ZYXEL
Your Networking Ally

# User's Guide
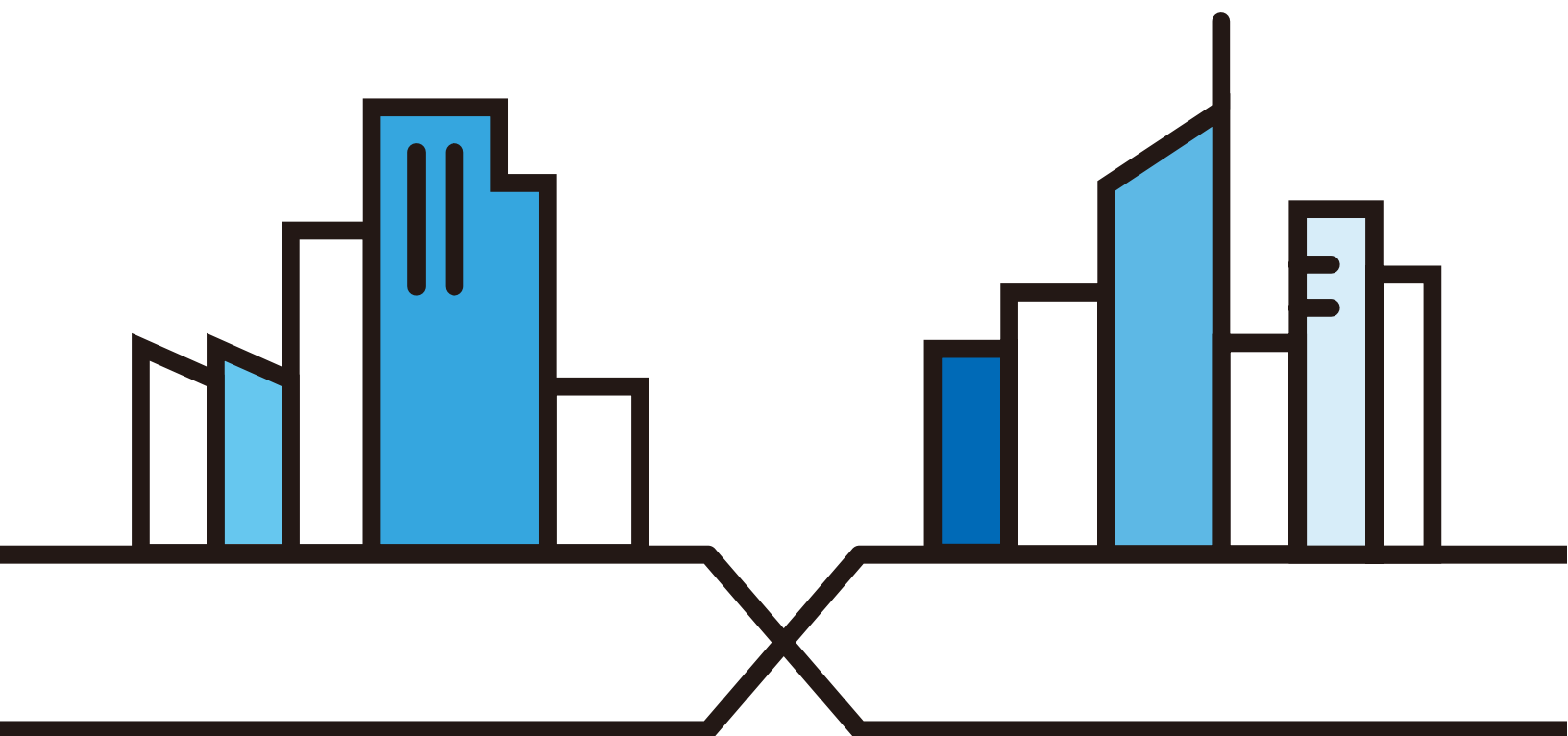
## GS1900 Series

GbE Smart Managed Switch

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

Version 2.60 Edition 1, 02/2020

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

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: 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.

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

## Related Documentation

- Online Help

  Click the help link for a description of the fields in the Switch menus.
- More Information

  Go to **https://businessforum.zyxel.com** for product discussions.
- Go to **support.zyxel.com** to find other information on the Switch.

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this guide.

**Warnings tell you about things that could harm you or your device.**

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- All models may be referred to as the "Switch" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Configuration > System > Information** means you first click **Configuration** in the navigation panel, then the **System** sub menu and finally the **Information** tab to get to that screen.

## Icons Used in Figures

Figures in this user guide may use the following generic icons. The Switch icon is not an exact representation of your device.

| Switch | Generic Switch | Generic Router |
|---|---|---|
| IP Camera | Firewall | Cell Tower |
| Printer | Server | |

# Contents Overview

# Table of Contents

# PART I
## User's Guide

# 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 | GS1900-10HP | GS1900-16 | GS1900-24E | GS1900-24EP | GS1900-24 | GS1900-24HP/ GS1900-24HPv2 | GS1900-48 | GS1900-48HP/ GS1900-48HPv2 |
|---|---|---|---|---|---|---|---|---|---|---|
| 100/1000 Mbps Port | 8 | - | - | 16 | 24 | 12 | 24 | - | 48 | 24 |
| 100/1000 Mbps PoE Port | - | 8 | 8 | - | - | 12 | - | 24 | - | 24 |
| 1G SFP Slots Fiber | - | - | 2 | - | - | - | 2 | 2 | 2 | 2 |
| Desktop | ✓ | ✓ | ✓ | ✓ | ✓ | - | - | - | - | - |
| Wall-mount | ✓ | ✓ | ✓ | ✓ | ✓ | - | - | - | - | - |
| Rack-mount | - | - | - | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Power ON/OFF Switch | ✓ | ✓ | ✓ | ✓ | ✓ | - | - | - | - | - |

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

## 1.2 Example Applications

This section shows a few examples of using the Switch in various network environments. Note that the Switch in the figure is just an example Switch and not your actual Switch.

### 1.2.1 PoE Example Application

The Switch can supply PoE (Power over Ethernet) to Powered Devices (PDs) such as an IP camera, a wireless router, an IP telephone and a general outdoor router that are not within reach of a power outlet.

**Figure 1** PoE Example Application
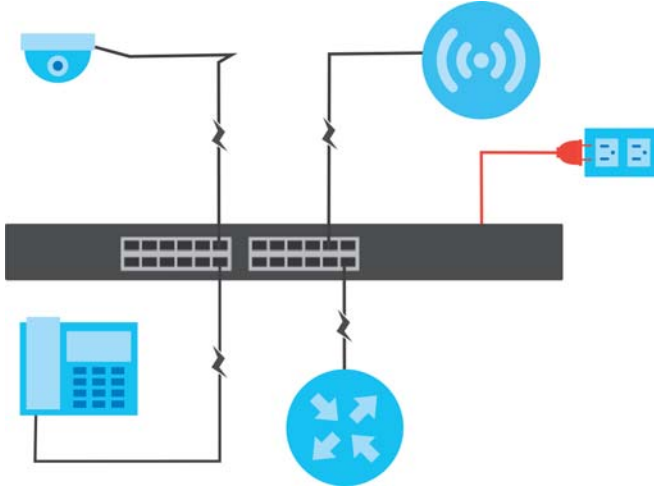


## 1.2.2 Backbone Example Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone 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.

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

**Figure 2** Backbone Example Application
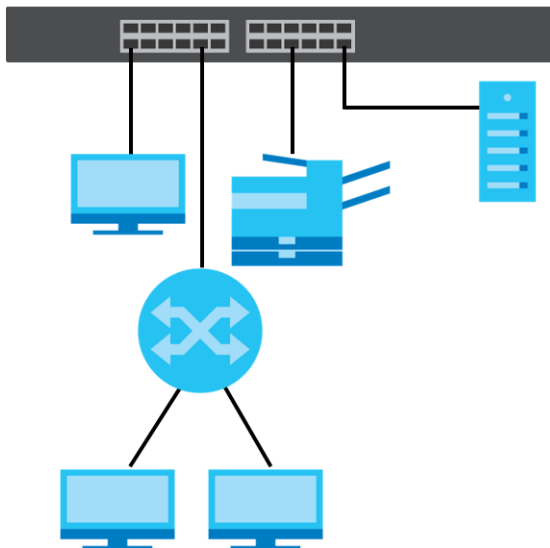


## 1.2.3 Bridging / Fiber Uplink Example Application

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. You can provide a super-fast uplink connection by using a Gigabit Ethernet/SFP port on the Switch.

**Figure 3** Bridging / Fiber Uplink Example Application
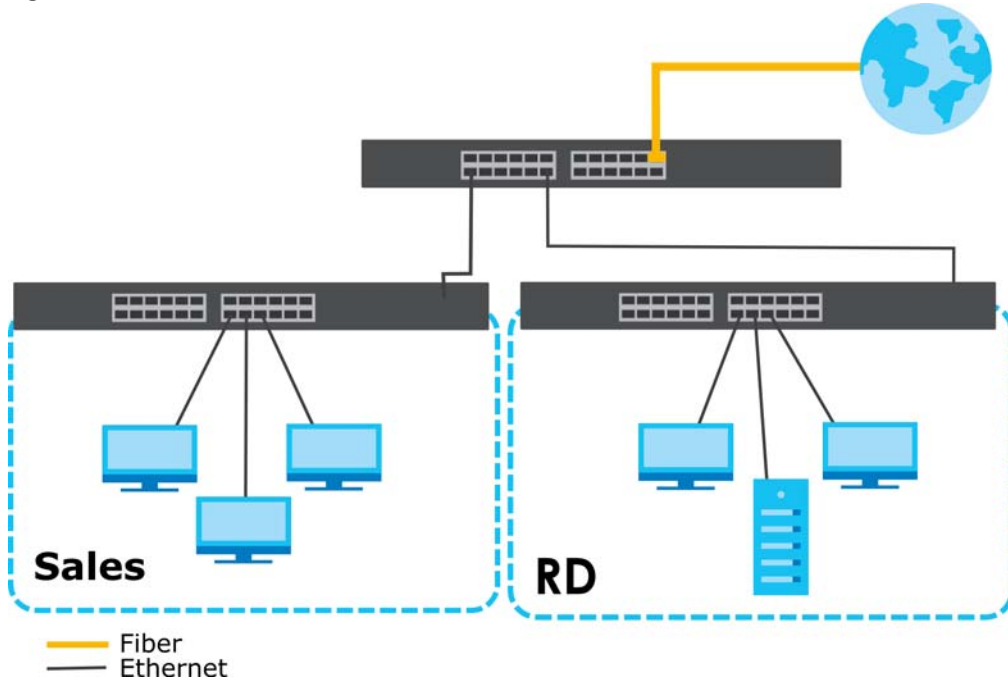


## 1.2.4  Gigabit Ethernet to the Desktop

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 4** Gigabit to the Desktop
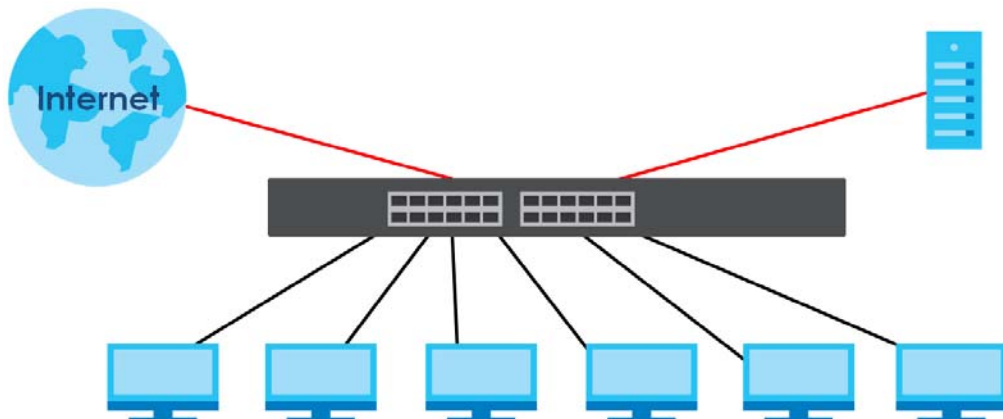


## 1.2.5  IEEE 802.1Q VLAN Application Example

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 .

### 1.2.5.1 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 5** Shared Server Using VLAN Example
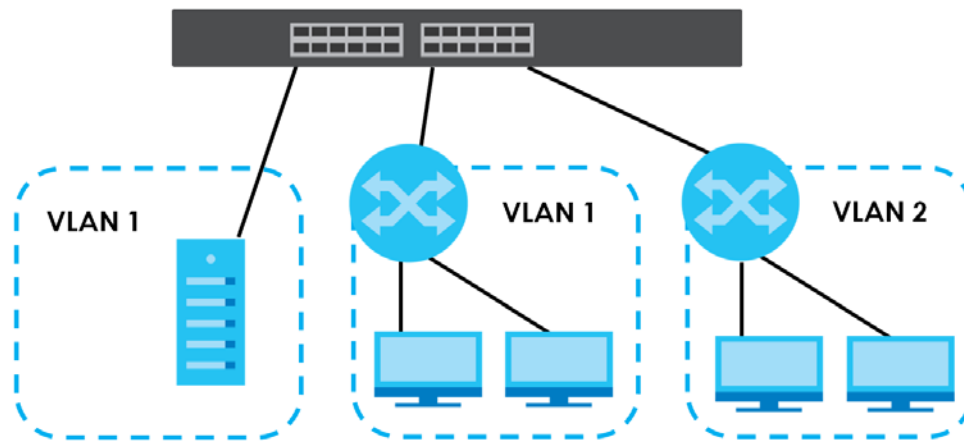


## 1.2.6 IPv6 Support

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, telnet, 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

# 1.3 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 5 on page 43.

- TFTP. Use Trivial File Transfer Protocol for firmware upgrades and configuration backup/restore. See Section 33.1 on page 229, Section 33.3 on page 232, and Section 33.4 on page 233.

- SNMP. The device can be configured by a SNMP manager. See Section 32.3 on page 215.

- ZON Utility. ZON Utility is a program designed to help you deploy and perform initial setup on a network more efficiently. See Section 4.1 on page 38.

# 1.4  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 is 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.

# CHAPTER 2
# Hardware Installation and Connection

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

## 2.1 Installation Scenarios

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

The Switch can be:

- Placed on a desktop.
- Mounted on a wall.
- Rack-mounted on a standard EIA rack.

Note: Ask an authorized technician to attach the Switch to the rack/wall. See the **Installation Requirements** sections in this chapter to know the types of screws and screwdrivers for wall-mounting.

> **WARNING! Failure to use the proper screws may damage the unit**.
>
> **Make sure you connect the Switch's power cord to a socket-outlet with an earthing connection or its equivalent.**
>
> **WARNING! This Switch is not suitable for use in locations where children are likely to be present.**

See Table 1 on page 17 for the comparison table of the hardware installation methods for each model.

## 2.2 Desktop Installation Procedure

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 at least 40 mm of clearance from the bottom to the Switch, and make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord. This is especially important for enclosed rack installations.

**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 6** Attaching Rubber Feet
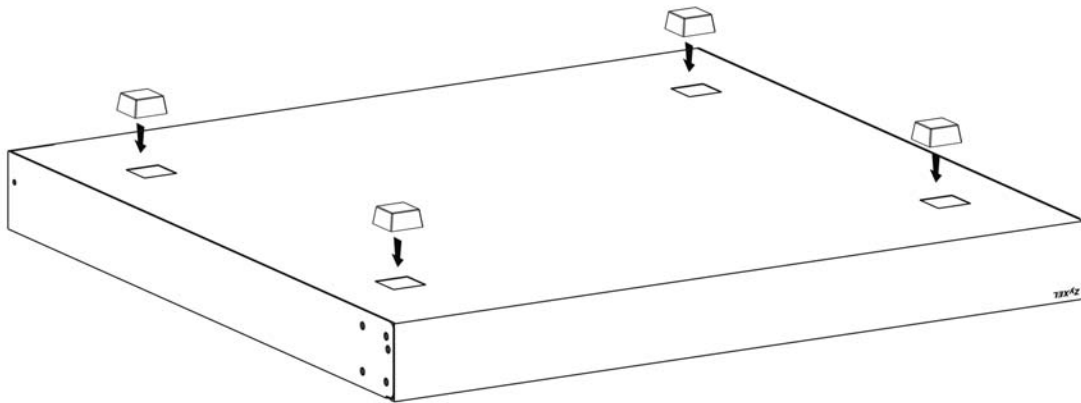


Note: Do NOT block the ventilation holes. Leave space between devices when stacking.

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.

# 2.3  Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

## 2.3.1  Wall-mounted Installation Requirement

The following are the wall-mounted installation requirements:

- Use screws with 6 mm ~ 8 mm (0.24" ~ 0.31") wide heads.
- 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 | GS1900-10HP | GS1900-16 | GS1900-24E |
|---|---|---|---|---|
| 176 mm | 176 mm | 176 mm | 148 mm | 207 mm |

The following figure shows the screw specifications used for wall mounting.

- D = 7.00 mm
- H = 2.00 mm
- L= 15.50 mm

- d = 3.50 mm
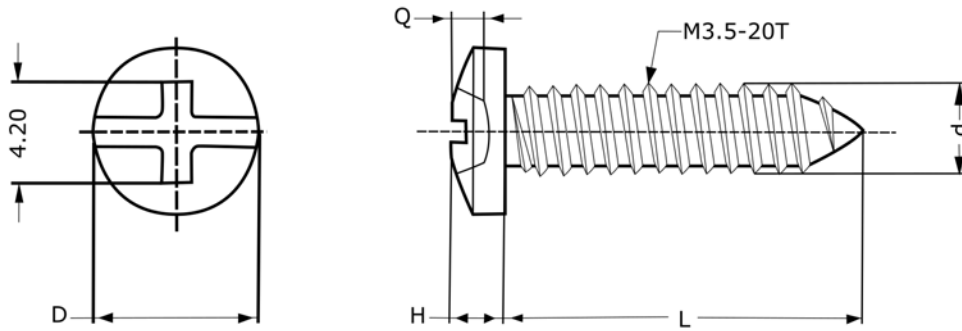


Do the following to attach your Switch to a wall.

**1** Select a position free of obstructions on a wall strong enough to hold the weight of the Switch.

**2** Mark two holes on the wall at the appropriate distance apart for the screws.

> **WARNING! Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.**

**3** If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap. 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.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap.
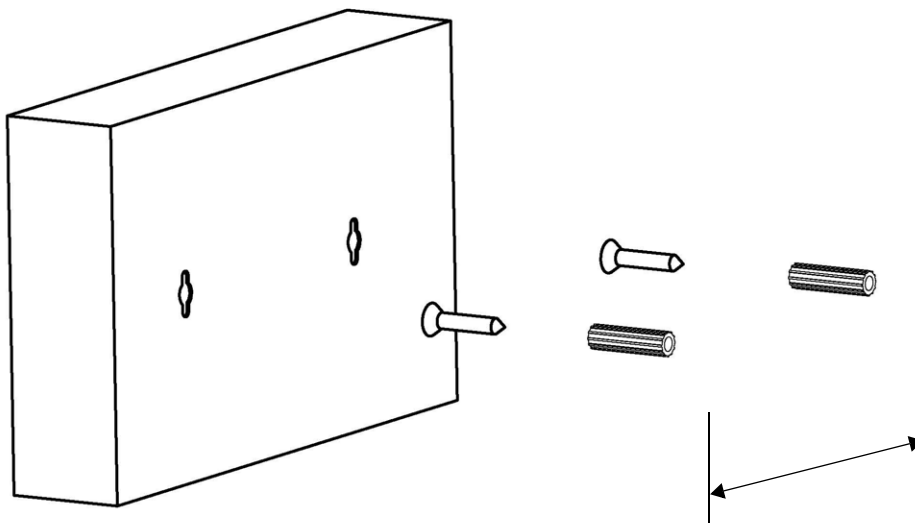


Note: Make sure the screws are fastened well enough to hold the weight of the Switch with the connection cables.

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

Note: Make sure there is enough clearance between the wall and the Switch to allow ventilation.

**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.**

# 2.4  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.

Note: Make sure there is enough clearance between each equipment on the rack for air circulation.

## 2.4.1  Rack-mounted Installation Requirements

The following are the 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.**

### 2.4.1.1  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.

## 2.4.2  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 7   Attaching the Mounting Brackets (GS1900-16, GS1900-24E, and GS1900-24EP)
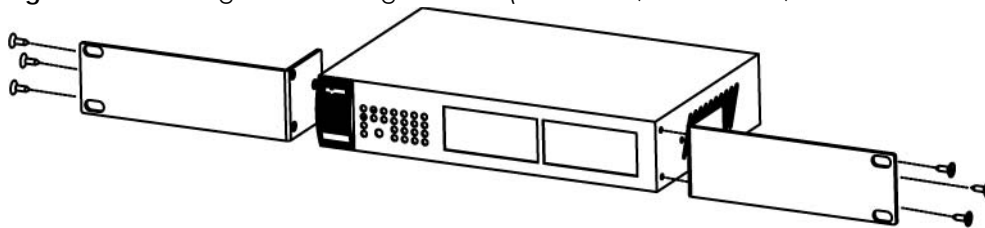
**Figure 8**   Attaching the Mounting Brackets (GS1900-24, GS1900-24HP/GS1900-24HPv2, GS1900-48, and GS1900-48HP/GS1900-48HPv2)
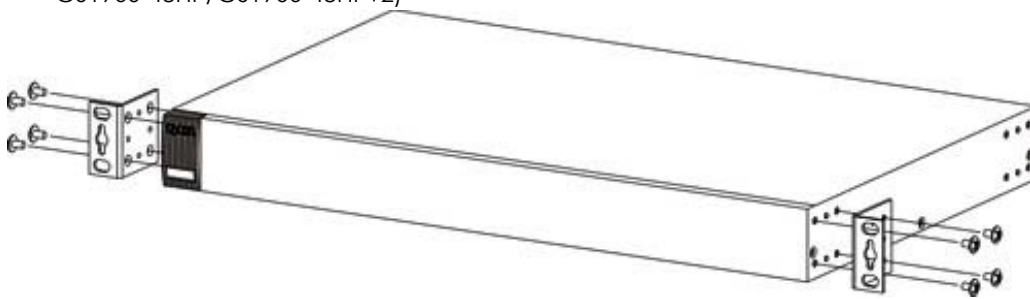


**2**   Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

**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.

## 2.4.3  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 9**   Mounting the Switch on a Rack (GS1900-16, GS1900-24E, and GS1900-24EP)
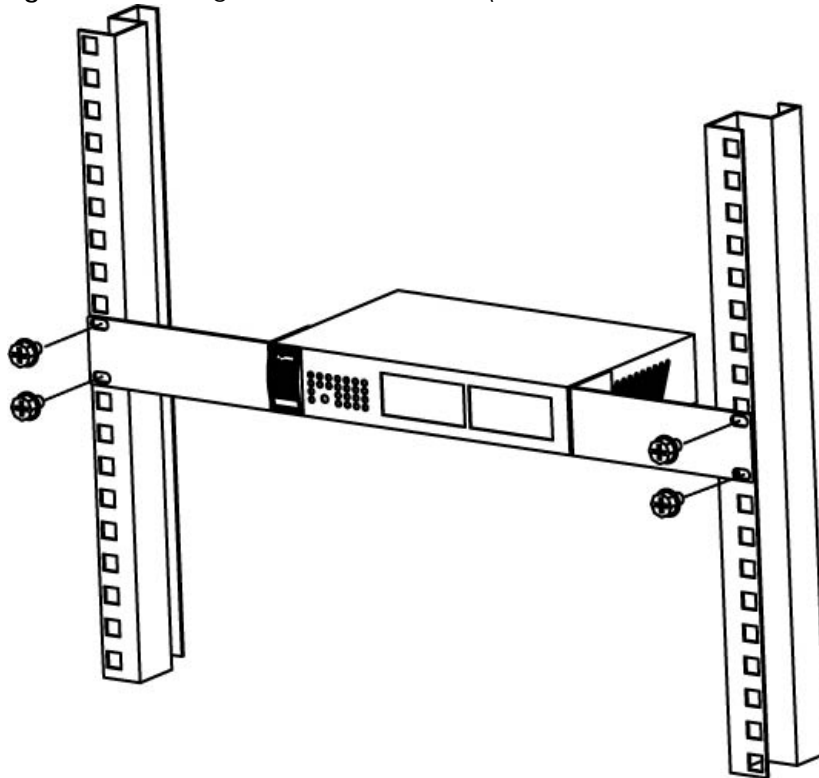
**Figure 10** Mounting the Switch on a Rack (GS1900-24, GS1900-24HP/GS1900-24HPv2, GS1900-48, and GS1900-48HP/GS1900-48HPv2)
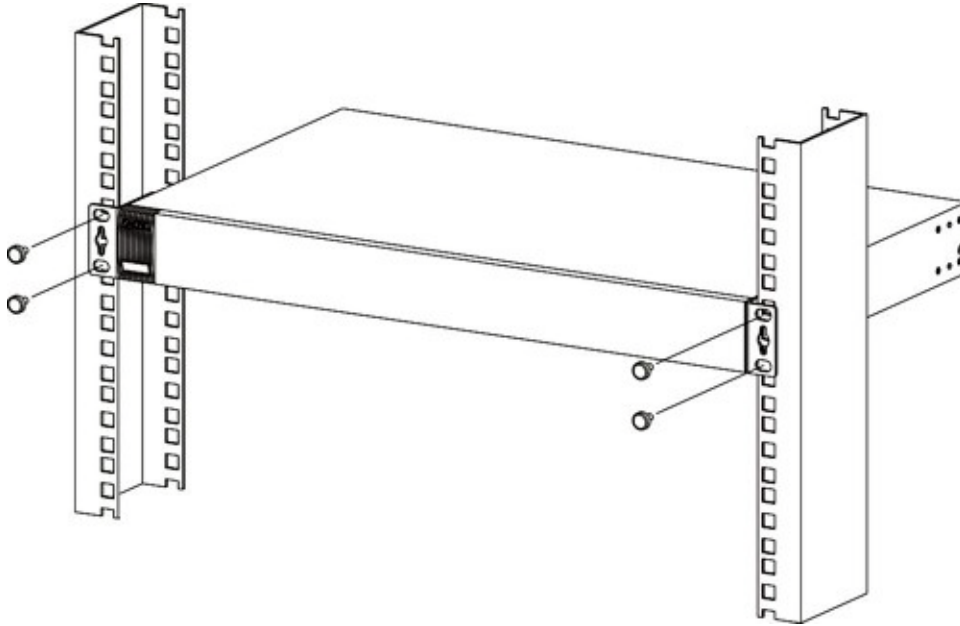


**2**   Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

Note: Make sure you tighten all the four screws to prevent the Switch from getting slanted.

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

# CHAPTER 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 11** Front Panel: GS1900-8
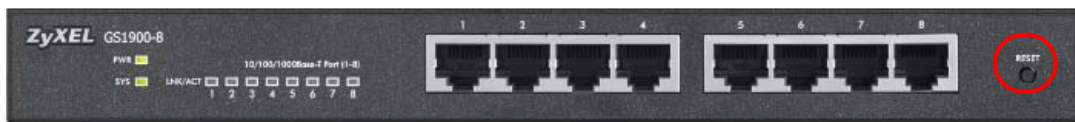


**Figure 12** Front Panel: GS1900-8HP

Revision A1



Revision B1
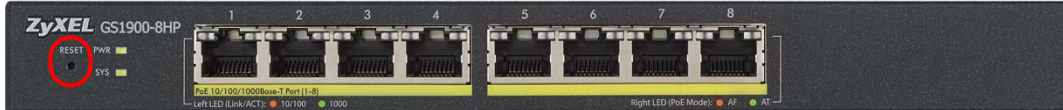


**Figure 13** Front Panel: GS1900-10HP



**Figure 14** Front Panel: GS1900-16

**Figure 15** Front Panel: GS1900-24E
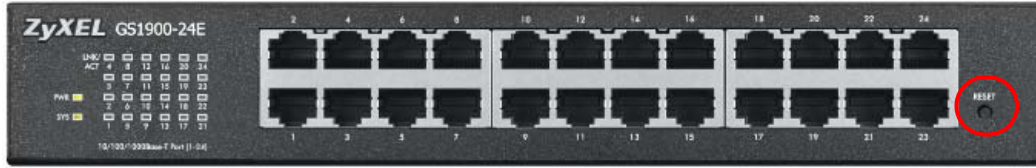


**Figure 16** Front Panel: GS1900-24EP



**Figure 17** Front Panel: GS1900-24



**Figure 18** Front Panel: GS1900-24HP



**Figure 19** Front Panel: GS1900-24HPv2



**Figure 20** Front Panel: GS1900-48
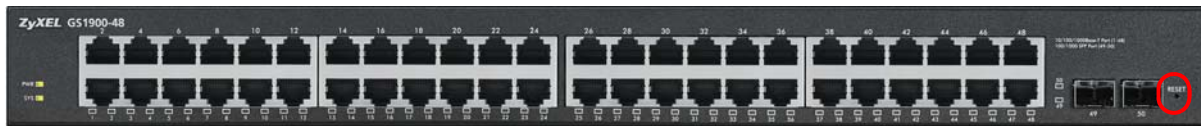


**Figure 21** Front Panel: GS1900-48HP



**Figure 22** Front Panel: GS1900-48HPv2



## 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 23** Transceiver Installation Example
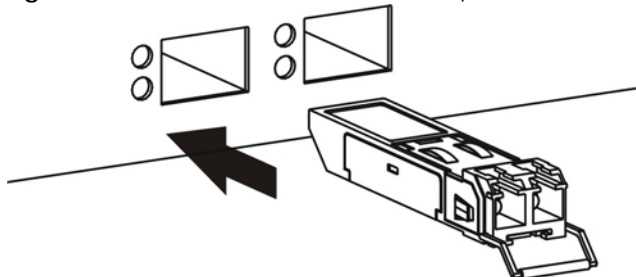


**2** Press the transceiver firmly until it clicks into place.

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

**Figure 24** Installed Transceiver
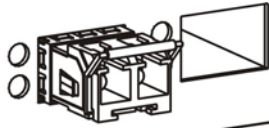


### 3.1.2.2 Transceiver Removal

Use the following steps to remove a transceiver.

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

**Figure 25** Opening the Transceiver's Latch Example
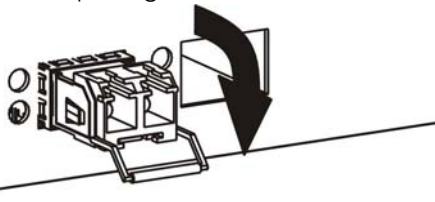


2 Pull the transceiver out of the slot.

**Figure 26** Transceiver Removal Example
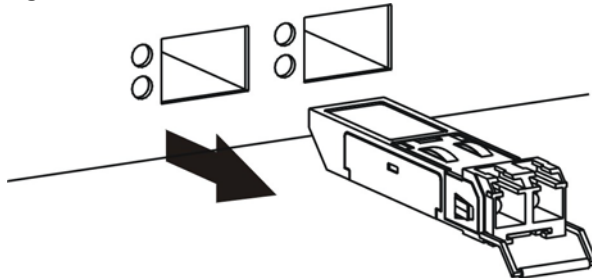


## 3.1.3 PoE Mode (GS1900-48HP and GS1900-48HPv2 only)

Push or release this button (see Figure 21 on page 29) to change how the **Link/ACT** LED works.

- Each Ethernet port's LED is changed to act as a **PoE Mode** LED by pushing the **PoE MODE** button on the front panel.
- Each Ethernet port's LED is changed back to act as a **Link/ACT** LED by releasing the **PoE MODE** button on the front panel.

View the LEDs to ensure proper functioning of the Switch and as an aid in troubleshooting (see Section 3.3 on page 35).

# 3.2 Rear Panel

The following figures show the rear panels of the Switch.

**Figure 27**   Rear Panel: GS1900-8

**Figure 28**   Rear Panel: GS1900-8HP

Revision A1

Revision B1

**Figure 29**   Rear Panel: GS1900-10HP

**Figure 30**   Rear Panel: GS1900-16

**Figure 31**   Rear Panel: GS1900-24E

**Figure 32**   Rear Panel: GS1900-24EP

**Figure 33**   Rear Panel: GS1900-24

**Figure 34** Rear Panel: GS1900-24HP

**Figure 35** Rear Panel: GS1900-24HPv2

**Figure 36** Rear Panel: GS1900-48

**Figure 37** Rear Panel: GS1900-48HP

**Figure 38** Rear Panel: GS1900-48HPv2

## 3.2.1  Grounding

Grounding is a safety measure to have unused electricity return to the ground. It prevents damage to the Switch, and protects you from electrocution.

Any device that is located outdoors and connected to this product must be properly grounded and surge protected. To the extent permissible by applicable law, failure to follow these guidelines could result in damage to your Switch which may not be covered by its warranty.

Note: The Switch must be grounded by qualified service personnel.

**1** Remove the M4 ground screw from the Switch's rear panel.

**2** Secure a green/yellow ground cable (16 AWG or smaller) to the Switch's rear panel using the M4 ground screw.

**3** Attach the other end of the cable to the ground, either to the same ground electrode as the rack you installed the device on or to the main grounding electrode of the building.

Follow your country's regulations and safety instructions to electrically ground the device properly.

if you are uncertain that suitable grounding is available, contact the appropriate electrical inspection authority or an electrician.

**Warning! Connect the ground cable before you connect any other cables or wiring.**

**Figure 39**   Grounding
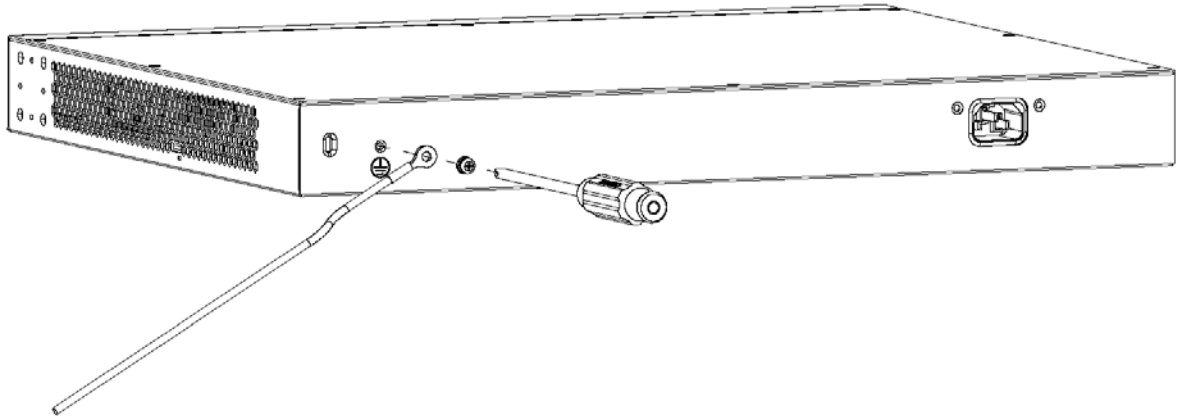


## 3.2.2  Power Connection

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 adapter 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 17), 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 17) | Green | On | Power is supplied to all PoE Ethernet ports. |
| | | Off | There is no power supplied. |
| 1G SFP Slots (Fiber Ports - see Section 1.1 on page 17) | | | |
| 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. |
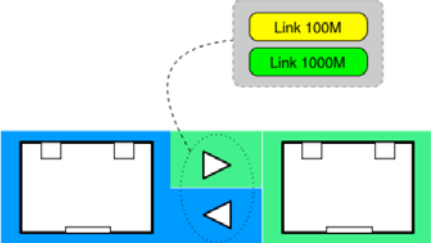
Table 4   LED Descriptions (GS1900-8HP (Revision B1) and GS1900-10HP Only)

| 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. |
| | Red | On | There is a system error. |
| PoE 10/100/1000Base-T Ports (1-8), 2 LEDs per port | | | |



| Right | Amber | On | The port is in PoE AF mode. That is, the Switch is following the IEEE 802.3af standard to supply power to this port. |
|---|---|---|---|
| | Green | On | The port is in PoE AT mode. That is, the Switch is following the IEEE 802.3at standard to supply power to this port. |
| | | Off | Power is not supplied to this port. |

Table 4   LED Descriptions (continued)(GS1900-8HP (Revision B1) and GS1900-10HP Only)

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| Left | Amber | On | The link to a 10/100 Mbps Ethernet network is up. |
| | | Blinking | The system is transmitting/receiving to/from a 100/1000 Mbps Fiber network. |
| | Green | On | The link to a 1 Gbps Ethernet network is up. |
| | | Blinking | The system is transmitting/receiving to/from 1 Gbps Mbps Ethernet network. |

LED Descriptions for SFP Port (GS1900-10HP Only)

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| Two arrow LEDs for 1G SFP Slots (Fiber Ports) | | | |
|  | | | |
| right/left arrows | Amber | On | The link to a 100 Mbps Fiber network is up. |
| | | Blinking | The system is transmitting/receiving to/from a 100 Mbps Fiber network. |
| | Green | On | The link to a 1 Gbps Fiber network is up. |
| | | Blinking | The system is transmitting/receiving to/from 1 Gbps Mbps Fiber network. |

# 3.4  Resetting the Switch (all models except GS1900-24EP/ GS1900-24HPv2/GS1900-48HPv2)

If you lock yourself (and others) from the Switch, or you forget your password, or cannot access the Web Configurator, you will need to reload the factory-default configuration file. Or use the **RESET** button at the front of the device.

This means that you will lose all configurations that you had previously and the default Switch IP address, user name and password will be reset to 192.168.1.1, admin and 1234 respectively.

If you backed up an earlier configuration file as advised in , you will not have to totally re-configure the Switch after resetting. You can simply restore your last configuration.

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

1   Make sure the **SYS** LED is steady green (not blinking). Use a pointed instrument such as a pin to access the **RESET** button on the front of the Switch as shown in .

2   Press the button for more than 6 seconds. After releasing the button, the **SYS** LED begins to blink. Wait for the Switch to restart (the **SYS** LED will be steady green again). This takes up to two minutes.

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).

# 3.5  Resetting the Switch (GS1900-24EP/GS1900-24HPv2/ GS1900-48HPv2 only)

Use the **RESTORE** button to reset the Switch back to factory defaults. Use the **RESET** button to reboot the Switch.

## 3.5.1  Restore Button

Press the **RESTORE** button for more than 6 seconds until the **SYS** LED begins to blink. The Switch will automatically reboot and restore the factory default file. See Section 3.3 on page 35 for more information about the LED behavior.

## 3.5.2  Reboot the Switch

Press the **RESET** button to reboot the Switch without turning the power off. See Section 3.3 on page 35 for more information about the LED behavior.

# CHAPTER 4
# ZON Utility

This chapter describes the screens for ZON Utility.

## 4.1  Zyxel One Network (ZON) Utility Screen

ZON Utility is a program designed to help you deploy and manage a network more efficiently. It detects devices automatically and allows you to do basic settings on devices in the network without having to be near it.

The ZON Utility issues requests via Zyxel Discovery Protocol (ZDP) and in response to the query, the device responds back with basic information including IP address, firmware version, location, system and model name in the same broadcast domain. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it on a PC (Windows operating system).

### 4.1.1  Requirements

Before installing the ZON Utility on your PC, please make sure it meets the requirements listed below.

### Operating System

At the time of writing, the ZON Utility is compatible with:

• Windows 7 (both 32-bit / 64-bit versions)
• Windows 8 (both 32-bit / 64-bit versions)
• Windows 8.1 (both 32-bit / 64-bit versions)
• Window 10 (both 32-bit / 64-bit versions)

Note: To check for your Windows operating system version, right-click on **My Computer > Properties**. You should see this information in the **General** tab.

Note: It is suggested that you install Npcap, the packet capture library for Windows operating systems, and remove WinPcap or any other installed packet capture tools before you install the ZON utility.

### Hardware

Here are the minimum hardware requirements to use the ZON Utility on your PC.

- Core i3 processor
- 2GB RAM
- 100MB free hard disk
- WXGA (Wide XGA 1280x800)

## 4.1.2  Run the ZON Utility

**1**  Double-click the ZON Utility to run it.

**2**  The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

**Figure 40**   Supported Devices and Versions
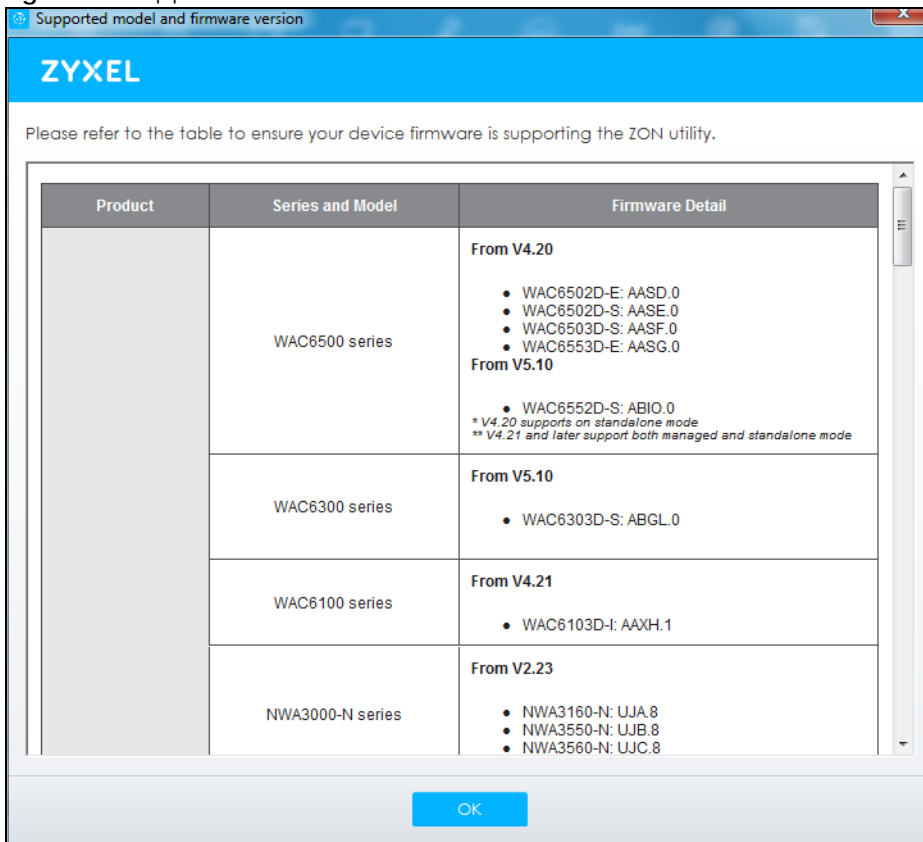


If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right hand corner of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for ZON utility support. The release notes are in the firmware zip file on the Zyxel web site.

**Figure 41** ZON Utility Screen
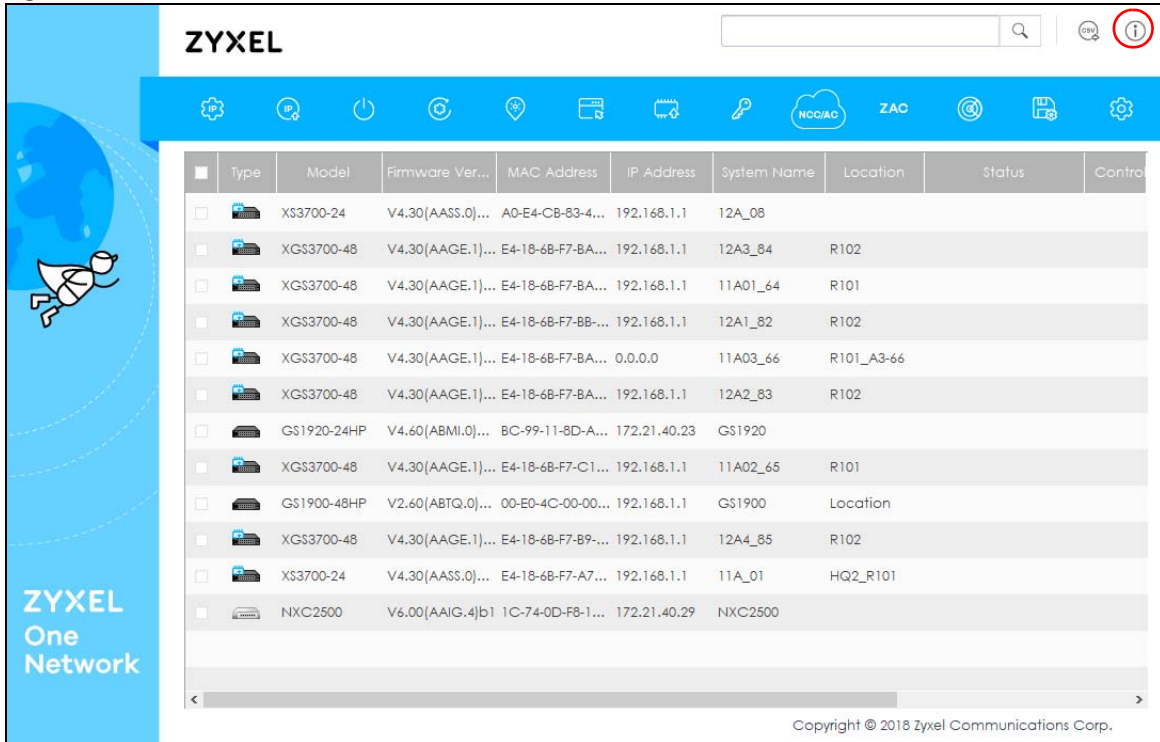


**3** Select a network adapter to which your supported devices are connected.

**4** Click the **Go** button for the ZON Utility to discover all supported devices in your network.

**Figure 42** Discovery
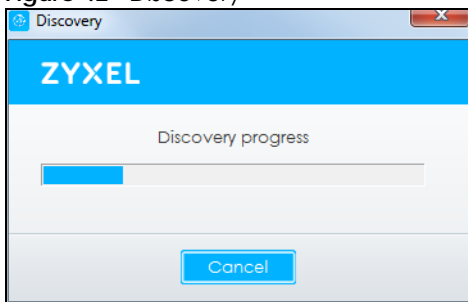


**5** The ZON Utility screen shows the devices discovered.

**Figure 43** ZON Utility Screen
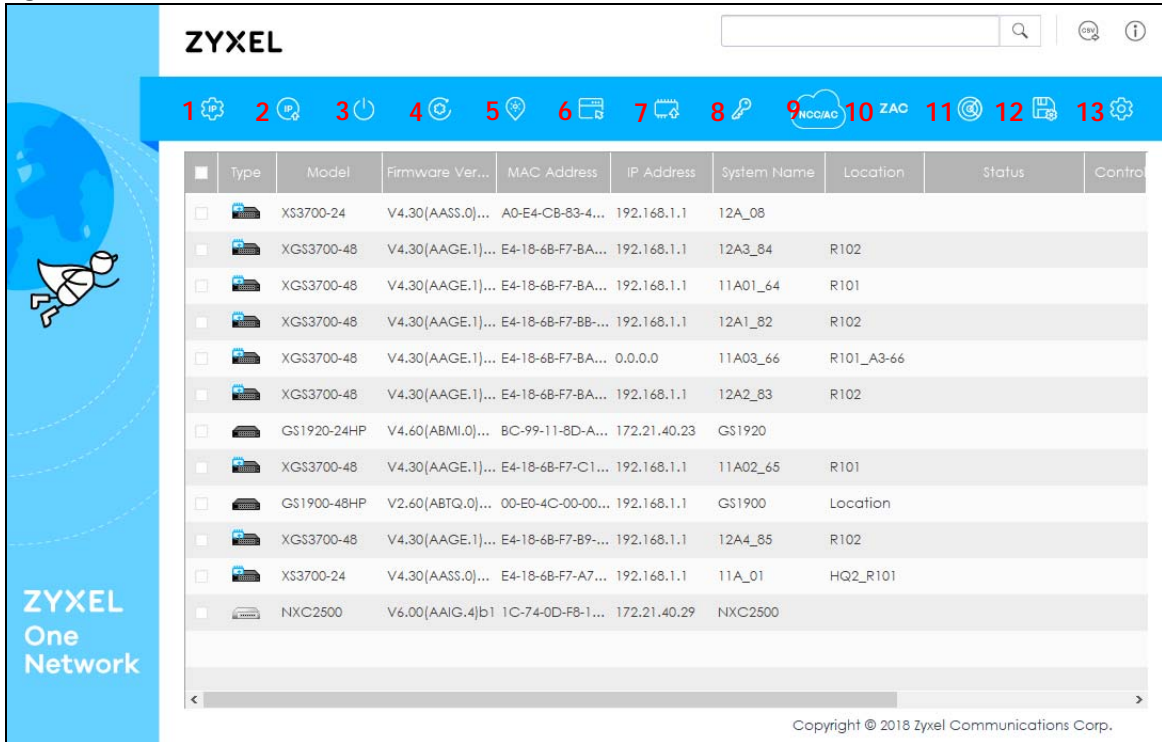


6 Select a device and then use the icons to perform actions. Some functions may not be available for your devices.

Note: You must know the selected device admin password before taking actions on the device using the ZON utility icons.

**Figure 44** Password Prompt
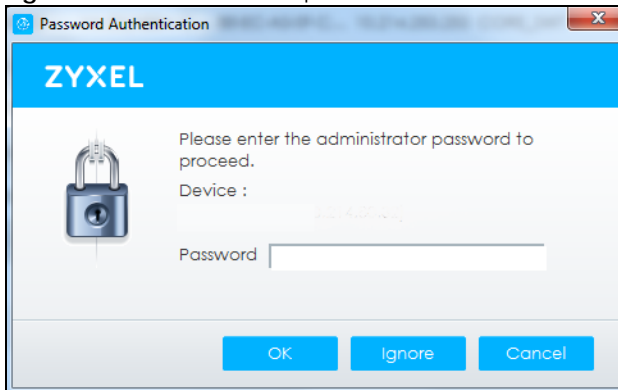


The following table describes the icons numbered from left to right in the ZON Utility screen.

Table 5 ZON Utility Icons

| ICON | DESCRIPTION |
|---|---|
| 1 IP configuration | Change the selected device's IP address. |
| 2 Renew IP Address | Update a DHCP-assigned dynamic IP address. |
| 3 Reboot Device | Use this icon to restart the selected device(s). This may be useful when troubleshooting or upgrading new firmware. |

Table 5   ZON Utility Icons

| ICON | DESCRIPTION |
|------|-------------|
| 4 Reset Configuration to Default | If you forget your password or cannot access the Web Configurator, you can use this icon to reload the factory-default configuration file. This means that you will lose all configurations that you had previously. |
| 5 Locator LED | Use this icon to locate the selected device by causing its Locator LED to blink. |
| 6 Web GUI | Use this to access the selected device web configurator from your browser. You will need a username and password to log in. |
| 7 Firmware Upgrade | Use this icon to upgrade new firmware to selected device(s) of the same model.<br><br>**Online upgrade**: If there's the latest firmware available, it'll show in the drop-down menu. You don't need to download the firmware first to upgrade firmware.<br><br>**Local upgrade**: Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance. |
| 8 Change Password | Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one. |
| 9 Configure NCC Discovery | You must have Internet access to use this feature. Use this icon to enable or disable the Nebula Control Center (NCC) discovery feature on the selected device. If it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the Nebula cloud management mode. |
| 10 ZAC | Use this icon to run the Zyxel AP Configurator of the selected AP. |
| 11 Clear and Rescan | Use this icon to clear the list and discover all devices on the connected network again. |
| 12 Save Configuration | Use this icon to save configuration changes to permanent memory on a selected device. |
| 13 Settings | Use this icon to select a network adapter for the computer on which the ZON utility is installed, and the utility language. |

The following table describes the fields in the ZON Utility main screen.

Table 6   ZON Utility Fields

| LABEL | DESCRIPTION |
|-------|-------------|
| Type | This field displays an icon of the kind of device discovered. |
| Model | This field displays the model name of the discovered device. |
| Firmware Version | This field displays the firmware version of the discovered device. |
| MAC Address | This field displays the MAC address of the discovered device. |
| IP Address | This field displays the IP address of an internal interface on the discovered device that first received an ZDP discovery request from the ZON utility. |
| System Name | This field displays the system name of the discovered device. |
| Location | This field displays where the discovered device is. |
| Status | This field displays whether changes to the discovered device have been done successfully. As the Switch does not support **IP Configuration**, **Renew IP address** and **Locator LED**, this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively. |
| NCC Discovery | This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature. If it's enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it'll go into the Nebula cloud management mode. |
| Serial Number | Enter the admin password of the discovered device to display its serial number. |
| Hardware Version | This field displays the hardware version of the discovered device. |

# Web Configurator

## 5.1  Overview

This section introduces the configuration and functions of the Web Configurator.

The Web Configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use a browser that supports HTML5, such as Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended screen resolution is 1024 by 768 pixels.
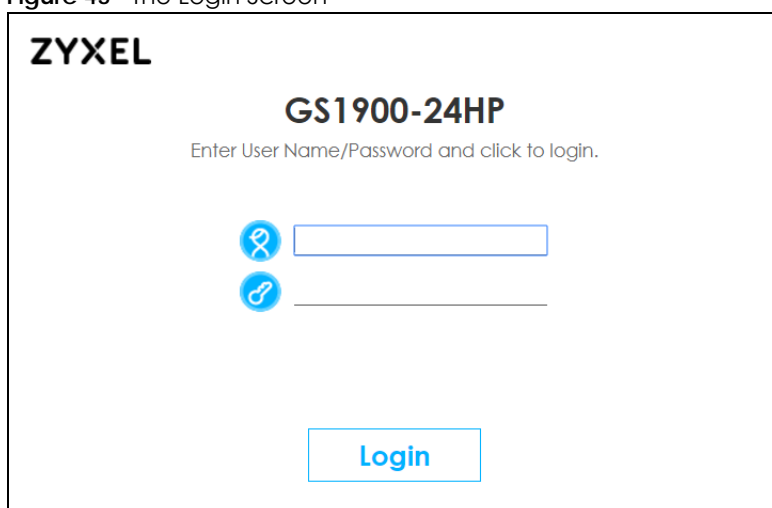
In order to use the Web Configurator, you need to allow:

- Web browser pop-up windows
- JavaScript (enabled by default)
- Java permissions (enabled by default)

## 5.2  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.
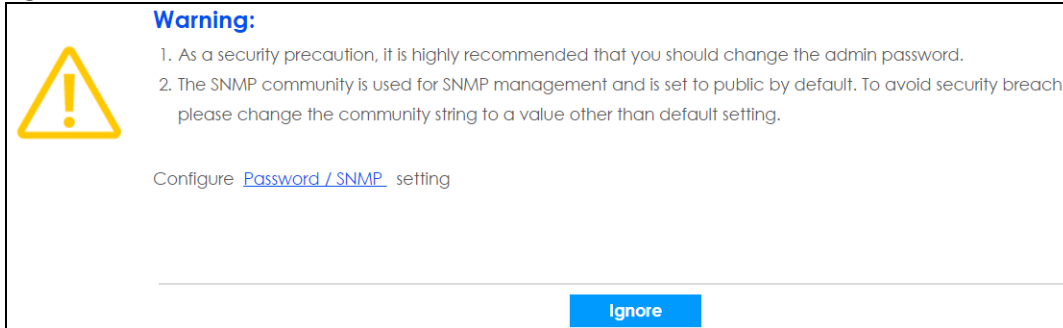
**Figure 45**   The Login Screen



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.

**5** If you did not change the default administrator password and/or SNMP community values, a warning screen displays each time you log into the Web Configurator. Click **Password / SNMP** to open a screen where you can change the administrator and SNMP passwords simultaneously. Otherwise, click Ignore to close it.

**Figure 46** Web Configurator: Warning
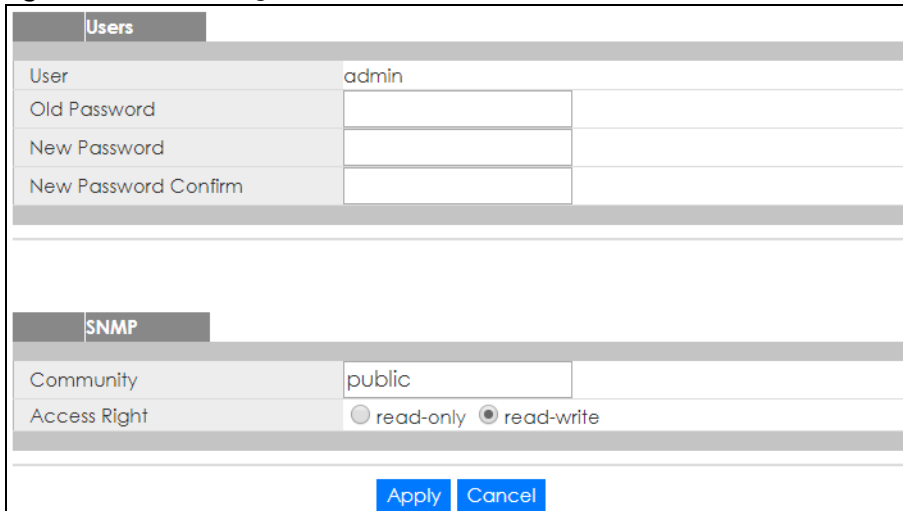


**Figure 47** Web Configurator: Password



Change the default administrator and/or SNMP passwords, and then click **Apply** to save your changes.

Table 7   Web Configurator: Password > Users/SNMP

| LABEL | DESCRIPTION |
|---|---|
| User | This is the default administrator account with the "admin" user name. You cannot change the default administrator user name. |
| Old Password | Type the existing system password (**1234** is the default password when shipped). |
| New Password | Enter your new system password. |
| New Password Confirm | Retype your new system password for confirmation. |
| SNMP

Use this section to specify the SNMP community (password) and access right values. | |
| Community | 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**. |

Table 7   Web Configurator: Password > Users/SNMP (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save 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. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 5.3  Navigating the Web Configurator

The following summarizes how to navigate the Web Configurator from the **Getting Start** screen. This guide uses the GS1900-24HP screens as an example. The screens may vary slightly for different models.

Figure 48   The Web Configurator's Main Screen
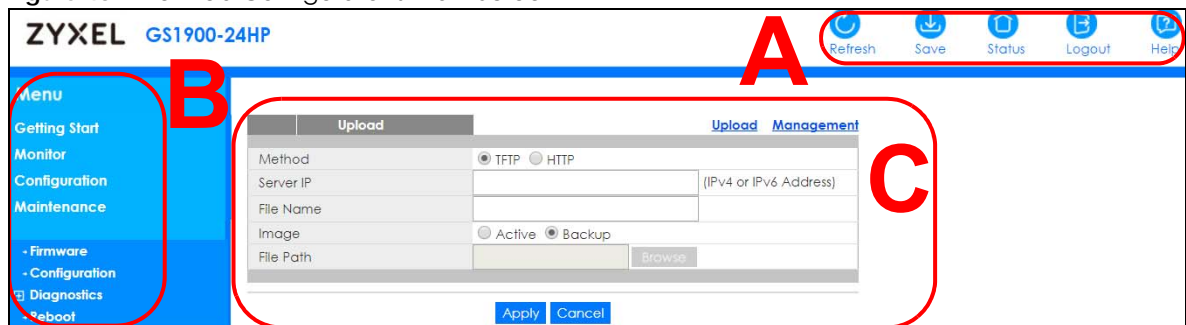


The Web Configurator's main screen is divided into these parts:

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

## 5.3.1  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 49   Title Bar



The icons provide the following functions.

Table 8   Title Bar: Web Configurator Icons

| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click **Refresh** to reload the page. |
| 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. |
| Status | Click this to display basic information about the Switch. |

Table 8   Title Bar: Web Configurator Icons (continued)

| LABEL | DESCRIPTION |
|-------|-------------|
| Logout | Click this to log out of the Web Configurator. |
| 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.

## 5.3.2  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 50**   Navigation Panel
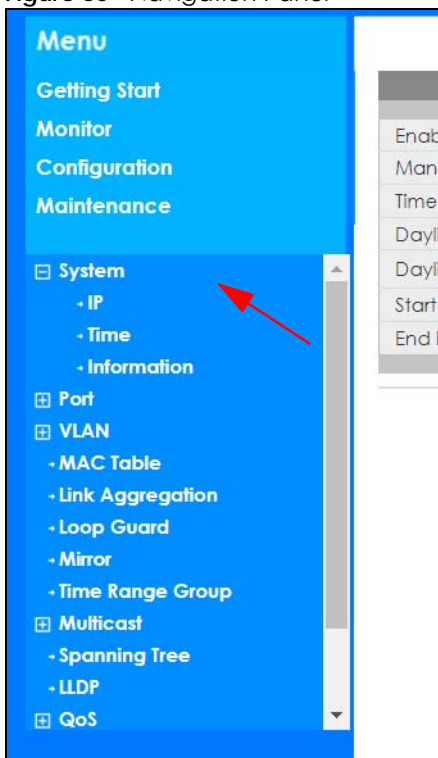


### Getting Start

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

For details on Getting Start features, see .

## Monitor Menu

The monitor menu screens display status and statistics information.

Table 9   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 | | Displays PoE status. |
| Bandwidth Management | | 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. |
| IGMP | VLAN | Displays VLAN settings. |
| | Statistics | Displays statistics settings. |
| | Group | Displays group settings. |
| | Router | Displays router settings. |

Table 9   Monitor Menu Screens Summary (continued)

| FOLDER OR LINK | TAB | FUNCTION |
|---|---|---|
| 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 10   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. |
| PoE | Global | This link takes you to a screen where you can configure the global settings for the Switch to supply power over Ethernet (PoE). |
| | Port | This link takes you to a screen where you can configure port PoE settings. |

Table 10   Configuration Menu Screens Summary (continued)

| FOLDER OR LINK | TAB | FUNCTION |
|---|---|---|
| Bandwidth Management | | Configure egress global burst and port rate. |
| Storm Control | | 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. |
| Time Range Group | | This link takes you to a screen where you can define different schedules. |
| 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. |

Table 10   Configuration Menu Screens Summary (continued)

| FOLDER OR LINK | TAB | FUNCTION |
|---|---|---|
| Spanning Tree | | This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops. |
| | Global | Configure global settings. |
| | 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. |
| 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. |

Table 10   Configuration Menu Screens Summary (continued)

| FOLDER OR LINK | TAB | FUNCTION |
|---|---|---|
| Syslog | Global | Configure global settings. |
| | Local | Configure local settings. |
| | 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 11   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 | | Manage cable diagnosis and test results. |
| PING | IPv4 | Manage ping test settings. |
| | IPv6 | Manage IPv6 ping test settings. |
| Trace | | Manage trace route settings. |
| Reboot | | Reset the system. |

# Getting Start

## 6.1  Overview

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

### 6.1.1  What You Can Do in this Chapter

- The main **Getting Start** screen (Section 6.2 on page 52) 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.

## 6.2  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 51**   Getting Start
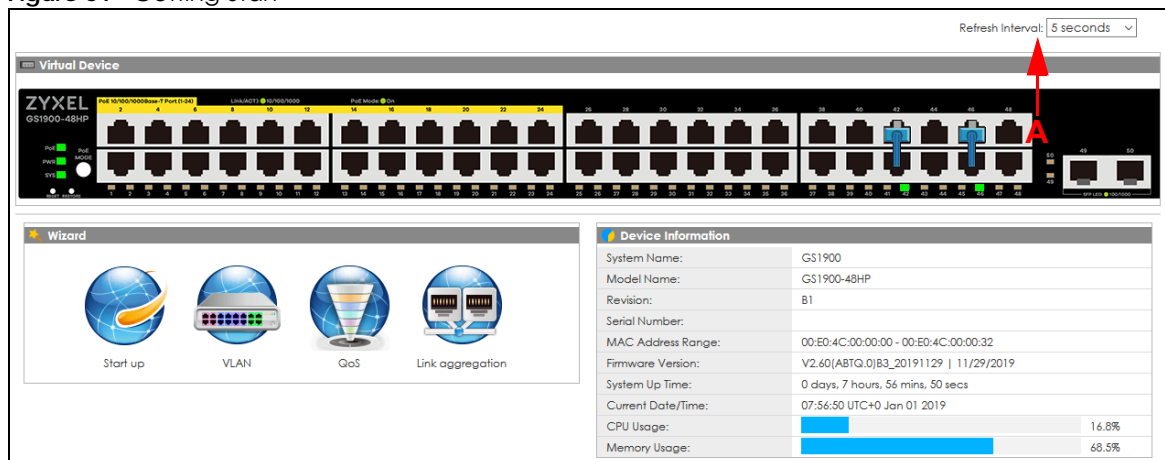


The following table describes the labels in this screen.

Table 12   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 | |

Table 12   Getting Start (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Name | This field displays the name used to identify the Switch on any network. |
| Model Name | This field displays the model name of this Switch. |
| Revision | This field displays the hardware revision number 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. |

## 6.2.1  Wizard

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

For details on Wizard features, see system Chapter 7 on page 62, VLAN Chapter 9 on page 74, QoS Chapter 29 on page 188, and link aggregation Chapter 11 on page 83.

### 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** to access this screen.

**Figure 52**   Getting Start > Start up > 1 Step 1 Set up IP

Each field is described in the following table.

Table 13   Getting Start > Start up > 1 Step 1 Set up IP

| 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.<br><br>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 user name screen appears.

**Figure 53**   Getting Start > Start up > 2 Step 2 Set up user name/password



Each field is described in the following table.

Table 14   Getting Start > Start up > 2 Step 2 Set up user name/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 54** Getting Start > Start up > 3 Step 3 Finish



Each field is described in the following table.

Table 15   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 55** Getting Start > VLAN > 1 Step 1 Create VLAN



Each field is described in the following table.

Table 16   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 56** Getting Start > VLAN > 2 Step 2 Tag VLAN Setting

Each field is described in the following table.

Table 17   Getting Start > VLAN > 2 Step 2 Tag VLAN Setting

| LABEL | DESCRIPTION |
|---|---|
| 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 do not 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 57   Getting Start > VLAN> 3 Step 3 Finish
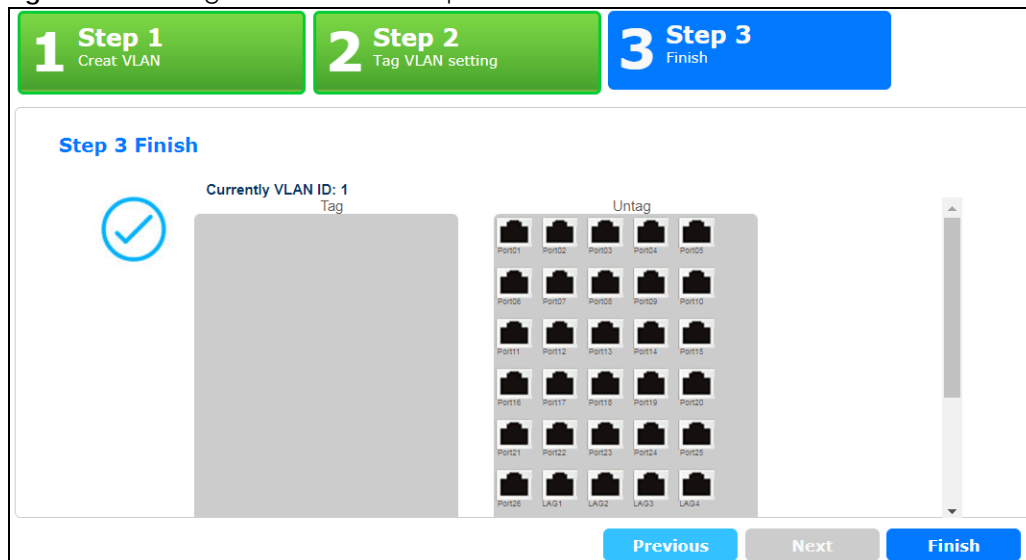


Each field is described in the following table.

Table 18   Getting Start > VLAN > 3 Step 3 Finish

| LABEL | DESCRIPTION |
|---|---|
| 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 do not 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 (Quality of Service)** to access this screen.

**Figure 58** Getting Start > QoS > 1 Step 1 QoS (Quality of Service)
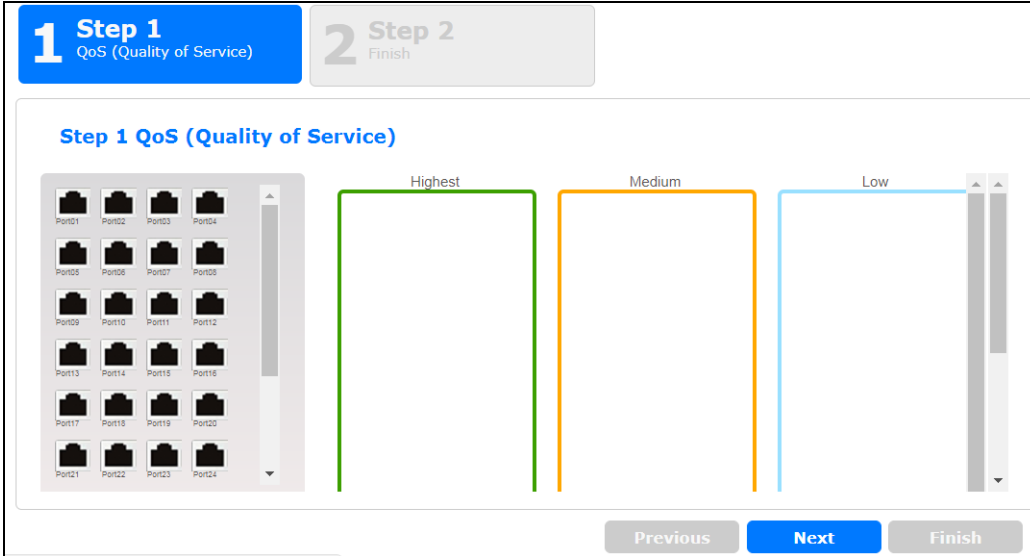


Each field is described in the following table.

Table 19   Getting Start > QoS > 1 Step 1 QoS (Quality of Service)

| 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 59** Getting Start > QoS > 2 Step 2 Finish
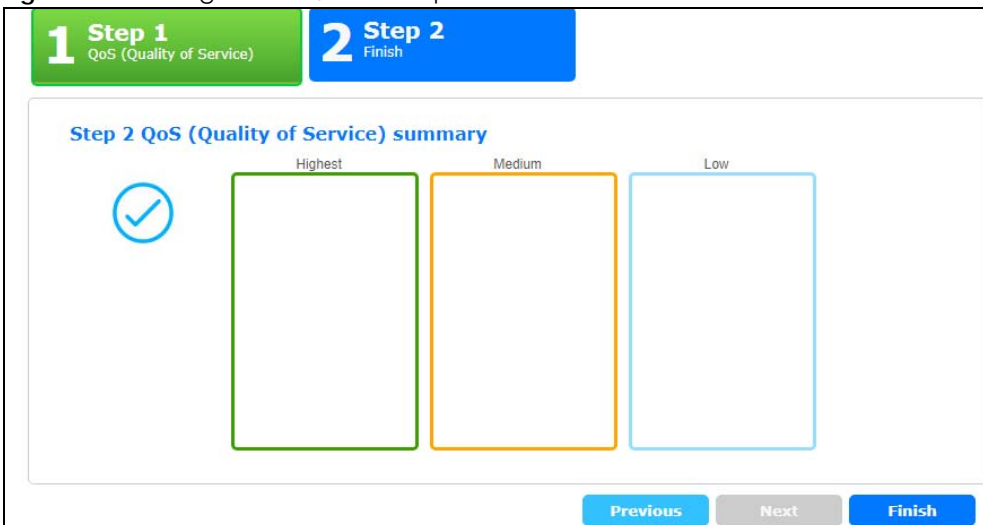
Each field is described in the following table.

Table 20   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 60**   Getting Start > Link aggregation > 1 Step 1 Link aggregation
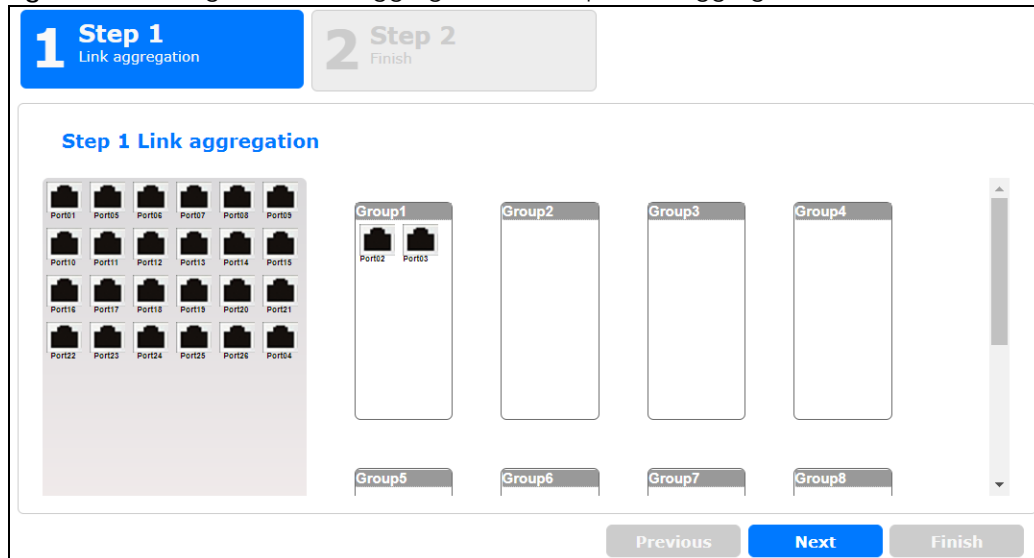


Each field is described in the following table.

Table 21   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 61** Getting Start > Link aggregation > 2 Step 2 Finish
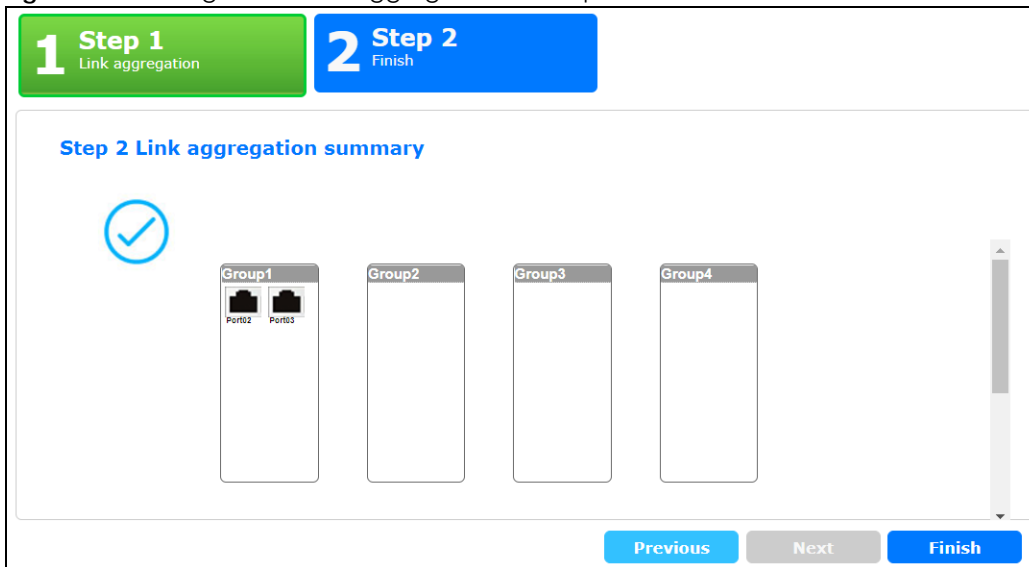


Each field is described in the following table.

Table 22 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

# Monitor: System

## 7.1 Overview

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

### 7.1.1 What You Can Do in this Chapter

- The **IP** screen (Section 7.2 on page 62) displays IPv4 and IPv6.
- The **Information** screen (Section 7.3 on page 63) displays the system information.
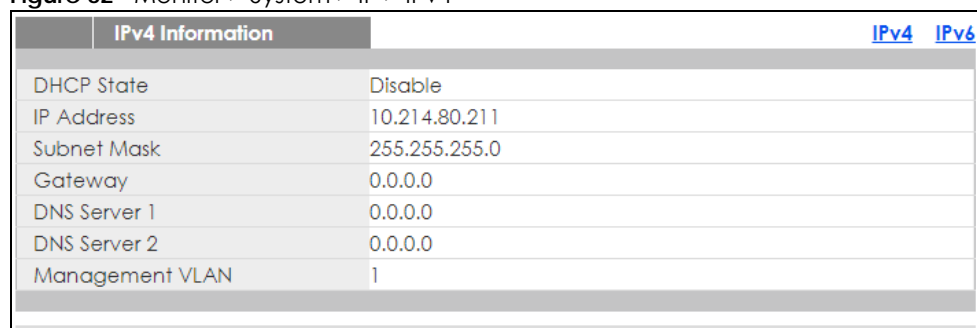
## 7.2 IP

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.

### 7.2.1 IPv4

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

**Figure 62**   Monitor > System > IP > IPv4

| IPv4 Information | IPv4   IPv6 |
|---|---|
| DHCP State | Disable |
| IP Address | 10.214.80.211 |
| Subnet Mask | 255.255.255.0 |
| Gateway | 0.0.0.0 |
| DNS Server 1 | 0.0.0.0 |
| DNS Server 2 | 0.0.0.0 |
| Management VLAN | 1 |

The following table describes the labels in this screen.

Table 23   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. |

Table 23   Monitor > System > IP > IPv4 (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 7.2.2  IPv6

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

Figure 63   Monitor > System > IP > IPv6

| **IPv6 Information** | | **IPv4**  **IPv6** |
|---|---|---|
| Auto Configuration | Enable | |
| IPv6 Address | fe80::4e9e:ffff:fe72:4a87 / 64 | |
| IPv6 Gateway | :: | |
| DHCPv6 Client | Disable | |

The following table describes the labels in this screen.

Table 24   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. |

# 7.3  Information

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

Figure 64   Monitor > System > Information > System Information

| **System Information** | |
|---|---|
| System Name | GS1900 |
| System Location | Location |
| System Contact | Contact |

The following table describes the labels in this screen.

Table 25   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. |

# 8.1  Overview

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

## 8.1.1  What You Can Do in this Chapter

- The **Port** screen (Section 8.2 on page 65) displays status, port counters, and bandwidth utilization.
- The **PoE** screen (Section 8.3 on page 69) displays PoE.
- The **Bandwidth Management** screen (Section 8.4 on page 71) displays bandwidth control.
- The **Storm Control** screen (Section 8.5 on page 72) displays port settings of the Switch.

# 8.2  Port

Use this screen to view Switch port settings.

## 8.2.1  Status

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

**Figure 65**   Monitor > Port > Port > Status

| | Status | | | | | Status  Port Counters  Bandwidth Utilization | |
|---|---|---|---|---|---|---|---|
| Port | Port Name | State | Link Status | Speed | Duplex | FlowCtrl Status | Type |
| 1 | | Enable | Down | Auto | Auto | Disable | Copper |
| 2 | | Enable | Down | Auto | Auto | Disable | Copper |
| 3 | | Enable | Down | Auto | Auto | Disable | Copper |
| 4 | | Enable | Down | Auto | Auto | Disable | Copper |
| 5 | | Enable | Down | Auto | Auto | Disable | Copper |
| 6 | | Enable | Down | Auto | Auto | Disable | Copper |
| 7 | | Enable | Down | Auto | Auto | Disable | Copper |
| 8 | | Enable | Down | Auto | Auto | | |
| 21 | | Enable | Down | Auto | Auto | Disable | Copper |
| 22 | | Enable | Up | Auto-1000M | Auto-full | Disable | Copper |
| 23 | | Enable | Down | Auto | Auto | Disable | Copper |
| 24 | | Enable | Up | Auto-1000M | Auto-full | Disable | Copper |
| 25 | | Enable | Down | Auto | Auto | Disable | Fiber |
| 26 | | Enable | Down | Auto | Auto | Disable | Fiber |

Each field is described in the following table.

Table 26   Monitor > Port > Port > Status

| LABEL | DESCRIPTION |
|---|---|
| Port | This is the port index number. |
| Port Name | A descriptive name that identifies this port. |
| State | This is port admin setting state. |
| Link Status | This field displays **Up**, **Down** or **Not Present**. It displays **Up** when the port is linked up or **Down** when it is not. When no any physical port is binding with this group, it displays **Not Present**. |
| 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. |

## 8.2.2  Port Counters

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

Figure 66   Monitor > Port > Port > Port Counters (Port 1 Interface mib Counters)

**Figure 67**  Monitor > Port > Port > Port Counters (Port 1 Etherlike mib Counters)



**Figure 68**  Monitor > Port > Port > Port Counters (Port 1 RMON mib Counters)



Each field is described in the following table.

Table 27   Monitor > Port > Port > Port Counters

| LABEL | DESCRIPTION |
|---|---|
| Port Counters | |
| Port | This field displays the port. |
| 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. |

Table 27   Monitor > Port > Port > Port Counters (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| etherStatsPkts | This field displays the etherStatsPkts. |
| 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. |
| etherStatsPkts256to511Octets | This field displays the etherStatsPkts256to511Octets. |
| etherStatsPkts512to1023Octets | This field displays the etherStatsPkts512to1023Octets. |
| etherStatsPkts1024to1518Octets | This field displays the etherStatsPkts1024to1518Octets. |

## 8.2.3  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 69** Monitor > Port > Port > Bandwidth Utilization



Each field is described in the following table.

Table 28 Monitor > Port > Port > Bandwidth Utilization

| LABEL | DESCRIPTION |
|---|---|
| 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 the time interval in seconds. |

# 8.3  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 70   Powered Device Examples
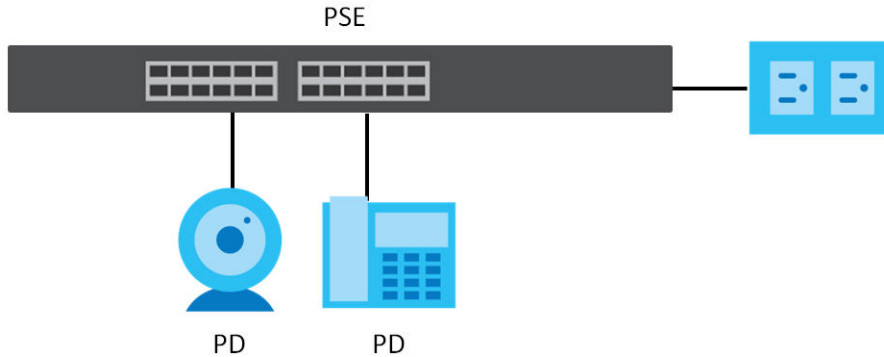


You can also set priorities so that the Switch is able to reserve and allocate power to certain PDs.

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 71   Monitor > Port > PoE



Each field is described in the following table.

Table 29   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. The total power of GS1900-10HP is 77W and GS1900-8HP is 70W. |
| Consuming Power(W) | This field displays the total amount of power the Switch is currently supplying to the connected PoE-enabled devices. |
| Allocated Power(W) | This field displays the total amount of power the Switch (in **Classification** mode) has reserved for PoE after negotiating with the connected PoE device(s). It shows **NA** when the Switch is in **Consumption** mode.<br><br>**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.<br><br>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. |

# 8.4  Bandwidth Management

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

## 8.4.1  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 72**  Monitor > Port > Bandwidth Management > Bandwidth Control

| Bandwidth Control | | |
| --- | --- | --- |
| Egress Global Burst | 40000(Byte) | |
| | | |
| **Port Rate** | | |
| **Port** | **Ingress RateLimit (Kbps)** | **Egress RateLimit (Kbps)** |
| 1 | Disable | Disable |
| 2 | Disable | Disable |
| 3 | Disable | Disable |
| 4 | Disable | Disable |
| 5 | Disable | Disable |
| 6 | Disable | Disable |
| 7 | Disable | Disable |
| 8 | Disable | Disable |
| 9 | Disable | Disable |
| 10 | Disable | Disable |
| 11 | Dis... | Di... |
| 22 | Disable | Disable |
| 23 | Disable | Disable |
| 24 | Disable | Disable |
| 25 | Disable | Disable |
| 26 | Disable | Disable |

Each field is described in the following table.

Table 30   Monitor > Port > Bandwidth Management > Bandwidth Control

| LABEL | DESCRIPTION |
| --- | --- |
| Bandwidth Control | |
| 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 30   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. |

# 8.5  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 73**   Monitor > Port > Storm Control

| Storm Control | | | | | |
|---|---|---|---|---|---|
| Port | State | Broadcast (pps) | Unknown Multicast (pps) | Unknown Unicast (pps) | Action |
| 1 | Disable | Disable | Disable | Disable | Drop |
| 2 | Disable | Disable | Disable | Disable | Drop |
| 3 | Disable | Disable | Disable | Disable | Drop |
| 4 | Disable | Disable | Disable | Disable | Drop |
| 5 | Disable | Disable | Disable | Disable | Drop |
| 6 | Disable | Disable | Disable | Disable | Drop |
| 7 | Disable | Disable | Disable | Disable | Drop |
| 8 | Disable | Disable | Disable | Disable | Drop |
| 9 | Disable | Disable | Disable | Disable | Drop |
| 10 | Disable | Disable | Disable | Disable | Drop |
| 11 | Disable | Disable | Disable | Disable | Drop |
| 12 | Disable | Disable | Disable | Disable | Drop |
| 13 | Disable | Disable | Disable | Disable | Drop |
| 14 | Disable | Disable | Disable | Disable | Drop |
| 15 | Disable | Disable | Disable | Disable | Drop |
| 16 | Disable | Disable | Disable | Disable | Drop |
| 17 | Disable | Disable | Disable | Disable | Drop |
| 18 | Disable | Disable | Disable | Disable | Drop |
| 19 | Disable | Disable | Disable | Disable | Drop |
| 20 | Disable | Disable | Disable | Disable | Drop |
| 21 | Disable | Disable | Disable | Disable | Drop |
| 22 | Disable | Disable | Disable | Disable | Drop |
| 23 | Disable | Disable | Disable | Disable | Drop |
| 24 | Disable | Disable | Disable | Disable | Drop |
| 25 | Disable | Disable | Disable | Disable | Drop |
| 26 | Disable | Disable | Disable | Disable | Drop |

Each field is described in the following table.

Table 31   Monitor > Port > Storm Control

| LABEL | DESCRIPTION |
|---|---|
| Storm Control | |
| 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:<br><br>• **Drop** - drop the packet.<br><br>• **Shutdown** - shutdown the connection. |

# Monitor: VLAN

## 9.1 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.

### 9.1.1 What You Can Do in this Chapter

- The **VLAN** screen (Section 9.2 on page 74) displays VLAN, port, and VLAN port settings.
- The **Guest VLAN** screen (Section 9.3 on page 77) displays the global and port settings of the Switch.
- The **Voice VLAN** screen (Section 9.4 on page 78) displays the global and port settings of the Switch.

## 9.2 VLAN

Use this screen to view Switch VLAN settings.

### 9.2.1 VLAN

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

**Figure 74** Monitor > VLAN > VLAN > VLAN

| VLAN | | VLAN   Port   VLAN Port |
|---|---|---|
| **VLAN ID** | **VLAN Name** | **VLAN Type** |
| 1 | default | Default |

---

Each field is described in the following table.

Table 32   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. |

## 9.2.2  Port

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

Figure 75   Monitor > VLAN > VLAN > Port



Each field is described in the following table.

Table 33   Monitor > VLAN > VLAN > Port

| LABEL | DESCRIPTION |
|---|---|
| Port | |
| Port | This field displays the port number. |
| PVID | This is the port VLAN identification number.<br><br>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 33   Monitor > VLAN > VLAN > Port (continued)

| LABEL | DESCRIPTION |
|---|---|
| Accept Frame Type | This field displays the type that is accepted by the frame. |
| | Specifies 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. |

## 9.2.3  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 76**   Monitor > VLAN > VLAN > VLAN Port

Each field is described in the following table.

Table 34   Monitor > VLAN > VLAN > VLAN Port

| LABEL | DESCRIPTION |
|---|---|
| VLAN Port | |
| VLAN ID | This is the VLAN identification number. |
| Port | Displays the port index value. |
| Membership | Displays the status of the VLAN group: **Forbidden**, **Excluded**, **Tagged** or **Untagged**. |

# 9.3  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 77   Guest VLAN Example
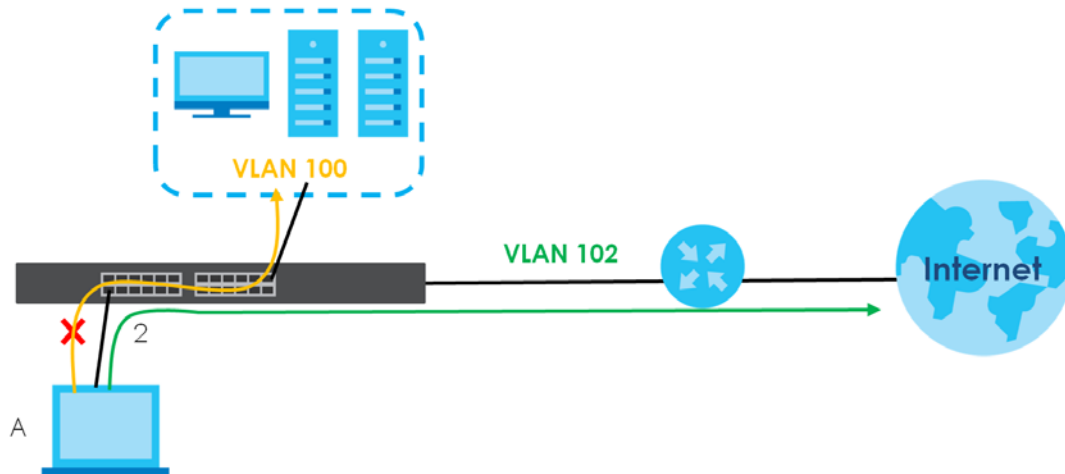


Use this screen to view the Switch's guest VLAN. Click **Monitor > VLAN > Guest VLAN** to access this screen.

**Figure 78** Monitor > VLAN > Guest VLAN

| Guset VLAN | | |
|---|---|---|
| State | Disable | |

**Port**

| Port | State | In Guest VLAN |
|---|---|---|
| 1 | Disable | No |
| 2 | Disable | No |
| 3 | Disable | No |
| 4 | Disable | No |
| 5 | Disable | No |
| 6 | Disable | No |
| 7 | Disable | No |
| 8 | Disable | No |
| | | No |
| 21 | Disable | No |
| 22 | Disable | No |
| 23 | Disable | No |
| 24 | Disable | No |
| 25 | Disable | No |
| 26 | Disable | No |

Each field is described in the following table.

Table 35   Monitor > VLAN > Guest VLAN

| LABEL | DESCRIPTION |
|---|---|
| Guest VLAN | |
| 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. |

# 9.4  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 79**   Monitor > VLAN > Voice VLAN



Each field is described in the following table.

Table 36   Monitor > VLAN > Voice VLAN

| LABEL | DESCRIPTION |
|---|---|
| Voice VLAN | |
| 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 | |
| Port | This field displays a port number. |
| State | This field displays the state of a port. |

# CHAPTER 10
# Monitor: MAC Table

## 10.1 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 80**   MAC Table Flowchart
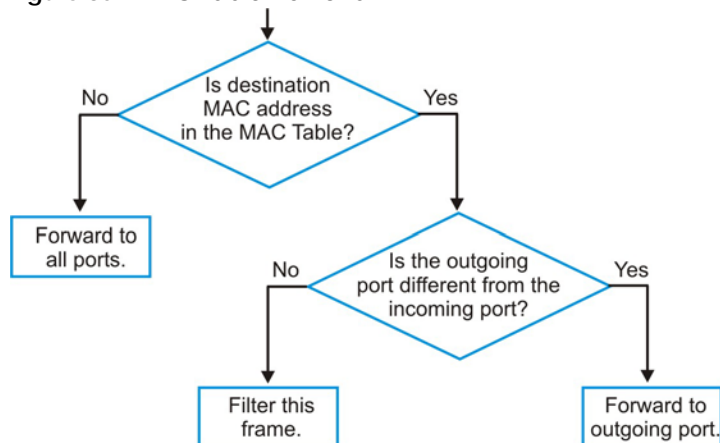


This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of MAC address it is.

### 10.1.1  What You Can Do in this Chapter

- The **MAC Table** screen (Section 10.2 on page 81) displays view filter and MAC table of the Switch.

## 10.2  MAC Table

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

**Figure 81**   Monitor > MAC Table

| MAC Table | | | |
|---|---|---|---|
| MAC Address | --- | (00:00:00:00:00:00) | |
| VLAN | --- ▼ | | |
| Port | --- ▼ | | |

View    Clear

| MAC Address | VLAN | Type | Port |
|---|---|---|---|
| 10:BF:48:D5:AB:72 | default(1) | Dynamic | 24 |
| 20:6A:8A:00:F2:57 | default(1) | Dynamic | 24 |
| 20:6A:8A:39:FB:38 | default(1) | Dynamic | 24 |
| 3C:97:0E:63:AF:24 | default(1) | Dynamic | 24 |
| 4C:9E:FF:72:4A:87 | default(1) | Static Unicast | CPU |
| 74:27:EA:2B:FA:AA | default(1) | Dynamic | 24 |
| 90:2B:34:BB:7A:A4 | default(1) | Dynamic | 24 |
| B8:EC:A3:0F:CF:9F | default(1) | Dynamic | 24 |
| C0:3F:D5:F9:9A:48 | default(1) | Dynamic | 24 |
| C0:3F:D5:F9:BA:0A | default(1) | Dynamic | 24 |
| DC:4A:3E:40:EC:5F | default(1) | Dynamic | 24 |
| DC:4A:3E:40:EC:67 | default(1) | Dynamic | 12 |
| E4:18:6B:F7:BA:79 | default(1) | Dynamic | 24 |
| E4:18:6B:F7:BA:8B | default(1) | Dynamic | 24 |

Total Entries: 14

Each field is described in the following table.

Table 37   Monitor > MAC Table

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| 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 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. |

Table 37   Monitor > MAC Table (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

# CHAPTER 11
# Monitor: Link Aggregation

## 11.1 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.

### 11.1.1 What You Can Do in this Chapter

- The **Link Aggregation** screen (Section 11.2 on page 83) displays link aggregation status.

## 11.2 Link Aggregation

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

**Figure 82** Monitor > Link Aggregation

| 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 38   Monitor > Link Aggregation

| 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. It displays **Up** when the port is linked up or **Down** when it is not. When no any physical port is binding with this group, it displays **NotPresent**. |
| 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. |

# CHAPTER 12
# Monitor: Loop Guard

## 12.1 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 83**   Switch in Loop State
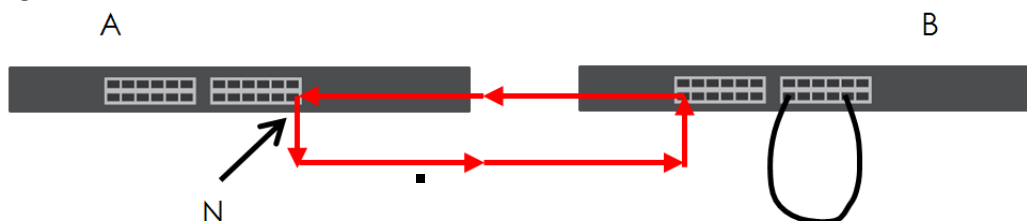


The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop 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 84**   Loop Guard - Probe Packet
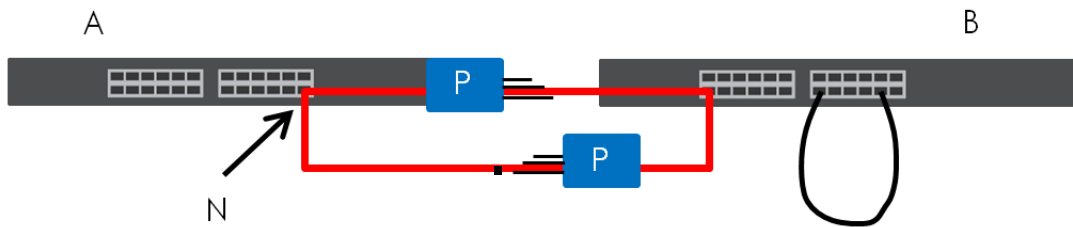


The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this 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 85**   Loop Guard - Network Loop
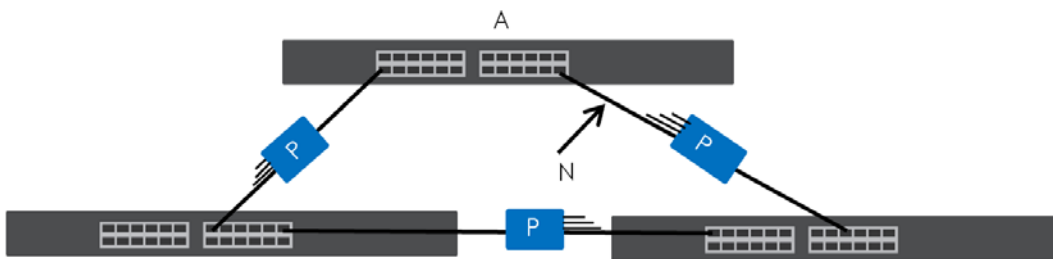


## 12.1.1  What You Can Do in this Chapter

- The **Loop Guard** screen (Section 12.2 on page 86) displays loop guard status.

# 12.2  Loop Guard

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

**Figure 86**   Monitor > Loop Guard

| Loop Guard | | | |
|---|---|---|---|
| **Port** | **Status** | **Time Left (sec)** | **Action** |
| 1 | No Loop | --- | Recovery |
| 2 | No Loop | --- | Recovery |
| 3 | No Loop | --- | Recovery |
| 4 | No Loop | --- | Recovery |
| 5 | No Loop | --- | Recovery |
| 6 | No Loop | --- | Recovery |
| 7 | No Loop | --- | Recovery |
| 8 | No Loop | --- | Recovery |
| | No Loop | --- | Recovery |
| 21 | No Loop | --- | Recovery |
| 22 | No Loop | --- | Recovery |
| 23 | No Loop | --- | Recovery |
| 24 | No Loop | --- | Recovery |
| 25 | No Loop | --- | Recovery |
| 26 | No Loop | --- | Recovery |

Each field is described in the following table.

Table 39   Monitor > Loop Guard

| LABEL | DESCRIPTION |
|---|---|
| Loop Guard | |
| 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. |

# Monitor: Multicast

## 13.1 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.

### 13.1.1 What You Can Do in this Chapter

- The **IGMP** screen (Section 13.2 on page 88) displays Vlan, statistics, group, and router.
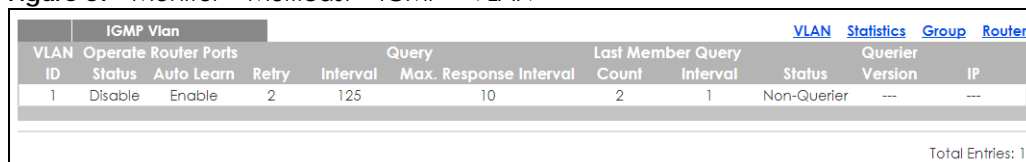
## 13.2 IGMP

Use this screen to view Switch various multicast features.

### 13.2.1 VLAN

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

**Figure 87** Monitor > Multicast > IGMP > VLAN

| | IGMP Vlan | | | | | | | | | VLAN | Statistics | Group | Router |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| VLAN ID | Operate Status | Router Ports Auto Learn | Retry | Interval | Query Max. Response Interval | | Last Member Query Count | Interval | | Status | Querier Version | IP | |
| 1 | Disable | Enable | 2 | 125 | 10 | | 2 | 1 | | Non-Querier | --- | --- | |

Total Entries: 1

Each field is described in the following table.

Table 40   Monitor > Multicast > IGMP > VLAN

| LABEL | DESCRIPTION |
|---|---|
| IGMP Vlan | |
| VLAN ID | Displays the identification for the VLAN. |
| Operate Status | Displays the status of the operation. |

Table 40   Monitor > Multicast > IGMP > VLAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. Response Interval (sec) | Displays the maximum response (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 | Allows the 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 entry querier IP address. |
| Total Entries | This field displays the number of total entries. |

## 13.2.2  Statistics

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

**Figure 88**   Monitor > Multicast > IGMP > Statistics



Each field is described in the following table.

Table 41   Monitor > Multicast > IGMP > Statistics

| LABEL | DESCRIPTION |
|---|---|
| IGMP Statistics | |
| Port | This field displays a port number. |
| Total RX | This field displays the total amount of RX. |

Table 41   Monitor > Multicast > IGMP > Statistics

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Action | Click **Action** to reset the statistics of the specific field back to zero. |
| Clear | Click **Clear** to clear statistics on this port. |
| Clear | Click **Clear** to reset the fields to the factory defaults. |
| Refresh | Click **Refresh** to reload the page. |

In the Action column, the **Action** option allows you to clear the statistics.

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 89**   Monitor > Multicast > IGMP > Statistics > Action
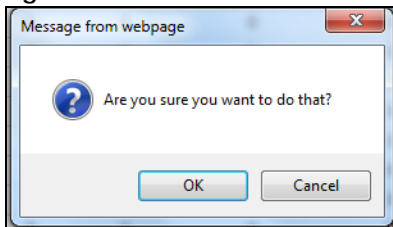


## 13.2.3  Group

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

**Figure 90**   Monitor > Multicast > IGMP > Group

Each field is described in the following table.

Table 42   Monitor > Multicast > IGMP > Group

| LABEL | DESCRIPTION |
|---|---|
| IGMP Group | |
| 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. |
| Clear | Click **Clear** to delete the dynamic groups. |
| Refresh | Click **Refresh** to reload the page. |

## 13.2.4  Router

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

Figure 91   Monitor > Multicast > IGMP > Router



Each field is described in the following table.

Table 43   Monitor > Multicast > IGMP > Router

| LABEL | DESCRIPTION |
|---|---|
| IGMP Router | |
| 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. |

# Monitor: Spanning Tree

## 14.1  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).

### 14.1.1  What You Can Do in this Chapter

- The **Spanning Tree** screen () displays CIST, CIST port, MST, MST port, STP statistics.

## 14.2  Spanning Tree

Use this screen to view Switch spanning tree settings.

### 14.2.1  CIST

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

Figure 92   Monitor > Spanning Tree > CIST

| CIST Instance | | CIST | CIST Port | MST | MST Port | STP Statistics |
|---|---|---|---|---|---|---|
| State | Disable | | | | | |
| Bridge Identifier | 32768/ 0/4C:9E:FF:72:4A:87 | | | | | |
| Designated Root Bridge | 0/ 0/00:00:00:00:00:00 | | | | | |
| External Root Path Cost | 0 | | | | | |
| Regional Root Bridge | 0/ 0/00:00:00:00:00:00 | | | | | |
| Internal Root Path Cost | 0 | | | | | |
| Designated Bridge | 0/ 0/00:00:00:00:00:00 | | | | | |
| Root Port | 0/0 | | | | | |
| Remaining Hops | 0 | | | | | |
| Last Topology Change | 0 | | | | | |

Each field is described in the following table.

Table 44   Monitor > Spanning Tree > CIST

| LABEL | DESCRIPTION |
|---|---|
| CIST Instance | |
| State | This field displays the state. |

Table 44   Monitor > Spanning Tree > CIST

| LABEL | DESCRIPTION |
|---|---|
| Bridge Identifier | This is the unique identifier for this bridge, consisting of the bridge priority plus the MAC address. |
| Designated 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. |
| Remaining Hops | This field displays the number of remaining hops. |
| Last Topology Change | Topology change information is directly propagated throughout the network from the device that generates the topology change. |

## 14.2.2  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 93   Monitor > Spanning Tree > CIST Port



Each field is described in the following table.

Table 45   Monitor > Spanning Tree > CIST Port

| LABEL | DESCRIPTION |
|---|---|
| Port | This field displays the port number. |
| Identifier (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. |

Table 45   Monitor > Spanning Tree > CIST Port

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Designated 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. |

## 14.2.3  MST

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

Figure 94   Monitor > Spanning Tree > MST



Each field is described in the following table.

Table 46   Monitor > Spanning Tree > MST

| LABEL | DESCRIPTION |
|---|---|
| MST Instance | |
| 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. |

Table 46   Monitor > Spanning Tree > MST

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Remaining Hops | This field displays the number of remaining hops. |
| Last Topology Change | Topology change information is directly propagated throughout the network from the device that generates the topology change. |

## 14.2.4  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 95   Monitor > Spanning Tree > MST Port



Each field is described in the following table.

Table 47   Monitor > Spanning Tree > MST Port

| LABEL | DESCRIPTION |
|---|---|
| MST Port | |
| 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. |
| Identifier (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. |

*Table 47   Monitor > Spanning Tree > MST Port (continued)*

| LABEL | DESCRIPTION |
| --- | --- |
| 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. |

## 14.2.5  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 96**   Monitor > Spanning Tree > STP Statistics

| Port | Configuration BDPUs Received | TCN BDPUs Received | MSTP BDPUs Received | Configuration BDPUs Transmitted | TCN BDPUs Transmitted | MSTP BDPUs Transmitted |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | | 0 | |
| | | | | | | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 |
| 26 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG1 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG2 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG3 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG4 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG5 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG6 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG7 | 0 | 0 | 0 | 0 | 0 | 0 |
| LAG8 | 0 | 0 | 0 | 0 | 0 | 0 |

Each field is described in the following table.

Table 48   Monitor > Spanning Tree > STP Statistics

| LABEL | DESCRIPTION |
|---|---|
| MST Port | |
| 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. |

# CHAPTER 15
# Monitor: LLDP

## 15.1 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.

### 15.1.1 What You Can Do in this Chapter

- The **LLDP** screen () displays statistics, remote information, and overloading.

## 15.2 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.

### 15.2.1 Statistics

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

**Figure 97**   Monitor > LLDP > Statistics

| Statistics | | | | | Statistics | Remote Information | Overloading |
|---|---|---|---|---|---|---|---|
| Insertions | 1 | | | | | | |
| Deletions | 0 | | | | | | |
| Drops | 0 | | | | | | |
| Age Outs | 0 | | | | | | |

Clear    Refresh

**LLDP Port Statistics**

| Port | TX Frames Total | RX Frames Total | RX Frames Discarded | Errors | RX TLVs Discarded | RX TLVs Unrecognized | RX Ageouts Total |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | | | | |
| | | | | 0 | 0 | | 0 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 465 | 465 | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Each field is described in the following table.

Table 49   Monitor > LLDP > Statistics

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Clear | Click **Clear** to clear statistics. |
| Refresh | Click **Refresh** to reload the page. |
| 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 Unrecognized | This field displays the number of unrecognized RX LLDP TLVs. |
| RX Ageouts Total | This field displays the total number of RX LLDP ageouts. |

## 15.2.2  Remote Information

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

**Figure 98** Monitor > LLDP > Remote Information



Each field is described in the following table.

Table 50   Monitor > LLDP > Remote Information

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

## 15.2.3  Overloading

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

**Figure 99** Monitor > LLDP > Overloading

Each field is described in the following table.

Table 51   Monitor > LLDP > Overloading

| LABEL | DESCRIPTION |
|---|---|
| Port Overloading | |
| 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 Detail | 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. |

CHAPTER 16
Monitor: Security

## 16.1 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.

### 16.1.1 What You Can Do in this Chapter

- The **Port Security** screen () displays global and port.
- The **802.1X** screen () displays port and authenticated hosts.

## 16.2 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 not be configured.

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

**Figure 100** Monitor > Security > Port Security



Each field is described in the following table.

Table 52 Monitor > Security > Port Security

| LABEL | DESCRIPTION |
|---|---|
| Port Security | |
| 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. |

# 16.3  802.1X

Use this screen to view Switch 802.1x security settings.

## 16.3.1  Port

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

**Figure 101**   Monitor > Security > 802.1X > Port



Each field is described in the following table.

Table 53   Monitor > Security > 802.1X > Port

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

## 16.3.2  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 102**   Monitor > Security > 802.1X > Authenticated Hosts



Each field is described in the following table.

Table 54   Monitor > Security > 802.1X > Authenticated Hosts

| LABEL | DESCRIPTION |
|---|---|
| Authenticated Hosts | |
| 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. |

# Monitor: Management

## 17.1 Overview

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

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

### 17.1.1 What You Can Do in this Chapter

- The **Syslog** screen (Section 17.2 on page 105) displays logging filter select and shows system log.
- The **Error Disable** screen (Section 17.3 on page 106) displays global and port.

## 17.2 Syslog

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

**Figure 103**   Monitor > Management > Syslog



Each field is described in the following table.

Table 55   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. |

---

Table 55   Monitor > Management > Syslog

| LABEL | DESCRIPTION |
|---|---|
| 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. |

# 17.3  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 104** Monitor > Management > Error Disable



Each field is described in the following table.

Table 56   Monitor > Management > Error Disable

| LABEL | DESCRIPTION |
|-------|-------------|
| Error Disable | |
| Recovery Interval | View the number of seconds (from 30 to 2592000) for the time interval of the recovery. |
| Reason Status | |
| 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. De-select this option to turn off this rule. |
| Port Status | |
| 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. |

# CHAPTER 18
# Configuration: System

## 18.1 Overview

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

### 18.1.1 What You Can Do in this Chapter

- The **IP** screen (Section 18.2 on page 108) displays IPv4 and IPv6 settings.
- The **Time** screen (Section 18.3 on page 110) displays the system time and SNTP settings.
- The **Information** screen (Section 18.4 on page 111) displays the system information.

## 18.2 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.

### 18.2.1 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 105**   Configuration > System > IP > IPv4

| IPv4 Address | | IPv4   IPv6 |
| --- | --- | --- |
| Mode | ● Static  ○ DHCP | |
| IP Address | 10.214.80.211 | |
| Subnet Mask | 255.255.255.0 | |
| Gateway | 0.0.0.0 | |
| DNS 1 | 0.0.0.0 | |
| DNS 2 | 0.0.0.0 | |
| Management VLAN | 1 | (1 - 4094) |
| | Apply Cancel | |

The following table describes the labels in this screen.

Table 57   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 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 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. |

## 18.2.2  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 106   Configuration > System > IP > IPv6



The following table describes the labels in this screen.

Table 58   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. |
| IPv6 Address | Enter the IPv6 address of the Switch in the IP domain. |
| Gateway | Enter the IPv6 address of the default outgoing gateway. |

Table 58   Configuration > System > IP > IPv6 (continued)

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

# 18.3  Time

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

## 18.3.1  The System Time Screen

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

**Figure 107**   Configuration > System > Time > System Time



The following table describes the labels in this screen.

Table 59   Configuration > System > Time > 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** to not adjust system time. |
| 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. |

## 18.3.2  The SNTP Server Screen

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

**Figure 108** Configuration > System > Time > SNTP Server

| SNTP Server | | System Time   SNTP Server |
|---|---|---|
| Server | | ( X.X.X.X or Hostname ) |
| Server Port | 123 | ( 1 - 65535 ) |
| | Apply  Cancel | |

The following table describes the labels in this screen.

Table 60   Configuration > System > Time > SNTP Server

| LABEL | DESCRIPTION |
|---|---|
| SNTP Server | |
| Server | 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. |

# 18.4  Information

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

## 18.4.1  The System Information Screen

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

**Figure 109** Configuration > System > Information > System Information

| System Information | | |
|---|---|---|
| System Name | GS1900 | |
| System Location | Location | |
| System Contact | Contact | |
| | Apply  Cancel | |

The following table describes the labels in this screen.

Table 61   Configuration > System > Information > 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. |

# Configuration: Port

## 19.1  Overview

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

### 19.1.1  What You Can Do in this Chapter

- The **Port** screen (Section 19.2 on page 113) displays general port settings.
- The **EEE** screen (Section 19.3 on page 115) displays the port EEE settings.
- The **PoE** screen (Section 19.4 on page 117) displays the port PoE settings.
- The **Bandwidth Management** screen (Section 19.5 on page 122) displays the port ingress and egress settings.
- The **Storm Control** screen (Section 19.6 on page 123) displays the port storm control settings.

## 19.2  Port

Use this screen to view and edit general port settings.

### 19.2.1  The Port Screen

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

**Figure 110** Configuration > Port > Port

| ☐ | Port | Port Name | State | Link Status | Speed | Duplex | FlowCtrl State |
|---|------|-----------|-------|-------------|-------|--------|----------------|
| ☐ | 1 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 2 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 3 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 4 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 5 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 6 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 7 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 8 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 9 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 10 | | | | | | |
| ☐ | 22 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 23 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 24 | | Enable | Up | Auto | Auto | Disable |
| ☐ | 25 | | Enable | Down | Auto | Auto | Disable |
| ☐ | 26 | | Enable | Down | Auto | Auto | Disable |

Edit  Cancel

The following table describes the labels in this screen.

Table 62 Configuration > Port > Port

| LABEL | DESCRIPTION |
|-------|-------------|
| 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.<br><br>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. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 19.2.2 The Port Edit Screen

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

**Figure 111** Configuration > Port > Port > Edit



The following table describes the labels in this screen.

Table 63  Configuration > Port > Port > Edit

| LABEL | DESCRIPTION |
|---|---|
| Port | |
| 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.<br><br>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. |

# 19.3  EEE

Use this screen to view and edit the port EEE settings.

## 19.3.1  The EEE Screen

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 112** Configuration > Port > EEE > EEE



The following table describes the labels in this screen.

Table 64   Configuration > Port > EEE > EEE

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

## 19.3.2  The EEE Edit Screen

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

**Figure 113** Configuration > Port > EEE > EEE > Edit

The following table describes the labels in this screen.

Table 65   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. |

# 19.4  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).

## 19.4.1  The Global Screen

In the navigation panel, click **Configuration > Port > PoE > Global** to display the screen as shown. Use this screen to configure Power over Ethernet (PoE) global settings.

Figure 114   Configuration > Port > PoE > Global



The following table describes the labels in this screen.

Table 66   Configuration > Port > PoE > Global

| LABEL | DESCRIPTION |
|---|---|
| PoE Mode | Select the power management mode you want the Switch to use.<br><br>• **Classification** - Select this if you want the Switch to reserve the maximum power for each PD according to the PD's power class and priority level. If the total power supply runs out, PDs with lower priority do not get power to function. In this mode, the maximum power is reserved based on what you configure in **Max Power** or the standard power limit for each class.<br>• **Consumption** - Select this if you want the Switch to supply the actual power that the PD needs. The Switch also allocates power based on a port's **Max Power** and the PD's power class and priority level. The Switch puts a limit on the maximum amount of power the PD can request and use. In this mode, the default maximum power that can be delivered to the PD is 33 W (IEEE 802.3at Class 4) or 22 W (IEEE 802.3af Classes 0 to 3). |
| Pre-Allocate | This field is only available on GS1900-8HP (Revision B1) and GS1900-10HP only.<br><br>Select **Enable** to have the Switch pre-allocate power to each port based on the classification of the PD device. Otherwise, select **Disable**. |

Table 66   Configuration > Port > PoE > Global (continued)

| LABEL | DESCRIPTION |
|---|---|
| Power Up Sequence Delay | This field is only available on GS1900-8HP (Revision B1) and GS1900-10HP only. |
| | Select **Enable** to allow PoE ports to be powered up one-by-one randomly or **Disable** to allow them all to be powered up at the same time. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 19.4.2 The Port Screen

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

**Figure 115** Configuration > Port > PoE > Port



The following table describes the labels in this screen.

Table 67   Configuration > Port > PoE > Port

| LABEL | DESCRIPTION |
|---|---|
| Edit | Select one or more ports in the first column of the table and click this to configure PoE settings for the ports. |
| 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 powered device (PD) connected to this port cannot get power. |
| | • **Enable** - The PD connected to this port can receive power. |

Table 67   Configuration > Port > PoE > Port (continued)

| LABEL | DESCRIPTION |
|---|---|
| Class | This shows the power classification of the PD. Each PD has a specified maximum power that fall under one of the classes.<br><br>The Class is a number from 0 to 4, where each value represents the range of power that the Switch provides to the PD. The power ranges for each class are as follows.<br><br>• **Class 0** - Default, 0.44 to 12.94<br>• **Class 1** - Optional, 0.44 to 3.84<br>• **Class 2** - Optional, 3.84 to 6.49<br>• **Class 3** - Optional, 6.49 to 12.95<br>• **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. |
| 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.<br><br>• **Critical** has the highest priority.<br>• **High** has the Switch assign power to the port after all critical priority ports are served.<br>• **Medium** has the Switch assign power to the port after all critical and high priority ports are served.<br>• **Low** has the Switch assign power to the port after all critical, high and medium priority ports are served. |
| Power-Up | This shows how the Switch provides power to the connected PD at power-up.<br><br>**802.3af** - the Switch follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up.<br><br>**Legacy** - the Switch can provide power to the connected PDs that require high inrush currents at power-up.<br><br>**Pre-802.3at** - the Switch initially offers power on the port according to the IEEE 802.3af standard, and then switches to support the IEEE 802.3at standard within 75 milliseconds after a PD is connected to the port. Select this option if the Switch is performing 2-event Layer-1 classification (PoE+ hardware classification) or the connected PD is NOT performing Layer 2 power classification using Link Layer Discovery Protocol (LLDP).<br><br>**802.3at** - the Switch supports the IEEE 802.3at High Power over Ethernet standard and can supply power of up to 30W per Ethernet port. IEEE 802.3at is also known as PoE+ or PoE Plus. An IEEE 802.3at compatible device is referred to as Type 2. Power Class 4 (High Power) can only be used by Type 2 devices. If the connected PD requires a Class 4 current when it is turned on, it will be powered up in this mode. |
| Wide Range Detection | This field is available on GS1900-8HP (Revision B1) and GS1900-10HP only.<br><br>This shows whether the Switch enables a wider detection range for the PD or not.<br><br>The Switch detects whether a connected device is a powered device or not before supplying power to the port. For the PD detection, the Switch applies a fixed voltage to the device and then receives returned current. If the returned current is within the IEEE 802.3AF/AT standard range, the device will be considered as a valid PD by the Switch.<br><br>However, in real cases, environmental interferences might easily cause the returned current out of the standard range. This field displays **Enable** if the Switch applies a wider range for PD detection. Otherwise, it displays **Disable**. |
| Consuming Power (mW) | This field displays the current amount of power consumed by the PD from the Switch on this port. |
| Max Power (mW) | This field displays the maximum amount of power the PD could use from the Switch on this port. |
| Time Range | |

Table 67   Configuration > Port > PoE > Port (continued)

| LABEL | DESCRIPTION |
|-------|-------------|
| Name | This field displays the name of the time range (schedule) rule which is applied to the port. PoE is enabled at the specified time/date. |
| Status | This field displays whether the port can receive power from the Switch (**In**) or not (**Out**) currently.<br><br>It shows - if there is no schedule applied to the port. |

## 19.4.3  The PoE Edit Screen

Use this screen to configure Switch port PoE settings. Select a port and click **Edit** in the **Configuration** > **Port** > **PoE** > **Port** screen to open this screen.

**Figure 116**   Configuration > Port > PoE > Port > Edit



The following table describes the labels in this screen.

Table 68   Configuration > Port > PoE > Port > Edit

| LABEL | DESCRIPTION |
|-------|-------------|
| PoE 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. |
| PD Priority | This field is not available for the SFP or SFP+ ports.<br><br>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.<br><br>Select **Critical** to give the PD connected to this port the highest priority.<br><br>Select **High** to set the Switch to assign the remaining power to the port after all critical priority ports are served.<br><br>Select **Medium** to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.<br><br>Select **Low** to set the Switch to assign the remaining power to the port after all critical, high and medium priority ports are served. |

Table 68   Configuration > Port > PoE > Port > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Power-Up | Set how the Switch provides power to a connected PD at power-up. |
|  | **802.3af** - the Switch follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up. |
|  | **Legacy** - the Switch can provide power to the connected PDs that require high inrush currents at power-up. |
|  | **Pre-802.3at** - the Switch initially offers power on the port according to the IEEE 802.3af standard, and then switches to support the IEEE 802.3at standard within 75 milliseconds after a PD is connected to the port. Select this option if the Switch is performing 2-event Layer-1 classification (PoE+ hardware classification) or the connected PD is NOT performing Layer 2 power classification using Link Layer Discovery Protocol (LLDP). |
|  | **802.3at** - the Switch supports the IEEE 802.3at High Power over Ethernet standard and can supply power of up to 30W per Ethernet port. IEEE 802.3at is also known as PoE+ or PoE Plus. An IEEE 802.3at compatible device is referred to as Type 2. Power Class 4 (High Power) can only be used by Type 2 devices. If the connected PD requires a Class 4 current when it is turned on, it will be powered up in this mode. |
| Wide Range Detection | This field is available on the GS1900-8HP (Revision B1) and GS1900-10HP only. |
|  | Select whether to enable a wider detection range for the PD or not. |
|  | The Switch detects whether a connected device is a powered device or not before supplying power to the port. For the PD detection, the Switch applies a fixed voltage to the device and then receives returned current. If the returned current is within the IEEE 802.3AF/AT standard range, the device will be considered as a valid PD by the Switch. |
|  | However, in real cases, environmental interferences might easily cause the returned current out of the standard range. This field displays **Enable** if the Switch applies a wider range for PD detection. Otherwise, it displays **Disable**. |
| Max Power Type | Select **Classification-based** to have the Switch automatically decide the maximum amount of power it can provide on the port according to the connected PD's power classification. |
|  | Select **User-defined** to manually specify the maximum amount of power the PD could use from the Switch on this port. |
| Max Power Threshold | Specify the maximum amount of power the Switch can provide on the port if you set **Max Power Type** to **User-defined**. |
|  | Enter a value between 1000 and 33000 in increments of 200. |
| Time Range | Select a pre-defined schedule (created using the **Time Range** screen) to control when the Switch enables PoE to provide power on the port. |
|  | If you leave this field blank, there is no schedule applied to the port. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 19.5  Bandwidth Management

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

## 19.5.1  The Bandwidth Control Screen

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

Figure 117   Configuration > Port > Bandwidth Management > Egress Global Burst



The following table describes the labels in this screen.

Table 69   Configuration > Port > Bandwidth Management > Egress Global Burst

| LABEL | DESCRIPTION |
|---|---|
| Egress Global Burst | |
| Egress Global Burst | Specify the current egress burst size in bytes for all ports. |
| Port Rate | |
| 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. |

Table 69   Configuration > Port > Bandwidth Management > Egress Global Burst (continued)

| LABEL | DESCRIPTION |
|---|---|
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 19.5.2  The Port Rate Edit Screen

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

Figure 118   Configuration > Port > Bandwidth Management > Egress Global Burst > Edit



The following table describes the labels in this screen.

Table 70   Configuration > Port > Bandwidth Management > Egress Global Burst > 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. |

## 19.6  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.

## 19.6.1 The Port Screen

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

**Figure 119** Configuration > Port > Storm Control > Storm Control



The following table describes the labels in this screen.

Table 71 Configuration > Port > Storm Control > Storm Control

| LABEL | DESCRIPTION |
|---|---|
| Storm Control | |
| 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:<br><br>• **Drop** - drop the packet.<br>• **Shutdown** - shutdown the connection. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 19.6.2 The Port Edit Screen

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

**Figure 120** Configuration > Port > Storm Control > Storm Control > Edit



The following table describes the labels in this screen.

Table 72   Configuration > Port > Storm Control > Storm Control > Edit

| LABEL | DESCRIPTION |
|---|---|
| Storm Control 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:<br><br>• **Drop** - drop the packet when limit is reached.<br>• **Shutdown** - shutdown the connection when a limit is reached. |
| Broadcast (pps) | Click the **Enable** checkbox to active the feature.<br><br>Enter the maximum number of broadcast packets the port can receive per second. |
| Unknown Multicast (pps) | Click the **Enable** checkbox to active the feature.<br><br>Enter the maximum number of multicast packets the port can receive per second. |
| Unknown Unicast (pps) | Click the **Enable** checkbox to active the feature.<br><br>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. |

# CHAPTER 20
# Configuration: VLAN

## 20.1 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.

### 20.1.1 What You Can Do in this Chapter

- The **VLAN** screen (Section 20.2 on page 127) displays VLAN, port, and VLAN port settings.
- The **Guest VLAN** screen (Section 20.3 on page 131) displays the global and port settings of the Switch.
- The **Voice VLAN** screen (Section 20.4 on page 133) displays the global, OUI, and port settings of the Switch.

# 20.2 VLAN

Use this screen to view and configure VLAN settings.

## 20.2.1 The VLAN Screen

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

Figure 121 Configuration > VLAN > VLAN > VLAN



The following table describes the labels in this screen.

Table 73 Configuration > VLAN > VLAN > VLAN

| LABEL | DESCRIPTION |
|---|---|
| VLAN | |
| 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**. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Add | Click **Add** to create a new VLAN entry. |

## 20.2.2 The VLAN Add Screen

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

Figure 122 Configuration > VLAN > VLAN > VLAN > Add



The following table describes the labels in this screen.

Table 74 Configuration > VLAN > VLAN > VLAN > Add

| LABEL | DESCRIPTION |
|---|---|
| VLAN | |
| VLAN List | Enter the VLAN ID number(s). |
| | 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. |

Table 74  Configuration > VLAN > VLAN > VLAN > Add (continued)

| LABEL | DESCRIPTION |
|-------|-------------|
| VLAN Name Prefix | Enter a prefix for the VLAN name. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 20.2.3  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 123**  Configuration > VLAN > VLAN > Port



The following table describes the labels in this screen.

Table 75  Configuration > VLAN > VLAN > Port

| LABEL | DESCRIPTION |
|-------|-------------|
| 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. |

Table 75   Configuration > VLAN > VLAN > Port (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 20.2.4  The Port Edit Screen

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

**Figure 124**   Configuration > VLAN > VLAN > Port > Edit



The following table describes the labels in this screen.

Table 76   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. |
| 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. |

## 20.2.5  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 125**   Configuration > VLAN > VLAN > VLAN Port



The following table describes the labels in this screen.

Table 77   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. |

Table 77   Configuration > VLAN > VLAN > VLAN Port (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

# 20.3  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 126**   Guest VLAN Example
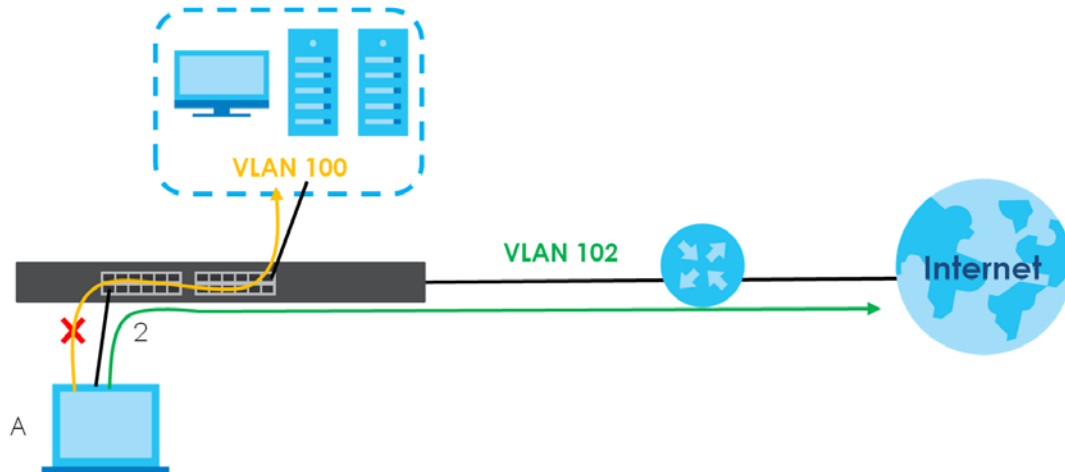


Use this screen to view and configure guest VLAN settings.

## 20.3.1  The Global Screen

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

**Figure 127**   Configuration > VLAN > Guest VLAN > Global

| Global | | Global  Port |
|---|---|---|
| State | ○ Enable  ● Disable | |
| Guest VLAN ID | 0 | |
| | Apply  Cancel | |

The following table describes the labels in this screen.

Table 78   Configuration > VLAN > Guest VLAN > Global

| LABEL | DESCRIPTION |
|---|---|
| Global | |
| State | Select to enable the global Guest VLAN feature. |
| Guest VLAN ID | Enter the global guest VLAN ID. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 20.3.2  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 128**   Configuration > VLAN > Guest VLAN > Port

| Port | | Global  Port |
|---|---|---|
| ☐ | **Port** | **State** |
| ☐ | 1 | Disable |
| ☐ | 2 | Disable |
| ☐ | 3 | Disable |
| ☐ | 4 | Disable |
| ☐ | 5 | Disable |
| ☐ | 6 | Disable |
| ☐ | 7 | Disable |
| ☐ | 21 | Disable |
| ☐ | 22 | Disable |
| ☐ | 23 | Disable |
| ☐ | 24 | Disable |
| ☐ | 25 | Disable |
| ☐ | 26 | Disable |
| | Edit  Cancel | |

The following table describes the labels in this screen.

Table 79   Configuration > VLAN > Guest VLAN > Port

| LABEL | DESCRIPTION |
|---|---|
| Port | |
| Port | Displays the port index number. |

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

| LABEL | DESCRIPTION |
|---|---|
| State | Display the state of the selected port. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 20.3.3  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 129   Configuration > VLAN > Guest VLAN > Port > Edit



The following table describes the labels in this screen.

Table 80   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. |

# 20.4  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.

Use this screen to view and configure voice VLAN settings.

## 20.4.1  The Global Screen

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

**Figure 130** Configuration > VLAN > Voice VLAN > Global



The following table describes the labels in this screen.

Table 81 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 4094. |
| 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. |

## 20.4.2 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 131** Configuration > VLAN > Voice VLAN > OUI

The following table describes the labels in this screen.

Table 82   Configuration > VLAN > Voice VLAN > OUI

| LABEL | DESCRIPTION |
|-------|-------------|
| OUI | |
| 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. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new OUI entry. |

## 20.4.3  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 132   Configuration > VLAN > Voice VLAN > OUI > Add/Edit



The following table describes the labels in this screen.

Table 83   Configuration > VLAN > Voice VLAN > OUI > Add/Edit

| LABEL | DESCRIPTION |
|-------|-------------|
| Add/Edit 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. |

## 20.4.4  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 133** Configuration > VLAN > Voice VLAN > Port
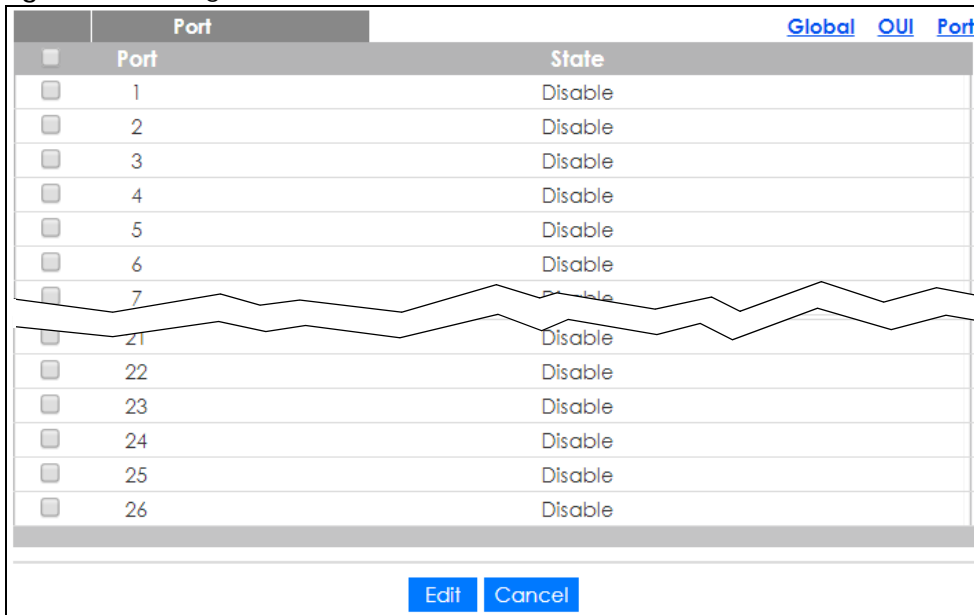


The following table describes the labels in this screen.

Table 84   Configuration > VLAN > Voice VLAN > Port

| LABEL | DESCRIPTION |
|-------|-------------|
| Port | |
| 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:<br><br>• **Enabled**: Enable Voice VLAN security mode operation.<br>• **Disabled**: Disable Voice VLAN security mode operation. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 20.4.5  The Port Edit Screen

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

**Figure 134** Configuration > VLAN > Voice VLAN > Port > Edit
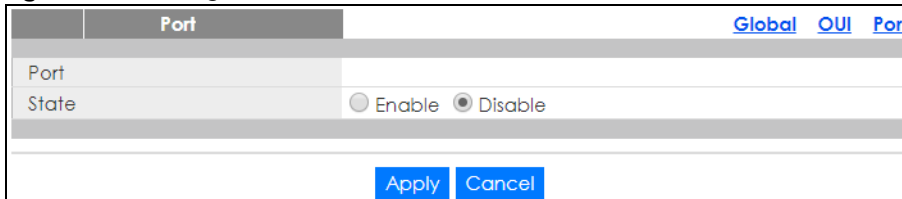
The following table describes the labels in this screen.

Table 85   Configuration > VLAN > Voice VLAN > Port > 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: <br><br> • **Enabled**: Enable Voice VLAN security mode operation. <br> • **Disabled**: Disable Voice VLAN security mode operation. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# Configuration: MAC Table

## 21.1 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).

### 21.1.1 What You Can Do in this Chapter
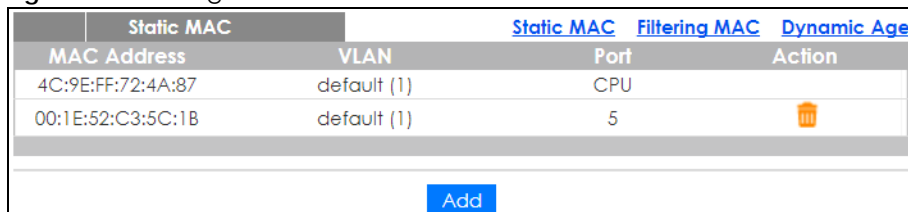
The **MAC Table** screen () displays Static MAC, Filtering MAC, and Dynamic MAC settings.

## 21.2 MAC Table

### 21.2.1 The Static MAC Screen

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

**Figure 135** Configuration > MAC Table > Static MAC

| Static MAC | | Static MAC | Filtering MAC | Dynamic Age |
|---|---|---|---|---|
| **MAC Address** | **VLAN** | **Port** | **Action** | |
| 4C:9E:FF:72:4A:87 | default (1) | CPU | | |
| 00:1E:52:C3:5C:1B | default (1) | 5 | 🗑 | |

Add

The following table describes the labels in this screen.

Table 86 Configuration > MAC Table > Static MAC

| LABEL | DESCRIPTION |
|---|---|
| Static MAC | |
| MAC Address | Displays the object MAC address from which this incoming frame came. |
| VLAN | Displays the VLAN group to which this frame belongs. |
| Port | Displays the port from which the above MAC address was learned. |

Table 86   Configuration > MAC Table > Static MAC (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action | Click **Delete** to remove the MAC address. |
| Add | Click **Add** to create a new **Static MAC** entry. |

## 21.2.2  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 136   Configuration > MAC Table > Static MAC > Add



The following table describes the labels in this screen.

Table 87   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. |

## 21.2.3  The Filtering MAC Screen

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

Figure 137   Configuration > MAC Table > Filtering MAC



The following table describes the labels in this screen.

Table 88   Configuration > MAC Table > Filtering MAC

| LABEL | DESCRIPTION |
|---|---|
| Filtering MAC | |
| MAC Address | Displays the filtering object MAC address from which this incoming frame came. |
| VLAN | Displays the VLAN group to which this frame belongs. |

Table 88   Configuration > MAC Table > Filtering MAC (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action | |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **Filtering MAC** entry. |

## 21.2.4  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 138   Configuration > MAC Table > Filtering MAC > Add



The following table describes the labels in this screen.

Table 89   Configuration > MAC Table > Filtering MAC > Add

| LABEL | DESCRIPTION |
|---|---|
| Add 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. |

## 21.2.5  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 139   Configuration > MAC Table > Dynamic Age



The following table describes the labels in this screen.

Table 90   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. |

Table 90   Configuration > Dynamic Age (continued)

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

# CHAPTER 22
# Configuration: Link Aggregation

## 22.1 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.

### 22.1.1 What You Can Do in this Chapter

The **Link Aggregation** screen () displays global, LAG management, LAG port, and LACP port settings.

## 22.2 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.

### 22.2.1 The Global Screen

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

**Figure 140** Configuration > Link Aggregation > Global



The following table describes the labels in this screen.

Table 91   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 **IP/MAC Address** 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.<br><br>Select **MAC Address** to distribute traffic based on a combination of the packet's source and destination MAC addresses.<br><br>Select **IP/MAC Address** 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. |

## 22.2.2  The LAG Management Screen

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

**Figure 141** Configuration > Link Aggregation > LAG Management



The following table describes the labels in this screen.

Table 92   Configuration > Link Aggregation > LAG Management

| LABEL | DESCRIPTION |
|---|---|
| LAG Management | |
| LAG | Displays the link aggregation group (LAG), that is, one logical link containing multiple ports. |
| Name | Displays the name of the link aggregation group. |

Table 92   Configuration > Link Aggregation > LAG Management (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | This field displays how these ports were added to the trunk group. It displays:<br><br>**Static** - if the ports are configured as static members of a trunk group.<br><br>**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. |
| Action | |
|    Edit | Click **Edit** to make changes to the entry. |
|    Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **LAG Management** entry. |

## 22.2.3  The LAG Add Screen

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

Figure 142   Configuration > Link Aggregation > LAG Management > Add



The following table describes the labels in this screen.

Table 93   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. |

Table 93   Configuration > Link Aggregation > LAG Management > Add (continued)

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

## 22.2.4  The LAG Port Screen

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

**Figure 143**   Configuration > Link Aggregation > LAG Port



The following table describes the labels in this screen.

Table 94   Configuration > Link Aggregation > LAG Port

| LABEL | DESCRIPTION |
|-------|-------------|
| LAG 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**). |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 22.2.5  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 144** Configuration > Link Aggregation > LAG Port > Edit

| LAG Port | Global | LAG Management | LAG Port | LACP Port |
|----------|--------|----------------|----------|-----------|
| LAG | | | | |
| State | ● Enable ○ Disable | | | |
| Speed | Auto ▼ | | | |
| Flow Control | ○ Enable ● Disable | | | |

Apply  Cancel

The following table describes the labels in this screen.

Table 95   Configuration > Link Aggregation > LAG Port > Edit

| LABEL | DESCRIPTION |
|-------|-------------|
| LAG Port | |
| LAG | Displays the LAG index values. |
| State | Select the state to be **Enable** or **Disable**. |
| Speed | Displays the speed value as **Auto**, **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. |

## 22.2.6  The LACP Port Screen

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

**Figure 145** Configuration > Link Aggregation > LACP Port

| LACP Port | Global | LAG Management | LAG Port | LACP Port |
|-----------|--------|----------------|----------|-----------|
| ☐ Port | Priority | | Timer(sec) | |
| ☐ 1 | 1 | | 30 | |
| ☐ 2 | 1 | | 30 | |
| ☐ 3 | 1 | | 30 | |
| ☐ 4 | 1 | | 30 | |
| ☐ 5 | 1 | | 30 | |
| ☐ 6 | 1 | | 30 | |
| ☐ 7 | 1 | | 30 | |
| ☐ 8 | 1 | | 30 | |
| ☐ 22 | | | 30 | |
| ☐ 23 | 1 | | 30 | |
| ☐ 24 | 1 | | 30 | |
| ☐ 25 | 1 | | 30 | |
| ☐ 26 | 1 | | 30 | |

Edit  Cancel

The following table describes the labels in this screen.

Table 96   Configuration > Link Aggregation > LACP Port

| LABEL | DESCRIPTION |
|---|---|
| LACP Port | |
| Port | Displays the port index number. |
| Priority | Displays the priority value. |
| Timer (sec) | Displays the Timer value in seconds.<br><br>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. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 22.2.7  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 146   Configuration > Link Aggregation > LACP Port > Edit



The following table describes the labels in this screen.

Table 97   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. |

# Configuration: Loop Guard

## 23.1 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.
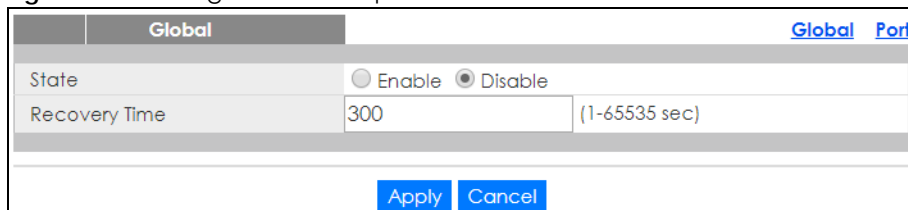
## 23.2 Loop Guard

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.

### 23.2.1 The Global Screen

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

**Figure 147**   Configuration > Loop Guard > Global



The following table describes the labels in this screen.

Table 98   Configuration > Loop Guard > Global

| LABEL | DESCRIPTION |
|---|---|
| Global | |
| State | Select **Enable** to activate loop protection on this Switch. |
| 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. |

## 23.2.2 The Loop Guard Port

Use this screen to view the port's Loop Guard settings. Click **Configuration** > **Loop Guard** > **Port** to open this screen.

*Figure 148* Configuration > Loop Guard > Port



The following table describes the labels in this screen.

Table 99   Configuration > Loop Guard > Port

| LABEL | DESCRIPTION |
|---|---|
| Port | |
| Port | Displays the port index number. |
| State | Displays whether the loop guard feature is **Enable** or **Disable** on the port. |
| Action | Displays the action to take by the Switch. The options are **Log**, **Shutdown Port**, and **Shutdown and Log**. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 23.2.3 The Port Edit Screen

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

*Figure 149* Configuration > Loop Guard > Port > Edit

The following table describes the labels in this screen.

Table 100   Configuration > Loop Guard > Port > Edit

| LABEL | DESCRIPTION |
|-------|-------------|
| Port | |
| Port List | Displays the list of port index numbers to be configured. |
| State | Select to enable or disable the loop guard feature on the port. |
| Action | Select to have the Switch shut down a port and/or generate a log message if it detects that packets sent out on that port loop back to the Switch. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# CHAPTER 24
# Configuration: Mirror

## 24.1 Overview

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

## 24.2 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.

### 24.2.1 The Mirror Screen

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

**Figure 150** Configuration > Mirror



The following table describes the labels in this screen.

Table 101   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. |

Table 101   Configuration > Mirror (continued)

| LABEL | DESCRIPTION |
|---|---|
| < | 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. |

# CHAPTER 25
# Configuration: Time Range Group

## 25.1  Overview

You can set up one-time and recurring schedules for time-oriented features, such as PoE. The Switch supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the Switch.

### 25.1.1  What You Can Do

The **Time Range** Group screen (Section 25.2.1 on page 154) displays or defines a time range (schedule) rule on the Switch.

## 25.2  Time Range Group

Use this screen to view or edit a time range rule on the Switch.

### 25.2.1  The Time Range Group Screen

Use this screen to view the time range rules. Click **Configuration > Time Range Group** in the navigation panel to display the screen as shown.

**Figure 151**   Configuration > Time Range Group



| Time Range Group | | | | |
| Index | Name | Type | Range | Action |
| 1 | Weekday | Periodic | Weekdays 08:00 to 17:00 | |
| 2 | Weekend | Absolute | 2017/08/26 08:00 to 2017/08/27 17:00 | |
| | | | Add | |

The following table describes the labels in this screen.

Table 102   Configuration > Time Range Group

| LABEL | DESCRIPTION |
|-------|-------------|
| Index | This field displays the index number of the rule. |
| Name | This field displays the descriptive name for this rule. This is for identification purpose only. |
| Type | This field displays the type of the rule. |

Table 102   Configuration > Time Range Group (continued)

| LABEL | DESCRIPTION |
|-------|-------------|
| Range | This field displays the time period(s) to which this rule applies. |
| Action | Click **Edit** to change the rule settings.<br><br>Click **Delete** to remove the rule. |
| Add | Click **Add** to create a new time range rule. |

## 25.2.2 The Time Range Add Screen

Use this screen to add a new time range (schedule) rule. Click **Configuration** > **Time Range Group**> **Add** in the navigation panel to display the screen as shown.

**Figure 152**   Configuration > Time Range Group > Add



The following table describes the labels in this screen.

Table 103   Configuration > Time Range Group > Add

| LABEL | DESCRIPTION |
|-------|-------------|
| Name | Enter a descriptive name for this rule for identifying purposes. |
| Type | Select **Absolute** to create a one-time schedule. One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.<br><br>Alternatively, select **Periodic** to create a recurring schedule. Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules are useful for defining the workday and off-work hours. |
| Absolute | This section is available only when you set **Type** to **Absolute**. |
| Start | Specify the year, month, day, hour and minute when the schedule begins. |
| End | Specify the year, month, day, hour and minute when the schedule ends. |
| Periodic | This section is available only when you set **Type** to **Periodic**.<br><br>Select the first option if you want to define a recurring schedule for a consecutive time period. You then select the day of the week, hour and minute when the schedule begins and ends respectively.<br><br>Select the second option if you want to define a recurring schedule for multiple non-consecutive time periods. You need to select each day of the week the recurring schedule is effective. You also need to specify the hour and minute when the schedule begins and ends each day. The schedule begins and ends in the same day. |

| LABEL | DESCRIPTION |
|-------|-------------|
| Apply | Click **Apply** to save 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. |
| Cancel | Click **Cancel** to reset the fields to your previous configuration. |

## 25.2.3  The Time Range Edit Screen

Use this screen to modify an existing time range rule. Click **Configuration** > **Time Range Group** > **Edit** in the navigation panel to display the screens as shown.

### 25.2.3.1  Edit an Absolute Time Range Rule

Click the **Edit** button in the **Action** field to modify an absolute time range rule.

**Figure 153**   Configuration > Time Range Group > Edit (Absolute)



The following table describes the labels in this screen.

Table 104   Configuration > Time Range Group > Edit (Absolute)

| LABEL | DESCRIPTION |
|-------|-------------|
| Name | This field displays the descriptive name for this rule. This is for identification purpose only. |
| Type | This field displays the type of the rule. |
| Range | Specify the year, month, day, hour and minute when the schedule begins and ends. |
| Apply | Click **Apply** to save 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. |
| Cancel | Click **Cancel** to reset the fields to your previous configuration. |

### 25.2.3.2  Edit a Periodic Time Range Rule

Click the **Edit** button in the **Action** field to modify a periodic time range rule. A screen will appear showing the name, type, and range of this rule. Click the **Edit** button again to modify it, or you can click the **Add** button to create a new range under a periodic time range rule.

**Figure 154** Configuration > Time Range Group > Edit (Periodic)



The following table describes the labels in this screen.

Table 105   Configuration > Time Range Group > Edit (Periodic)

| LABEL | DESCRIPTION |
|---|---|
| Time Range Group | |
| Name | This field displays the descriptive name for this rule. This is for identification purpose only. |
| Type | This field displays the type of the rule. |
| Index | This field displays the index number of the rule. |
| Range | This field displays the time period(s) to which this rule applies. |
| Action | Click **Edit** to change the rule settings. |
| | Click **Delete** to remove the rule. |
| Add | Click **Add** to create a new range. |

**Figure 155** Configuration > Time Range Group > Edit (Periodic) > Edit



The following table describes the labels in this screen.

Table 106   Configuration > Time Range Group > Edit (Periodic) > Add

| LABEL | DESCRIPTION |
|---|---|
| Time Range Group | |
| Name | Enter a descriptive name for this rule for identifying purposes. |
| Type | This field displays the type of the rule. |
| Range | Select the first option if you want to define a recurring schedule for a consecutive time period. You then select the day of the week, hour and minute when the schedule begins and ends respectively. |
| | Select the second option if you want to define a recurring schedule for multiple non-consecutive time periods. You need to select each day of the week the recurring schedule is effective. You also need to specify the hour and minute when the schedule begins and ends each day. The schedule begins and ends in the same day. |

Table 106   Configuration > Time Range Group > Edit (Periodic) > Add (continued)

| LABEL | DESCRIPTION |
| --- | --- |
| Apply | Click **Apply** to save 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. |
| Cancel | Click **Cancel** to reset the fields to your previous configuration. |

# CHAPTER 26
# Configuration: Multicast

## 26.1 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.

## 26.2 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.

### 26.2.1 The Global Screen

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

**Figure 156** Configuration > Multicast > IGMP > Global



The following table describes the labels in this screen.

Table 107   Configuration > Multicast > IGMP > Global

| LABEL | DESCRIPTION |
|---|---|
| Global | |
| Snooping State | Select **Enable** to turn on IGMP packet snooping or **Disable** to turn snooping off. |
| Snooping Version | Select **v2** or **v3** depending on the snooping version you require. |

Table 107   Configuration > Multicast > IGMP (continued)> Global

| LABEL | DESCRIPTION |
|---|---|
| Unknown Multicast Action | Select to send the IPv4 unknown multicast frame to the router port. The following options are available:<br><br>• **Flood** - select to send the frame(s) to all ports.<br>• **Drop** - select to discard the frame(s).<br>• **Router Port** - select to send the frame to router port. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 26.2.2  The VLAN Screen

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

**Figure 157**   Configuration > Multicast > IGMP > VLAN



The following table describes the labels in this screen.

Table 108   Configuration > Multicast > IGMP > VLAN

| LABEL | DESCRIPTION |
|---|---|
| IGMP Vlan | |
| VLAN ID | Displays the ID of a static VLAN; the valid range is between 1 and 4094. |
| State | 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 | 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 | 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 | |
| State | Displays the Switch current VLAN querier entry as **Enable** or **Disable**. |
| Version | Displays the Switch current VLAN querier entry version. |
| Edit | Click **Edit** to change the properties of the IGMP VLAN entry. |

## 26.2.3 The Edit IGMP Screen

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

**Figure 158** Configuration > Multicast > IGMP > VLAN > Edit



The following table describes the labels in this screen.

Table 109 Configuration > Multicast > IGMP > VLAN > Edit

| 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. |
| Query Interval | 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. |
| Query Max. Response Interval | Enter 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 | Enter the number of queries. |
| Last Member Query Interval | 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. |
| 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. |

## 26.2.4  The Router Port Screen

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

**Figure 159**  Configuration > Multicast > IGMP > Router Port

| | Router Port | | Global | VLAN | Router Port | Profile | Throttling |
|---|---|---|---|---|---|---|---|
| VLAN ID | Static Router Ports | Forbidden Router Ports | | | Action | | |

Add

The following table describes the labels in this screen.

Table 110   Configuration > Multicast > IGMP > Router Port

| LABEL | DESCRIPTION |
|---|---|
| Router Port | |
| 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. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **Router Port** entry. |

## 26.2.5  The Add/Edit Router Port Screen

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

**Figure 160** Configuration > Multicast > IGMP > Router Port > Add/Edit



The following table describes the labels in this screen.

Table 111   Configuration > Multicast > IGMP > Router Port > Add/Modify

| LABEL | DESCRIPTION |
|---|---|
| IGMP Router Edit | |
| 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. |

## 26.2.6  The Profile Screen

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

**Figure 161** Configuration > Multicast > IGMP > Profile

The following table describes the labels in this screen.

Table 112   Configuration > Multicast > IGMP > Profile

| LABEL | DESCRIPTION |
|---|---|
| IGMP Profile | |
| Profile | Displays the **Profile** index number. |
| Group From | Displays the profile start group IP address. |
| Group To | Displays the profile end group IP address. |
| Match Action | Displays the action of the profile as **Permit** or **Deny**. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **IGMP Profile** entry. |

## 26.2.7  The Add/Edit Profile Screen

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

Figure 162   Configuration > Multicast > IGMP > Profile > Add/Edit



The following table describes the labels in this screen.

Table 113   Configuration > Multicast > IGMP > Profile > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| IGMP Profile | |
| Profile | Enter the **Profile** index number. |
| Group From | Enter the profile start group IP address. |
| Group To | Enter the profile end group IP address. |
| Match 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. |

## 26.2.8  The Throttling Screen

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

**Figure 163** Configuration > Multicast > IGMP > Throttling



The following table describes the labels in this screen.

Table 114   Configuration > Multicast > IGMP > Throttling

| LABEL | DESCRIPTION |
|---|---|
| IGMP Port Throttling | |
| 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. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 26.2.9  The Edit Throttling Screen

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

**Figure 164** Configuration > Multicast > IGMP > Throttling > Edit

| IGMP Port Throttling | Global VLAN Router Port Profile Throttling |
|---|---|
| Port List | |
| Max. Groups | 256 (0-256) |
| Exceed Group Number Action | ● Deny ○ Replace |
| Filter Profile ID | None ▼ |

Apply  Cancel

The following table describes the labels in this screen.

Table 115  Configuration > Multicast > IGMP > Throttling > 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. |

# Configuration: Spanning Tree

## 27.1 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.

## 27.2 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.

### 27.2.1 The Global Screen

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

**Figure 165** Configuration > Spanning Tree > Global

The following table describes the labels in this screen.

Table 116   Configuration > Spanning Tree > Global

| 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.<br><br>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:<br><br>• **STP**<br>• **RSTP**<br>• **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. |

## 27.2.2  The STP Port Screen

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

Figure 166   Configuration > Spanning Tree > STP Port

The following table describes the labels in this screen.

Table 117   Configuration > Spanning Tree > STP Port

| LABEL | DESCRIPTION |
|---|---|
| STP 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**. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 27.2.3  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 167   Configuration > Spanning Tree > STP Port > Edit



The following table describes the labels in this screen.

Table 118   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.<br><br>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. |

Table 118   Configuration > Spanning Tree > STP Port > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 27.2.4  The CIST Screen

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

**Figure 168**   Configuration > Spanning Tree > CIST



The following table describes the labels in this screen.

Table 119   Configuration > Spanning Tree > CIST

| LABEL | DESCRIPTION |
|---|---|
| CIST Instance | |
| Priority | Configure priority of CIST bridge ID.<br><br>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.<br><br>As a general rule:<br><br>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. |

## 27.2.5 The CIST Port Screen

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

**Figure 169** Configuration > Spanning Tree > CIST Port



The following table describes the labels in this screen.

Table 120 Configuration > Spanning Tree > CIST Port

| LABEL | DESCRIPTION |
|---|---|
| CIST 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. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 27.2.6 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 170** Configuration > Spanning Tree > CIST Port > Edit

| STP CIST Port | | Global STP Port CIST CIST Port MST MST Port |
|---|---|---|
| Port List | | |
| Priority | 128 ▼ | |
| Internal Path Cost(0 = Auto) | 0 | |
| | Apply Cancel | |

The following table describes the labels in this screen.

Table 121 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. |

## 27.2.7 The MST Screen

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

**Figure 171** Configuration > Spanning Tree > MST

| MST Instance | | Global STP Port CIST CIST Port MST MST Port |
|---|---|---|
| MSTI | VLAN List | VLAN Count Priority Action |
| | Add | |

The following table describes the labels in this screen.

Table 122 Configuration > Spanning Tree > MST

| LABEL | DESCRIPTION |
|---|---|
| MST Instance | |
| MSTI | This displays the Multiple Spanning Tree Instance(s) (MSTI). |
| VLAN List | This displays a list of MSTI VLANs. |
| VLAN Count | This displays the VLAN count. |
| Priority | This displays the priority for each port here. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **MST Instance** entry. |

## 27.2.8 The Add/Edit MST Screen

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

**Figure 172** Configuration > Spanning Tree > MST > Add/Edit



The following table describes the labels in this screen.

Table 123 Configuration > Spanning Tree > MST > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| MST Instance | |
| MST ID | Select a Multiple Spanning Tree Instance (MSTI) ID. |
| VLAN List | Enter a MSTI VLAN ID |
| Priority | Select a MSTI bridge ID priority value. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 27.2.9 The MST Port Screen

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

**Figure 173** Configuration > Spanning Tree > MST Port



The following table describes the labels in this screen.

Table 124   Configuration > Spanning Tree > MST Port

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

## 27.2.10 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 174** Configuration > Spanning Tree > MST Port > Edit

| MST Port | | Global | STP Port | CIST | CIST Port | MST | MST Port |
|---|---|---|---|---|---|---|---|
| MSTI ID | 1 | | | | | | |
| Port List | | | | | | | |
| Priority | 128 ▼ | | | | | | |
| Internal Path Cost(0 = Auto) | 0 | | | | | | |

Apply Cancel

The following table describes the labels in this screen.

Table 125   Configuration > Spanning Tree > MST Port > Edit

| LABEL | DESCRIPTION |
|---|---|
| STP MST Port | |
| MST ID | This displays the MST ID number. |
| Port List | Enter the index number of the MTP port(s). |
| Priority | Configure the priority for each port here.<br><br>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. |

# Configuration: LLDP

## 28.1  Overview

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

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

## 28.2  LLDP

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

### 28.2.1  The Global Screen

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

**Figure 175**   Configuration > LLDP > Global



The following table describes the labels in this screen.

Table 126   Configuration > LLDP > Global

| LABEL | DESCRIPTION |
|-------|-------------|
| Global | |
| State | Select **Enable** to activate the global LLDP. |
| Transmission Interval | Enter the transmission interval value.<br><br>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. |

Table 126   Configuration > LLDP > Global (continued)

| LABEL | DESCRIPTION |
|---|---|
| Hold Multiplier | Enter the hold multiplier value.<br><br>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.<br><br>When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds. |
| Transmit Delay | Enter the transmission delay value.<br><br>If some configuration is changed (for example, 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.<br><br>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. |

## 28.2.2  The Port Screen

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

**Figure 176** Configuration > LLDP > Port



The following table describes the labels in this screen.

Table 127   Configuration > LLDP > Port

| LABEL | DESCRIPTION |
|-------|-------------|
| LLDP VLAN | |
| 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:<br><br>• SN - System Name<br>• PD - Port Description<br>• SD - System Description<br>• SC - System Capability<br>• MP - 802.3 MAC-PHY<br>• LA - 802.3 Link Aggregation<br>• MFS - 802.3 Maximum Frame Size<br>• MA - Management Address |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 28.2.3  The Port Edit Screen

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

**Figure 177** Configuration > LLDP > Port > Edit



The following table describes the labels in this screen.

Table 128   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:<br><br>• **SN** - System Name<br>• **PD** - Port Description<br>• **SD** - System Description<br>• **SC** - System Capability<br>• **MP** - 802.3 MAC-PHY<br>• **LA** - 802.3 Link Aggregation<br>• **MFS** - 802.3 Maximum Frame Size<br>• **MA** - Management Address |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 28.2.4  The Local Information Screen

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

**Figure 178** Configuration > LLDP > Local Information



The following table describes the labels in this screen.

Table 129   Configuration > LLDP > Local Information

| LABEL | DESCRIPTION |
|---|---|
| Local Information | |
| 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 129   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 | |
| 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 (for example, 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. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 28.2.5  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 179** Configuration > LLDP > Local Information > Edit



The following table describes the labels in this screen.

Table 130 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. |
| 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. |

Table 130   Configuration > LLDP > Local Information > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Longitude | **Longitude** SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.<br><br>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.<br><br>It is possible to select between two altitude types (floors or meters).<br><br>**Meters**: Representing meters of Altitude defined by the vertical datum specified.<br><br>**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:<br><br>**WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.<br><br>**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).<br><br>**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).<br><br>• **Country code:** The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.<br>• **State:** National subdivisions (state, canton, region, province, prefecture).<br>• **County:** County, parish, gun (Japan), district.<br>• **City:** City, township, shi (Japan) - Example: Copenhagen.<br>• **City district:** City division, borough, city district, ward, chou (Japan).<br>• **Block (Neighborhood):** Neighborhood, block.<br>• **Street:** Street - Example: Poppelvej.<br>• **Leading street direction:** Leading street direction - Example: N.<br>• **Trailing street suffix:** Trailing street suffix - Example: SW.<br>• **Street suffix:** Street suffix - Example: Ave, Platz.<br>• **House no.:** House number - Example: 21.<br>• **House no. suffix:** House number suffix - Example: A, 1/2.<br>• **Landmark:** Landmark or vanity address - Example: Columbia University.<br>• **Additional location info:** Additional location info - Example: South Wing.<br>• **Name:** Name (residence and office occupant) - Example: Flemming Jahn.<br>• **Zip code:** Postal/zip code - Example: 2791.<br>• **Building:** Building (structure) - Example: Low Library.<br>• **Apartment:** Unit (Apartment, suite) - Example: Apt 42.<br>• **Floor:** Floor - Example: 4.<br>• **Room no.:** Room number - Example: 450F.<br>• **Place type:** Place type - Example: Office.<br>• **Postal community name:** Postal community name - Example: Leonia.<br>• **P.O. Box:** Post office box (P.O. BOX) - Example: 12345. |
| Location ECS ELIN | Emergency Call Service (for example, E911 and others), such as defined by TIA or NENA.<br><br>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. |

Table 130   Configuration > LLDP > Local Information > Edit (continued)

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

## 28.2.6  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 180**   Configuration > LLDP > MED Network Policy



The following table describes the labels in this screen.

Table 131   Configuration > LLDP > MED Network Policy

| LABEL | DESCRIPTION |
|---|---|
| Network Policy Configuration | |
| 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**. |
| Action | |
|    Edit | Click **Edit** to make changes to the entry. |
|    Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **Network Policy Configuration** entry. |

## 28.2.7  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 181**   Configuration > LLDP > MED Network Policy > Add/Edit

The following table describes the labels in this screen.

Table 132   Configuration > LLDP > MED Network Policy > Edit

| LABEL | DESCRIPTION |
|---|---|
| New Network Policy | |
| 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 Signaling** - for use in network topologies that require a different policy for the voice signaling 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 Signaling** - for use in network topologies that require a different policy for the guest voice signaling 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** Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media. |
| 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**. <br><br> **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. <br><br> **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. |

## 28.2.8  The MED Port Screen

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

**Figure 182** Configuration > LLDP > MED Port



The following table describes the labels in this screen.

Table 133   Configuration > LLDP > MED Port

| LABEL | DESCRIPTION |
|---|---|
| MED 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. |
| Location | Displays the **Location** value. |
| PoE | Displays the **PoE** value. |
| Inventory | Displays the **Inventory** value. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 28.2.9  The MED Port Edit Screen

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

**Figure 183** Configuration > LLDP > MED Port > Edit



The following table describes the labels in this screen.

Table 134 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:<br><br>• **Network Policy**<br>• **Location**<br>• **PoE PSE**<br>• **Inventory** |
| MED Network Policy | Select one or more of the **MED Network Policies** in **Available** and move them to **Acting** to activate. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# CHAPTER 29
# Configuration: QoS

## 29.1  Overview

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

## 29.2  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.

### 29.2.1  The Port Screen

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

**Figure 184** Configuration > QoS > General > Port

| QoS Port | | Port Queue CoS Mapping DSCP Mapping IP Precedence Mapping | | |
|---|---|---|---|---|
| **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 |
| ☐ 9 | 0 | Disable | Disable | Disable |
| ☐ | 0 | Disable | Disable | Disable |
| ☐ 24 | 0 | Disable | Disable | Disable |
| ☐ 25 | 0 | Disable | Disable | Disable |
| ☐ 26 | 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 |

Edit  Cancel

The following table describes the labels in this screen.

Table 135  Configuration > QoS > General > Port

| LABEL | DESCRIPTION |
|---|---|
| QoS 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. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 29.2.2  The Port Edit Screen

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

**Figure 185** Configuration > QoS > General > Port > Edit



The following table describes the labels in this screen.

Table 136  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. |

## 29.2.3  The Queue Screen

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

**Figure 186** Configuration > QoS > General > Queue

The following table describes the labels in this screen.

Table 137   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. |

## 29.2.4  The CoS Mapping Screen

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

Figure 187   Configuration > QoS > General > CoS Mapping



The following table describes the labels in this screen.

Table 138   Configuration > QoS > General > CoS Mapping

| LABEL | DESCRIPTION |
|---|---|
| CoS to Queue Mapping | |
| Class of Service (CoS) | Displays a listing of the CoS, range: 0 - 7. |

Table 138   Configuration > QoS > General > CoS Mapping (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 29.2.5  The DSCP Mapping Screen

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

**Figure 188**   Configuration > QoS > General > DSCP Mapping

The following table describes the labels in this screen.

Table 139   Configuration > QoS > General > DSCP Mapping

| LABEL | DESCRIPTION |
|---|---|
| DSCP Mapping | |
| 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. |

## 29.2.6  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 189   Configuration > QoS > General > IP Precedence Mapping



The following table describes the labels in this screen.

Table 140   Configuration > QoS > General > IP Precedence Mapping

| LABEL | DESCRIPTION |
|---|---|
| IP Precedence Mapping | |
| IP Precedence to Queue Mapping | |

Table 140   Configuration > QoS > General > IP Precedence Mapping (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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). |
| 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. |

# 29.3  Trust Mode

## 29.3.1  The Global Screen

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

Figure 190   Configuration > QoS > Trust Mode > Global



The following table describes the labels in this screen.

Table 141   Configuration > QoS > Trust Mode > Global

| 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. |

## 29.3.2  The Port Screen

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

**Figure 191** Configuration > QoS > Trust Mode > Port

| QoS Port | | Global Port |
|---|---|---|
| **Port** | **Mode** | |
| ☐ 1 | Untrust | |
| ☐ 2 | Untrust | |
| ☐ 3 | Untrust | |
| ☐ 4 | Untrust | |
| ☐ 5 | Untrust | |
| ☐ 6 | Untrust | |
| ☐ 7 | Untrust | |
| ☐ 8 | Untrust | |
| ☐ 24 | Untrust | |
| ☐ 25 | Untrust | |
| ☐ 26 | Untrust | |
| ☐ LAG1 | Untrust | |
| ☐ LAG2 | Untrust | |
| ☐ LAG3 | Untrust | |
| ☐ LAG4 | Untrust | |
| ☐ LAG5 | Untrust | |
| ☐ LAG6 | Untrust | |
| ☐ LAG7 | Untrust | |
| ☐ LAG8 | Untrust | |
| Edit Cancel | | |

The following table describes the labels in this screen.

Table 142   Configuration > QoS > Trust Mode > Port

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

## 29.3.3  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 192**   Configuration > QoS > Trust Mode > Port > Edit



The following table describes the labels in this screen.

Table 143   Configuration > QoS > Trust Mode > Port > Edit

| LABEL | DESCRIPTION |
| --- | --- |
| QoS Port | |
| 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. |

# CHAPTER 30
# Configuration: Security

## 30.1 Overview
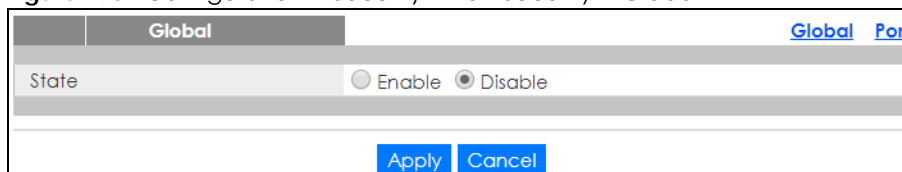
This section provides information for **Security** in **Configuration**.

## 30.2 Port Security

### 30.2.1 The Global Screen

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

**Figure 193** Configuration > Security > Port Security > Global

| Global | | Global Port |
|---|---|---|
| State | ○ Enable ● Disable | |

Apply Cancel

The following table describes the labels in this screen.

Table 144  Configuration > Security > Port Security > Global

| 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. |

### 30.2.2 The Port Screen

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

**Figure 194** Configuration > Security > Port Security > Port

| | Port | | | Global Port |
|---|---|---|---|---|
| | Port | State | Max. MAC Entry Number | Action |
| ☐ | 1 | Disable | Unlimited | --- |
| ☐ | 2 | Disable | Unlimited | --- |
| ☐ | 3 | Disable | Unlimited | --- |
| ☐ | 4 | Disable | Unlimited | --- |
| ☐ | 5 | Disable | Unlimited | --- |
| ☐ | 6 | Disable | Unlimited | --- |
| ☐ | 7 | Disable | Unlimited | --- |
| ☐ | 23 | Disable | Unlimited | --- |
| ☐ | 24 | Disable | Unlimited | --- |
| ☐ | 25 | Disable | Unlimited | --- |
| ☐ | 26 | Disable | Unlimited | --- |
| ☐ | LAG1 | Disable | Unlimited | --- |
| ☐ | LAG2 | Disable | Unlimited | --- |
| ☐ | LAG3 | Disable | Unlimited | --- |
| ☐ | LAG4 | Disable | Unlimited | --- |
| ☐ | LAG5 | Disable | Unlimited | --- |
| ☐ | LAG6 | Disable | Unlimited | --- |
| ☐ | LAG7 | Disable | Unlimited | --- |
| ☐ | LAG8 | Disable | Unlimited | --- |

Edit | Cancel

The following table describes the labels in this screen.

Table 145   Configuration > Security > Port Security > Port

| LABEL | DESCRIPTION |
|---|---|
| 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**. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 30.2.3  The Port Edit Screen

Use this screen to configure the **Port** settings. Select the port(s) you want to configure and then click **Edit** in the **Configuration** > **Security** > **Port Security** > **Port** screen to open this screen.

**Figure 195** Configuration > Security > Port Security > Port > Edit

| Port Security | | Global  Port |
|---|---|---|
| Port List | | |
| State | ⚪ Enable  ⚫ Disable | |
| Max MAC Entry Number | 256 | (0-256) |
| Action | ⚫ Discard  ⚪ Shutdown | |
| | Apply  Cancel | |

The following table describes the labels in this screen.

Table 146   Configuration > Security > Port Security > Port > Edit

| LABEL | DESCRIPTION |
|---|---|
| Port Security | |
| 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. |

# 30.3  Protected Port

## 30.3.1  The Protected Port Screen

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

**Figure 196** Configuration > Security > Protected Port



The following table describes the labels in this screen.

Table 147 Configuration > Security > Protected Port

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

## 30.3.2 The Protected Port Edit Screen

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

**Figure 197** Configuration > Security > Protected Port > Edit

The following table describes the labels in this screen.

Table 148   Configuration > Security > Protected Port > Edit

| LABEL | DESCRIPTION |
|---|---|
| Protected Port | |
| Port List | Displays the port list index value(s). |
| State | Select **Enable** or **Disable** for the **Protected Port** status. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 30.4  802.1X

## 30.4.1  The Global Screen

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

Figure 198   Configuration > Security > 802.1X > Global
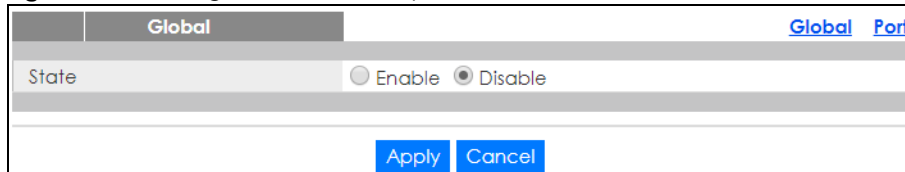


The following table describes the labels in this screen.

Table 149   Configuration > Security > 802.1X > Global

| LABEL | DESCRIPTION |
|---|---|
| Global | |
| State | 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. |

## 30.4.2  The Port Screen

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

**Figure 199** Configuration > Security > 802.1X > Port

| | Port | State | Reauthentication | Reauthentication Period | Quiet Period | Supplicant Timeout | Maximum Request Retries |
|---|---|---|---|---|---|---|---|
| ☐ | 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 |
| | | No Authentication | Enable | | 60 | 30 | 2 |
| ☐ | 21 | No Authentication | Enable | 3600 | 60 | 30 | 2 |
| ☐ | 22 | No Authentication | Enable | 3600 | 60 | 30 | 2 |
| ☐ | 23 | No Authentication | Enable | 3600 | 60 | 30 | 2 |
| ☐ | 24 | No Authentication | Enable | 3600 | 60 | 30 | 2 |
| ☐ | 25 | No Authentication | Enable | 3600 | 60 | 30 | 2 |
| ☐ | 26 | No Authentication | Enable | 3600 | 60 | 30 | 2 |

Global  Port

Edit  Cancel

The following table describes the labels in this screen.

Table 150   Configuration > Security > 802.1X > Port

| LABEL | DESCRIPTION |
|---|---|
| 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 when 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 respond. |
| Maximum Request Retries | Enter the maximum number of request retries. |
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 30.4.3  The Port Edit Screen

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

**Figure 200** Configuration > Security > 802.1X > Port > Edit



The following table describes the labels in this screen.

Table 151 Configuration > Security > 802.1X > Port > Edit

| LABEL | DESCRIPTION |
|---|---|
| 802.1X Port | |
| Port List | Displays the port index value. |
| 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 respond. |
| Maximum Request Retries | Enter the maximum number of request retries. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 30.5 DoS

The Switch protects against Denial of Service (DoS) attacks, such as Scan attack and Ping of Death. The goal of DoS attacks is not to steal information, but to disable a device or network on the Internet.

By default, the DoS feature is disabled. You need to enable it on the Switch and its port(s). See Table 155 on page 205 for the types of DoS attacks that the Switch prevents when you turn on this feature. You cannot set the Switch to block a specific type of DoS attacks.

Note: DoS protection does not work on LACP-enabled ports.

## 30.5.1 The Global Screen

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

**Figure 201** Configuration > Security > DoS > Global



The following table describes the labels in this screen.

Table 152   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. |

## 30.5.2  The Port Screen

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

**Figure 202**   Configuration > Security > DoS > Port



The following table describes the labels in this screen.

Table 153   Configuration > Security > DoS > Port

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

Table 153   Configuration > Security > DoS > Port

| LABEL | DESCRIPTION |
|-------|-------------|
| Edit | Select this check box to configure the properties of a port. Click the **Edit** button change the properties of the port. |
| Cancel | Click **Cancel** to discard the changes. |

## 30.5.3  The Port Edit Screen

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

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

Figure 203   Configuration > Security > DoS > Port > Edit



The following table describes the labels in this screen.

Table 154   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. |

## 30.5.4  DoS Attack Types

The following table describes the types of DoS attacks that the Switch can prevent when you enable the DoS feature on the Switch and the port(s).

Table 155   DoS Attack Types

| TYPE | PACKET TYPE | DESCRIPTION |
|------|-------------|-------------|
| DA_EQUAL_SA | Layer 2 | These attacks result from sending a specially crafted packet to a machine where the source MAC address is the same as the destination MAC address. The system attempts to reply to itself, resulting in system lockup. |
| LAND | Layer 3 IPv4/IPv6 | These attacks result from sending a specially crafted packet to a machine where the source host IPv4/IPv6 address is the same as the destination host IPv4/IPv6 address. The system attempts to reply to itself, resulting in system lockup. |
| UDP_BLAT / TCP_BLAT (Blat Attack) | Layer 3 IPv4/IPv6 | These attacks result from sending a specially crafted packet to a machine where the source host UDP/TCP port is the same as the destination host UDP/TCP port. The system attempts to reply to itself, resulting in system lockup. |

Table 155   DoS Attack Types (continued)

| TYPE | PACKET TYPE | DESCRIPTION |
|---|---|---|
| PoD (Ping of Death) | Layer 3 IPv4/IPv6 | Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot. |
| IPv6_FRAG_LEN_MIN | Layer 3 IPv6 | This attack uses IPv6 fragmented packets (excluding the last one) whose payload length is less than 1240 bytes. |
| ICMP_FRAG_PKT | Layer 3 IPv4/IPv6 | This attack uses many small fragmented ICMP packets. |
| ICMPv4_PING_MAX / ICMPv6_PING_MAX | Layer 3 IPv4/IPv6 | This attack uses Ping packets whose length is larger than 512 bytes. |
| SMURF | Layer 3 IPv4 | This attack uses Internet Control Message Protocol (ICMP) echo requests packets (pings) to cause network congestion or outages. |
| SYNchronization (SYN), ACKnowledgment (ACK) and FINish (FIN) packets are used to initiate, acknowledge and conclude TCP/IP communication sessions. The following scans exploit weaknesses in the TCP/IP specification and try to illicit a response from a host to identify ports for an attack: | | |
| TCP_HDR_LEN_MIN | Layer 3 IPv4 | TCP packets with header length less than 20 bytes. |
| SYN_SPORT_LESS_1024 | Layer 3 IPv4/IPv6 | TCP SYN packets with source port less than 1024. |
| NULL_SCAN (Scan Attack) | Layer 3 IPv4/IPv6 | TCP sequence number is zero and all control bits are zeros. |
| XMAS (Scan Attack) | Layer 3 IPv4/IPv6 | TCP sequence number is zero and the FIN, URG and PSH bits are set. |
| SYN_FIN | Layer 3 IPv4/IPv6 | SYN and FIN bits are set in the TCP packet. |

# CHAPTER 31
# Configuration: AAA

## 31.1 Overview

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

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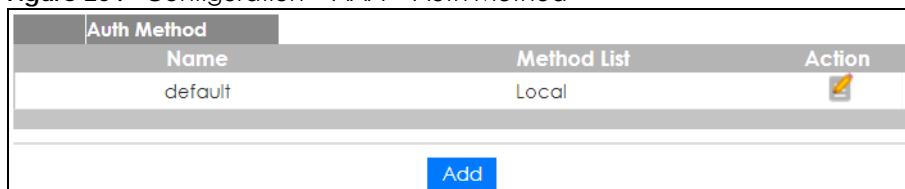
## 31.2 Auth Method

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.

### 31.2.1 The Auth Method Screen

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

Figure 204   Configuration > AAA > Auth Method



The following table describes the labels in this screen.

Table 156   Configuration > AAA > Auth Method

| LABEL | DESCRIPTION |
|---|---|
| Auth Method | |
| 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+**. |
| Action | Click the **Action** button to change the configuration settings for a VLAN entry. |
| Add | Click **Add** to create a new **Auth Method** entry. |

### 31.2.2 The Auth Method Add/Edit Screen

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

**Figure 205** Configuration > AAA > Auth Method > Add/Edit



The following table describes the labels in this screen.

Table 157 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. |

# 31.3  RADIUS

## 31.3.1  The RADIUS Screen

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

**Figure 206** Configuration > AAA > RADIUS



The following table describes the labels in this screen.

Table 158 Configuration > AAA > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| RADIUS Servers | |
| 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. |

Table 158   Configuration > AAA > RADIUS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Priority | Displays the server priority as **High** or **Low**. |
| Usage Type | Displays the server usage type as **Login**, **802.1X**, or **All**. |
| Action | |
|    Edit | Click to **Edit** modify the entry. |
|    Delete | Click **Delete** to delete the entry. |
| Add | Click **Add** to create a new **Server** entry. |

## 31.3.2  The RADIUS Add/Edit Screen

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

**Figure 207**   Configuration > AAA > RADIUS > Add/Edit



The following table describes the labels in this screen.

Table 159   Configuration > AAA > RADIUS > Add/Edit

| 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. |

# 31.4  TACACS+

## 31.4.1  The TACACS+ Screen

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

Figure 208   Configuration > AAA > TACACS+



The following table describes the labels in this screen.

Table 160   Configuration > AAA > TACACS+

| LABEL | DESCRIPTION |
|---|---|
| TACACS+ Servers | |
| 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**. |
| Action | |
| Edit | Click to **Edit** modify the entry. |
| Delete | Click **Delete** to delete the entry. |
| Add | Click **Add** to create a new **Server** entry. |

## 31.4.2  The TACACS+ Add/Edit Screen

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

Figure 209   Configuration > AAA > TACACS+ > Add/Edit

The following table describes the labels in this screen.

Table 161   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. |
| Server Priority | Select the server priority as **High** or **Low**. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# Configuration: Management

## 32.1 Overview

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

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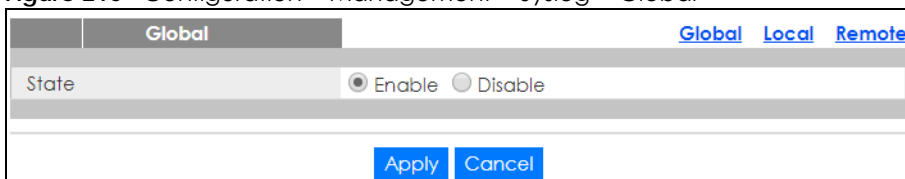
## 32.2 Syslog

The syslog feature can stores logs in the Switch's memory or sends logs to an external syslog server.

### 32.2.1 The Global Screen

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

**Figure 210** Configuration > Management > Syslog > Global



The following table describes the labels in this screen.

Table 162 Configuration > Management > Syslog > Global

| LABEL | DESCRIPTION |
|-------|-------------|
| Global | |
| State | Select **Enable** to turn on syslog (system logging) on the Switch. Otherwise, select **Disable** to turn it off. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

### 32.2.2 The Local Screen

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

**Figure 211** Configuration > Management > Syslog > Local

| Local | | Global Local Remote |
|---|---|---|
| **Target** | **Severity** | **Action** |
| Buffered | notice | ✎ 🗑 |
| | | |
| | Add | |

The following table describes the labels in this screen.

Table 163 Configuration > Management > Syslog > Local

| LABEL | DESCRIPTION |
|---|---|
| Local | |
| Target | Displays the local storage target for logging messages. |
| | It shows whether the logs are stored in the Switch's run-time memory buffer or flash (permanent) memory. If the logs are stored in the Switch's memory buffer, the logs will be erased when the Switch reboots. |
| Severity | Displays the severity level of messages to be stored in the Switch's memory. |
| | The Switch stores the messages of that severity level or higher. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **Local** entry. |

## 32.2.3 The Local Add/Edit Screen

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

**Figure 212** Configuration > Management > Syslog > Local > Add/Edit

| Local | | Global Local Remote |
|---|---|---|
| Target | ● Buffered ○ Flash | |
| Severity | emerg ▼ | |
| | | |
| | Apply Cancel | |
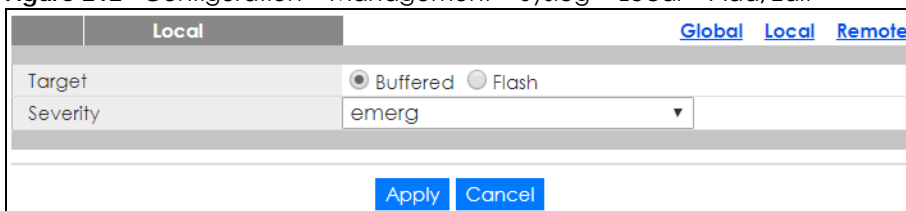
The following table describes the labels in this screen.

Table 164 Configuration > Management > Syslog > Local > Add/Modify

| LABEL | DESCRIPTION |
|---|---|
| Local | |
| Target | Select the local storage target for logging messages. The options are **Buffered** or **Flash**. |
| Severity | Select the severity level of the messages that you want to save in the Switch's memory. The Switch stores the logging messages with the severity level equal to or higher than what you selected. For example, if you select **warning**, all messages with the **warning**, **error**, **crit**, **alert** or **emerg** severity level will be stored. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 32.2.4 The Remote Screen

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

**Figure 213** Configuration > Management > Syslog > Remote

| | | | | |
|---|---|---|---|---|
| **Remote** | | | Global Local Remote | |
| **Server** | **Severity** | **Facility** | **Action** | |
| | | Add | | |

The following table describes the labels in this screen.

Table 165   Configuration > Management > Syslog > Remote

| LABEL | DESCRIPTION |
|---|---|
| Remote | |
| Server | Displays the external syslog server information which includes the server IP address and port number. |
| Severity | Displays the severity level of messages to be sent to the syslog server.<br><br>The Switch sends the messages of that severity level or higher. |
| 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. |
| Add | Click **Add** to create a new **Remote** entry. |

## 32.2.5 The Remote Add/Edit Screen

Use this screen to add an external syslog server. Click **Configuration** > **Management** > **Syslog** > **Remote** > **Add/Edit** to open this screen.

**Figure 214** Configuration > Management > Syslog > Remote > Add/Edit

| | | |
|---|---|---|
| **Remote** | | Global Local Remote |
| Server | | ( X.X.X.X or Hostname) |
| Server Port | 514 | |
| Severity | emerg ▼ | |
| Facility | local0 ▼ | |
| | Apply Cancel | |

The following table describes the labels in this screen.

Table 166   Configuration > Management > Syslog > Remote > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Remote | |
| Server | Enter the IP address or domain name of the syslog server. |
| Server Port | Enter port number of the syslog server. |

Table 166   Configuration > Management > Syslog > Remote > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Severity | Select the severity level of the messages that you want the Switch to send to this syslog server. The Switch sends the logging messages with the severity level equal to or higher than what you selected. For example, if you select **warning**, all messages with the **warning**, **error**, **crit**, **alert** or **emerg** severity level will be sent. |
| Facility | Select the log facility from the dropdown list. The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 32.3  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 SNMP version 3.

## 32.3.1  The Global Screen

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

Figure 215   Configuration > Management > SNMP > Global
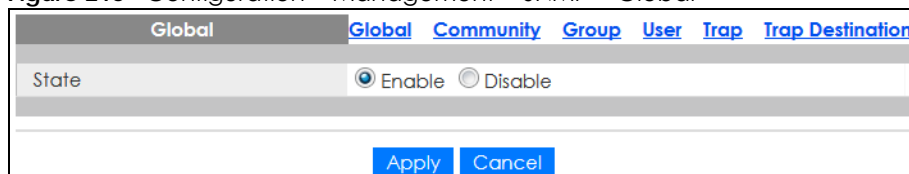


The following table describes the labels in this screen.

Table 167   Configuration > Management > SNMP > Global

| 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. |

## 32.3.2  The Community Screen

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

**Figure 216** Configuration > Management > SNMP > Community



The following table describes the labels in this screen.

Table 168 Configuration > Management > SNMP > Community

| LABEL | DESCRIPTION |
|---|---|
| Community | |
| 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**. |
| Action | |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **SNMP Community** entry. |

## 32.3.3 The Community Add Screen

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

**Figure 217** Configuration > Management > SNMP > Community > Add



The following table describes the labels in this screen.

Table 169 Configuration > Management > SNMP > Community > Add

| LABEL | DESCRIPTION |
|---|---|
| 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. |

## 32.3.4 The Group Screen

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

**Figure 218** Configuration > Management > SNMP > Group

| SNMPv3 Group | | | Global Community Group User Trap **Trap Destination** | |
|---|---|---|---|---|
| **Group Name** | **Security Model** | **Security Level** | **Access Right** | **Action** |
| | | | | |
| | | Add | | |

The following table describes the labels in this screen.

Table 170   Configuration > Management > SNMP > Group

| LABEL | DESCRIPTION |
|---|---|
| SNMPv3 Group | |
| 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:<br><br>• **any**: Any security model accepted(v1\|v2c\|usm).<br>• **v1**: Reserved for SNMPv1.<br>• **v2c**: Reserved for SNMPv2c.<br>• **usm**: User-based Security Model (USM). |
| Security Level | Displays the security model that this entry belongs to. Possible security models are:<br><br>• **noauth**: No authentication and no privacy.<br>• **auth**: Authentication and no privacy.<br>• **Priv**: Authentication and privacy. |
| 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. |
| Add | Click **Add** to create a new **SNMPv3 Group** entry. |

## 32.3.5  The Group Add Screen

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

**Figure 219** Configuration > Management > SNMP > Group > Add

| SNMPv3 Group | Global Community Group User Trap **Trap Destination** |
|---|---|
| Group Name | |
| Security Level | noauth ▾ |
| Access Mode | ● Read-Only ○ Read-Write |
| | Apply Cancel |

The following table describes the labels in this screen.

Table 171   Configuration > Management > SNMP > Group > Add

| LABEL | DESCRIPTION |
|---|---|
| SNMPv3 Group | |
| 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**. |

Table 171   Configuration > Management > SNMP > Group > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Security Level | Select the security model that this entry belongs to. Possible security models are:<br><br>• **noauth**: No authentication and no privacy.<br>• **auth**: Authentication and no privacy.<br>• **priv**: Authentication and privacy. |
| Access Mode | 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. |

## 32.3.6  The User Screen

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

Figure 220   Configuration > Management > SNMP > User



The following table describes the labels in this screen.

Table 172   Configuration > Management > SNMP > User

| LABEL | DESCRIPTION |
|---|---|
| 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:<br><br>• **None**: No authentication protocol.<br>• **MD5**: An optional flag to indicate that this user uses MD5 authentication protocol.<br>• **SHA**: An optional flag to indicate that this user uses SHA authentication protocol.<br><br>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. |
| Add | Click **Add** to create a new SNMP user. |

## 32.3.7 The User Add Screen

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

**Figure 221** Configuration > Management > SNMP > User > Add

| SNMP User | Global Community Group User Trap Trap Destination |
|---|---|
| User Name | |
| Group Name | Test ▾ |
| Auth Potocol | ⦿ MD5 ○ SHA |
| Auth Password | |
| Priv Password | |
| | Apply Cancel |

The following table describes the labels in this screen.

Table 173   Configuration > Management > SNMP > User > Add

| 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:<br><br>• **MD5**: An optional flag to indicate that this user uses MD5 authentication protocol.<br>• **SHA**: An optional flag to indicate that this user uses SHA authentication protocol.<br><br>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. |

## 32.3.8 The Trap Screen

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

**Figure 222** Configuration > Management > SNMP > Trap



The following table describes the labels in this screen.

Table 174  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:<br><br>• **Enabled**: Enable SNMP trap authentication failure.<br>• **Disabled**: Disable SNMP trap authentication failure. |
| SNMP LinkupDown Trap State | Select the SNMP trap link-up and link-down mode operation. Possible modes are:<br><br>• **Enabled**: Enable SNMP trap link-up and link-down mode operation.<br>• **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. |

## 32.3.9  The Trap Destination Screen

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

**Figure 223** Configuration > Management > SNMP > Trap Destination



The following table describes the labels in this screen.

Table 175  Configuration > Management > SNMP > Trap Destination

| LABEL | DESCRIPTION |
|---|---|
| SNMP Trap Host | |
| Server | Displays a string identifying the server address that this entry belongs to. |

Table 175   Configuration > Management > SNMP > Trap Destination (continued)

| LABEL | DESCRIPTION |
|---|---|
| Version | Indicates the SNMP trap supported version. Possible versions are: <br><br> • **v1**: Set SNMP trap supported version 1. <br> • **v2c**: Set SNMP trap supported version 2c. <br> • **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. |
| Add | Click **Add** to create a new **SNMP Trap Host** entry. |

## 32.3.10  The Trap Destination Add Screen

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

Figure 224   Configuration > Management > SNMP > Trap Destination > Add



The following table describes the labels in this screen.

Table 176   Configuration > Management > SNMP > Trap Destination > Add

| LABEL | DESCRIPTION |
|---|---|
| Trap Destination | |
| Server | Enter the IP address of the server or a string identifying the server address that this entry belongs to. |
| Version | Select the SNMP trap supported version. Possible versions are: <br><br> • **v1**: Set SNMP trap supported version 1. <br> • **v2c**: Set SNMP trap supported version 2c. <br> • **v3**: Set SNMP trap supported version 3. |
| 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. |

# 32.4  Error Disable

## 32.4.1  The Error Disabled Screen

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

Figure 225   Configuration > Management > Error Disable

| | | |
|---|---|---|
| **Error Disable** | | |
| Recovery Interval | 300 | (0-86400 sec) |
| Broadcast Flood | ○ Enable  ● Disable | |
| Unknown Multicast Flood | ○ Enable  ● Disable | |
| Unicast Flood | ○ Enable  ● Disable | |
| Port Security | ○ Enable  ● Disable | |
| | **Apply  Cancel** | |

The following table describes the labels in this screen.

Table 177   Configuration > Management > Error Disable

| LABEL | DESCRIPTION |
|---|---|
| Error Disable | |
| 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. |
| 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. |

# 32.5  HTTP/HTTPS

## 32.5.1  The HTTP Screen

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

The following table describes the labels in this screen.

Table 178   Configuration > Management > HTTP/HTTPS > HTTP

| 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. |

## 32.5.2  The HTTPS Screen

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

**Figure 227** Configuration > Management > HTTP/HTTPS > HTTPS



The following table describes the labels in this screen.

Table 179   Configuration > Management > HTTP/HTTPS > HTTPS

| LABEL | DESCRIPTION |
|---|---|
| HTTPS | |
| State | Select the HTTPS mode operation. Possible modes are: • **Enable**: Enable HTTPS mode operation. |
| Authentication Method | Select the authentication method from the dropdown list. |

Table 179   Configuration > Management > HTTP/HTTPS > HTTPS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Session Timeout | Enter the session timeout value. The timeout can be between 0 and 86400 minutes. |
| Re-Generate Certificate | Click this to renew the HTTPS certificate that is verified by a third party to create secure HTTPS connections between your computer and the Switch. This allows you to securely access the Switch using the Web Configurator.<br><br>Note: Re-generating the certificate will cause a network connection reset. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 32.6  Telnet/SSH

## 32.6.1  The Telnet Screen

Use this screen to configure the **Telnet** settings. Click **Configuration** > **Management** > **Telnet/SSH** > **Telnet** to open this screen.

Figure 228   Configuration > Management > Telnet/SSH > Telnet



The following table describes the labels in this screen.

Table 180   Configuration > Management > Telnet/SSH > Telnet

| LABEL | DESCRIPTION |
|---|---|
| Telnet | |
| State | You can allow the Switch for remote Telnet access. The administrator uses Telnet from a computer on a remote network to access the Switch.<br><br>• **Enable**: allow remote Telnet access.<br>• **Disable**: do not allow remote Telnet access. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 32.6.2  The SSH Screen

Use this screen to configure the **SSH** settings. Click **Configuration** > **Management** > **Telnet/SSH** > **SSH** to open this screen.

Figure 229   Configuration > Management > Telnet/SSH > SSH

The following table describes the labels in this screen.

Table 181   Configuration > Management > Telnet/SSH > SSH

| LABEL | DESCRIPTION |
|-------|-------------|
| SSH | |
| State | You can allow a remote computer to access the Switch using SSH (Secure SHell protocol). <br><br> • **Enable**: allow SSH connection. <br> • **Disable**: do not allow SSH connection. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 32.7  Users

## 32.7.1  The Users Screen

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

Figure 230   Configuration > Management > Users



The following table describes the labels in this screen.

Table 182   Configuration > Management > Users

| LABEL | DESCRIPTION |
|-------|-------------|
| Users | |
| 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. |
| 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. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new **User** entry. |

## 32.7.2  The Users Add/Edit Screen

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

**Figure 231** Configuration > Management > Users > Add/Edit



The following table describes the labels in this screen.

Table 183   Configuration > Management > Users > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Users | |
| 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. |
| Password | Enter a password for the user. The allowed string length is 0 to 64. |
| 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. |

# 32.8  Remote Access Control

## 32.8.1  The Global Screen

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

**Figure 232** Configuration > Management > Remote Access Control > Global

The following table describes the labels in this screen.

Table 184   Configuration > Management > Remote Access Control > Global

| 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 | |
| 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. |
| Source IP Mask | Displays the source IP mask. |
| Port | Display the port value. |
| Service | Display the service used for remote access. The values are **ALL**, **HTTP**, **HTTPS**, or **SNMP**. |
| Action | |
| Edit | Click **Edit** to make changes to the entry. |
| Delete | Click **Delete** to remove the entry. |
| Add | Click **Add** to create a new profile entry. |

## 32.8.2  The Profile Add/Edit Screen

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

Figure 233   Configuration > Management > Remote Access Control > Global > Add/Edit

The following table describes the labels in this screen.

Table 185   Configuration > Management > Remote Access Control > Global > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Management Access List | |
| 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/Mask**. |
| IPv4/Mask | Select and enter the IPv4 address and subnet mask of a computer which will be allowed or denied to access the Switch. |
| 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. |

# CHAPTER 33
# Maintenance

## 33.1 Firmware Upgrade

### 33.1.1 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's firmware.

**Figure 234** Maintenance > Firmware > Upload



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

Table 186 Maintenance > Firmware > Upload

| LABEL | DESCRIPTION |
|---|---|
| Upload | |
| 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. |
| File Path | Browse to the path on your computer to upload the firmware you want as the active image. |

### 33.1.2 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.

### 33.1.3 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 .bix 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. In **File Path**, click **Browse** to display the **Choose File** screen from which you can locate the firmware file in the bix 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.

## 33.2 Firmware Management

### 33.2.1 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 235** Maintenance > Firmware > Management



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

Table 187   Maintenance > Firmware > Management

| LABEL | DESCRIPTION |
|-------|-------------|
| Image Select | |
| Active Image | Select which firmware should load, click **Apply** and reboot the Switch to see changes. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |
| Images Information | |
| Flash Partition | Displays the partition number. |
| 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. |

## 33.2.2  Select the Active Image

The available partition is shown under **Image Select**.

Follow the steps below to choose the active image, which will be the default partition during boot. When you selected the active image and saved the changes, the other one will be the backup.

If you are facing problems with the active partition when booting, the Switch will use the backup one and it'll be loaded automatically.

1. In **Active Image**, choose the backup image according to the information displayed in **Images Information**.
2. Click **Apply** to activate the backup image.
   OR
   Click **Cancel** to discard the changes.

# 33.3 Backup a Configuration File

## 33.3.1 Overview

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

Click **Maintenance** > **Configuration** > **Backup** to display the 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 236**   Maintenance > Configuration > Backup



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

Table 188   Maintenance > Configuration > Backup

| LABEL | DESCRIPTION |
|---|---|
| Backup | |
| 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: **Backup configuration** - 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. **Startup configuration** - this is the configuration used when the Switch is booting up. **Running configuration** - this is the configuration when the Switch is running. There are two different types of log files: **Flash log**: Select this to save logs in the Switch's flash (permanent) memory. **Buffer log**: Select this to save logs in the Switch's memory buffer. If the logs are stored in the Switch's memory buffer, the logs will be erased when the Switch reboots. **Tech Support**: Select this to upload the configuration/log files to the TFTP server. The log files contain useful information such as CPU utilization, history, memory and Mbuf (Memory Buffer) log, and crash reports for issue analysis by customer support should you have difficulty with your Switch. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 33.3.2 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.

## 33.3.3 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.

# 33.4 Restore a Configuration File

## 33.4.1 Overview

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

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

**Figure 237** Maintenance > Configuration > Restore



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

Table 189   Maintenance > Configuration > Restore

| LABEL | DESCRIPTION |
|-------|-------------|
| Configuration Restore | |
| 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. |

Table 189   Maintenance > Configuration > Restore

| LABEL | DESCRIPTION |
|---|---|
| File Name | Enter the name of the configuration file on the TFTP server. |
| File Path | Browse to the path on your computer to upload the configuration you want to restore. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

## 33.4.2  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.

## 33.4.3  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.  In **File Path**, 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.

# 33.5  Manage Configuration Files

## 33.5.1  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.

Click **Maintenance** > **Configuration** > **Management** to display the screen as shown next. Use this screen to replace startup and backup configuration files.

**Figure 238** Maintenance > Configuration > Management

| File Management | Backup Restore Management Factory Default |
|---|---|
| Source File | ⦿ Running configuration<br>○ Startup configuration<br>○ Backup configuration |
| Destination File | ⦿ Startup configuration<br>○ Backup configuration |
| | Apply Cancel |

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.

# 33.6 Reset to Factory Defaults

## 33.6.1 Overview

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

Click **Maintenance** > **Configuration** > **Factory Default** to display the screen as shown next. Use this screen to reset the Switch back to factory defaults.

Table 190   Maintenance > Configuration > Factory Default

| Restore Factory Default | Backup Restore Management Factory Default |
|---|---|
| | This would reset the configuration to factory default and will reboot the system. |
| | Restore |

## 33.6.2 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 2 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).

# 33.7  Network Diagnostics

Use the network utilities to perform diagnostics.

## 33.7.1  Port Test

Click **Maintenance** > **Diagnostics** > **Port Test** > **Cable Diag** in the navigation panel to open this screen. Use this screen to perform an internal loop-back test on an Ethernet port.

Note: The Switch measures the cable length by sending an electric signal through the cable and reading the signal that is reflected back. To prevent possible interference from a connected device, it is suggested that you disconnect the other end of the Ethernet cable which is connected to the specified port.

**Figure 239**  Maintenance > Diagnostics > Port Test > Cable Diag



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**.

## 33.7.2  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 240**   Maintenance > Diagnostics > PING > IPv4

| Ping Test | | IPv4  IPv6 |
|---|---|---|
| IP Address | 192.168.1.100 | (x.x.x.x or hostname) |
| Count | 4 | (1 - 5) |
| Interval | 1 | (1 - 5 sec) |
| Size | 56 | (8 - 5120 byte) |
| Result | | |

Apply   Cancel

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

Table 191   Maintenance > Diagnostics > PING > IPv4

| LABEL | DESCRIPTION |
|---|---|
| Ping Test | |
| 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. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

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**.

## 33.7.3 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 241** Maintenance > Diagnostics > PING > IPv6

| IPv6 Ping Test | | | IPv4 IPv6 |
|---|---|---|---|
| IPv6 Address | | | (XX:XX::XX:XX or hostname) |
| Count | 4 | (1 - 5 ) | |
| Interval | 1 | (1 - 5 sec) | |
| Size | 56 | (8 - 5120 byte) | |
| Result | | | |

Apply    Cancel

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

Table 192   Maintenance > Diagnostics > PING > IPv6

| LABEL | DESCRIPTION |
|---|---|
| IPv6 Ping Test | |
| 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. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

Follow the steps to perform a ping test.

1. In **IPv6 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**.

## 33.7.4 Trace Route

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

**Figure 242** Maintenance > Diagnostics > Trace > Trace Route



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

Table 193   Maintenance > Diagnostics > Trace > Trace Route

| LABEL | DESCRIPTION |
|---|---|
| Trace Route | |
| IP Address | 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. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

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**.

# 33.8  Reboot

## 33.8.1  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 243**   Maintenance > Reboot
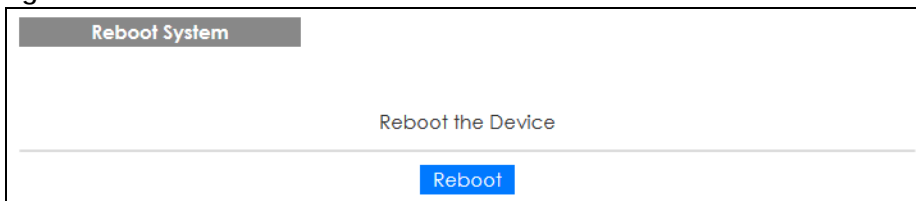


## 33.8.2  Reboot the Switch

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.

# CHAPTER 34
# 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

## 34.1 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 adapter or cord included with the Switch.

3   Make sure the power adapter 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 adapter 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.

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 35.

2   Check the hardware connections. See Chapter 2 on page 22.

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 adapter 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.

# 34.2  Switch Access and Login

I forgot the IP address for the Switch.

1    The default in-band IP address is **192.168.1.1** or **http://DHCP-assigned IP** (when connecting to a DHCP server).

2    If this does not work, you have to reset the device to its factory defaults. See Section 3.4 on page 36 or Section 33.6 on page 235.

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 3.4 on page 36 or Section 33.6 on page 235.

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 Chapter 2 on page 22.

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 3.4 on page 36 or Section 33.6 on page 235.

**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 HTTPS. 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** Check that you have enabled logins for HTTP. 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 3.4 on page 36 or Section 33.6 on page 235.

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).

# 34.3  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 5.3.1 on page 45 for more information about how to save your configuration.

# APPENDIX A
# Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See *https://www.zyxel.com/homepage.shtml* and also *https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

Please have the following information ready when you contact an office.

## Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

## Corporate Headquarters (Worldwide)

### Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

## Asia

### China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

### India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

### Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

### Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

### Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

### Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

### Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

### Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

### Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

### Thailand

- Zyxel Thailand Co., Ltd.
- https://www.zyxel.com/th/th/

### Vietnam

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

## Europe

### Belarus

- Zyxel BY
- https://www.zyxel.by

### Belgium

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/

- https://www.zyxel.com/be/fr/

## Bulgaria

- Zyxel България
- https://www.zyxel.com/bg/bg/

## Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

## Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

## Estonia

- Zyxel Estonia
- https://www.zyxel.com/ee/et/

## Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

## France

- Zyxel France
- https://www.zyxel.fr

## Germany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

## Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

## Italy

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

## Latvia

- Zyxel Latvia
- https://www.zyxel.com/lv/lv/

### Lithuania

- Zyxel Lithuania
- https://www.zyxel.com/lt/lt/

### Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

### Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

### Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

### Romania

- Zyxel Romania
- https://www.zyxel.com/ro/ro

### Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

### Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

### Spain

- Zyxel Communications ES Ltd.
- https://www.zyxel.com/es/es/

### Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

### Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

### Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

### UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

### Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

## South America

### Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

### Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

### Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

### Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

### South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

## Middle East

### Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

### Middle East

- Zyxel Communications Corporation
- https://www.zyxel.com/me/en/

## North America

### USA

- Zyxel Communications, Inc. - North America Headquarters
- https://www.zyxel.com/us/en/

## Oceania

### Australia

- Zyxel Communications Corporation
- https://www.zyxel.com/au/en/

## Africa

### South Africa

- Nology (Pty) Ltd.
- https://www.zyxel.com/za/en/

# APPENDIX B
# Legal Information

## Copyright

Copyright © 2020 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

### 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.

## Regulatory Notice and Statement (Class A)

Model List: GS1900-8HP (Revision A1), GS1900-24, GS1900-24EP, GS1900-24HP/GS1900-24HPv2, GS1900-48, GS1900-48HP/GS1900-48HPv2

### United States of America



The following information applies if you use the product within USA area.

#### Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment 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.

### Canada

The following information applies if you use the product within Canada area

#### Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

### European Union



The following information applies if you use the product within the European Union.

#### CE EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

## List of National Codes

| COUNTRY | ISO 3166 2 LETTER CODE | COUNTRY | ISO 3166 2 LETTER CODE |
|---|---|---|---|
| Austria | AT | Liechtenstein | LI |
| Belgium | BE | Lithuania | LT |
| Bulgaria | BG | Luxembourg | LU |
| Croatia | HR | Malta | MT |
| Cyprus | CY | Netherlands | NL |
| Czech Republic | CZ | Norway | NO |
| Denmark | DK | Poland | PL |
| Estonia | EE | Portugal | PT |
| Finland | FI | Romania | RO |
| France | FR | Serbia | RS |
| Germany | DE | Slovakia | SK |
| Greece | GR | Slovenia | SI |
| Hungary | HU | Spain | ES |
| Iceland | IS | Sweden | SE |
| Ireland | IE | Switzerland | CH |
| Italy | IT | Turkey | TR |
| Latvia | LV | United Kingdom | GB |

## 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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Caution: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic device. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- 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.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

- This device must be grounded. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  - Install the power supply before connecting the power cable to the power supply.

  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.

- CLASS 1 LASER PRODUCT (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

- APPAREIL À LASER DE CLASS 1 (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

## Environment Statment

### European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



## 台灣

警告使用者：

* 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。」

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

* 請勿將此產品接近水、火焰或放置在高溫的環境。
* 避免設備接觸
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
* 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
* 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
* 若接上不正確的電源變壓器會有爆炸的風險。。
* 請勿隨意更換產品內的電池。
* 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
* 請將廢電池丟棄在適當的電器或電子設備回收處。
* 請勿將設備解體。
* 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
* 請插在正確的電壓供給插座 ( 如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
* 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
* 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
* 請勿將此設備安裝於室外，此設備僅適合放置於室內。
* 請勿隨一般垃圾丟棄。
* 請參閱產品背貼上的設備額定功率。
* 請參考產品型錄或是彩盒上的作業溫度。

- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則
  - 先連接電源線至設備連，再連接電源。
  - 先斷開電源再拔除連接至設備的電源線。
  - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

## Regulatory Notice and Statement (Class B)

Model List: GS1900-8, GS1900-8HP (Revision B1), GS1900-10HP, GS1900-16, GS1900-24E

## UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

### FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

## CANADA

The following information applies if you use the product within Canada area

### Industry Canada ICES statement
CAN ICES-3 (B)/NMB-3(B)

## EUROPEAN UNION



The following information applies if you use the product within the European Union.

### List of national codes

| COUNTRY | ISO 3166 2 LETTER CODE | COUNTRY | ISO 3166 2 LETTER CODE |
|---|---|---|---|
| Austria | AT | Liechtenstein | LI |
| Belgium | BE | Lithuania | LT |
| Bulgaria | BG | Luxembourg | LU |
| Croatia | HR | Malta | MT |
| Cyprus | CY | Netherlands | NL |
| Czech Republic | CZ | Norway | NO |
| Denmark | DK | Poland | PL |
| Estonia | EE | Portugal | PT |
| Finland | FI | Romania | RO |
| France | FR | Serbia | RS |
| Germany | DE | Slovakia | SK |
| Greece | GR | Slovenia | SI |
| Hungary | HU | Spain | ES |
| Iceland | IS | Switzerland | CH |
| Ireland | IE | Sweden | SE |
| Italy | IT | Turkey | TR |
| Latvia | LV | United Kingdom | GB |

## 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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

    - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

    - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

- CLASS 1 LASER PRODUCT (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

- APPAREIL À LASER DE CLASS 1 (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

## Environment Statement

### ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or

- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to "Wireless" chapter for more detail.)

## European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

### 台灣

安全警告 - 為了您的安全，請先閱讀以下警告及指示：
- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
- 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 ( 如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

### Explanation of the Symbols

| SYMBOL | EXPLANATION |
|---|---|
| ∿ | Alternating current (AC):<br><br>AC is an electric current in which the flow of electric charge periodically reverses direction. |
| === | Direct current (DC):<br><br>DC if the unidirectional flow or movement of electric charge carriers. |
| ⏚ | Earth; ground:<br><br>A wiring terminal intended for connection of a Protective Earthing Conductor. |
| ▣ | Class II equipment:<br><br>The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation. |

## 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 at www.zyxel.com to receive e-mail notices of firmware upgrades and related information.

## Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. If you cannot find it there, contact your vendor or Zyxel Technical Support at support@zyxel.com.tw.

To obtain the source code covered under those Licenses, please contact your vendor or Zyxel Technical Support at support@zyxel.com.

# Index

## A

access  **43**
administrator password  **44**
applications
   backbone  **18**
   bridging  **18**
   fiber uplink  **18**
   IEEE 802.1Q VLAN  **19**
   PoE  **17**

## B

Backbone  **18**

## C

certifications  **254**
   viewing  **256**
contact information
   customer support  **244**
cookies  **43**
copyright  **250**
current date/time  **53**
customer support  **244**

## D

DHCP
   and domain name  **62**, **109**, **114**, **115**, **116**, **117**, **118**, **120**, **122**, **133**
disclaimer  **250**
domain name  **62**, **109**, **114**, **115**, **116**, **117**, **118**, **120**, **122**, **133**

## E

Ethernet ports
   default settings  **30**

## F

FCC interference statement  **250**
Firefox  **43**
firmware
   current version  **53**
front panel  **28**
FTP  **21**

## H

hardware installation  **22**
hardware overview  **28**

## I

installation
   freestanding  **22**
   precautions  **25**
interfaces
   as DHCP servers  **62**, **109**, **114**, **115**, **116**, **117**, **118**, **120**, **122**, **133**
Internet Explorer  **43**
Internet Protocol version 6, see IPv6
introduction  **17**
IPv6  **20**
   Neighbor Discovery Protocol  **20**
   ping  **20**