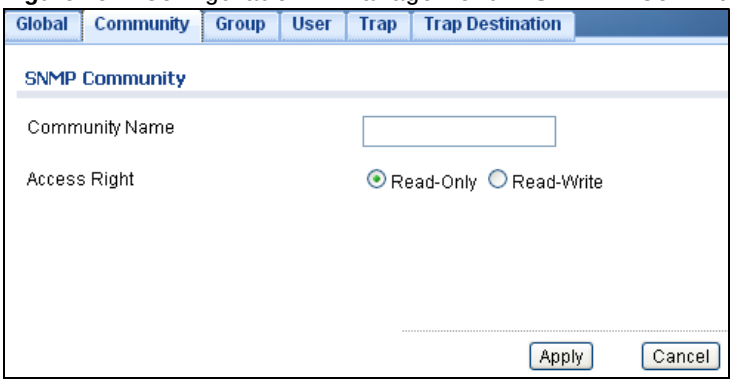
Table 157 Configuration > Management > SNMP > Community

LABEL	DESCRIPTION
SNMP community	
Add	Click **Add** to create a new **SNMP Community** entry.
Community Name	Displays a string identifying the community name that this entry should belong to. The allowed string length is 1 to 20, and the allowed content is ASCII characters from 33 to 126.
Access Right	Displays the access mode for this entry. The possible values are **Read-Only** and **Read-Write**.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

30.3.3 The Community Add/Modify Screen

Use this screen to configure the **Community** settings. Click **Configuration** > **Management** > **SNMP** > **Community** > **Add/Modify** to open this screen.

Figure 191 Configuration > Management > SNMP > Community > Add/Modify



The following table describes the labels in this screen.

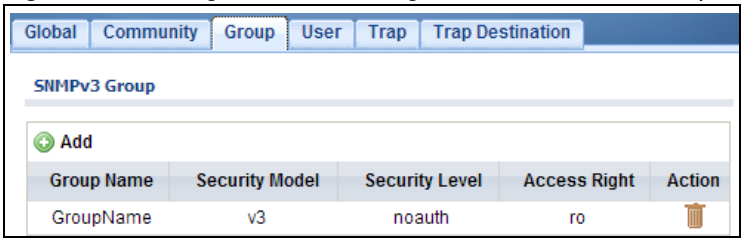
Table 158 Configuration > Management > SNMP > Community > Add/Modify

LABEL	DESCRIPTION
SNMP Community	
Community Name	Enter a string identifying the community name that this entry should belong to. The allowed string length is 1 to 20, and the allowed content is ASCII characters from 33 to 126.
Access Right	Select the access mode for this entry. The possible values are **Read-Only** and **Read-Write**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.3.4 The Group Screen

Use this screen to view the **Group** settings. Click **Configuration** > **Management** > **SNMP** > **Group** to open this screen.

Figure 192 Configuration > Management > SNMP > Group



The following table describes the labels in this screen.

Table 159 Configuration > Management > SNMP > Group

LABEL	DESCRIPTION
SNMPv3 Group	
Add	Click **Add** to create a new **SNMPv3 Group** entry.

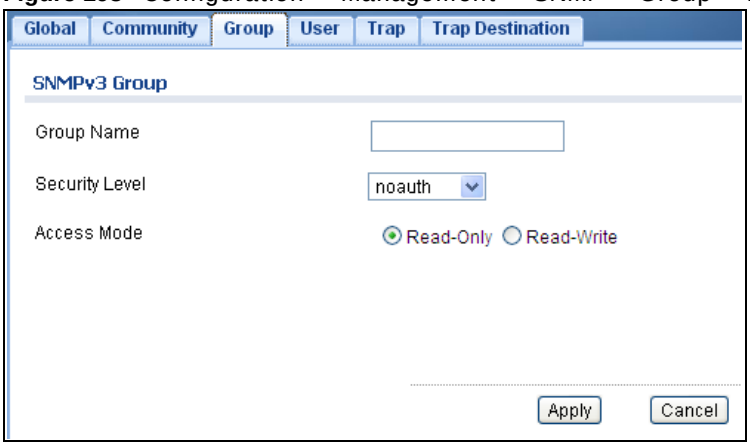
Table 159 Configuration > Management > SNMP > Group (continued)

LABEL	DESCRIPTION
Group Name	Displays a string identifying the group name that this entry should belong to. The allowed string length is 1 to 30, and the allowed content is ASCII characters from 33 to 126.
Security Model	Displays the security model that this entry belongs to. Possible security models are: • **any**: Any security model accepted(v1|v2c|usm). • **v1**: Reserved for SNMPv1. • **v2c**: Reserved for SNMPv2c. • **usm**: User-based Security Model (USM).
Security Level	Displays the security model that this entry belongs to. Possible security models are: • **NoAuth**, **NoPriv**: No authentication and no privacy. • **Auth**, **NoPriv**: Authentication and no privacy. • **Auth**, **Priv**: Authentication and privacy.
Access Right	Displays the access mode for this entry. The possible values are **Read Only** and **Read-Write**.
Action	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

30.3.5 The Group Add/Modify Screen

Use this screen to configure the **Group** settings. Click **Configuration** > **Management** > **SNMP** > **Group** > **Add / Modify** to open this screen.

Figure 193 Configuration > Management > SNMP > Group > Add/Modify



The following table describes the labels in this screen.

Table 160 Configuration > Management > SNMP > Group > Add/Modify

LABEL	DESCRIPTION
SNMPv3 Group Edit	
Group Name	Enter a string identifying the group name that this entry should belong to. The allowed string length is 1 to 30, and the allowed content is ASCII characters from 33 to 126.
Security Level	Select the security model that this entry belongs to. Possible security models are: • **NoAuth**, **NoPriv**: No authentication and no privacy. • **Auth**, **NoPriv**: Authentication and no privacy. • **Auth**, **Priv**: Authentication and privacy.
Access Right	Select the access mode for this entry. The possible values are **Read-Only** and **Read-Write**.

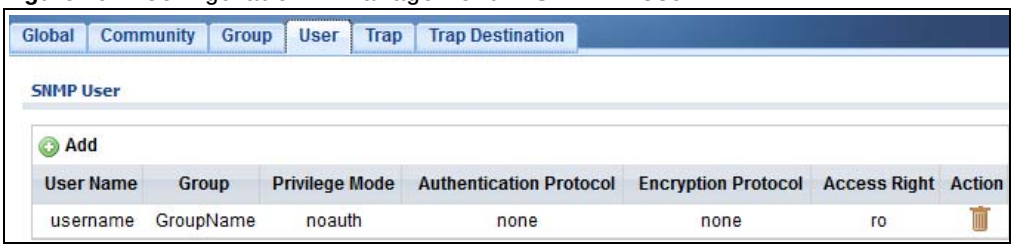
Table 160 Configuration > Management > SNMP > Group > Add/Modify (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.3.6 The User Screen

Use this screen to view the **User** settings. Click **Configuration** > **Management** > **SNMP** > **User** to open this screen.

Figure 194 Configuration > Management > SNMP > User



The following table describes the labels in this screen.

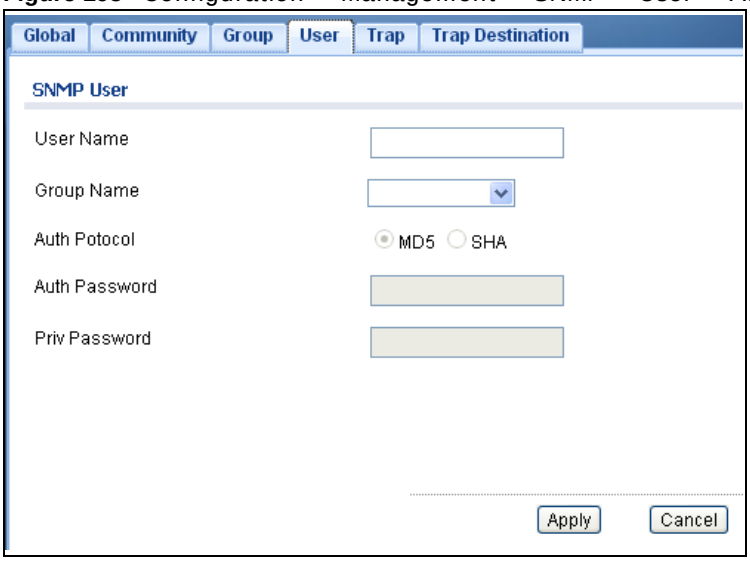
Table 161 Configuration > Management > SNMP > User

LABEL	DESCRIPTION
SNMP User	
Add	Click **Add** to create a new SNMP user.
User Name	Displays a string identifying the user name that this entry belongs to. The allowed string length is 1 to 30, and the allowed content is ASCII characters from 33 to 126.
Group	Displays a string identifying the group name that this entry belongs to. The allowed string length is 1 to 30, and the allowed content is ASCII characters from 33 to 126.
Privilege Mode	Displays the privilege mode that this entry belongs to.
Authentication Protocol	Displays the authentication protocol that this entry belongs to. Possible authentication protocols are: • **None**: No authentication protocol. • **MD5**: An optional flag to indicate that this user uses MD5 authentication protocol. • **SHA**: An optional flag to indicate that this user uses SHA authentication protocol. The value of the security level cannot be modified if the entry already exists. That means you must first ensure that the value is set correctly.
Encryption Protocol	Displays the encryption protocol that this entry belongs to.
Access Right	Displays the access mode for this entry. The possible values are **Read-Only** and **Read-Write**.
Action	
Delete	Click **Delete** to remove the entry.

30.3.7 The User Add/Modify Screen

Use this screen to configure the **User** settings. Click **Configuration** > **Management** > **SNMP** > **User** > **Add/Modify** to open this screen.

Figure 195 Configuration > Management > SNMP > User > Add/Modify



The following table describes the labels in this screen.

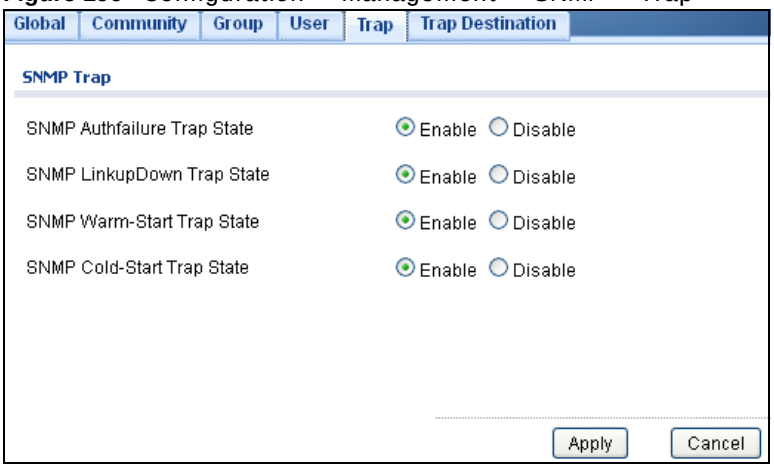
Table 162 Configuration > Management > SNMP > User > Add/Modify

LABEL	DESCRIPTION
SNMP User	
User Name	Enter a string identifying the user name that this entry belongs to. The allowed string length is 1 to 30, and the allowed content is ASCII characters from 33 to 126.
Group Name	Enter a string identifying the group name that this entry belongs to. The allowed string length is 1 to 30, and the allowed content is ASCII characters from 33 to 126.
Auth Protocol	Select the authentication protocol that this entry belongs to. Possible authentication protocols are: • **MD5**: An optional flag to indicate that this user uses MD5 authentication protocol. • **SHA**: An optional flag to indicate that this user uses SHA authentication protocol. The value of the security level cannot be modified if the entry already exists. That means you must first ensure that the value is set correctly.
Auth Password	Enter a string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 32. The allowed content is ASCII characters from 33 to 126.
Priv password	Enter a string identifying the privacy password phrase. The allowed string length is 8 to 64 and the allowed content is ASCII characters from 33 to 126.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.3.8 The Trap Screen

Use this screen to configure the **Trap** settings. Click **Configuration** > **Management** > **SNMP** > **Trap** to open this screen.

Figure 196 Configuration > Management > SNMP > Trap



The following table describes the labels in this screen.

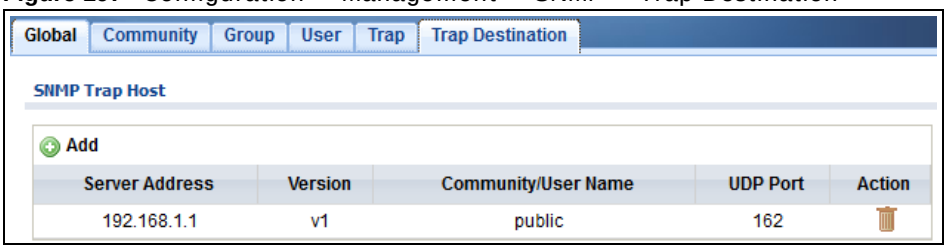
Table 163 Configuration > Management > SNMP > Trap

LABEL	DESCRIPTION
SNMP Trap	
SNMP Authfailure Trap State	Select 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.
SNMP LinkupDown Trap State	Select the SNMP trap link-up and link-down mode operation. Possible modes are: • **Enabled**: Enable SNMP trap link-up and link-down mode operation. • **Disabled**: Disable SNMP trap link-up and link-down mode operation.
SNMP Warm-Start Trap State	Reboot using software or hardware button reboot.
SNMP Cold-Start Trap State	Reboot though power off.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.3.9 The Trap Destination Screen

Use this screen to view the **Trap Destination** settings. Click **Configuration** > **Management** > **SNMP** > **Trap Destination** to open this screen.

Figure 197 Configuration > Management > SNMP > Trap Destination



The following table describes the labels in this screen.

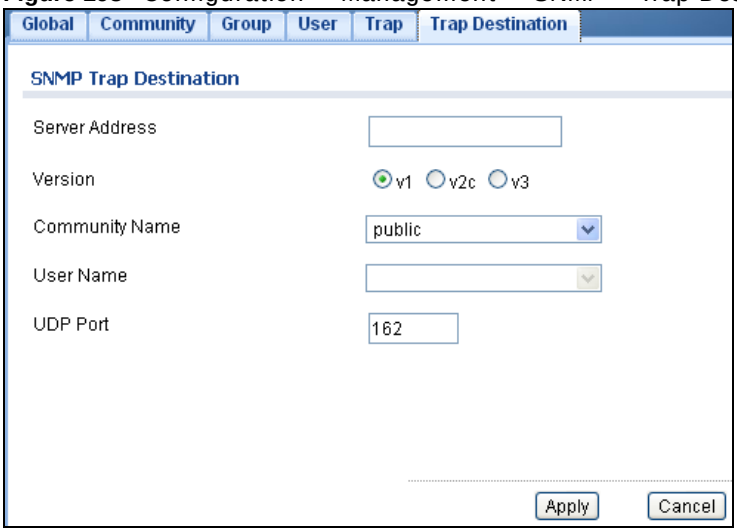
Table 164 Configuration > Management > SNMP > Trap Destination

LABEL	DESCRIPTION
SNMP Trap Host	
Add	Click **Add** to create a new **SNMP Trap Host** entry.
Server Address	Displays a string identifying the server address that this entry belongs to.
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.
Community/ User Name	Displays the community / user name that this entry belongs to.
UDP Port	Displays the trap use destination for the UDP port.
Action	
Delete	Click **Delete** to remove the entry.

30.3.10 The Trap Destination Add/Modify Screen

Use this screen to configure the **Trap Destination** settings. Click **Configuration** > **Management** > **SNMP** > **Trap Destination** > **Add / Modify** to open this screen.

Figure 198 Configuration > Management > SNMP > Trap Destination > Add/Modify



The following table describes the labels in this screen.

Table 165 Configuration > Management > SNMP > Trap Destination > Add/Modify

LABEL	DESCRIPTION
SNMP Trap Destination	
Server Address	Enter a string identifying the server address that this entry belongs to.
Version	Select 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.

Table 165 Configuration > Management > SNMP > Trap Destination > Add/Modify (continued)

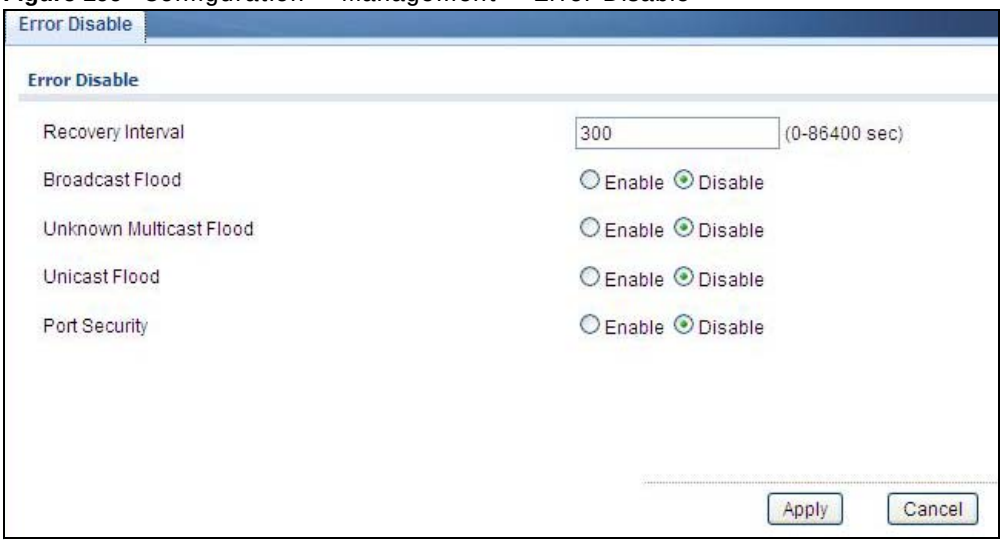
LABEL	DESCRIPTION
Community Name	Displays the community name that this entry belongs to.
User Name	Displays the user name that this entry belongs to.
UDP Port	Enter a UDP port for this entry.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.4 Error Disable

30.4.1 The Error Disabled Screen

Use this screen to configure the **Error Disabled** settings. Click **Configuration** > **Management** > **Error Disable** to open this screen.

Figure 199 Configuration > Management > Error Disable



The following table describes the labels in this screen.

Table 166 Configuration > Management > Error Disable

LABEL	DESCRIPTION
Error Disabled Settings	
Recovery Interval	Enter the recovery interval value.
Broadcast Flood	Select an option to **Enable** or **Disable** the Broadcast Flood.
Unknown Multicast Flood	Select an option to **Enable** or **Disable** the Unknown Multicast Flood.
Unicast Flood	Select an option to **Enable** or **Disable** the Unicast Flood.
Port Security	Select an option to **Enable** or **Disable** the Port Security.

Table 166 Configuration > Management > Error Disable

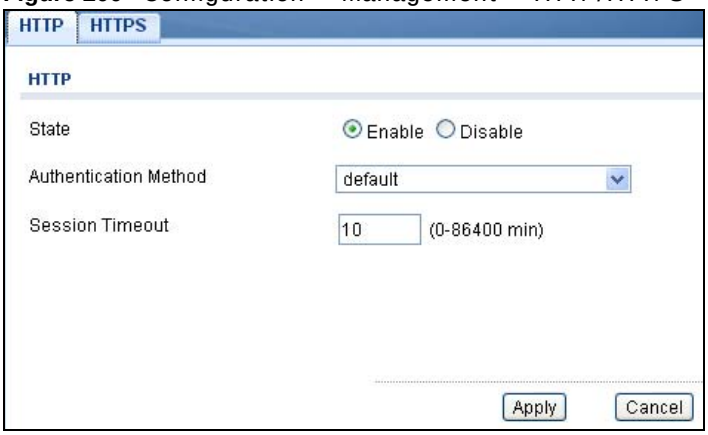
LABEL	DESCRIPTION
POE Inline Power	Select an option to **Enable** or **Disable** the POE Inline Power.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.5 HTTP/HTTPS

30.5.1 The HTTP Screen

Use this screen to configure the **HTTP** settings. Click **Configuration** > **Management** > **HTTP/HTTPS** to open this screen.

Figure 200 Configuration > Management > HTTP/HTTPS



The following table describes the labels in this screen.

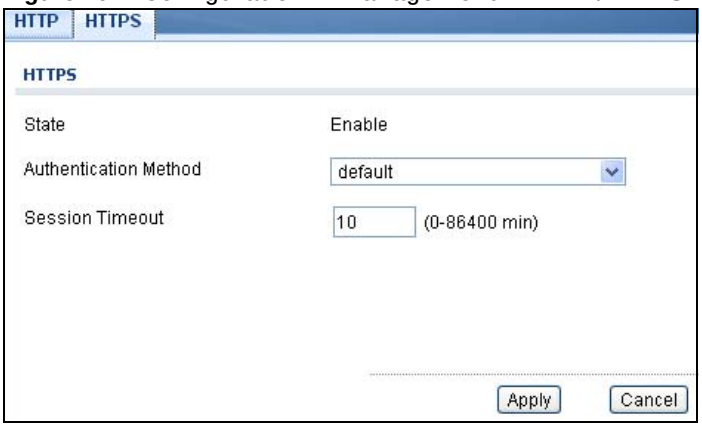
Table 167 Configuration > Management > HTTP/HTTPS

LABEL	DESCRIPTION
HTTP	
State	Select the HTTP mode operation. Possible modes are: • **Enabled**: Enable HTTP mode operation. • **Disabled**: Disable HTTP mode operation.
Authentication Method	Select the authentication method from the dropdown list.
Session Timeout	Enter the session timeout value. The timeout can be between 0 and 86400 minutes.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.5.2 The HTTPS Screen

Use this screen to configure the **HTTPS** settings. Click **Configuration** > **Management** > **HTTP/HTTPS** > **HTTPS** to open this screen.

Figure 201 Configuration > Management > HTTP/HTTPS > HTTPS



The following table describes the labels in this screen.

Table 168 Configuration > Management > HTTP/HTTPS > HTTPS

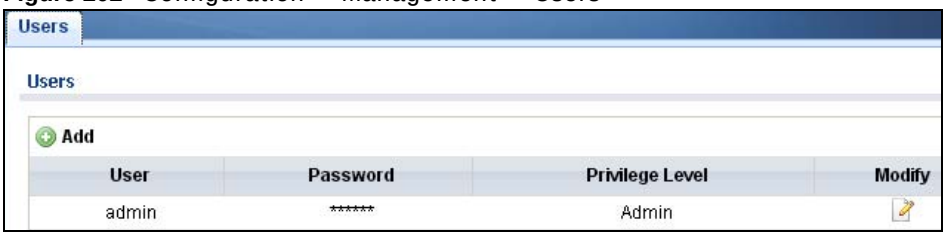
LABEL	DESCRIPTION
HTTPS	
State	Select the HTTPS mode operation. Possible modes are: • **Enabled**: Enable HTTPS mode operation.
Authentication Method	Select the authentication method from the dropdown list.
Session Timeout	Enter the session timeout value. The timeout can be between 0 and 86400 minutes.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.6 Users

30.6.1 The Users Screen

Use this screen to configure the **Users** settings. Click **Configuration** > **Management** > **Users** to open this screen.

Figure 202 Configuration > Management > Users



The following table describes the labels in this screen.

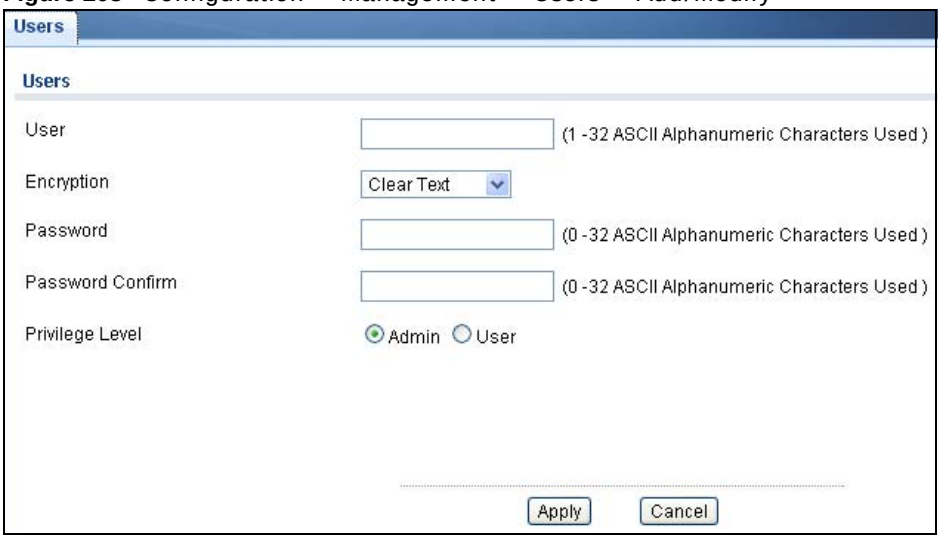
Table 169 Configuration > Management > Users

LABEL	DESCRIPTION
Users	
Add	Click **Add** to create a new **User** entry.
User	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32. The valid user name is a combination of letters, numbers and underscores.
Encryption	Displays the encryption status. The values can be **Clear Text**, **Encrypted**, and **No Password**.
Password	Displays the password of the user. The allowed string length is 0 to 32.
Privilege Level	Displays the privilege level of the user, range: admin and user.
Modify	
Edit	Click **Edit** to make changes to the entry.

30.6.2 The Users Add/Modify Screen

Use this screen to configure the **Users** settings. Click **Configuration** > **Management** > **Users** > **Add / Modify** to open this screen.

Figure 203 Configuration > Management > Users > Add/Modify



The following table describes the labels in this screen.

Table 170 Configuration > Management > Users > Add/Modify

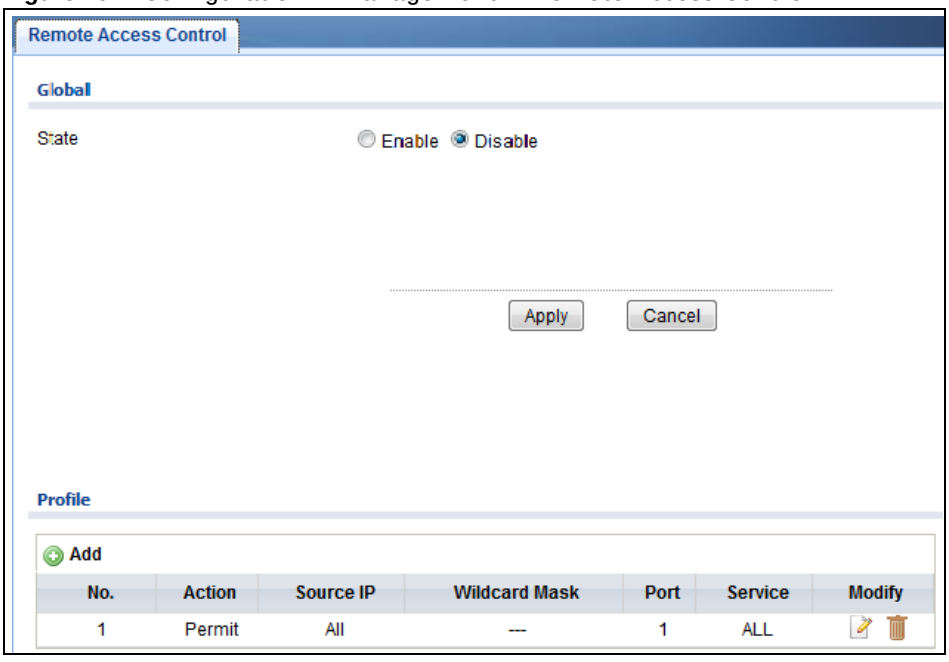
LABEL	DESCRIPTION
Add New Local User	
User	Enter a string identifying the user name that this entry should belong to. The allowed string length is 1 to 32. The valid user name is a combination of letters, numbers and underscores.
Encryption	Select the encryption type. The values can be **Clear Text**, **Encrypted**, and **No Password**.
Password	Enter a password for the user. The allowed string length is 0 to 32.
Password Confirm	Enter the same password again to confirm.
Privilege Level	Select the privilege level of the user range: admin and user.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

30.7 Remote Access Control

30.7.1 The Global Screen

Use this screen to configure the **Global** settings. Click **Configuration** > **Management** > **Remote Access Control** to open this screen.

Figure 204 Configuration > Management > Remote Access Control



The following table describes the labels in this screen.

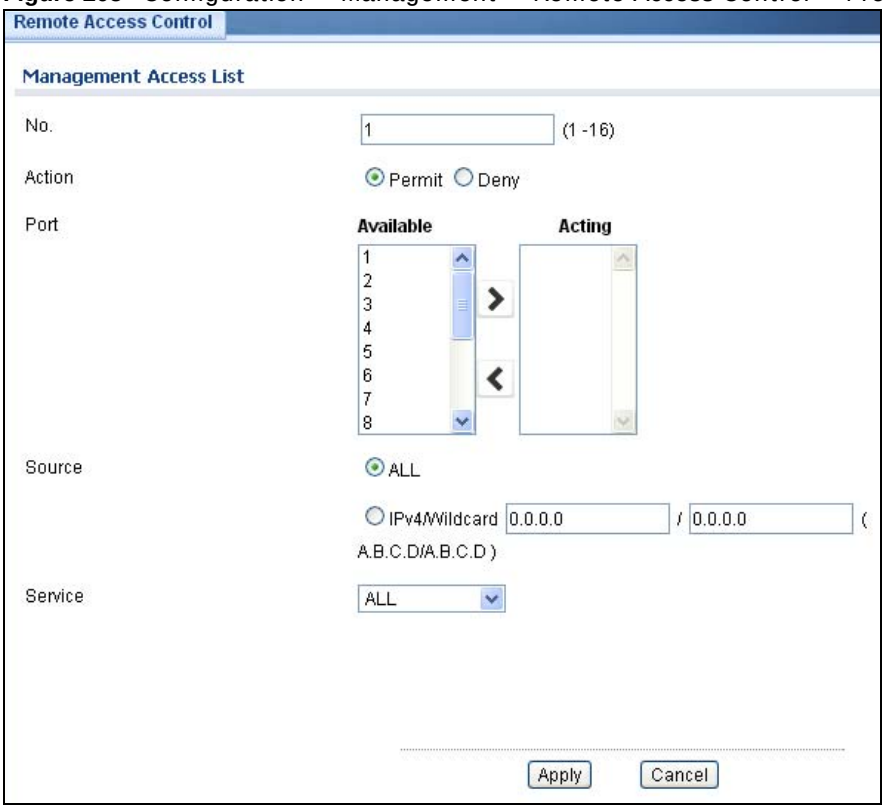
Table 171 Configuration > Management > Remote Access Control

LABEL	DESCRIPTION
Global	
State	Select the global remote access setting to be enabled or disabled.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.
Profile	
Add	Click **Add** to create a new profile entry.
No.	Displays the priority level of the entry. The value can be between 1 and 16.
Action	Displays the action value. The values are **Permit** or **Deny**.
Source IP	Display the source IP value.
Wildcard Mask	Displays the source IP wildcard.
Port	Display the port value.
Service	Display the service used for remote access. The values are **ALL**, **HTTP**, **HTTPS**, or **SNMP**.
Modify	
Edit	Click **Edit** to make changes to the entry.
Delete	Click **Delete** to remove the entry.

30.7.2 The Profile Add/Modify Screen

Use this screen to configure the **Profile** settings. Click **Configuration** > **Management** > **Remote Access Control** > **Profile** > **Add/Modify** to open this screen.

Figure 205 Configuration > Management > Remote Access Control > Profile > Add/Modify



The following table describes the labels in this screen.

Table 172 Configuration > Management > Remote Access Control > Profile > Add/Modify

LABEL	DESCRIPTION
Management Access List Add	
No.	Enter the priority level of the entry. The value can be between 1 and 16.
Action	Select the action value. The values are **Permit** or **Deny**.
Port	Select a value in **Available** and click the **Add** (>) icon to transfer to the Acting column. Select a value in **Acting** and click the **Remove** (<) icon to transfer to the Available column.
Source	Select the source IP value. The options are **ALL** or **IPv4/Wildcard**.
IPv4/Wildcard	Select and enter the IPv4/Wildcard source.
Service	Select the service to use for remote access. The values are **ALL**, **HTTP**, **HTTPS**, or **SNMP**.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard the changes.

31

Maintenance

31.1 Firmware Upgrade

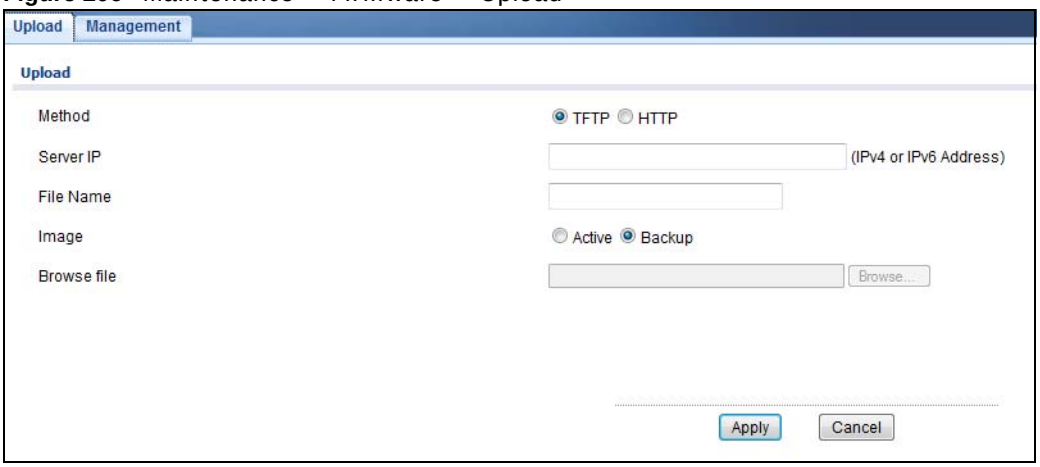
31.1.1 Overview

Firmware updates contain bug fixes and fixes for security vulnerabilities. It is recommended to keep the Switch's firmware up to date. You can upgrade the Switch's firmware manually using a file downloaded on your computer or through the online web configurator.

Note: Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Upload** screen as shown next. Use this screen to upgrade the Switch firmware.

Figure 206 Maintenance > Firmware > Upload



The following table describes the labels under **Upload**.

Table 173 Maintenance > Firmware > Upload

LABEL	DESCRIPTION
Method	Choose **HTTP** to use the web configurator for the firmware upload. Alternatively, choose **TFTP** to download the firmware from a TFTP server.
Server IP	To download from a TFTP server, enter the TFTP server IP address.
File Name	Enter the name of the firmware file on the TFTP server.
Image	Choose **Backup** to upload the firmware file as the backup image. Alternatively, choose **Active** to upload the firmware file as the active image.
Browse File	Browse to the path on your computer where the firmware you want to upload to be the active image is kept.

Upgrade the firmware from a file on a server

Follow the steps below to upgrade the firmware from a TFTP server.

1. In **Method**, choose **TFTP**.
2. In **Server IP**, enter the TFTP server IP address.
3. In **File Name**, enter the name of the firmware file on the TFTP server.
4. In **Image**, choose **Backup** to upload the firmware file as the backup image.
   OR
   Choose **Active** to upload the firmware file as the active image.
5. Click **Apply** to upgrade the chosen image.
   OR
   Click **Cancel** to discard the changes.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

31.1.2 Upgrade the firmware from a file on your computer

Note: For manual upgrade, make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading it to the device. The file name should have a .bin extension.

Follow the steps below to upgrade the firmware from a file on your computer.

1. In **Method**, choose **HTTP**.
2. In **Image**, choose **Active** to upload the firmware file on the active partition image.
   OR
   Choose **Backup** to upload the firmware file on the Backup partition image.
3. Click **Browse** to display the **Choose File** screen from which you can locate the firmware file in the bin format on your computer.
4. Click **Apply** to upload the chosen file.
   OR
   Click **Cancel** to discard the changes.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

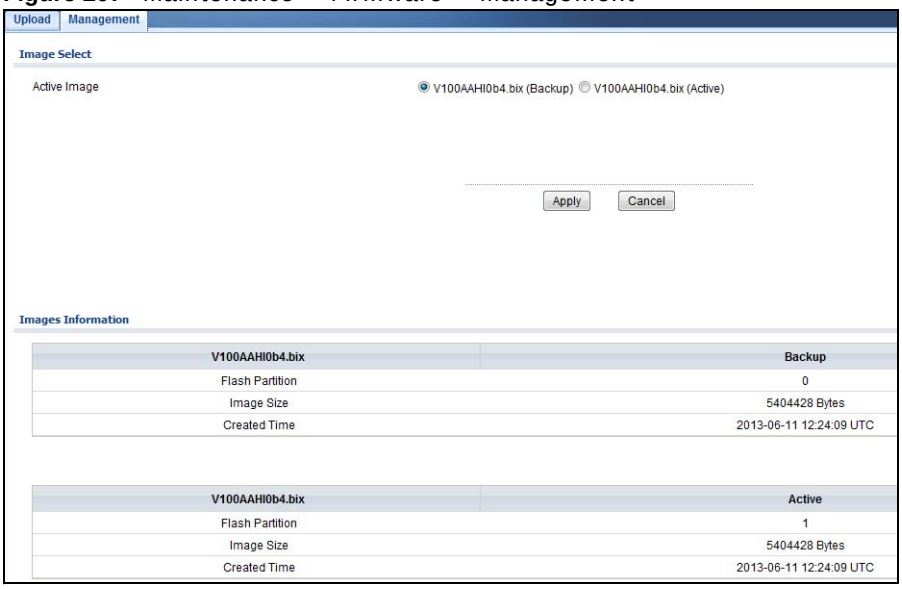
31.2 Firmware Management

31.2.1 Overview

The Firmware Management screen provides instant access to the firmware versions installed on your Switch. Active and backup firmware versions are saved as images on flash partitions. The backup image is used when the active partition has problems during boot.

From the **Maintenance** screen, display the **Firmware Management** screen as shown next. Use this screen to view image information and activate an image.

Figure 207 Maintenance > Firmware > Management



The following table describes the labels shown under **Images Information**.

Table 174 Maintenance > Firmware > Management

LABEL	DESCRIPTION
Flash Partition	Displays the partition number.
Image Name	Displays the name given to the partition image, if any. This field also displays the imagine type: Active or Backup.
Image Size	Displays the size of the partition image in bytes.
Created Time	Displays the date and time when the image was created in the Coordinated Universal Time (UTC) format.

31.2.2 Activate the Backup Image

The current active partition is shown under **Image Select.**

Follow the steps below to choose the backup image if you are facing problems with the active partition during boot.

1. In **Active Image**, choose **Partition0 (Backup)**.
2. Click **Apply** to activate the backup image.
   OR
   Click **Cancel** to discard the changes.

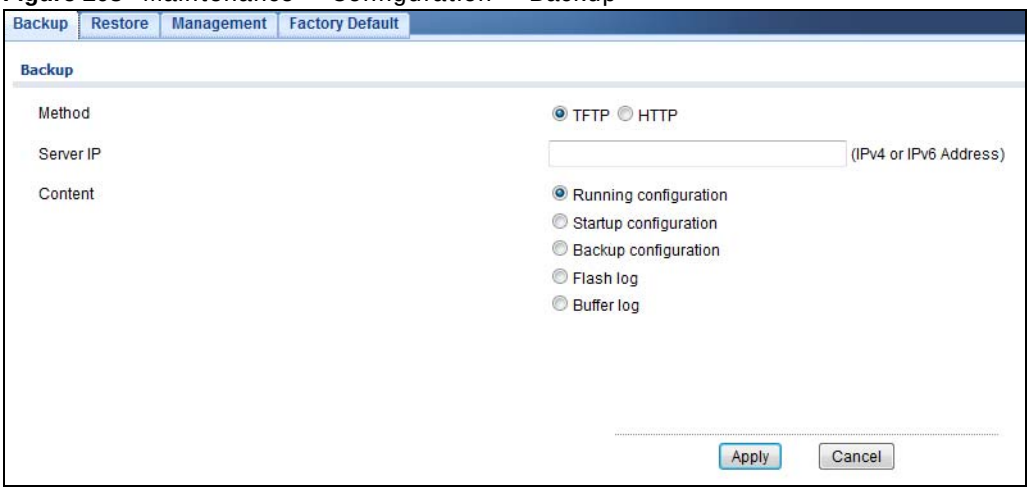
31.3 Backup a Configuration File

31.3.1 Overview

You can save various “snapshots” of your device to the server or your computer and restore them at a later date, if required.

From the **Maintenance** screen, display the **Backup** screen as shown next. Use this screen to back up your current Switch configuration and log files to a server or as local files to your computer.

Figure 208 Maintenance > Configuration > Backup



The following table describes the labels under **Backup**.

Table 175 Maintenance > Configuration > Backup

LABEL	DESCRIPTION
Method	Choose **HTTP** to use the web configurator to backup the configuration. Alternatively, choose **TFTP** to upload the snapshot to a TFTP server.
Server IP	To upload the backup to a TFTP server, enter the TFTP server IP address.
Content	Choose the type of file for backup. You can back up configuration files (running, startup, or backup) or log files (flash or buffer). There are three different types of configuration files: Startup - this is the configuration used when the switch is booting up. Running - this is the configuration when the switch is running. Backup - this is saved in the Switch. If you make changes to the current configuration, and there are problems, you can revert to the Backup configuration without having to restore a new file.

31.3.2 Back up configuration or log files to a server

Follow the steps below to backup configuration or log files to a TFTP server.

1. In **Method**, choose **TFTP**.
2. In **Server IP**, enter the TFTP server IP address.
3. In **Content**, choose any one file type.
4. Click **Apply** to save a snapshot of your current configuration to the TFTP server.
   OR
   Click **Cancel** to discard the changes.

31.3.3 Back up configuration or log files to your computer

Follow the steps below to backup configuration or log files to your computer.

1. In **Method**, choose **HTTP**.
2. In **Content**, choose any one file type.
3. Click **Apply** to display the **Save File** screen from which you can save the configuration file in the cfg format or the log file in the log format to your computer.
   OR
   Click **Cancel** to discard the changes.

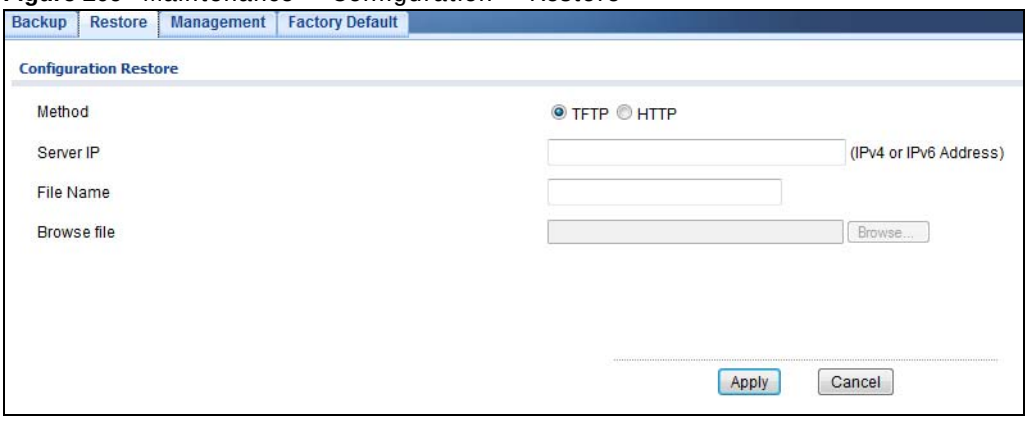
31.4 Restore a Configuration File

31.4.1 Overview

You can restore a previously saved device configuration from the server or your computer.

From the **Maintenance** screen, display the **Restore** screen as shown next. Use this screen to restore a previously saved configuration from a server or your computer.

Figure 209 Maintenance > Configuration > Restore



The following table describes the labels under **Configuration Restore**.

Table 176 Maintenance > Configuration > Restore

LABEL	DESCRIPTION
Method	Choose **HTTP** to use the web configurator for restoring the configuration file. Alternatively, choose **TFTP** to download the snapshot from a TFTP server.
Server IP	To download from a TFTP server, enter the TFTP server IP address.
File Name	Enter the name of the configuration file on the TFTP server.
Browse File	Browse to the path on your computer where the configuration you want to upload to be the active image is kept.

31.4.2 Restore the configuration from a file on a server

Follow the steps below to restore the configuration from a server.

1. In **Method**, choose **TFTP**.
2. In **Server IP**, enter the TFTP server IP address.
3. In **File Name**, enter the name of the configuration file on the TFTP server.

4. Click **Apply** to restore to the chosen file as the running configuration.
   OR
   Click **Cancel** to discard the changes.

31.4.3 Restore the configuration from a file on your computer

Follow the steps below to restore the configuration from a file on your computer.

1. In **Method**, choose **HTTP**.
2. Click **Browse** to display the **Choose File** screen from which you can locate the configuration file in the cfg format on your computer.
3. Click **Apply** to restore to the chosen file as the running configuration.
   OR
   Click **Cancel** to discard the changes.

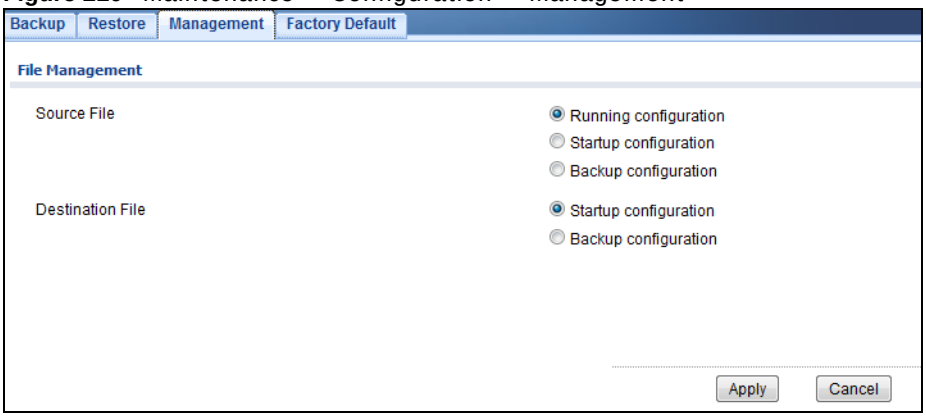
31.5 Manage Configuration Files

31.5.1 Overview

The Configuration Management screen provides instant access to the configuration files of your Switch. You can overwrite the startup and backup configurations with the current running, startup, or backup configuration file.

From the **Maintenance** screen, display the **Management** screen as shown next. Use this screen to replace startup and backup configuration files.

Figure 210 Maintenance > Configuration > Management



Follow the steps to overwrite the startup or backup configuration file.

1. In **Source File**, select the file to be used as a reference.
2. In **Destination File**, select the file to be overwritten.
3. Click **Apply** to restore to overwrite the destination file with the source file.
   OR
   Click **Cancel** to discard the changes.

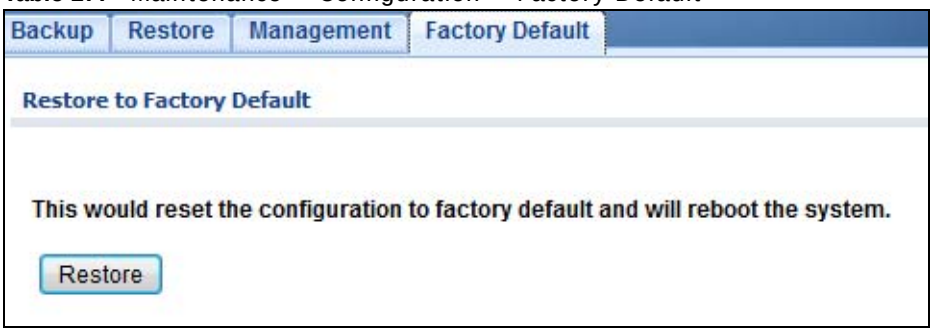
31.6 Reset to Factory Defaults

31.6.1 Overview

You can reset the Switch to it's original settings.

From the **Maintenance** screen, display the **Factory Default** screen as shown next. Use this screen to reset the Switch back to factory defaults.

Table 177 Maintenance > Configuration > Factory Default



31.6.2 Reset the Switch to Factory Defaults

Follow the steps below to reset the Switch back to factory defaults.

1. Click **Restore**.
2. Click **OK** to reset all Switch configurations to the factory defaults. Wait for the Switch to restart. This takes up to two minutes.
   OR
   Click **Cancel** to discard the changes.

Note: If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

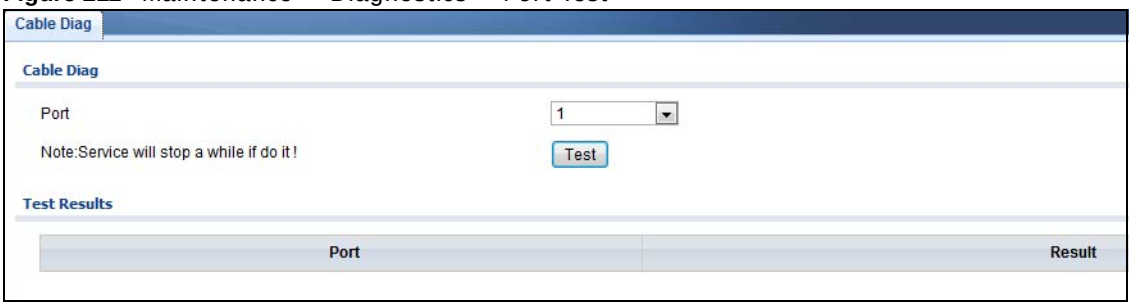
31.7 Network Diagnostics

Use the network utilities to perform diagnostics.

31.7.1 Port Test

Click **Maintenance** > **Diagnostics** > **Port Test** in the navigation panel to open this screen. Use this screen to perform an internal loopback test on an ethernet port.

Figure 211 Maintenance > Diagnostics > Port Test



Follow the steps to perform the port test.

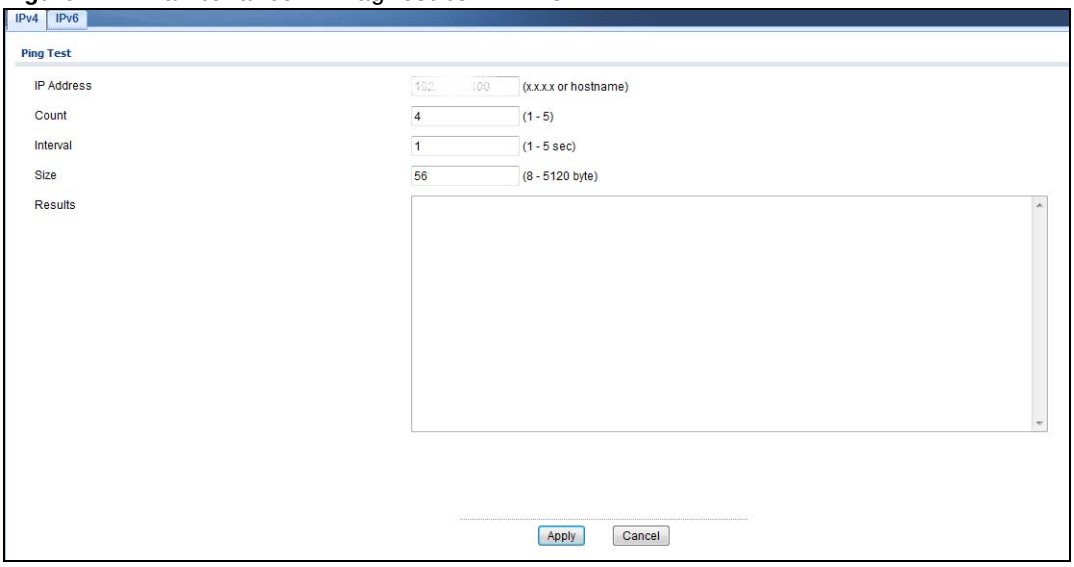
1. In **Port Test**, select the port number from the **Port** drop-down list.
2. Click **Test** to start the port test.

The test results are displayed in **Test Results**.

31.7.2 IPv4 Ping Test

Click **Maintenance** > **Diagnostics** > **PING > IPv4** in the navigation panel to open this screen. Use this screen to ping an IPv4 server.

Figure 212 Maintenance > Diagnostics > PING > IPv4



The following table describes the labels under **Ping Test**.

Table 178 Maintenance > Diagnostics > PING > IPv4

LABEL	DESCRIPTION
IP Address	Enter the address of the target host server.
Count	Enter the number of ping packets to send. The range is 1 to 5 packets; the default count is 4.
Interval	Enter the time in seconds between sending ping packets. The range is 1 to 5 seconds; the default is 1 second.
Size	Enter the individual packet size in bytes. The range is 8 to 5120 bytes; the default is 56 bytes.

Follow the steps to perform a ping test.

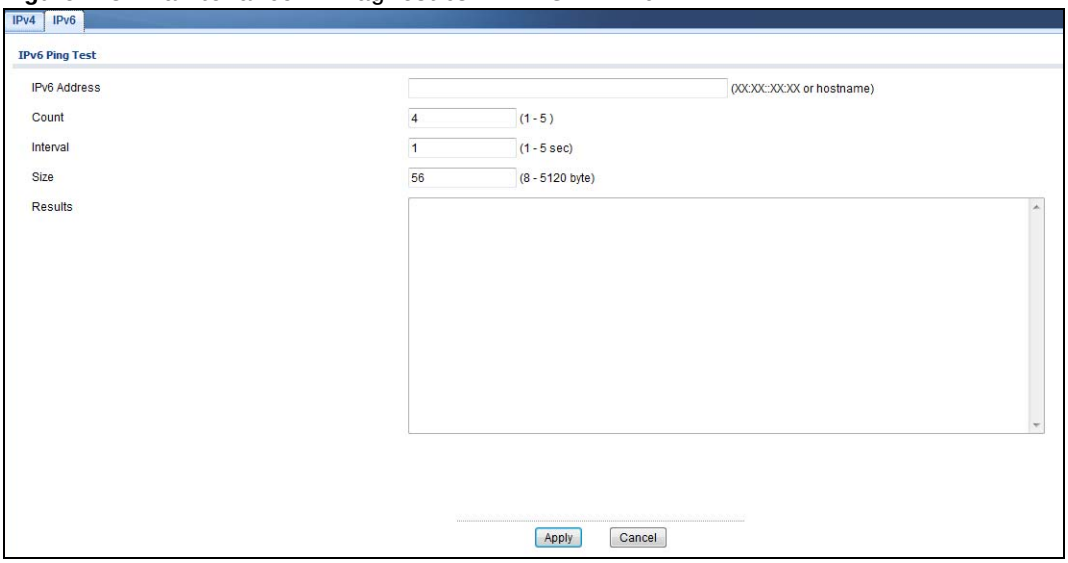
1. In **IP Address**, enter the IPv4 address.
2. In **Count**, enter the number of ping packets.
3. In **Interval**, enter the time interval in seconds.
4. In **Size**, enter the packet size in bytes
5. Click **Apply** to perform the ping test.
   OR
   Click **Cancel** to discard the changes.

The test results are displayed in **Results**.

31.7.3 IPv6 Ping Test

Click **Maintenance** > **Diagnostics** > **PING > IPv6** in the navigation panel to open this screen. Use this screen to ping an IPv6 server.

Figure 213 Maintenance > Diagnostics > PING > IPv6



The following table describes the labels in **IPv6 Ping Test**.

Table 179 Maintenance > Diagnostics > PING > IPv6

LABEL	DESCRIPTION
IPv6 Address	Enter the address of the target host server.
Count	Enter the number of ping packets to send. The range is 1 to 5 packets; the default count is 4.
Interval	Enter the time in seconds between sending ping packets. The range is 1 to 5 seconds; the default is 1 second.
Size	Enter the individual packet size in bytes. The range is 8 to 5120 bytes; the default is 56 bytes.

Follow the steps to perform a ping test.

1. In **IP Address**, enter the IPv6 address.
2. In **Count**, enter the number of ping packets.
3. In **Interval**, enter the time interval in seconds.
4. In **Size**, enter the packet size in bytes

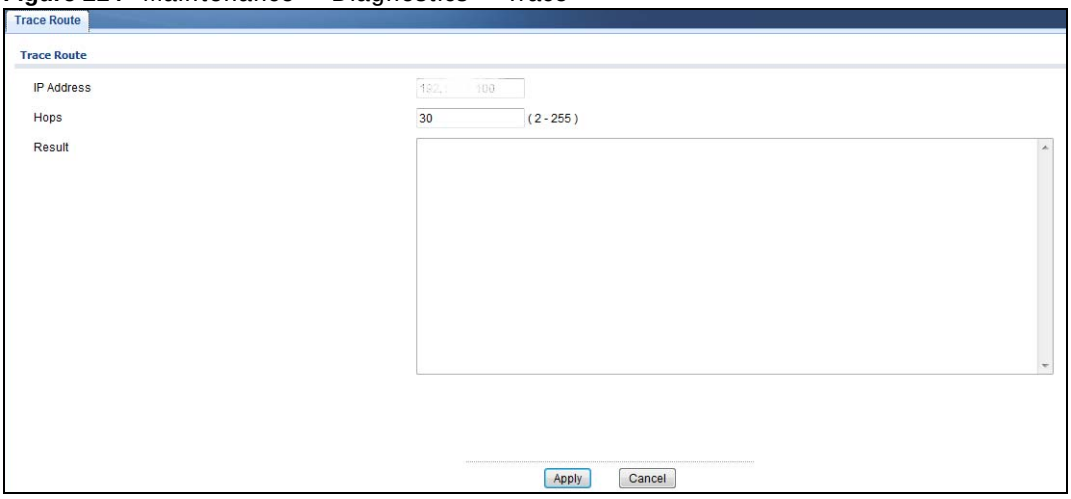
5. Click **Apply** to perform the ping test.
   OR
   Click **Cancel** to discard the changes.

The test results are displayed in **Results**.

31.7.4 Trace Route

Click **Maintenance** > **Diagnostics** > **Trace** in the navigation panel to open this screen. Use this screen to print the route that IP packets take to a network host.

Figure 214 Maintenance > Diagnostics > Trace



The following table describes the labels in **Trace Route**.

Table 180 Maintenance > Diagnostics > Trace

LABEL	DESCRIPTION
IP Addres	Enter the address of the target host server.
Hops	Enter the maximum number of time-to-live or hops used in outgoing probe packets. The range is 2 to 255 packets; the default is 30 hops.

Follow the steps to perform a trace route.

1. In **IP Address**, enter the IPv6 address.
2. In **Hops**, enter the number of hops.
3. Click **Apply** to perform the test.
   OR
   Click **Cancel** to discard the changes.

The test results are displayed in **Result**.

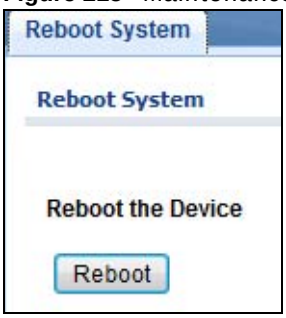
31.8 Reboot

31.8.1 Overview

You can reboot the Switch from the web configurator.

Click **Maintenance** > **Reboot** in the navigation panel to open this screen. Use this screen to restart the Switch without physically turning the power off.

Figure 215 Maintenance > Reboot



31.8.2 Reboot the Switch

Follow the steps below to restart the Switch.

1. Click **Reboot**.
2. Click **OK** and then wait for the Switch to restart. This process takes up to two minutes and does not affect the Switch's configuration.
   OR
   Click **Cancel** to discard the changes.

32

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Switch Access and Login
- Switch Configuration

32.1 Power, Hardware Connections, and LEDs

The Switch does not turn on. None of the LEDs turn on.

1. Make sure the Switch is turned on (in DC models or if the DC power supply is connected in AC/DC models).
2. Make sure you are using the power adaptor or cord included with the Switch.
3. Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
5. Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
6. If the problem continues, contact the vendor.

The **ALM** LED is on.

1. Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).
2. Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
3. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 3.3 on page 30.

2 Check the hardware connections. See Chapter 2 on page 20.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).

5 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).

6 If the problem continues, contact the vendor.

32.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default in-band IP address is **192.168.1.1**.

2 Use the console port to log in to the Switch.

3 Use the **MGMT** port to log in to the Switch, the default IP address of the **MGMT** port is 192.168.0.1.

4 If this does not work, you have to reset the device to its factory defaults. See Section 31.6 on page 217.

I forgot the username and/or password.

1 The default username is **admin** and the default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 31.6 on page 217.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default in-band IP address is **192.168.1.1**.

- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Switch.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section on page 20.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)

5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See Section 31.6 on page 217.

6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Switch.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.

3 Disconnect and re-connect the cord to the Switch.

4 If this does not work, you have to reset the device to its factory defaults. See Section 31.6 on page 217.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

I cannot see some of **Advanced Application** submenus at the bottom of the navigation panel.

The recommended screen resolution is 1024 by 768 pixels. Adjust the value in your computer and then you should see the rest of **Advanced Application** submenus at the bottom of the navigation panel.

There is unauthorized access to my Switch via telnet, HTTP and SSH.

Click the **Maintenance > Diagnostics** screen to check for unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **Configuration > Management** > **Remote Access Control** screen for telnet, HTTP and SSH (see Section 30.7 on page 208). Computers not belonging to the secured client set cannot get permission to access the Switch.

32.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's nonvolatile memory each time you make changes. Click **Save** at the top right corner of the web configurator to save the configuration permanently. See also Section 4.3.1 on page 32 for more information about how to save your configuration.

A

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device 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. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CE

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL À LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of

purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Do not obstruct the device ventillation slots as insufficient airflow may harm your device.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- For DC power input, the length of exposed (bare) power wire should not exceed 7 mm.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

M

N

P

R

S

T

U

V

W