ZYXEL
NETWORKS

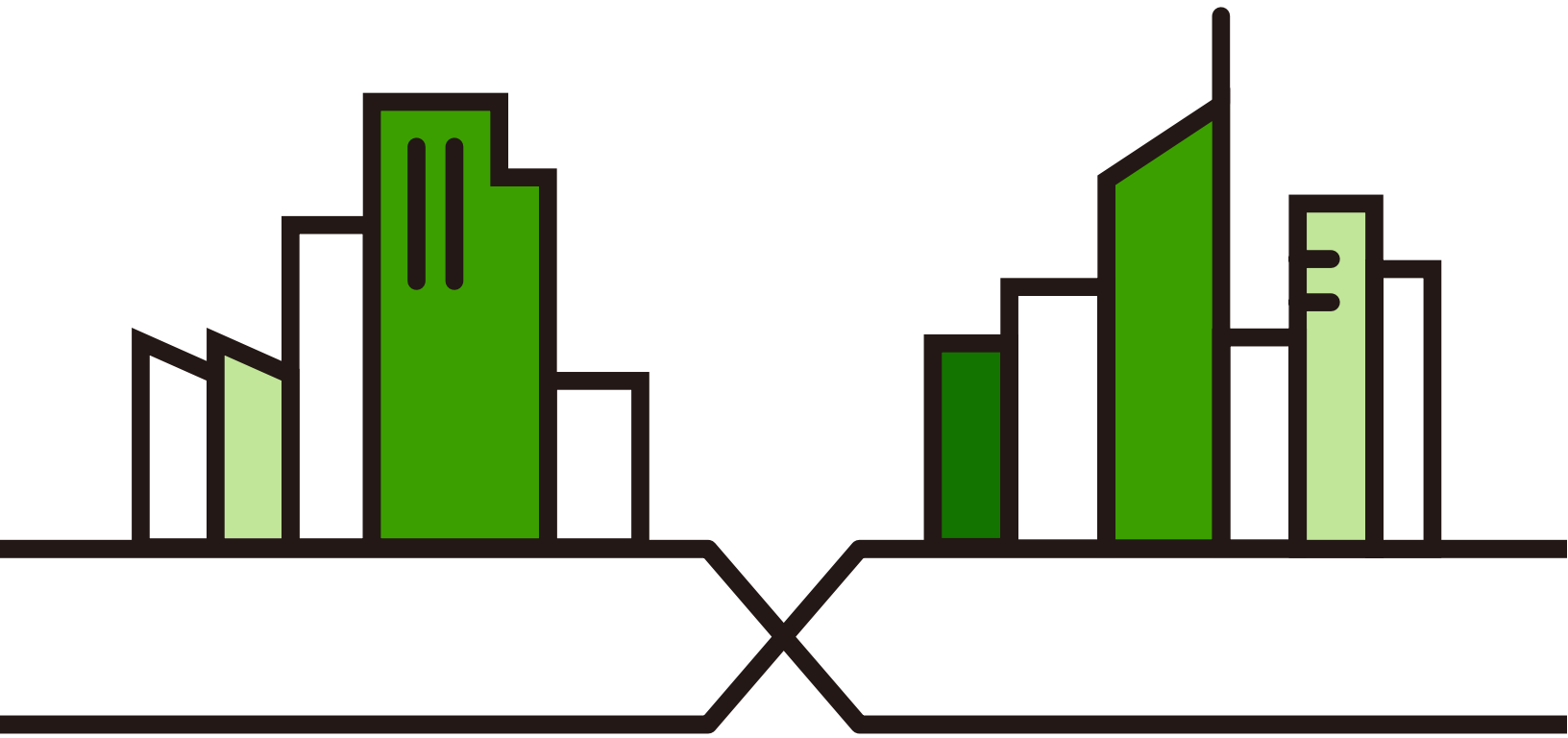
User's Guide

GS1920v2 Series

8/24/48-port GbE Smart Managed Switch

Default Login Details	
Management IP Address	https://setup.zyxel or https://DHCP-assigned IP or 192.168.1.1
User Name	admin
Password	1234 (Standalone mode) or Local Credentials Password (Cloud Mode)

Version 5.00 Edition 1, 02/2025



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This User's Guide is for the platform version listed on the cover. Not all products support all firmware features. 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: The version number on the cover page refers to the Switch'es latest firmware version to which this User's Guide applies.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Switch.

- Web Configurator Online Help

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

- Nebula Control Center (NCC) User's Guide

  Go to ***nebula.zyxel.com*** or ***support.zyxel.com*** to get this User's Guide on how to configure the Switch using Nebula.

- More Information
  Go to ***https://community.zyxel.com/en*** 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, **SYSTEM** > **IP Setup** > **Network Proxy Configuration** means you first click **SYSTEM** in the navigation panel, then the **IP Setup** sub menu, then **Network Proxy Configuration** 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 Router 	Wireless Router / Access Point 
Generic Switch 	Smart TV 	Desktop 
Laptop 	IP Camera 	Printer 
Server 		

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Getting to Know Your Switch

1.1 Introduction

This User Guide is for the platform version listed on the cover. This chapter introduces the main features and applications of the Switch.

The GS1920v2 Series consists of the following models:

- GS1920-8HPv2
- GS1920-24v2
- GS1920-24HPv2
- GS1920-48v2
- GS1920-48HPv2

References to PoE models in this User's Guide only apply to GS1920-8HPv2, GS1920-24HPv2 and GS1920-48HPv2.

See the following table for the cables required and distance limitation to attain the corresponding speed.

Table 1 Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100M	100 m	100 MHz
Category 5e or better	1G / 2.5G	100 m	100 MHz

Note: Make sure to select the correct speed for the port in **PORT** > **Port Setup** > **Port Setup**.

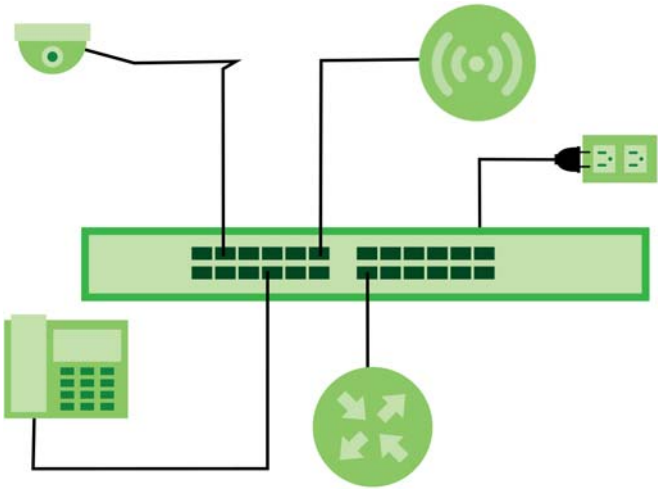
1.2 Example Applications

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 following example figure shows a Switch supplying 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

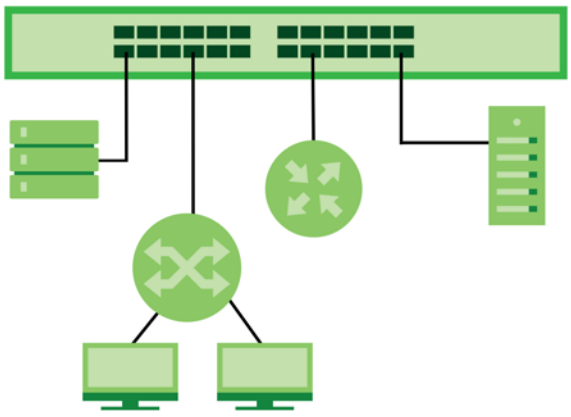


1.2.2 Backbone Example Application

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.

In this example, 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 Application

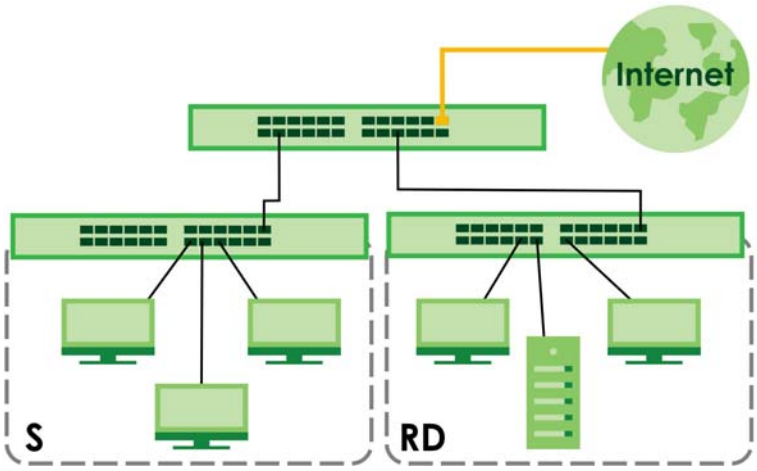


1.2.3 Bridging with Fiber Optic Uplink Example Application

In this example, the Switch connects different company departments (**RD** and Sales(**S**)) 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 through the Switch. You can provide a super-fast uplink connection by using a Gigabit Ethernet or SFP port on the Switch.

Moreover, the Switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 3 Bridging with Fiber Optic Uplink Example Application



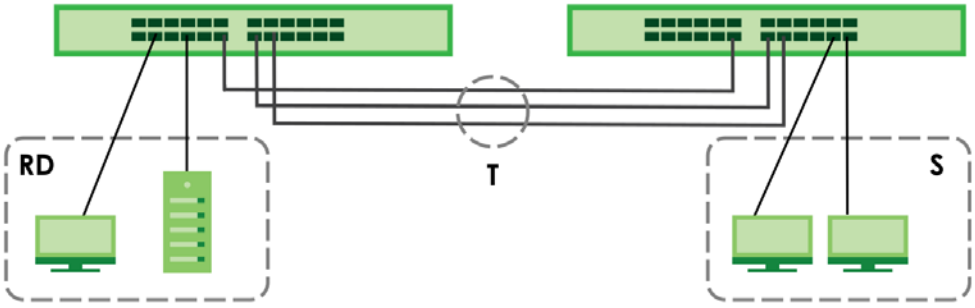
1.2.4 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use link aggregation (trunking, **T**) to connect these two networks (**RD**, **S**).

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The Switch can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

This helps you switch to higher-speed LANs without the need for replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance.

Figure 4 High Performance Switched Workgroup Application



1.2.5 IEEE 802.1Q VLAN Application Examples

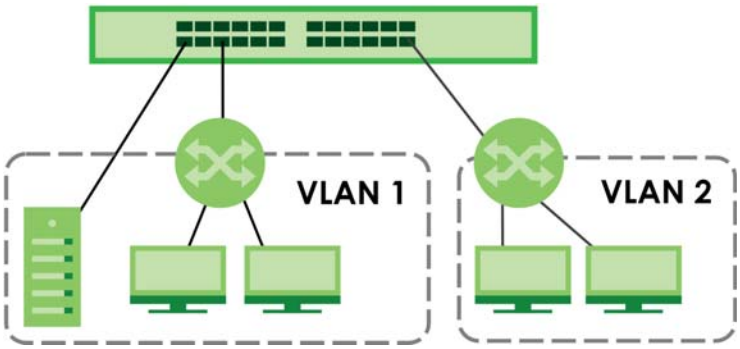
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same groups unless such traffic first goes through a router.

1.2.5.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thereby increase network performance through reduced 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



1.3 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

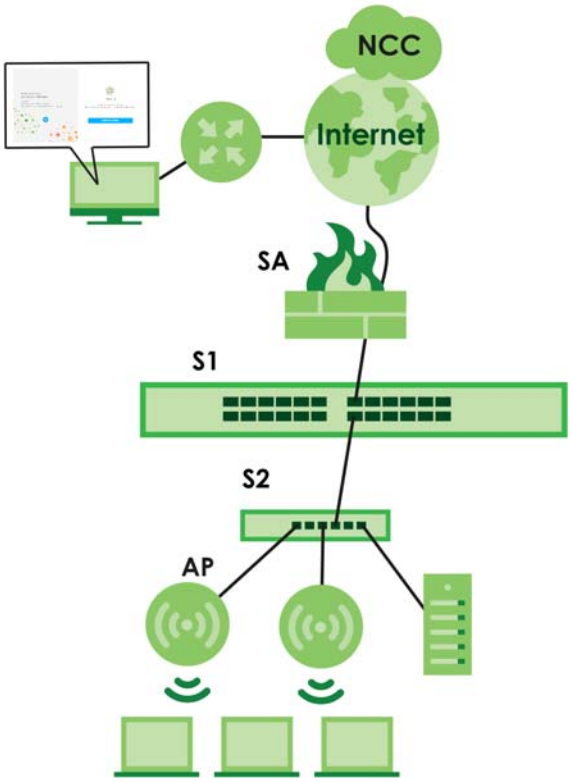
- NCC (Zyxel Nebula Control Center). With the NCC, you can remotely manage and monitor the Switch through a cloud-based network management system. See the NCC User's Guide for detailed information on how to access the NCC, manage your Switch through the NCC, and configure Nebula managed devices.
- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 50.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup or restore. See Section 66.3.1 on page 431.
- SNMP. The Switch can be monitored and/or managed by an SNMP manager. See Section 23.6.1 on page 152.
- Cluster Management. Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See Chapter 66 on page 429.
- ZON Utility. ZON Utility is a program designed to help you deploy and perform initial setup on a network more efficiently. See Section 4.3 on page 54.

1.4 Management Modes

The Switch can operate in either standalone or Nebula cloud management mode. When the Switch is in standalone mode, it can be configured and managed by the Web Configurator. When the Switch is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control Center (NCC).

Use the Web Configurator to configure and manage the Switch directly in standalone mode or use Nebula Control Center (NCC) to configure and manage the Switch in cloud mode. The Nebula Control Center (NCC) is an alternative cloud-based network management system that allows you to remotely manage and monitor the Zyxel Nebula Security Appliances (**SA**), Ethernet Switches (**S1** and **S2**), and Access Points (**AP**). You may also access the Web Configurator in cloud mode.

Figure 6 NCC Example Network Topology



Nebula Cloud Management

To have Nebula manage the Switch, you must first register it at the Nebula web portal at https://nebula.zyxel.com, and ensure that **Nebula Control Center (NCC) Discovery** is enabled in **SYSTEM** > **Cloud Management** in the Switch Web Configurator.

Note: See the Switch's datasheet for the feature differences between standalone and Nebula cloud management modes. You can find the Switch's datasheet at the Zyxel website.

See the NCC User's Guide for how to configure the Switch using Nebula.

1.4.1 Mode Changing

This section describes how to change the Switch's management mode. Refer to the Switch's standalone mode User's Guide for LED descriptions, including **CLOUD** LED behavior.

From Standalone to Nebula Cloud Management

To manage your Switch through Nebula, connect the Switch to the Internet, and register it to a site and

organization at the Nebula web portal (*https://nebula.zyxel.com*).

See the following steps or the Switch Quick Start Guide for registering the Switch.

Go to the NCC to Register the Switch

1 Go to the Nebula web portal in one of three ways.

- Enter *https://nebula.zyxel.com* in a supported web browser. See the Nebula User's Guide for more information about supported browsers.
- Click **Visit Nebula** in the Switch's login page.
- Click the **Nebula Control Center** icon in the upper right of the Switch's Web Configurator.

2 Click **Get Started** in the Nebula web portal. Enter your Zyxel Account information. You will be redirected to another screen where you can sign up for a Zyxel Account if you do not have one.

3 Create an organization and a site (using the Nebula setup wizard) or select an existing site.

4 Register the Switch by entering its Registration MAC address and serial number and assign it to the site. The serial number and Registration MAC address can be found in the **DASHBOARD** screen or the device back label on the Switch.

Use the Zyxel Nebula Mobile App to Register the Switch

1 Download and open the Zyxel Nebula Mobile app in your mobile device (see Section 17.2 on page 115 to download the app). Click **Start** on the first page. Click **Create account** to create a Zyxel Account or enter your existing account information to log in.

2 Create an organization and site, or select an existing site using the Zyxel Nebula Mobile app.

3 Select a site and scan the Switch's QR code or manually enter the information to add it to the site. You can find the QR code:

- On a label on the Switch or
- On its box or
- In the Web Configurator at **SYSTEM** > **Cloud Management**.

See Section 3.4 on page 46 for more information about the **CLOUD** LED or Section Table 13 on page 86 for more information about the **Cloud Control Status** field in the **DASHBOARD** screen to see if the Switch goes into Nebula cloud management mode successfully.

Local Credentials Password

The Switch goes into Cloud mode automatically after it can access the Nebula web portal and is successfully registered there. Its login password and settings are then overwritten with what you have configured in the Nebula web portal. To access the Web Configurator when the Switch is in Cloud mode, use the Local credentials password to login.

Note: The **Local credentials**: **Password** can be found in **Site-wide** > **Configure** > **Site settings** > **Device configuration** in the NCC portal. See the NCC User's Guide for more information.

Figure 7 Site-wide > Configure > Site settings: Device configuration: Local credentials

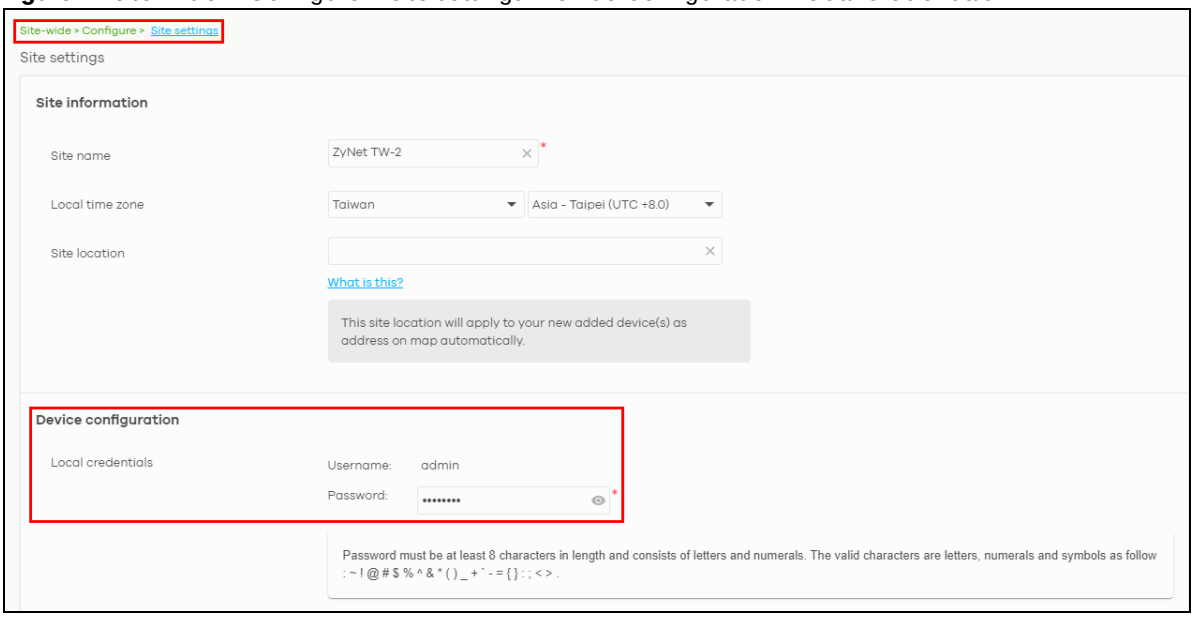


Table 2 Management Method Comparison

MODE	ACCESS	LOGIN USER NAME	LOGIN PASSWORD	LOGIN IP ADDRESS/URL/ DOMAIN NAME
Cloud mode	NCC (Nebula Control Center) portal	Zyxel Account email	Zyxel Account password	https://nebula.zyxel.com
	Web Configurator (Local GUI)	admin	Local credentials password	https://setup.zyxel OR https://DHCP-assigned IP OR a configured static IP address
You can configure the Switch using both the NCC and the Web Configurator. Note: The latest configuration made in either the NCC or the Web Configurator will be applied to the Switch. Settings are pushed from the NCC to the Switch, but not from the Switch to the NCC. • The settings you configure in the NCC will appear in the Web Configurator settings and will be applied to the Switch. • The settings you configure in the Web Configurator will not appear in the NCC settings, but will be applied to the Switch. To avoid inconsistency, we recommend you use NCC to configure the Switch. Only use the Web Configurator for advanced settings not available in the NCC or for troubleshooting if you cannot access the NCC.				
Standalone mode	Web Configurator	admin	1234	https://setup.zyxel OR https://DHCP-assigned IP OR https://192.168.1.1

From Nebula-managed to Standalone Mode

To return to direct management standalone mode, remove (unregister) the Switch from the inventory in the Nebula web portal.

Note: When you change the Switch's management mode from Cloud mode to standalone mode, the Switch will reboot and restore its factory-default settings.

To unregister the Switch:

1 Go to the Nebula Control Center (*https://nebula.zyxel.com*).

2 Go to the **Organization-wide** > **License & inventory** > **Devices** screen.

3 Select the Switch you want to remove (unregister) from the organization.

4 Click **Actions**, then click **Remove from organization**.

It will take a while for the Switch to reboot and reset to factory default.

1.4.2 ZON Utility

With its built-in Web Configurator, including the Neighbor Management feature (Section 11.1 on page 98), viewing, managing and configuring the Switch and its neighboring devices is simplified.

In addition, Zyxel offers a proprietary software program called Zyxel One Network (ZON) Utility, it is a utility tool that assists you to set up and maintain network devices in a more simple and efficient way. You can download the ZON Utility at *www.zyxel.com* and install it on a PC (Windows operation system). For more information on ZON Utility see Section 4.3 on page 54.

The following table shows which firmware version supports ZON and Neighbor Management (Smart Connect) for each Switch. The firmware on each Switch is identified by the firmware trunk version, followed by a unique model code and release number in brackets. For example, 4.80(ABMK.0) is a firmware version for GS1920-48HPv2 where 4.80 is the firmware trunk version, ABMK identifies the GS1920-48HPv2 and .0 is the first release of trunk version 4.80.

Table 3 Models and Firmware Version

SWITCH MODEL	FIRMWARE VERSION
GS1920-8HPv2	4.80(ABKZ.0) and later
GS1920-24v2	4.80(ABMH.0) and later
GS1920-24HPv2	4.80(ABMI.0) and later
GS1920-48v2	4.80(ABMJ.0) and later
GS1920-48HPv2	4.80(ABMK.0) and later

1.4.3 PoE

The Switch is a Power Sourcing Equipment (PSE) because it provides a source of power through its Ethernet ports. Each device that receives power through an Ethernet port is a Powered Device (PD).

The Switch can adjust the power supplied to each PD according to the PoE standard the PD supports. PoE standards are:

- IEEE 802.3af Power over Ethernet (PoE)
- IEEE 802.3at Power over Ethernet (PoE) +

The following table describes the PoE features of the Switch by PoE standard.

The GS1920-8HPv2, GS1920-24HPv2, and GS1920-48HPv2 come with a Power-over-Ethernet (PoE)

Table 4 PoE Standards

PoE FEATURES	PoE	PoE+
IEEE Standard	IEEE 802.3af	IEEE 802.3at
PoE Type	Type 1	Type 2
Switch Port Power		
Maximum Power Per Port	15.4 W	30 W
Port Voltage Range	44 – 57 V	50 – 57 V
Cables		
Twisted Pairs Used	2-pair	2-pair
Supported Cables	Cat3 or better	Cat5 or better

feature. The GS1920-8HPv2, GS1920-24HPv2, and GS1920-48HPv2 support the IEEE 802.3at High Power over Ethernet (PoE) standard and IEEE 802.3af PoE standard.

Key feature differences between Switch models are as follows. Other features are common to all models.

The following table describes the PoE features of the Switch by model.

Table 5 Models and PoE Features

SWITCH MODEL	POE FEATURES
GS1920-8HPv2	IEEE 802.3af PoE
GS1920-24HPv2	IEEE 802.3at High Power over Ethernet (PoE)
GS1920-48HPv2	Power management mode – Classification
	Power management mode – Consumption
	Scheduled PoE (PoE Time Range)

1.5 Good Habits for Managing the Switch

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

- Change the Web Configurator login 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

2.1 Installation Scenarios

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

The Switch can be:

- Placed on a desktop.
- Desk-mounted under a table.
- Wall-mounted on a wall.
- Rack-mounted on a standard EIA rack.

2.2 Safety Precautions

Please observe the following before using the Switch:

- It is recommended to ask an authorized technician to attach the Switch on a desk or to the rack or wall. Use the proper screws to prevent damage to the Switch. See the **Installation Requirements** sections in this chapter to know the types of screws and screwdrivers for each mounting method.
- Make sure there is at least 2 cm of clearance on the top and bottom of the Switch, and at least 5 cm of clearance on all four sides of the Switch. This allows air circulation for cooling.
- Do NOT block the ventilation holes nor store cables or power cords on the Switch. Allow clearance for the ventilation holes to prevent your Switch from overheating. This is especially crucial when your Switch does not have fans. Overheating could affect the performance of your Switch, or even damage it.
- The surface of the Switch could be hot when it is functioning. Do NOT put your hands on it. You may get burned. This could happen especially when you are using a fanless Switch.
- The Switches with fans are not suitable for use in locations where children are likely to be present.

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

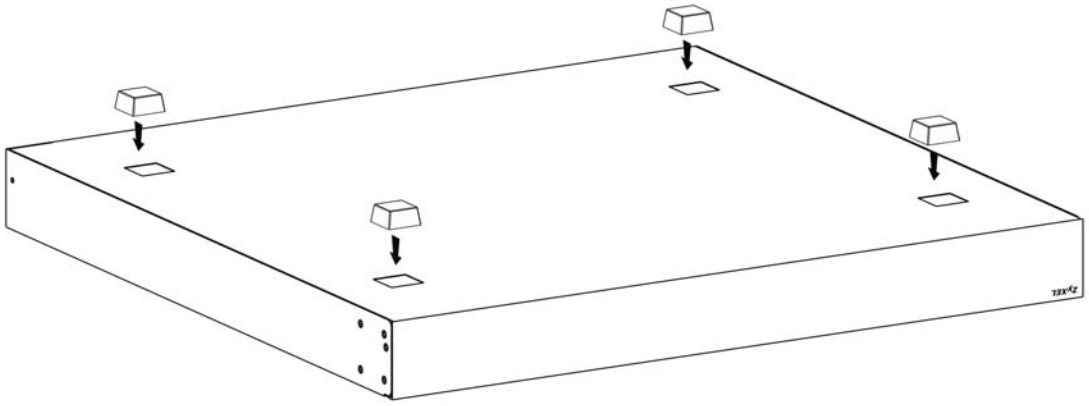
2.3 Freestanding Installation Procedure

1 Make sure the Switch is clean and dry.

2 Remove the adhesive backing from the rubber feet.

3 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 8 Attaching Rubber Feet



4 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.

Cautions:

- Avoid stacking fanless Switches to prevent overheating.
- Ensure enough clearance around the Switch to allow air circulation for cooling.
- Do NOT remove the rubber feet as it provides space for air circulation.

2.4 Desk Mounting (GS1920-8HPv2 Only)

The GS1920-8HPv2 can be mounted under a table. Follow the steps below to mount your Switch under a table.

2.4.1 Installation Requirements

- Two mounting brackets
- Eight M3 flat head screws and a #2 Philips screwdriver
- Four M4 flat head screws and a #2 Philips screwdriver
- Four washers (inside diameter: 3.5 mm; outside diameter: 11.5 mm)

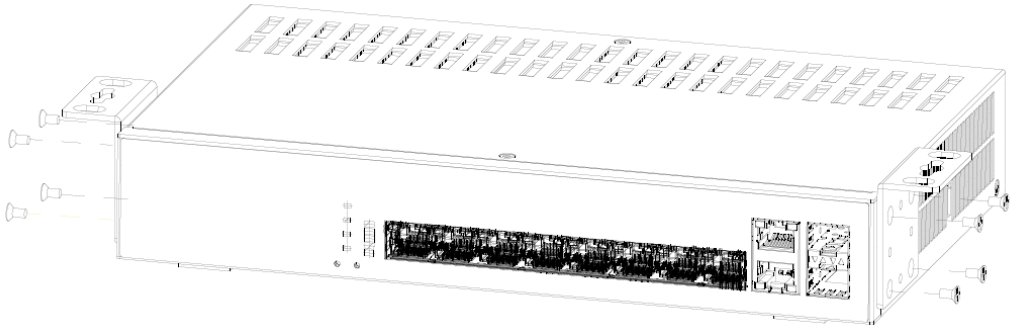
2.4.2 Precautions

- Make sure to place the Switch horizontally under a smooth level surface.
- Make sure the table is sturdy enough for desk mounting.
- Make sure there is enough table thickness to drill screws.
- Make sure there is sufficient space for port connections.

2.4.3 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 9 Attaching the Mounting Brackets



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 under a table. Proceed to the next section.

2.4.4 Mounting the Switch under a Table

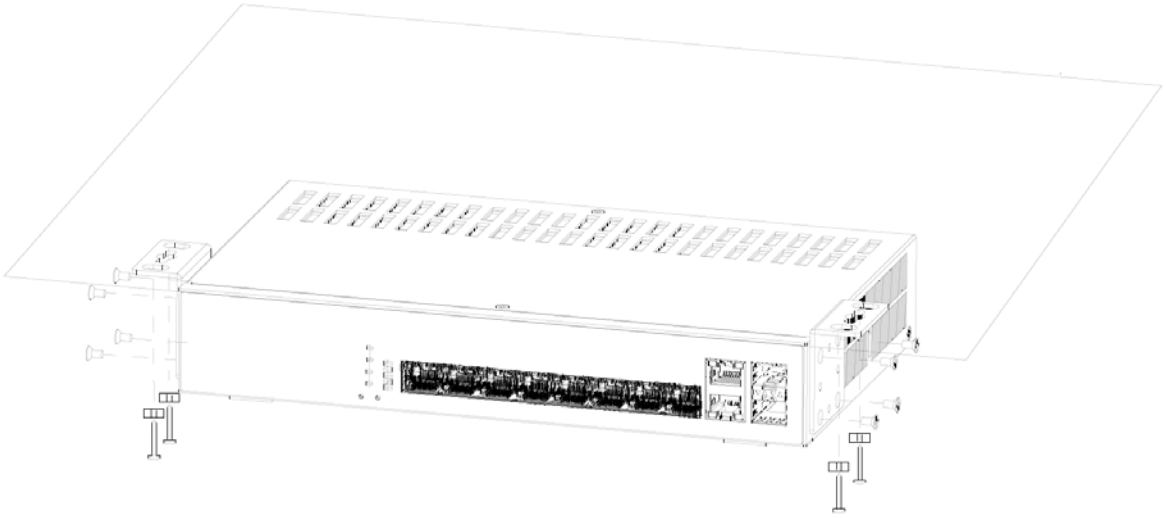
1 Determine where you want to mount the Switch under a table. See Section 2.4 on page 33 to choose a suitable location.

2 Position the Switch in place and mark the places for drilling with the attached brackets.

3 Drill holes at the marked places under the table.

4 Line up the two screw holes on the bracket with the screw holes under the table.

Figure 10 Mounting the Switch under a Table



5 Place the washers on the screw holes of the bracket.

6 Using a #2 Philips screwdriver, install the M4 flat head screws through the washers and mounting bracket holes into the table. The washers should be in between the M4 flat head screws and the brackets.

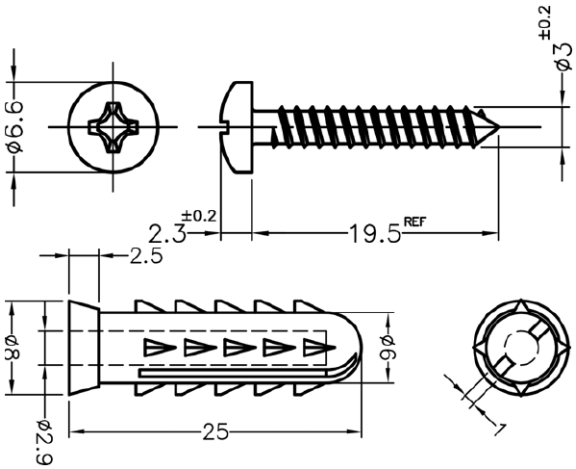
7 Repeat steps 1 and 6 to attach the second mounting bracket under the table.

2.5 Wall Mount (GS1920-8HPv2 Only)

The Switch can be mounted on a wall. You may need screw anchors if mounting on a concrete or brick wall.

2.5.1 Installation Requirements

- Distance above the floor: At least 1.8 m (5.9 feet)
- Distance between holes: 78 mm (3.071 inches)
- Two M4 screws and a #2 Philips screwdriver
- Two screw anchors (optional)



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.

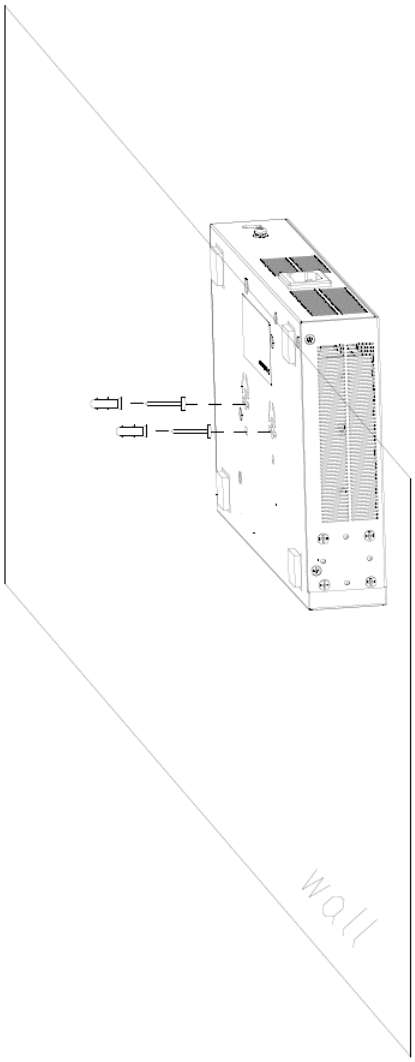
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do NOT insert the screws all the way in – leave a small gap of about 0.5 cm.

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 of about 0.5 cm.

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

5 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.



WARNING! The Switch should be wall-mounted horizontally, and make sure the front panel is facing down. The Switch's side panels with ventilation slots should not be facing up or down as this position is less safe.

2.6 Mount the Switch on a Rack

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.

2.6.1 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.

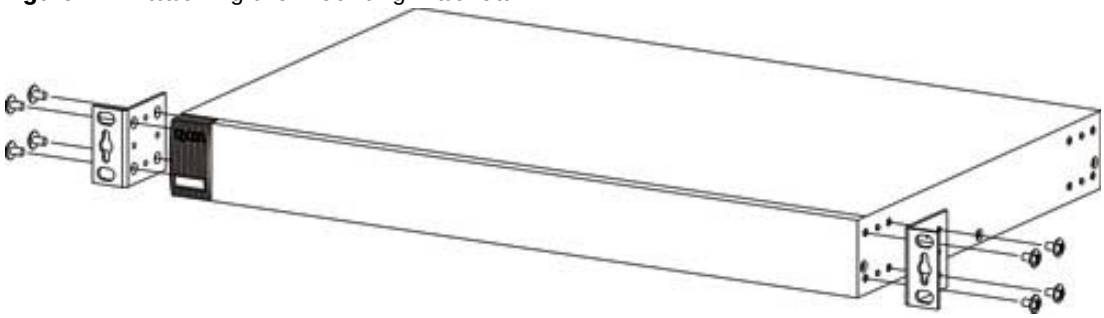
2.6.2 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains. The maximum weight a bracket can hold is 21.5 kg.
- 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.

2.6.3 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 11 Attaching the Mounting Brackets



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

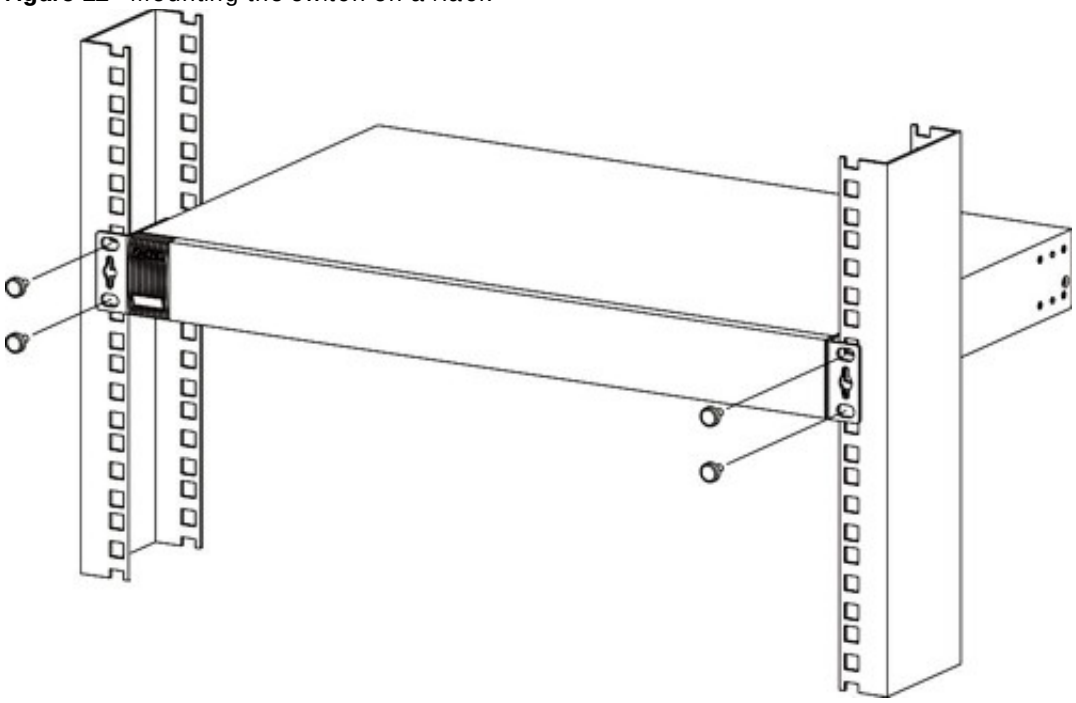
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

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

2.6.4 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 12 Mounting the Switch on a Rack



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 Panels

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

3.1 Switch Hardware Features

The following table describes the hardware features of the Switch by model.

Table 6 GS1920v2 Series Comparison Table

FEATURE	GS1920-8HPV2	GS1920-24V2	GS1920-24HPV2	GS1920-48V2	GS1920-48HPV2
10/100/1000 Mbps Ethernet Ports	No	24	No	44	No
10/100/1000 Mbps PoE Ports	8	No	24	No	48
GbE Dual Personality Interface	2	4	4	4	4
1 Gbps SFP Interface	No	No	No	2	2
FAN	No	No	2	1	2
Wall-mount	Yes	No	No	No	No
Rack-mount	No	Yes	Yes	Yes	Yes
Desk-mount	Yes	No	No	No	No

3.2 Front Panel Connections

Note that the front panels of the Switch do not state the v2 model names.

Figure 13 Front Panel: GS1920-8HPv2

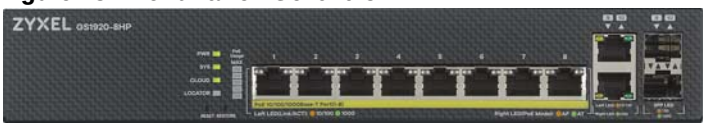


Figure 14 Front Panel: GS1920-24v2

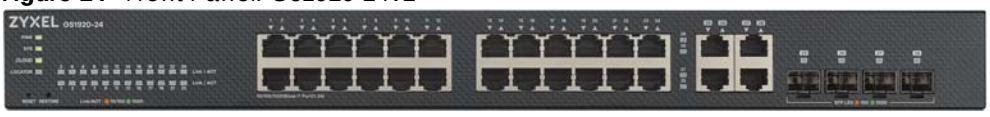


Figure 15 Front Panel: GS1920-24HPv2

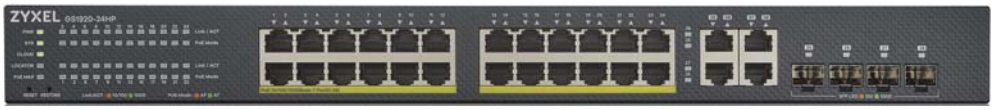


Figure 16 Front Panel: GS1920-48v2

Figure 17 Front Panel: GS1920-48HPv2

3.2.1 Gigabit Ethernet Ports

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

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.

Two/Four 1000Base-T Ethernet ports are paired with an SFP slot to create a dual personality interface. The Switch uses up to one connection for each SFP and 1000Base-T Ethernet pair. The SFP slots have priority over the Gigabit ports. This means that if an SFP slot and the corresponding GbE port are connected at the same time, the GbE port will be disabled.

Note: The combo ports (dual personality interfaces) change to fiber optic mode directly when inserting the fiber module.

When auto-negotiation is turned on, an Ethernet port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thereby requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

3.2.1.1 Default Ethernet Negotiation Settings

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

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

3.2.1.2 Auto-crossover

All ports support auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches or hubs.

3.2.2 PoE (GS1920-8HPv2, GS1920-24HPv2, and GS1920-48HPv2)

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

3.2.3 SFP Slots

These are slots for SFP (Small Form-Factor Pluggable) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. 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 or even copper cable connectors.

- Type: SFP connection interface
- Connection speed: 100/1000 Mbps

WARNING! To avoid possible eye injury, do not look into an operating fiber optic module's connectors.
HANDLING! All transceivers are static sensitive. To prevent damage from electrostatic discharge (ESD), it is recommended you attach an ESD preventive wrist strap to your wrist and to a bare metal surface when you install or remove a transceiver.
STORAGE! All modules are dust sensitive. When not in use, always keep the dust plug on. Avoid getting dust and other contaminant into the optical bores, as the optics do not work correctly when obstructed with dust.

3.2.3.1 Transceiver Installation

Use the following steps to install a transceiver.

1. Attach an ESD preventive wrist strap to your wrist and to a bare metal surface.
2. Align the transceiver in front of the slot opening.
3. Make sure the latch is in the lock position (latch styles vary), then insert the transceiver into the slot with the exposed section of PCB board facing down.
4. Press the transceiver firmly until it clicks into place.

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

6 Remove the dust plugs from the transceiver and cables (dust plug styles vary).

7 Identify the signal transmission direction of the fiber optic cables and the transceiver. Insert the fiber optic cable into the transceiver.

Figure 18 Latch in the Lock Position

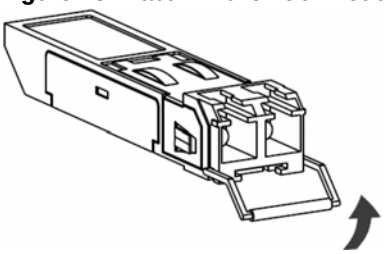


Figure 19 Transceiver Installation Example

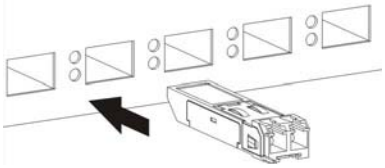
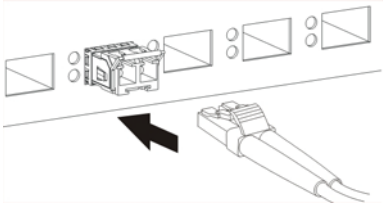


Figure 20 Connecting the Fiber Optic Cables



3.2.3.2 Transceiver Removal

Use the following steps to remove an SFP transceiver.

1 Attach an ESD preventive wrist strap to your wrist and to a bare metal surface on the chassis.

2 Remove the fiber optic cables from the transceiver.

3 Pull out the latch and down to unlock the transceiver (latch styles vary).

Note: Make sure the transceiver's latch is pushed all the way down, so the transceiver can be pulled out successfully.

4 Pull the latch, or use your thumb and index finger to grasp the tabs on both sides of the transceiver, and carefully slide it out of the slot.

Note: Do NOT pull the transceiver out by force. You could damage it. If the transceiver will not slide out, grasp the tabs on both sides of the transceiver with a slight up or down motion and carefully slide it out of the slot. If unsuccessful, contact Zyxel Support to prevent damage to your Switch and transceiver.

5 Insert the dust plug into the ports on the transceiver and the cables.

Figure 21 Removing the Fiber Optic Cables

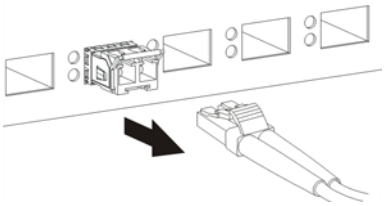


Figure 22 Opening the Transceiver's Latch Example

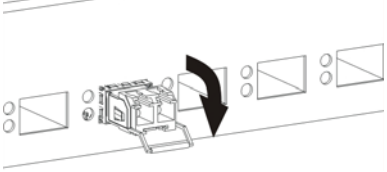
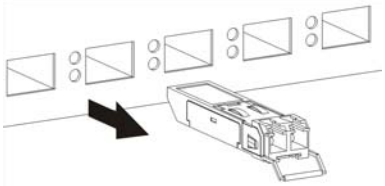


Figure 23 Transceiver Removal Example



3.3 Rear Panel

The following figures show the rear panel of the Switch. The rear panel contains:

Figure 24 Rear Panel: GS1920-8HPv2

Figure 25 Rear Panel: GS1920-24v2

Figure 26 Rear Panel: GS1920-24HPv2

Figure 27 Rear Panel: GS1920-48v2

Figure 28 Rear Panel: GS1920-48HPv2

3.3.1 Grounding

Grounding is a safety measure to direct excess electric charge to the ground. It prevents damage to the Switch, and protects you from electrocution. Use the grounding screw on the rear panel and the ground wire of the AC power supply to ground the Switch.

The grounding terminal and AC power ground where you install the Switch must follow your country's regulations. Qualified service personnel must ensure the building's protective earthing terminals are valid terminals.

Installation of Ethernet cables must be separate from AC power lines. To avoid electric surge and electromagnetic interference, use a different electrical conduit or raceway (tube/trough or enclosed conduit for protecting electric wiring) that is 15 cm apart, or as specified by your country's electrical regulations.

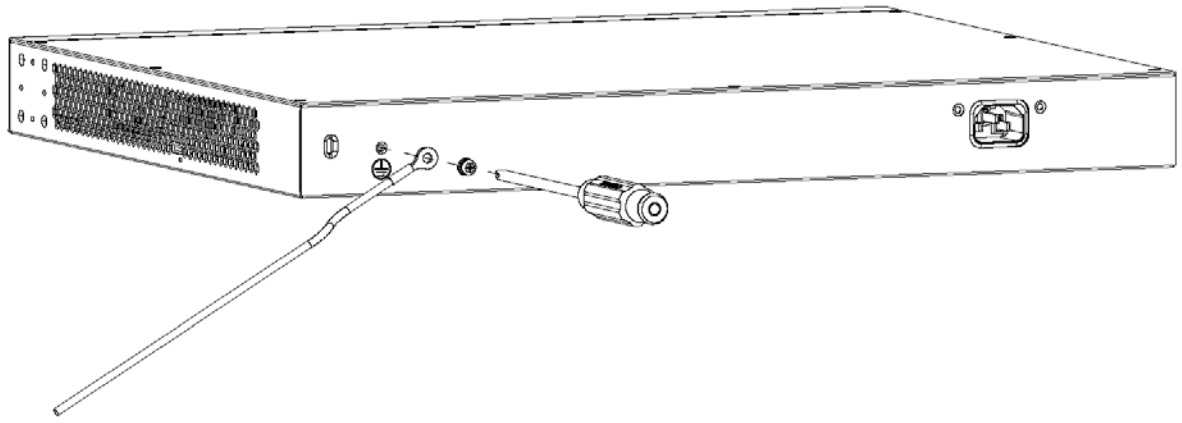
Any device that is located outdoors and connected to this product must be properly grounded and surge protected. To the extent permissible by your country's applicable law, failure to follow these guidelines could result in damage to your Switch which may not be covered by its warranty.

Note: The specification for surge or ESD protection assumes that the Switch is properly grounded.

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

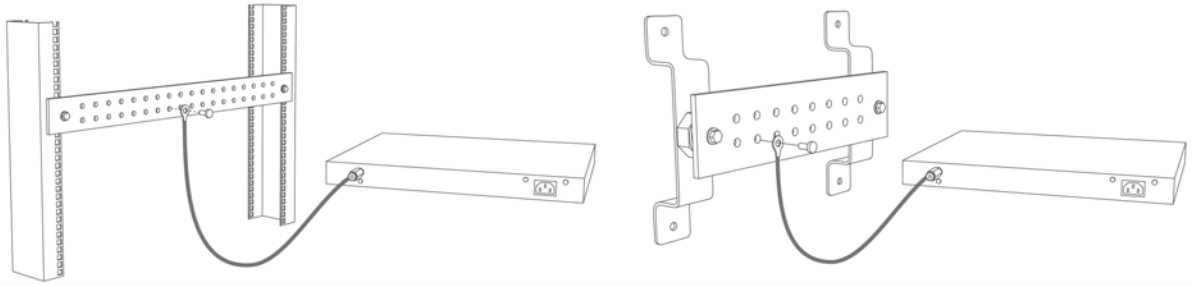
2 Secure a green or yellow ground cable (16 AWG or smaller) to the Switch's rear panel using the M4 ground screw.

Figure 29 Grounding



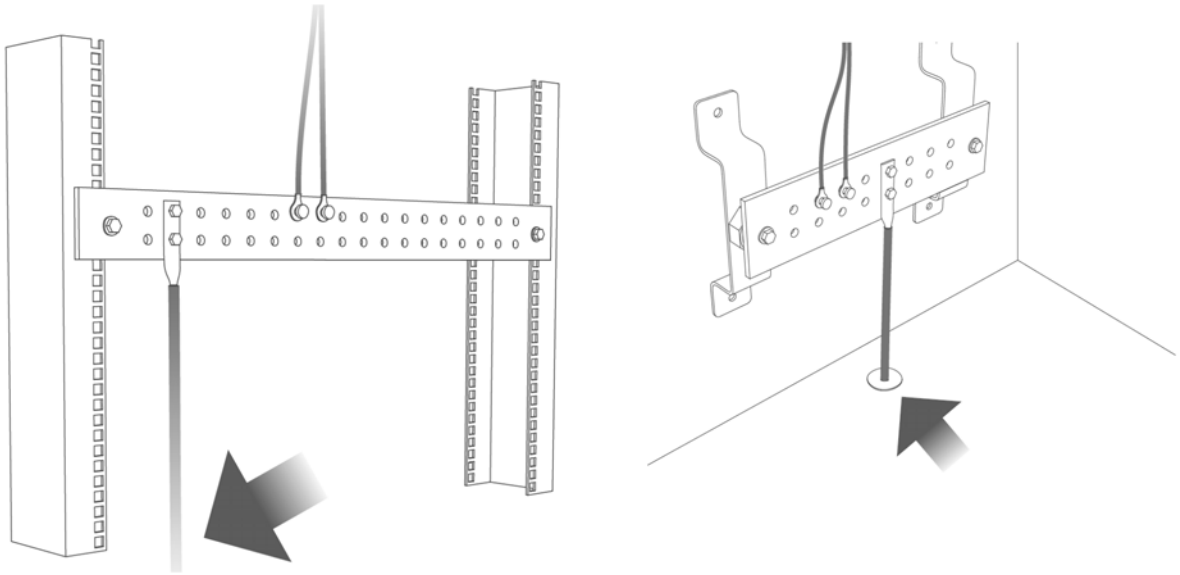
3 Attach the other end of the ground cable to a grounding bar located on the rack where you install the Switch or to an on-site grounding terminal.

Figure 30 Attach Ground Cable to Grounding Bar or On-site Grounding Terminal



4 The grounding terminal of the server rack or on-site grounding terminal must also be grounded and connected to the building's main grounding electrode. Make sure the grounding terminal is connected to the buildings grounding electrode and has an earth resistance of less than 10 ohms, or according to your country's electrical regulations.

Figure 31 Connecting to the Building's Main Grounding Electrode



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

This device must be grounded. Do this before you make other connections.

3.3.2 AC Power Connection

Note: Make sure you are using the correct power source as shown on the panel and that no objects obstruct the airflow of the fans.

To connect power to the Switch, insert the female end of the power cord to the AC power receptacle on the rear panel. Connect the other end of the supplied power cord to a power outlet.

3.3.3 Power Connection

Note: Make sure you are using the correct power source.

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.

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.

3.4 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 7 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Switch is receiving power from the power module in the power slot.
		Blinking	The Switch is returning to the last-saved custom default configuration settings.
	Amber	On	The Switch is returning to its factory default configuration settings.
		Off	The Switch is not receiving power from the power module in the power slot.
SYS	Green	On	The Switch is on and functioning properly.
		Blinking	The Switch is rebooting and performing self-diagnostic tests.
	Red	On	The Switch is functioning abnormally.
		Off	The power is off or the Switch is not ready or malfunctioning.

Table 7 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
CLOUD	Green	On	The Switch has successfully connected to the NCC (Nebula Control Center).
		Blinking	The Switch cannot connect to the NCC because it is not registered.
	Amber	On	The Switch is registered at NCC but cannot connect to the NCC. Please check the Internet connection of the Switch.
		Blinking	The Switch is not registered at NCC and cannot connect to the NCC. Please check the Internet connection of the Switch and register the Switch at NCC.
		Off	The Switch is operating in standalone mode. Nebula Control Center Discovery is disabled in **SYSTEM** > **Cloud Management** > **Nebula Control Center Discovery** in the Switch Web Configurator.
LOCATOR	Blue	On	The Switch is uploading firmware. While the Switch is doing this, do not turn off the power.
		Blinking	Shows the actual location of the Switch between several devices in a rack. The default timer is 30 minutes when you are configuring the Switch.
		Off	The locator is not functioning or malfunctioning.
PoE Usage MAX (GS1920-8HPv2) Bar1 is the bar at the bottom; bar 5 is the bar at the top.	Green (Bar1-Bar3)	On	Each bar represents 20 percent of PoE Power consumption. **Bar 1**: PoE power usage is below 20 percent of the power supplied budget. **Bar 2**: PoE power usage is below 40 percent of the power supplied budget, but over 20 percent of the power supplied budget. **Bar 3**: PoE power usage is below 60 percent of the power supplied budget, but over 40 percent of the power supplied budget.
	Yellow (Bar4)	On	PoE power usage is below 80 percent of the power supplied budget, but over 60 percent of the power supplied budget.
	Red (Bar5)	On	PoE power usage is more than 80 percent of the power supplied budget or exceeds the **PoE Usage Threshold (%)** configured in **PoE Setting**.
		Blinking	Less than 5 percent of the power supplied budget remains. 5 percent is the default value.
		Off	PoE power usage is 0 percent of the power supplied budget.
PoE MAX (GS1920-24HPv2 & GS1920-48HPv2)	Amber	On	Less than 5 percent of the power supplied budget remains. 5 percent is the default value.
		Off	The Switch has a sufficient power supplied budget.
Ethernet Ports and PoE			

Table 7 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
LNK/ACT 1 – 8 (GS1920-8HPv2) 1 – 24 (GS1920-24v2/24HPv2) and 1 – 48 (GS1920-48v2/48HPv2)	Green	Blinking	The Switch is transmitting or receiving to or from a 1000 Mbps Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The Switch is transmitting or receiving to or from a 10 Mbps or a 100 Mbps Ethernet network.
		On	The link to a 10 Mbps or a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
PoE 1 – 8 (GS1920-8HPv2) 1 – 24 (GS1920-24HPv2) 1 – 48 (GS1920-48HPv2)	Green	On	Power supplied to all PoE Ethernet ports meets the IEEE 802.3at standard.
	Amber	On	Power supplied to all PoE Ethernet ports meets the IEEE 802.3af standard.
		Off	There is no power supplied.
Dual Personality Interface			
Ethernet Ports 9 – 10 (GS1920-8HPv2) 25 – 28 (GS1920-24v2/24HPv2) 45 – 48 (GS1920-48v2/48HPv2)	Green	Blinking	The Switch is transmitting or receiving to or from a 1000 Mbps Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The Switch is transmitting or receiving to or from a 10 Mbps or a 100 Mbps Ethernet network.
		On	The link to a 10 Mbps or a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
SFP Slots 9 – 10 (GS1920-8HPv2) 25 – 28 (GS1920-24v2/24HPv2) 45 – 48 (GS1920-48v2/48HPv2)	Green	On	The uplink port is linking at 1000 Mbps.
		Blinking	The Switch is transmitting or receiving data 1000 Mbps.
	Amber	On	The uplink port is linking at 100 Mbps.
		Blinking	The Switch is transmitting or receiving data 100 Mbps.
		Off	There is no link or port, the uplink port is shut down.
SFP Slots			
49 – 50 (GS1920-48v2/48HPv2)	Green	On	The uplink port is linking at 1000 Mbps.
		Blinking	The Switch is transmitting or receiving data 1000 Mbps.
	Amber	On	The uplink port is linking at 100 Mbps.
		Blinking	The Switch is transmitting or receiving data 100 Mbps.
		Off	There is no link or port, the uplink port is shut down.

PART II
Technical Reference

CHAPTER 4
Web Configurator

4.1 Overview

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

The Web Configurator is an HTML-based management interface that allows easy system setup and management through a web browser. Use a web browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows on your computer.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: In Cloud mode, the settings you configure in the Web Configurator will apply to the Switch but will not appear in the Nebula settings. The settings you configure in Nebula will overwrite the Web Configurator settings. It is the latest settings that will apply to the Switch.

Note: To avoid inconsistency, we recommend you use Nebula to configure the Switch and only use the Web Configurator for troubleshooting.

4.2 System Login

1 Start your web browser.

2 The Switch is a DHCP client by default. Type "https://DHCP-assigned IP" in the **Location** or **Address** field. Press [ENTER].

Note: You can always use the domain name "setup.zyxel" to access the Web Configurator whether the Switch is using a DHCP-assigned IP or static IP address. This requires your computer to be directly connected to the Switch. Make sure your computer can connect to a DNS server through the Switch.

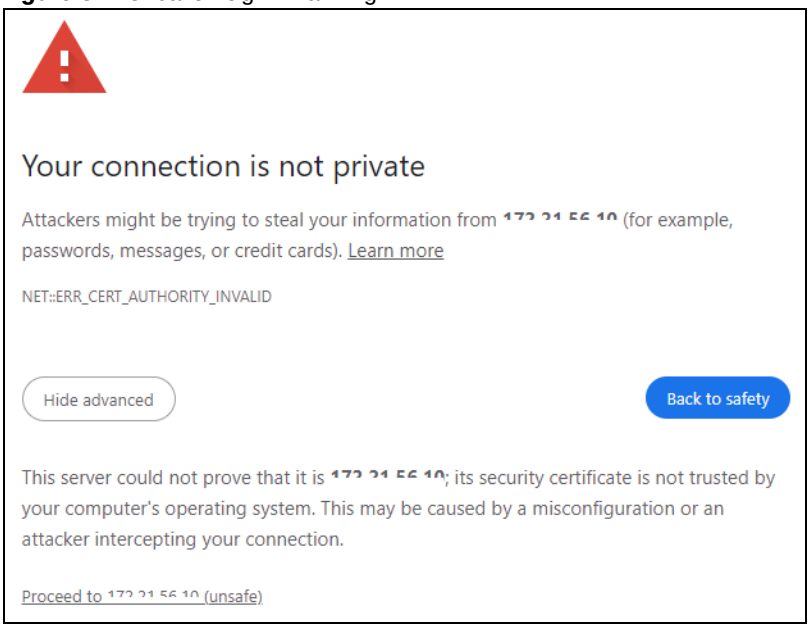
If the Switch is not connected to a DHCP server, type "http://" and the static IP address of the Switch (for example, the default management IP address is 192.168.1.1) in the **Location** or **Address** field. Press [ENTER]. Your computer must be in the same subnet in order to access this website address.

Also, you can use the ZON Utility to check your Switch's IP address. See Section 4.3 on page 54 for more information on the ZON utility.

3 If a "Your connection is not private" screen appears, click **Advanced** and **Proceed to DHCP-assigned IP (unsafe)** to go to the **Login** screen. This screen appears as the Zyxel Device uses a certificate for the HTTPS connection. See Section 66.2 on page 429 for information on using an HTTPS certificate verified by a third party to create secure HTTPS connections between your computer and the Switch.

Note: If you see this warning page, it indicates that your browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to the login IP address.

Figure 32 Unsafe Login Warning



The **Login** screen appears.

Figure 33 Web Configurator: Login (Standalone mode)

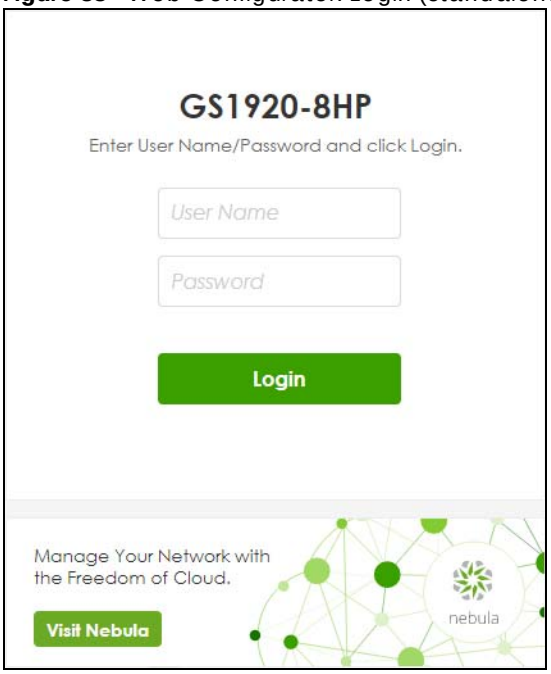
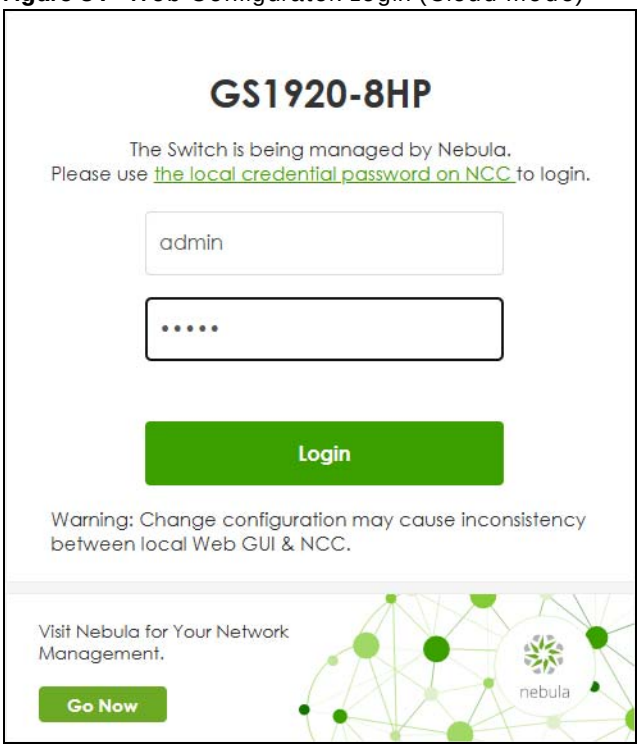


Figure 34 Web Configurator: Login (Cloud mode)



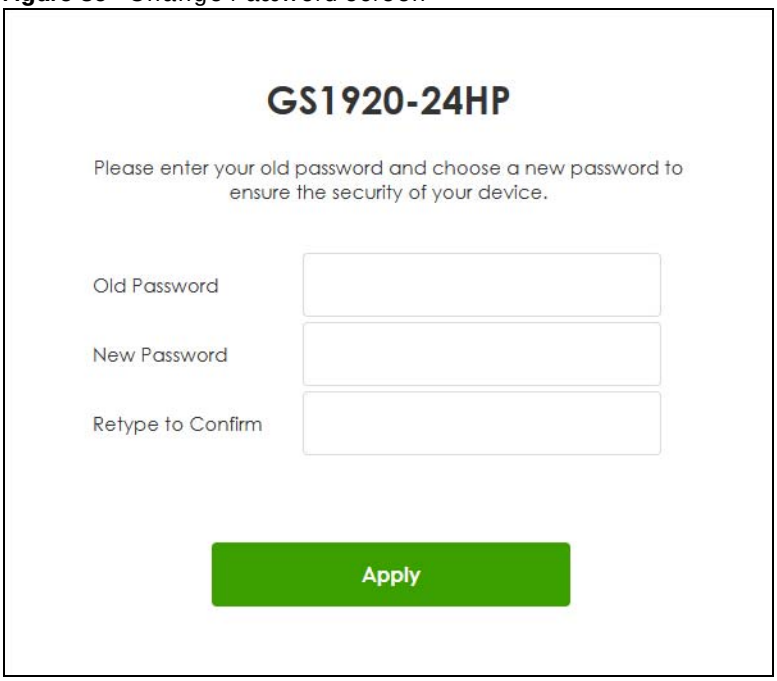
4 In Standalone mode, click the **Visit Nebula** button if you want to open the Zyxel Nebula Control Center (NCC) login page in a new tab or window. In Cloud mode, click the **Go Now** button. The NCC is a cloud-based network management system that allows you to remotely manage and monitor the Switch. See Section 1.4.1 on page 27 for information on changing your Switch to Nebula Cloud management.

Figure 35 Visit Nebula

5 Alternatively, click **Login** to log into the Web Configurator to manage the Switch directly.
In Standalone mode, the default user name is **admin** and associated default password is **1234**.
In Cloud mode, use the **Local credentials: password** to login. The **Local credentials: Password** can be found in **Site-wide** > **Configure** > **Site settings** > **Device configuration** in the NCC portal. See the NCC User's Guide for more information.

In Standalone mode, the change password screen appears the first time you log in using the default password.

Figure 36 Change Password Screen



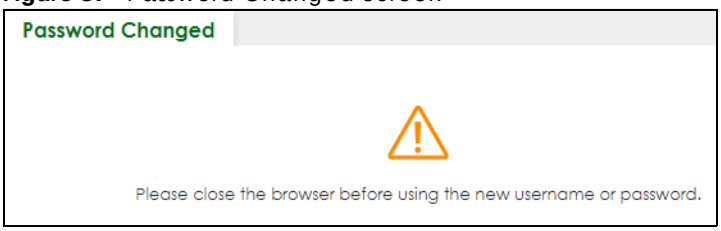
Note: The new password rules are:

4 to 32 characters in length

[?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed

6 After setting the new password, close and restart your web browser. Enter the 'https://DHCP-assigned IP' in the URL field and press [ENTER]. When the login screen appears, enter the user name (default: 'admin') and new password.

Figure 37 Password Changed Screen



4.3 Zyxel One Network (ZON) Utility

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 through 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 *https://www.zyxel.com/global/en/form/zon-utility-download* and unzip it first before installing it in a computer (Windows operating system).

4.3.1 Requirements

Before installing the ZON Utility in your computer, 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)
- Windows 10 (both 32-bit / 64-bit versions)
- Windows 11 (64-bit version)

Hardware

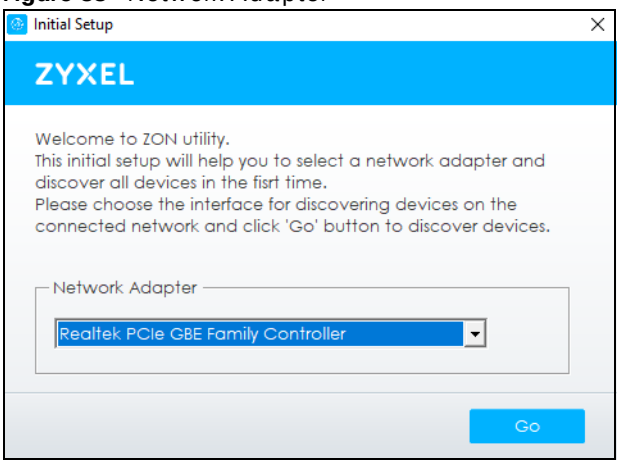
Here are the minimum hardware requirements to use the ZON Utility on your computer.

- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280 by 800)

4.3.2 Run the ZON Utility

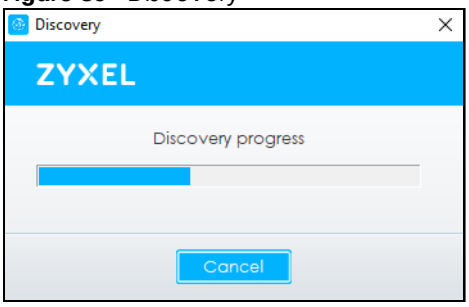
1. Double-click the ZON Utility to run it.
2. Select a network adapter to which your supported devices are connected.

Figure 38 Network Adapter



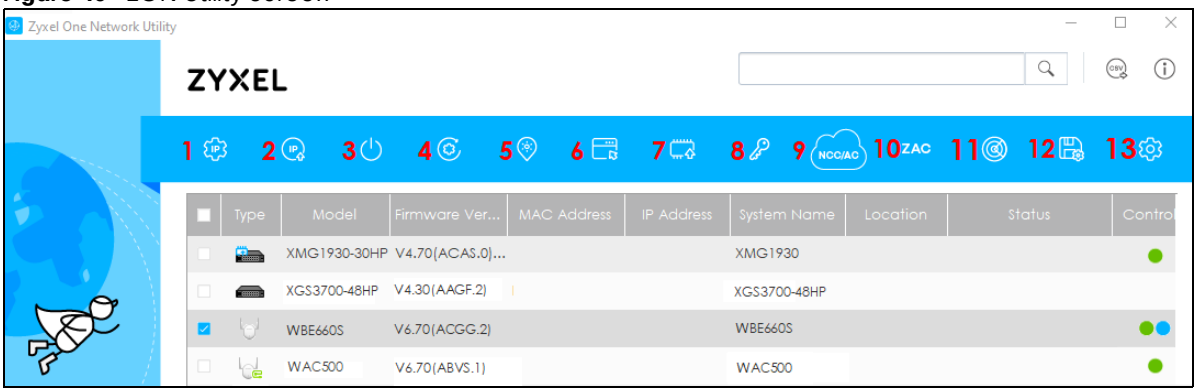
3 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 39 Discovery



4 The ZON Utility screen shows the devices discovered.

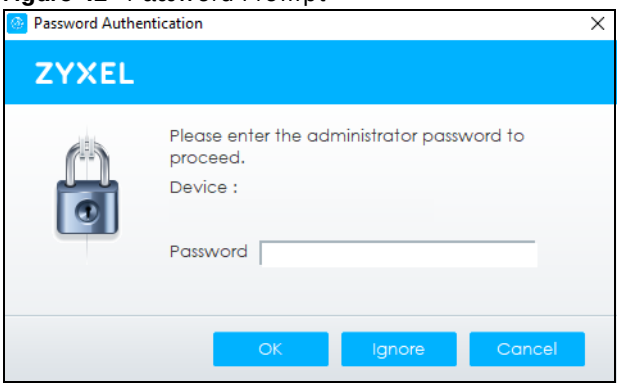
Figure 40 ZON Utility Screen



5 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 41 Password Prompt



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

Table 8 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 devices. This may be useful when troubleshooting or upgrading new firmware.
4 Reset Configuration to Default	Use this icon to reload the factory-default configuration file. This means that you will lose all previous configurations.
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 user name and password to log in.
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected devices of the same model. 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 is 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 will 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 9 ZON Utility Fields

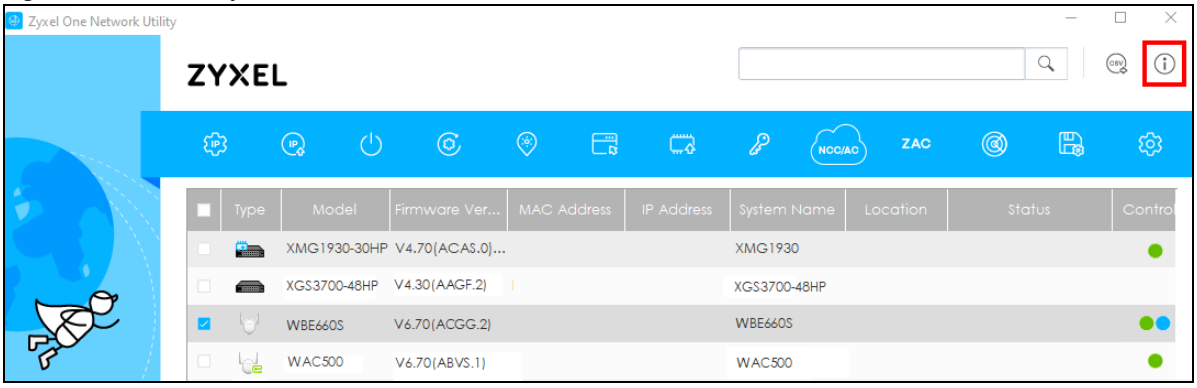
LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.

Table 9 ZON Utility Fields (continued)

LABEL	DESCRIPTION
IP Address	This field displays the IP address of an internal interface on the discovered device that first received a 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 **Flash Locator LED**, this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively.
Controller Discovery	This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature. If it is 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 will 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.
IPv6 Address	This field displays the IPv6 address on the discovered device that first received a ZDP discovery request from the ZON Utility.

If you want to check the supported models and firmware versions, you can click the **Show information about ZON** icon in the upper right 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 42 ZON Utility Screen



4.4 Web Configurator Layout

The **DASHBOARD** screen is the first screen that displays when you access the Web Configurator.

This guide uses the GS1920-8HP and GS1920-24HP screens as examples. The screens may vary slightly for different models.

The following figure shows the navigating components of a Web Configurator screen.

Figure 43 Web Configurator Layout (Standalone mode)

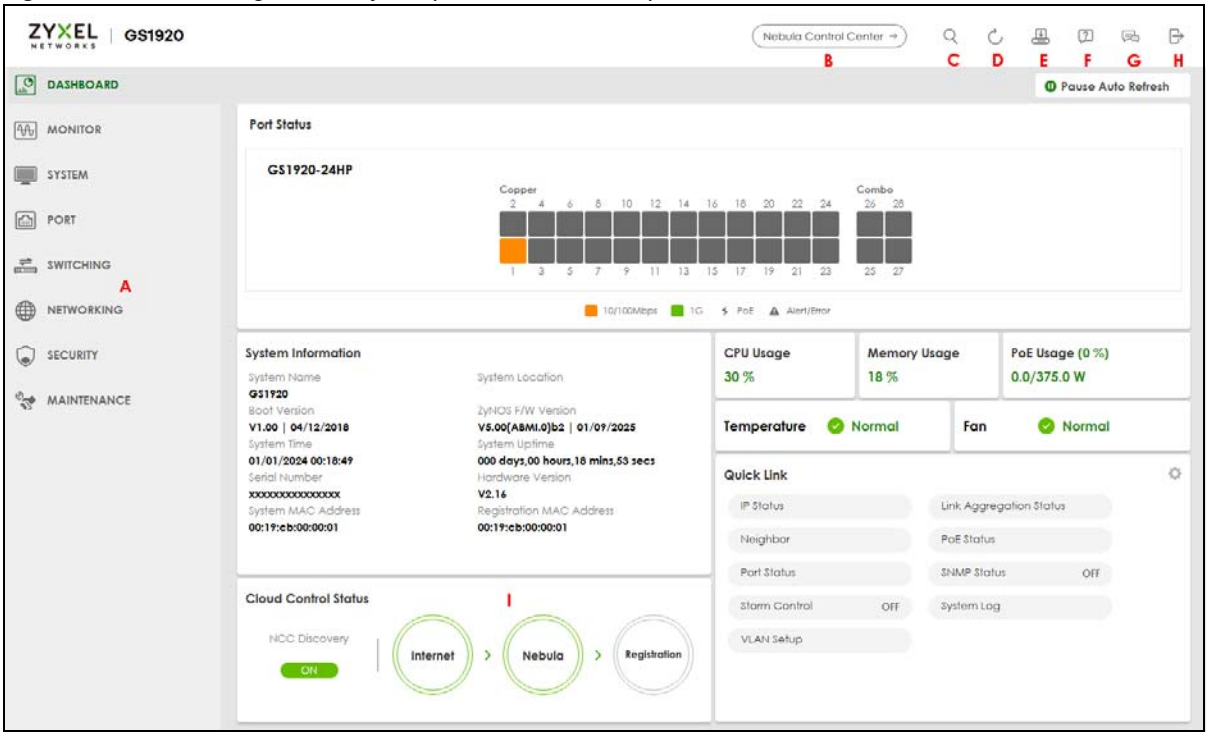
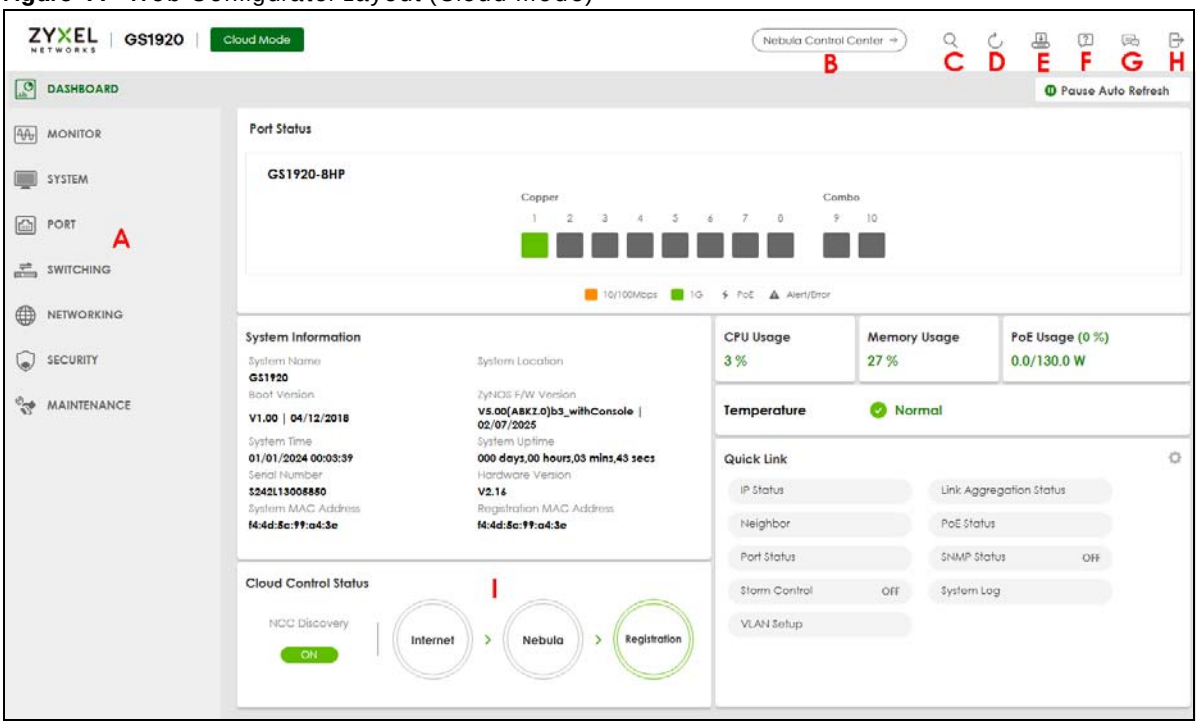


Figure 44 Web Configurator Layout (Cloud mode)



A – Click the menu items to open sub-menu links, and then click on a sub-menu link to open the screen in the main window.

B, **C**, **D**, **E**, **F**, **G, H** – These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B – Click this icon to go to the NCC (Nebula Control Center) portal website.

C – Click this icon to search for specific configurations or status you are looking for. Enter the keywords and click the result link. This will direct you to the specific configuration or status page.

D – Click this icon to update the information in the screen you are currently viewing.

E – Click this icon to save your configuration into the Switch's non-volatile memory. Non-volatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

F – Click this icon to display web help pages. The help pages provide descriptions for all of the configuration screens.

G – Click this icon to go to the Zyxel Community Biz Forum.

H – Click this icon to log out of the Web Configurator.

I – This displays the Nebula Cloud Control Status. The ON/OFF switch displays if **NCC Discovery** is enabled. If a status circle turns Orange, it means the Switch is unable to connect to NCC. Hover the mouse over the status circle to check the diagnostic message. You can also click the ON/OFF switch to go to the **SYSTEM** > **Cloud Management** > **Cloud Management** screen and check the diagnostic messages. See Table 26 on page 116 for more information.

In the navigation panel, click a main link to reveal a list of sub-menu links.

The following table describes the links in the navigation panel. The navigation panel varies depending on the product model you use.

Table 10 Navigation Panel Links

LINK	DESCRIPTION
DASHBOARD	This link takes you to the main dashboard screen that displays general system and device information.
MONITOR	
ARP Table	This link takes you to a screen that displays the current ARP table of the Switch. You can view the IP and MAC address mapping, VLAN ID, ARP aging time, and ARP entry type of a device attached to a port.
IPv6 Neighbor Table	This link takes you to a screen where you can view the Switch's IPv6 neighbor table.
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.
Neighbor	This link takes you to a screen where you can view neighbor devices (including non-Zyxel devices) connected to the Switch.
Path MTU Table	This link takes you to a screen where you can view the IPv6 path MTU information on the Switch.
Port Status	This link takes you to a screen where you can view the port statistics.
System Information	This link takes you to a screen that displays general system information.
System Log	This link takes you to a screen where you can view the system log including fail log and system status.
SYSTEM	

Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
Cloud Management	This link takes you to a screen where you can enable or disable the **Nebula Control Center (NCC) Discovery** feature and view the NCC connection status. If **Nebula Control Center (NCC) Discovery** is enabled, you can have the Switch search for the NCC (Nebula Control Center). The screen also displays a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Interface Setup	This link takes you to a screen where you can configure settings for individual interface type and ID.
IP Setup	This link takes you to a screen where you can configure the DHCP client, and a static IP address (IP address and subnet mask).
IPv6	Click the link to unfold the following sub-link menu.
IPv6 Status	This link takes you to a screen where you can view the IPv6 table and DNS server.
IPv6 Global Setup	This link takes you to a screen where you can configure the global IPv6 settings.
IPv6 Interface Setup	This link takes you to a screen where you can view and configure IPv6 interfaces.
IPv6 Addressing	This link takes you to a screen where you can view and configure IPv6 link-local and global addresses.
IPv6 Neighbor Discovery	This link takes you to a screen where you can view and configure neighbor discovery settings on each interface.
IPv6 Neighbor Setup	configure static IPv6 neighbor entries in the Switch's IPv6 neighbor table.
DHCPv6 Client Setup	This link takes you to a screen where you can configure the Switch's DHCP settings when it is acting as a DHCPv6 client.
Logins	This link takes you to a screen where you can change the system login password, as well as configure up to four login details.
SNMP	This link takes you to screens where you can specify the SNMP version and community (password) values, configure where to send SNMP traps from the Switch, enable loopguard/errdisable/poe/linkup/linkdown/lldp/transceiver-ddm/storm-control on the Switch, specify the types of SNMP traps that should be sent to each SNMP manager, and add/edit user information.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type.
Syslog Setup	This link takes you to a screen where you can configure the Switch's system logging settings and configure a list of external syslog servers.
Time Range	This link takes you to a screen where you can configure time range for time-oriented features like Classifier.
PORT	
Green Ethernet	This link takes you to a screen where you can configure the Switch to reduce port power consumption.
Link Aggregation	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
LLDP	Click the link to unfold the following sub-link menu.
LLDP	This link takes you to screens where you can view LLDP information and configure LLDP and TLV settings.
LLDP MED	This link takes you to screens where you can configure LLDP-MED parameters.
OAM	This link takes you to screens where you can enable Ethernet OAM on the Switch, view the configuration of ports on which Ethernet OAM is enabled and perform remote-loopback tests.

Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
PoE Setup	For PoE models. This link takes you to a screen where you can set priorities, PoE power-up settings and schedule so that the Switch is able to reserve and allocate power to certain PDs.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.
SWITCHING	
Layer 2 Protocol Tunneling	This link takes you to a screen where you can configure L2PT (Layer 2 Protocol Tunneling) settings on the Switch.
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.
Mirroring	Click the link to unfold the following sub-link menu.
Mirroring	This link take you to a screen where you can copy traffic from one port or ports to another port in order to examine the traffic from the first port without interference.
Multicast	Click the link to unfold the following sub-link menu.
IPv4 Multicast	This link takes you to screens where you can configure various IPv4 multicast features, IGMP snooping, filtering and create multicast VLANs.
IPv6 Multicast	This link takes you to screen where you can configure various IPv6 multicast features, MLD snooping-proxy, filtering and create multicast VLANs.
MVR	This link takes you to screens where you can create multicast VLANs and select the receiver ports and a source port for each multicast VLAN.
Static Multicast Forwarding By MAC	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
PPPoE Intermediate Agent	This link takes you to screens where you can enable PPPoE (Point-to-Point Protocol over Ethernet) Intermediate Agent and configure per-port, per-port-per-VLAN settings.
QoS	Click the link to unfold the following sub-link menu.
Diffserv	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
Queuing Method	This link takes you to a screen where you can set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.
Priority Queue	This link takes you to a screen where you can set priority tags for different traffic types and specify the priority levels.
Bandwidth Control	This link takes you to a screen where you can cap the maximum bandwidth allowed on a port.
Spanning Tree Protocol	Click the link to unfold the following sub-link menu.
Spanning Tree Protocol Status	This link takes you to a screen where you can view the STP status in the different STP modes (RSTP, MRSTP or MSTP) you can configure on the Switch.
Spanning Tree Setup	This link takes you to a screen where you can activate one of the STP modes (RSTP, MRSTP or MSTP) on the Switch.
RSTP	This link takes you to a screen where you can configure the RSTP (Rapid Spanning Tree Protocol) settings on the Switch.
MRSTP	This link takes you to a screen where you can configure the MRSTP (Multiple Rapid Spanning Tree Protocol) settings on the Switch.
MSTP	This link takes you to a screen where you can configure the MSTP (Multiple Spanning Tree Protocol) settings on the Switch.
Static MAC Filtering	This link takes you to a screen to set up static MAC filtering rules.

Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
VLAN	Click the link to unfold the following sub-link menu.
VLAN Status	This link takes you to a screen where you can view and search all VLAN groups.
VLAN Setup	This link takes you to screens where you can: • configure port-based or 802.1Q VLAN. • view detailed port settings and status of the VLAN group. • configure and view 802.1Q VLAN parameters for the Switch. • configure the static VLAN settings on a port.
Subnet Based VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
Protocol Based VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
Voice VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group voice traffic with defined priority and enable the Switch port to carry the voice traffic separately from data traffic to ensure the sound quality does NOT deteriorate.
MAC Based VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. This eliminates the need to reconfigure the Switch when you change ports. The Switch will forward the packets based on the source MAC address you set up previously.
Vendor ID Based VLAN Setup	This link takes you to screens where you can set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. You can specify a mask for the MAC address to create a MAC address filter and enter a weight to set the VLAN rule's priority.
VLAN Isolation	This link takes you to a screen where you can block traffic between ports in a VLAN on the Switch.
NETWORKING	
ARP Setup	Click the link to unfold the following sub-link menu.
ARP Learning	This link takes you to a screen where you can configure ARP learning mode on a per-port basis.
DHCP	Click the link to unfold the following sub-link menu.
DHCPv4 Relay	This link takes you to screens where you can view DHCPv4 relay status, mode, and configure DHCPv4 relay settings.
DHCPv6 Relay	This link takes you to a screen where you can enable and configure DHCPv6 relay.
Static Routing	Click the link to unfold the following sub-link menu.
IPv4 Static Route	This link takes you to a screen where you can configure IPv4 static routes. A static route defines how the Switch should forward traffic by destination IP address and subnet mask.
SECURITY	
AAA	Click the link to unfold the following sub-link menu.
RADIUS Server Setup	This link takes you to a screen where you can configure your RADIUS (Remote Authentication Dial-In User Service) server settings for authentication.
TACACS+ Server Setup	This link takes you to a screen where you can configure your TACACS+ (Terminal Access Controller Access Control System Plus) server settings for authentication.
AAA Setup	This link takes you to a screen where you can configure authentication, authorization and accounting services through external servers. The external servers can be either RADIUS or TACACS+ (Terminal Access Controller Access Control System Plus).

Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
Access Control	Click the link to unfold the following sub-link menu.
Service Access Control	This link takes you to a screen where you can decide what services you may use to access the Switch.
Remote Management	This link takes you to a screen where you can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Account Security	This link takes you to a screen where you can configure account security settings on the Switch.
ACL	Click the link to unfold the following sub-link menu.
Classifier	This link takes you to screens where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Storm Control	This link takes you to a screen to set up broadcast filters.
Errdisable	This link takes you to screens where you can view errdisable status and configure errdisable settings in CPU protection, errdisable detect, and errdisable recovery.
IPv4 Source Guard	Click the link to unfold the following sub-link menu.
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
DHCP Snooping	This link takes you to screens where you can view DHCP snooping database details and configure DHCP snooping settings on ports or VLANs. You can use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
ARP Inspection	This link takes you to screens where you can view ARP inspection status, and configure ARP inspection settings on ports or VLANs. You can use ARP inspection to filter unauthorized ARP packets on the network.
Port Authentication	Click the link to unfold the following sub-link menu. These links take you to screens where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating through the Switch.
802.1x	The link takes you to a screen where you can activate IEEE 802.1x security on a port.
MAC Authentication	The link takes you to a screen where you can activate MAC authentication on a port.
Guest VLAN	The link takes you to a screen where you can activate enable and assign a guest VLAN to a port.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
MAINTENANCE	
Certificates	The link takes you to a screen where you can import the Switch's CA-signed certificates.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
Configuration	Click the link to unfold the following sub-link menu.
Restore Configuration	This link takes you to a screen where you can upload a stored device configuration file.
Backup Configuration	This link takes you to a screen where you can save your Switch’s configurations (settings) for later use.

Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
Erase Running-Configuration	This link takes you to a screen where you can reset the configuration to the Zyxel default configuration settings.
Save Configuration	This link takes you to a screen where you can save the current configuration (settings) to a specific configuration file on the Switch.
Configure Clone	This link takes you to a screen where you can copy the basic and advanced settings from a source port to a destination port or ports.
Diagnostic	This link takes you to a screen where you can ping IP addresses, run traceroute, test ports and show the location of the Switch.
Firmware Upgrade	This link takes you to a screen to upload firmware to your Switch.
Reboot System	This link takes you to a screen to reboot the Switch without turning the power off.
SSH Authorized Keys	This link takes you to a screen where you can authenticate secure SSH connections between a client computer and the Switch (also called the server) without needing a password to connect to the Switch.
SSH Host Keys	This link takes you to a screen where you can regenerate the Switch's SSH host key.
Tech-Support	This link takes you to a screen where you can download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.

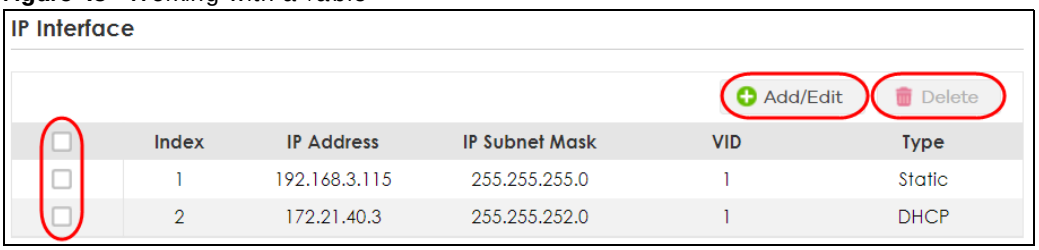
4.4.1 Tables and Lists

The Web Configurator tables and lists provide several options for how to work with their entries.

4.4.1.1 Working with Table Entries

Tables have tool icons for working with table entries as shown next. You can select one or more entries, or select the checkbox in the heading row to select all entries. Use the tool icons to modify the selected entries.

Figure 45 Working with a Table



The following table describes the most common table icons.

Table 11 Common Table Icons

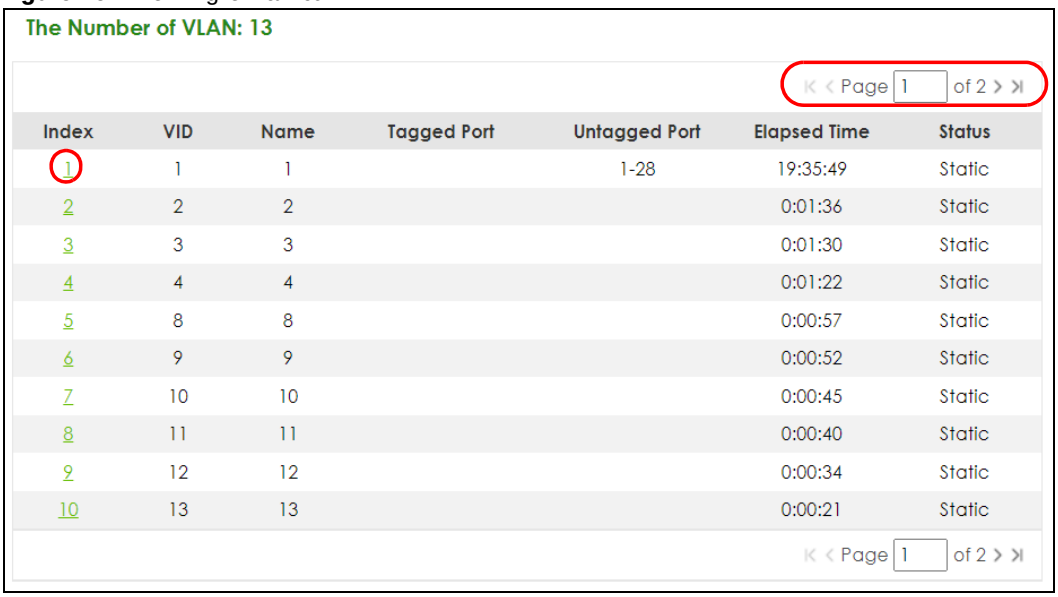
LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 11 Common Table Icons

LABEL	DESCRIPTION
Add/Edit	Click this to create a new entry or edit a selected entry. A configuration screen where you can add a new entry or modify the settings of the selected entry will open. In some configuration screens, the **Add/Edit** button is replaced by the **Edit** button. This means you can only edit the existing entries in the table.
Delete	To remove entries, select the entries and click **Delete**.

When viewing a list, you can click on an index number to view more details about the entry. If the list has more than one page, click the arrow button to navigate to different pages of entries.

Figure 46 Working on a List



4.5 Save Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right of the Web Configurator to save your configuration to non-volatile memory. Non-volatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

Note: Use the **Save** link when you are done with a configuration session.

4.6 Switch Lockout

You could block yourself (and all others) from managing the Switch if you do one of the following:

1 Delete the management VLAN (default is VLAN 1).

2 Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.

3 Filter all traffic to the CPU port.

4 Disable all ports.

5 Misconfigure the text configuration file.

6 Forget the password and/or IP address.

7 Prevent all services from accessing the Switch.

8 Change a service port number but forget it.

9 You forgot to log out of the Switch from a computer before logging in again on another computer.

Note: Be careful not to lock yourself and others out of the Switch.

4.7 Reset the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.7.1 Restore Button

Press the **RESTORE** button for more than 7 seconds to have the Switch automatically reboot and restore the factory default file. See Section 3.4 on page 46 for more information about the LED behavior.

4.7.2 Restore Custom Default (Standalone mode only)

Press the **RESTORE** button for 3 to 7 seconds to have the Switch automatically reboot and restore the last-saved custom default file. See Section 3.4 on page 46 for more information about the LED behavior.

4.7.3 Reboot the Switch

Press the **RESET** button to reboot the Switch without turning the power off. See Section 3.4 on page 46 for more information about the LED behavior.

4.8 Log Out of the Web Configurator

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.

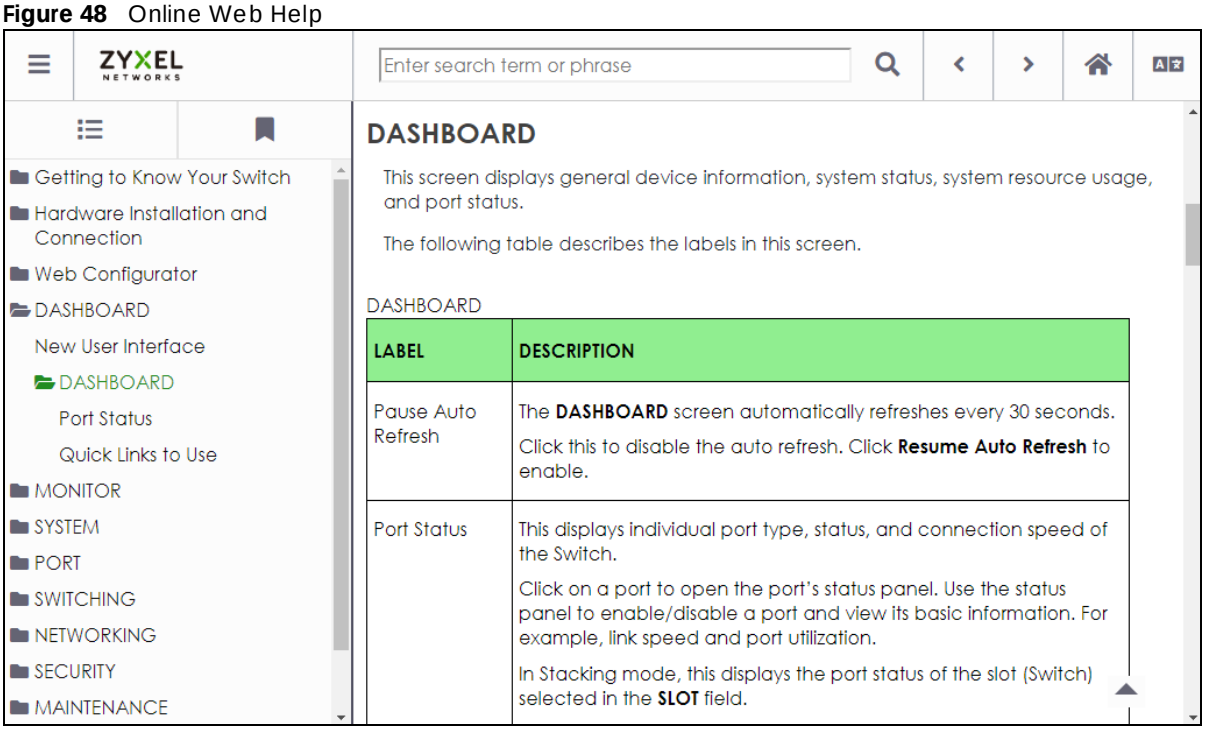
Figure 47 Logout button

4.9 Help

The Web Configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** icon on a Web Configurator screen to view an online help description (shown as below) of that screen.

Figure 48 Online Web Help



CHAPTER 5
Initial Setup Example

5.1 Overview

This chapter shows how to set up the Switch for an example network.

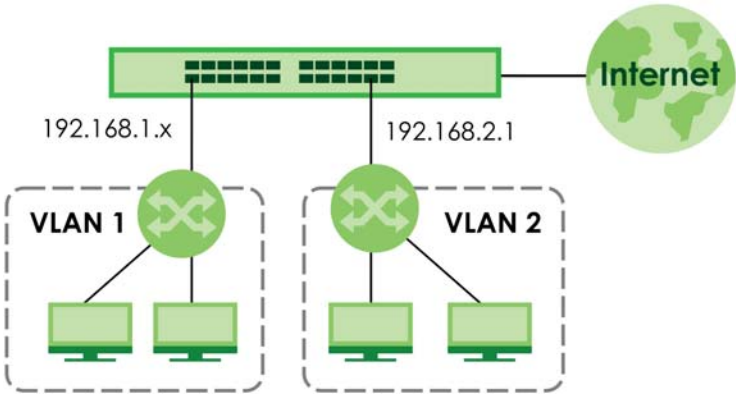
The following lists the configuration steps for the initial setup:

- Configure Switch Management IP Address
- Change the Administrator Login Password
- Create a VLAN
- Set Port VID
- How to Use DHCPv4 Snooping on the Switch
- How to Use DHCPv4 Relay on the Switch
- How to Back Up the Configuration
- How to Restore the Configuration
- How to Upgrade the Firmware

5.2 Configure Switch Management IP Address

If the Switch fails to obtain an IP address from a DHCP server, the Switch will use 192.168.1.1 as the management IP address. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 49 Getting Started: Management IP Address

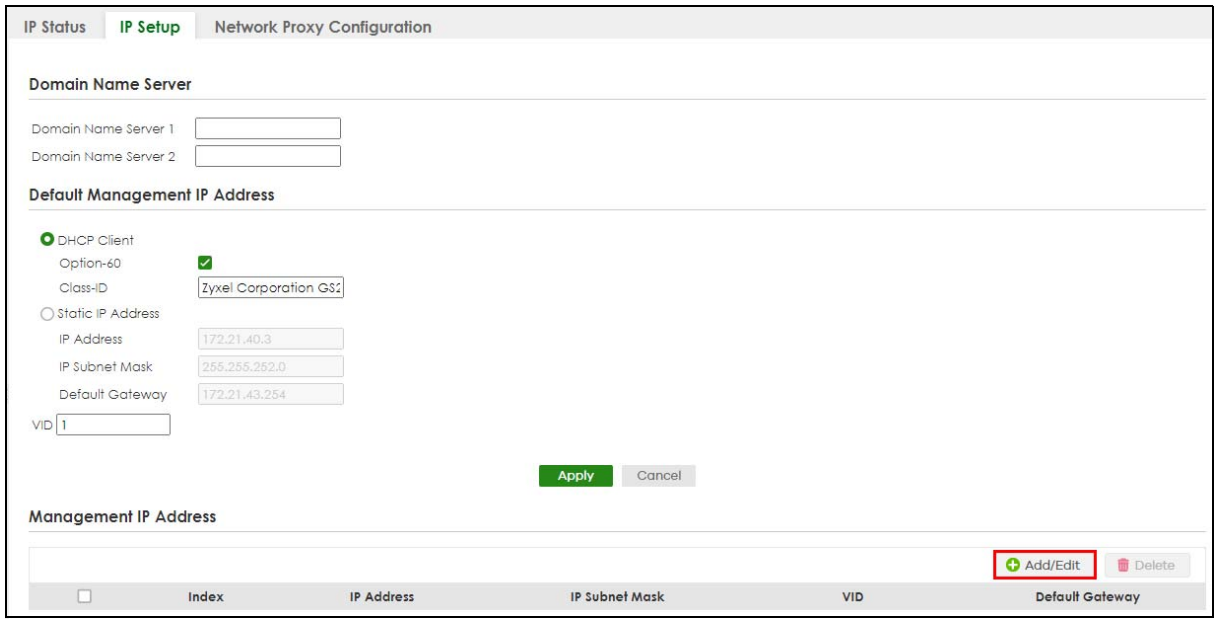


1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.

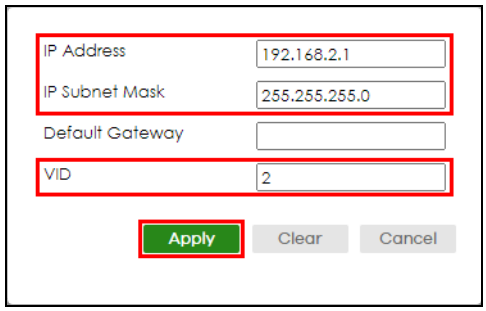
2 Open your web browser and enter “setup.zyxel” or “192.168.1.1” (the default IP address) in the address bar to access the Web Configurator. See Section 4.2 on page 50 for more information.

Note: You can always use the domain name “setup.zyxel” to access the Web Configurator whether the Switch is using a DHCP-assigned IP or static IP address. This requires your PC to be directly connected to the Switch.

3 Go to the **SYSTEM** > **IP Setup** > **IP Setup** screen. Click **Add/Edit**.



The following screen appears.



4 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

5 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. In this example, enter VLAN ID 2. This is the same as the VLAN ID you configure in the **Static VLAN** screen. See Section 5.4 on page 70 for more information.

6 Click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch’s power is turned off.

5.3 Change the Administrator Login Password

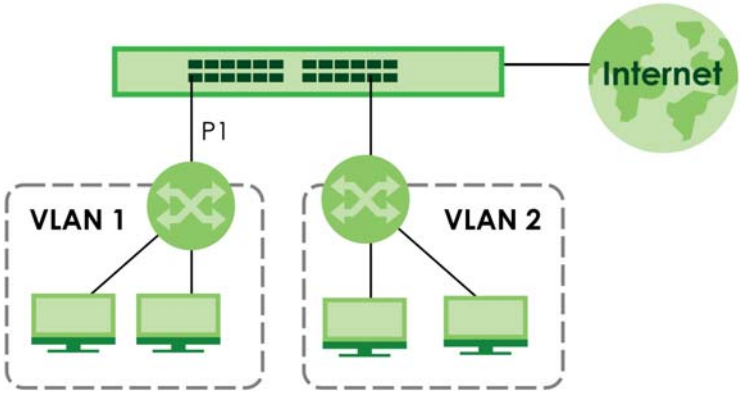
You can change the administrator login password regularly to ensure the security of your Switch. See Section 22.1 on page 142 for more information.

5.4 Create a VLAN

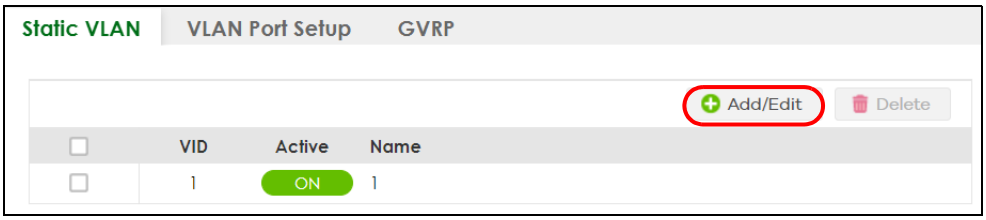
VLANs confine broadcast frames to the VLAN group in which the ports belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 (**P1**) as a member of VLAN 2.

Figure 50 Getting Started: VLAN



1 Go to the **SWITCHING** > **VLAN** > **Static VLAN** screen. Click **Add/Edit**.



2 The following screen appears. Click the switch to set this VLAN to **Active**, enter a descriptive name in the **Name** field and enter “2” in the **VLAN Group ID** field for the **VLAN2** network.

Note: The **VLAN Group ID** field in this screen and the **VID** field in the **SYSTEM** > **IP Setup** > **IP Status** screen refer to the same VLAN ID.

3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.

4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **Tx Tagging** checkbox to set the Switch to remove VLAN tags before sending.

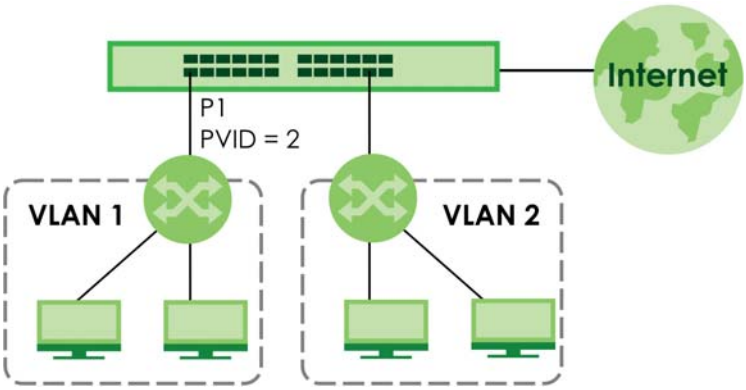
5 Click **Apply** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch’s power is turned off.

5.5 Set Port VID

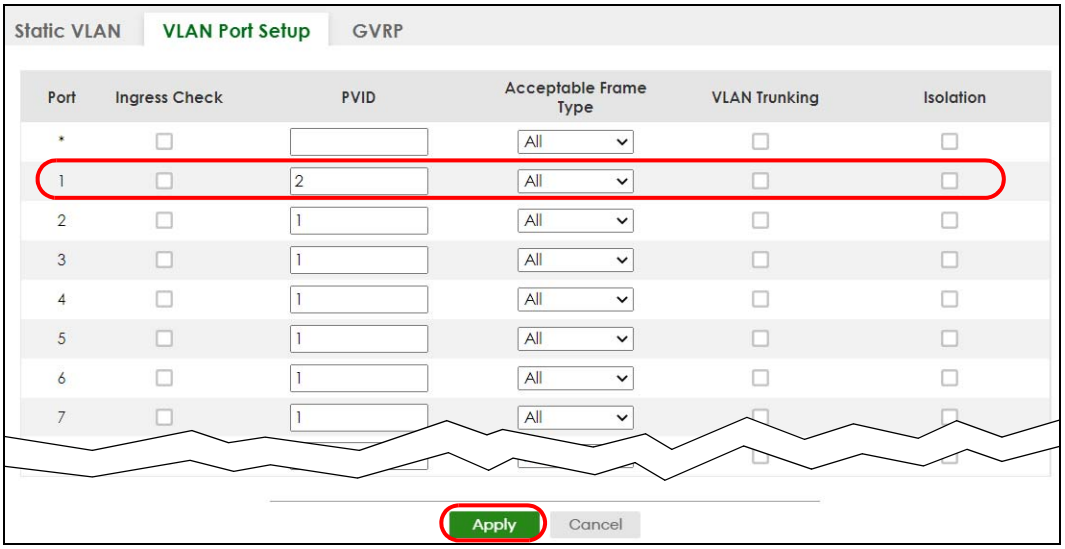
Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure **2** as the port VID (**PVID**) on port 1 (**P1**) so that any untagged frames received on that port get sent to VLAN 1.

Figure 51 Getting Started: Port VID



1 Go to the **SWITCHING** > **VLAN** > **VLAN Setup** > **VLAN Port Setup** screen.

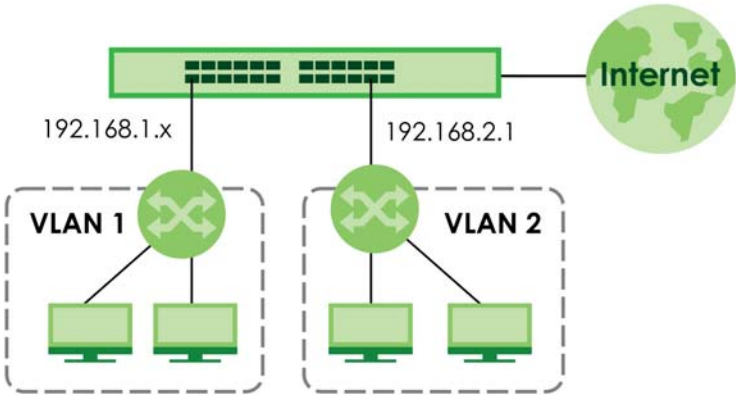


2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.5.1 Configure Switch Management IP Address

If the Switch fails to obtain an IP address from a DHCP server, the Switch will use 192.168.1.1 as the management IP address. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 52 Getting Started: Management IP Address

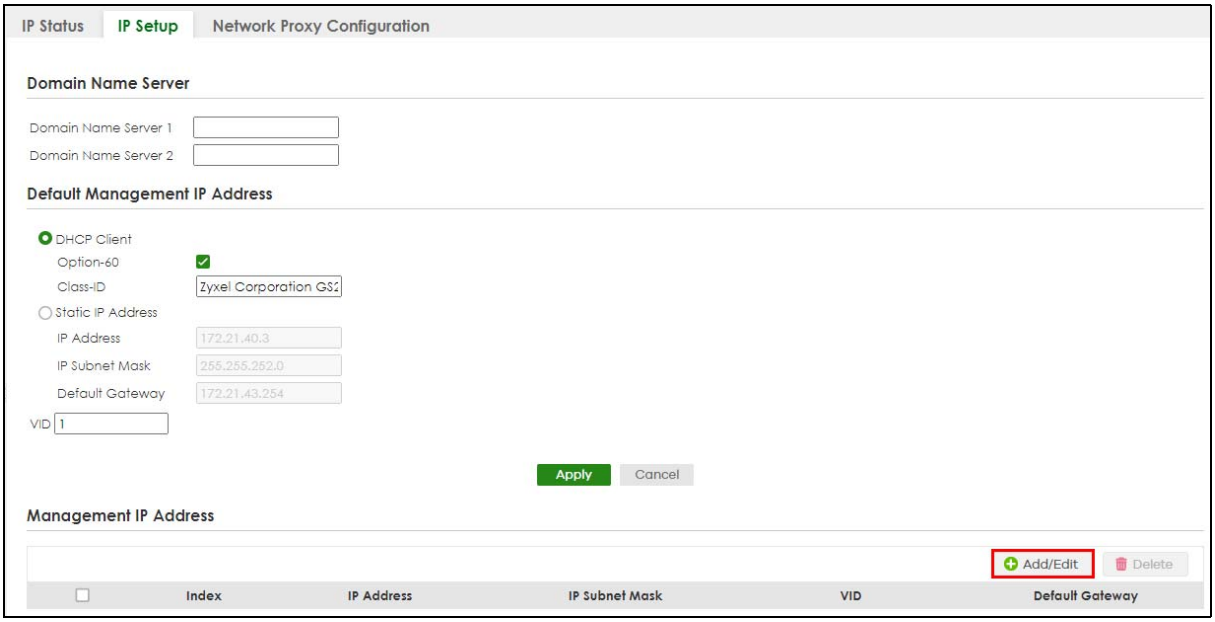


1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.

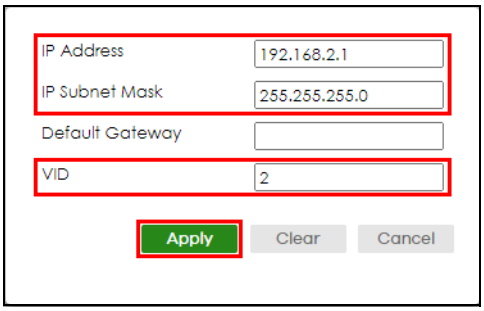
2 Open your web browser and enter “setup.zyxel” or “192.168.1.1” (the default IP address) in the address bar to access the Web Configurator. See Section 4.2 on page 50 for more information.

Note: You can always **use** the domain name “setup.zyxel” to access the Web Configurator whether the Switch is using a DHCP-assigned IP or static IP address. This requires your PC to be directly connected to the Switch.

3 Go to the **SYSTEM** > **IP Setup** > **IP Setup** screen. Click **Add/Edit**.



The following screen appears.



4 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

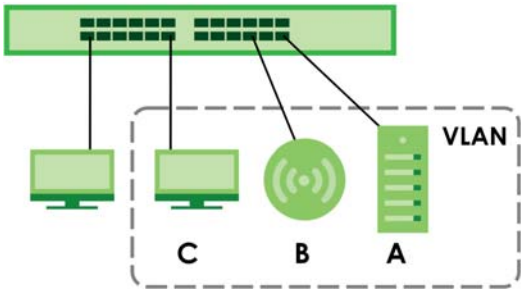
5 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. In this example, enter VLAN ID 2. This is the same as the VLAN ID you configure in the **Static VLAN** screen.

6 Click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.6 How to Use DHCPv4 Snooping on the Switch

You only want DHCP server **A** connected to port 5 to assign IP addresses to all devices in VLAN network. Create a VLAN containing ports 4, 5 and 6. Connect a computer to the Switch for management.

Figure 53 Tutorial: DHCP Snooping Tutorial Overview



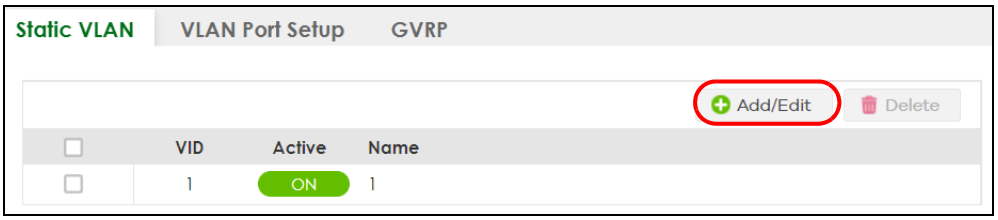
The settings in this tutorial are as the following.

Table 12 Tutorial: Settings in this Tutorial

HOST	PORT CONNECTED	VLAN	PVID	DHCP SNOOPING PORT TRUSTED
DHCP Server (**A**)	4	1 and 100	100	Yes
DHCP Client (**B**)	5	1 and 100	100	No
DHCP Client (**C**)	6	1 and 100	100	No

1 Connect your computer to the out-of-band management port (so you can access the Switch without being affected by any IP change caused by configurations). Access the Switch through **http://192.168.0.1**. Access the Switch through http://192.168.1.1 by default. Log into the Switch by entering the user name (default: **admin**) and password (default: **1234**).

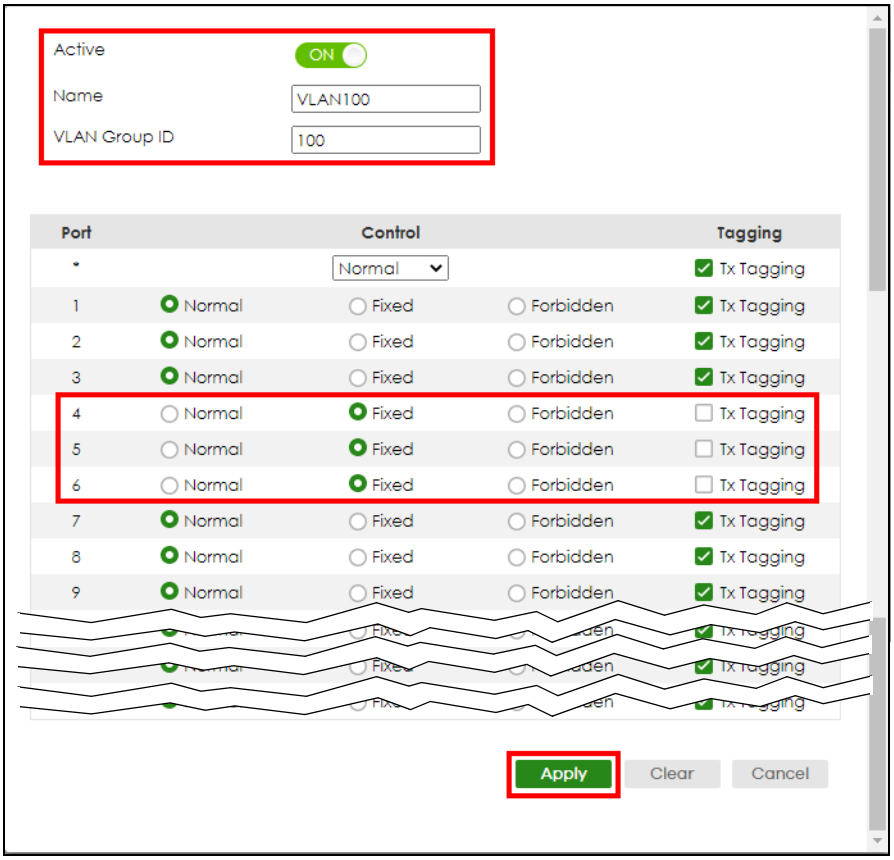
2 Go to **SWITCHING** > **VLAN** > **VLAN Setup** > **Static VLAN**. Click **Add/Edit**.



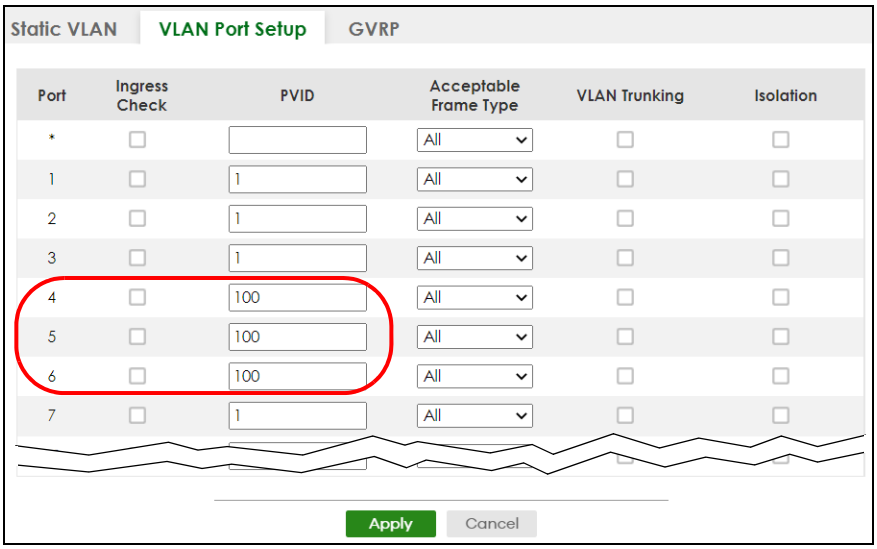
3 The following screen appears. Enable the switch button to set this VLAN to **ACTIVE**. Create a VLAN with ID of 100. Add ports 4, 5 and 6 in the VLAN by selecting **Fixed** in the **Control** field as shown.

De-select **Tx Tagging** because you do not want outgoing traffic to contain this VLAN tag.

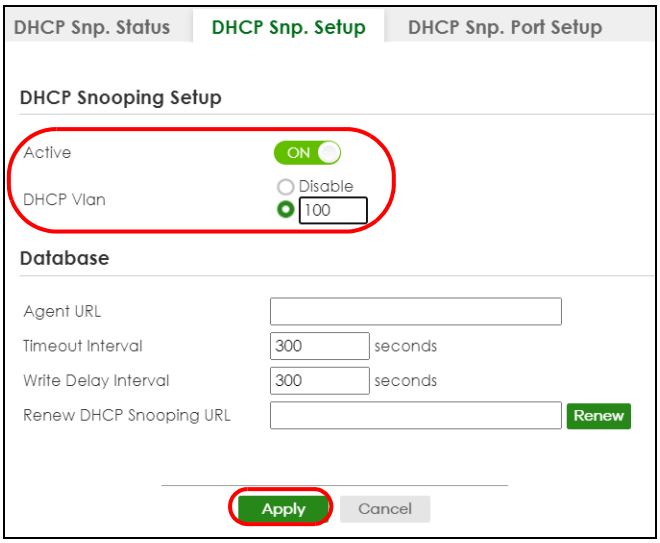
Click **Apply**.



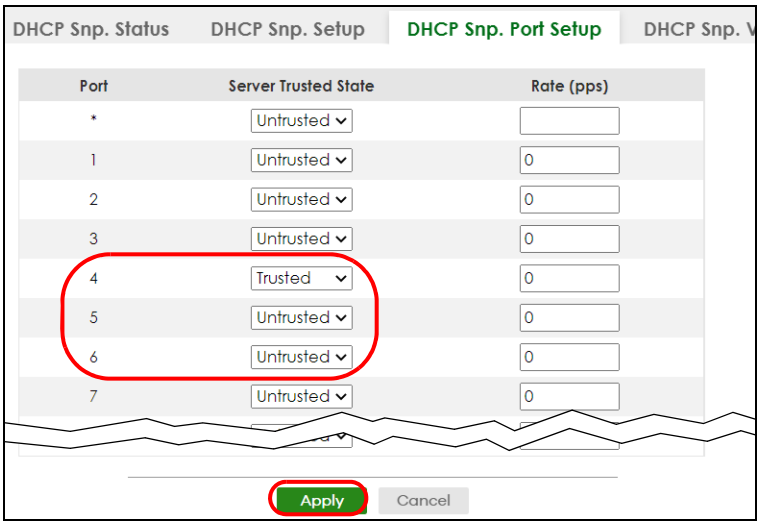
4 Go to **SWITCHING** > **VLAN** > **VLAN Setup** > **VLAN Port Setup**, and set the PVID of the ports 4, 5 and 6 to 100. This tags untagged incoming frames on ports 4, 5 and 6 with the tag 100. Click **Apply**.



5 Go to **SECURITY** > **DHCP Snooping** > **DHCP Snp. Setup**, activate and specify VLAN 100 as the DHCP VLAN as shown. Click **Apply**.
IP requests from VLANs you enable on the **SECURITY** > **DHCP Snooping** > **DHCP Snp. VLAN Setup** screen will be broadcast to the DHCP VLAN you set on this screen, which is VLAN100 in this example.



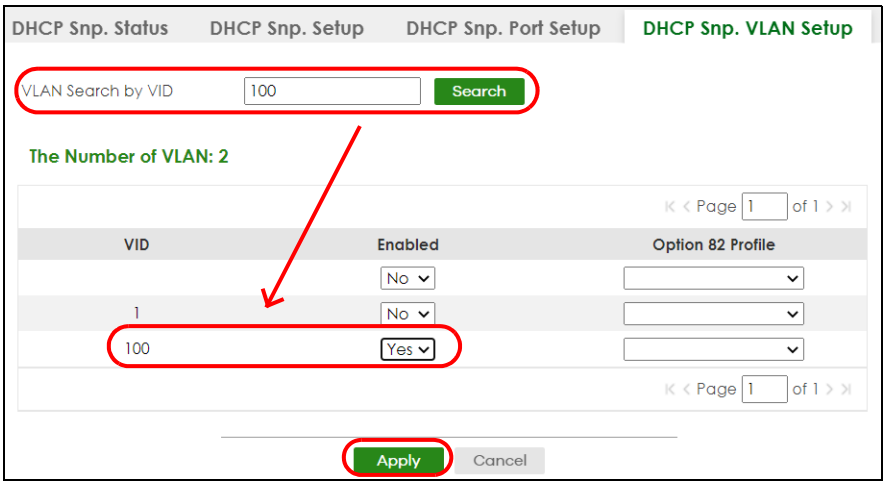
6 Go to **SECURITY** > **DHCP Snooping** > **DHCP Snp. Port Setup**. Select **Trusted** in the **Server Trusted state** field for port 4 because the DHCP server is connected to port 4. Keep ports 5 and 6 **Untrusted** because they are connected to DHCP clients. Click **Apply**.



7 Go to **SECURITY** > **DHCP Snooping** > **DHCP Snp. VLAN Setup**, show VLAN 100 by entering 100 in the **VLAN Search by VID** field and click **Search**.
Select **Yes** in the **Enabled** field of the VLAN 100 entry shown in the search result. Click **Apply**.

This enables DHCP snooping on VLAN100 (and other VLANs you enabled on this screen).

If you want the Switch to add more information in the DHCP request packets, such as source VLAN ID or system name, you can select an **Option82 Profile** in the entry. The Switch will add DHCP option 82 information to DHCP requests that the Switch relays to a DHCP server for the specified VLAN.



8 Connect your DHCP server to port 4 and a DHCP client (an AP, for example) to either port 5 or 6. The AP should be able to get an IP address from the DHCP server. If you put the DHCP server on port 5 or 6, the computer will NOT be able to get an IP address.

9 Click **Save** at the top right of the Web Configurator to save the configuration permanently.

10 To check if DHCP snooping works, go to **SECURITY** > **IPv4 Source Guard** > **IP Source Guard**, you should see an IP assignment with the type **DHCP-Snooping** as shown.

IP Source Guard | Static Binding

Index	IP Address	VLAN	MAC Address	Port	Lease	Type
1	192.168.2.178	100	88:88:88:88:88:8b	5	0d23h59m55s	DHCP-Snooping

You can also use telnet. Use the command "show dhcp snooping binding" to see the DHCP snooping binding table as shown next.

```
sysname# show dhcp snooping binding
         MacAddress        IpAddress         Lease           Type  VLAN   Port
  -----------------  ---------------  ------------  -------------  ----  -----
  88:88:88:88:88:8b    192.168.2.178   0d23h59m20s  dhcp-snooping   100      5
  Total number of bindings: 1
```

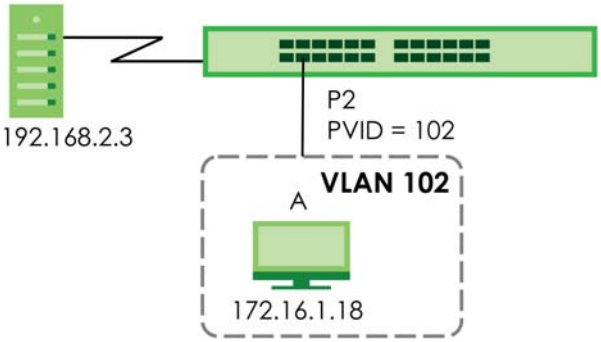
5.7 How to Use DHCPv4 Relay on the Switch

This tutorial describes how to configure your Switch to forward DHCP client requests to a specific DHCP server. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

5.7.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (192.168.2.3) and want to have it assign a specific IP address (say 172.16.1.18) to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the Switch's port 2 (**P2**) in VLAN 102.

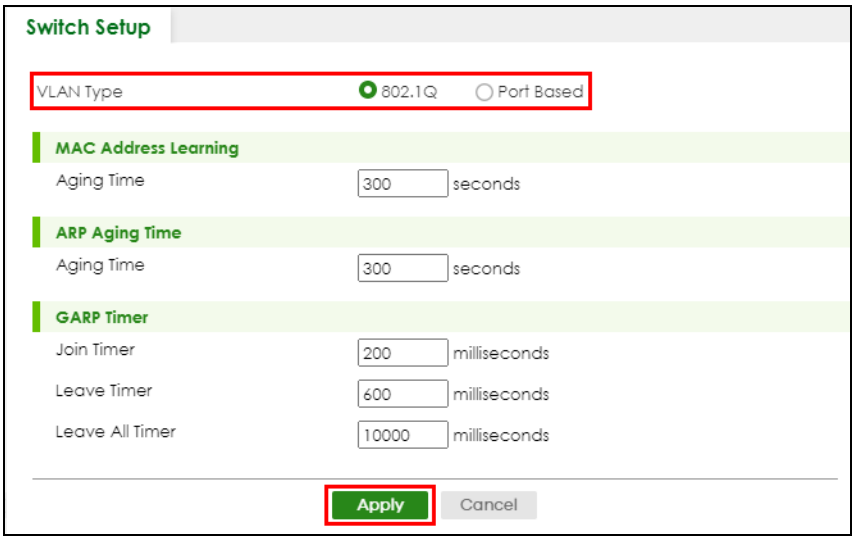
Figure 54 Getting Started: DHCP Relay Scenario



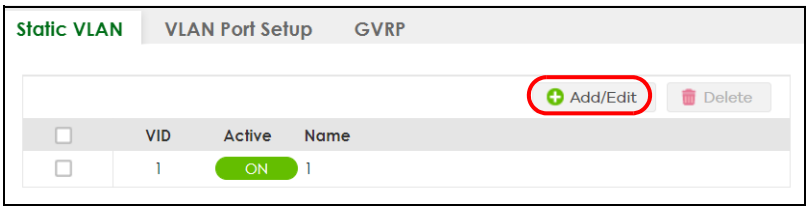
5.7.2 Create a VLAN

Follow the steps below to configure port 2 as a member of VLAN 102.

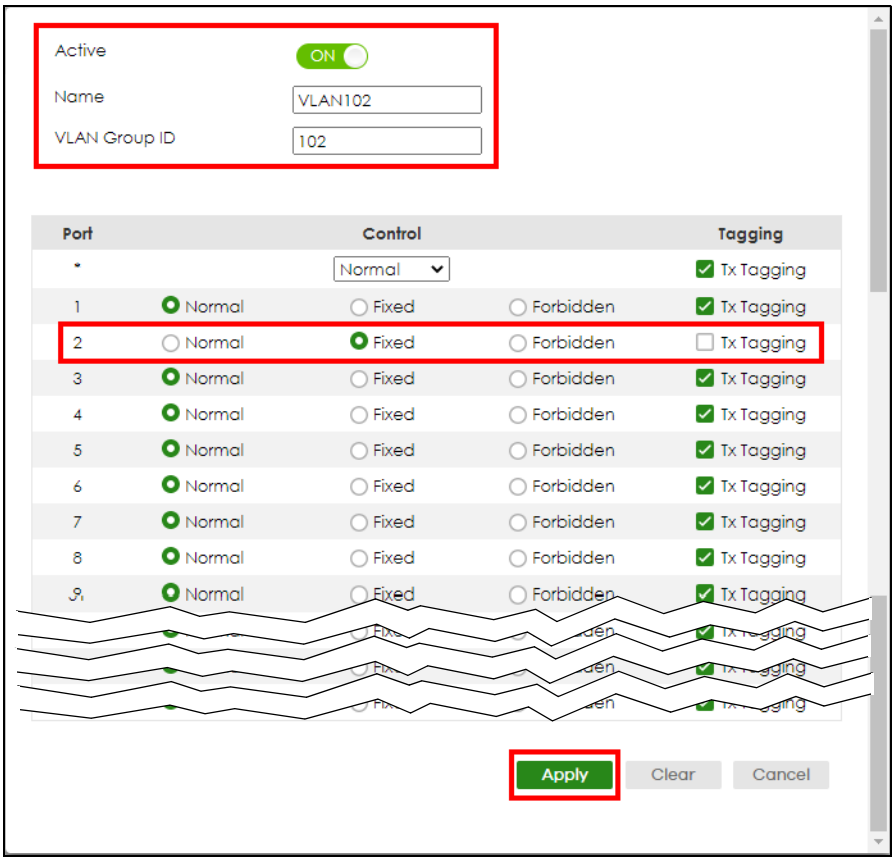
1. Access the Web Configurator through the Switch's management port.
2. Go to **SYSTEM** > **Switch Setup** > **Switch Setup** and set the **VLAN Type** to **802.1Q**. Click **Apply** to save the settings to the run-time memory.



3 Go to **SWITCHING** > **VLAN** > **VLAN Setup** > **Static VLAN**. Click **Add/Edit**.



4 The following screen appears. Enable the switch button to set this VLAN to **Active**. Enter a descriptive name (VLAN 102 for example) in the **Name** field and enter “102” in the **VLAN Group ID** field.

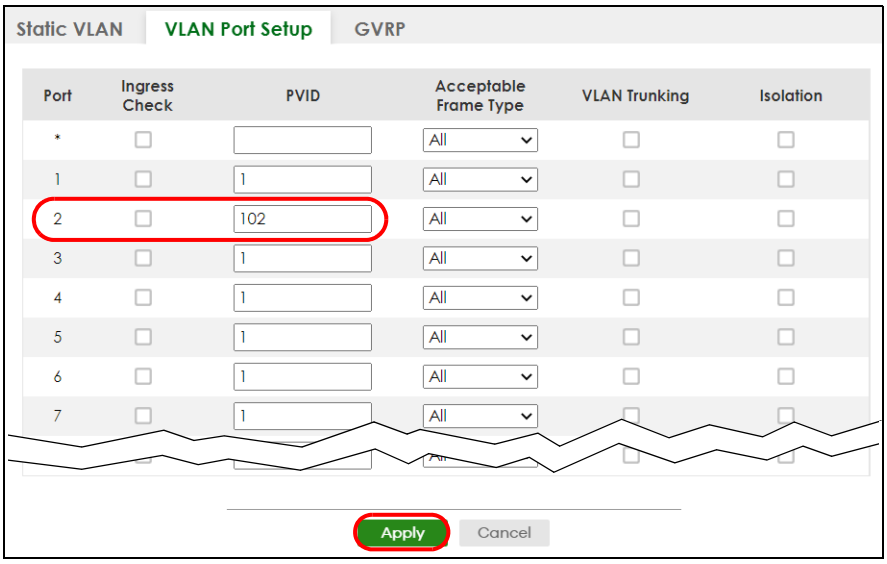


5 Set port 2 to be a permanent member of this VLAN by selecting **Fixed** in the **Control** field.

6 Clear the **Tx Tagging** checkbox to set the Switch to remove VLAN tags before sending.

7 Click **Apply** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

8 Go to **VLAN** > **VLAN Setup** > **VLAN Port Setup**. Enter "102" in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.



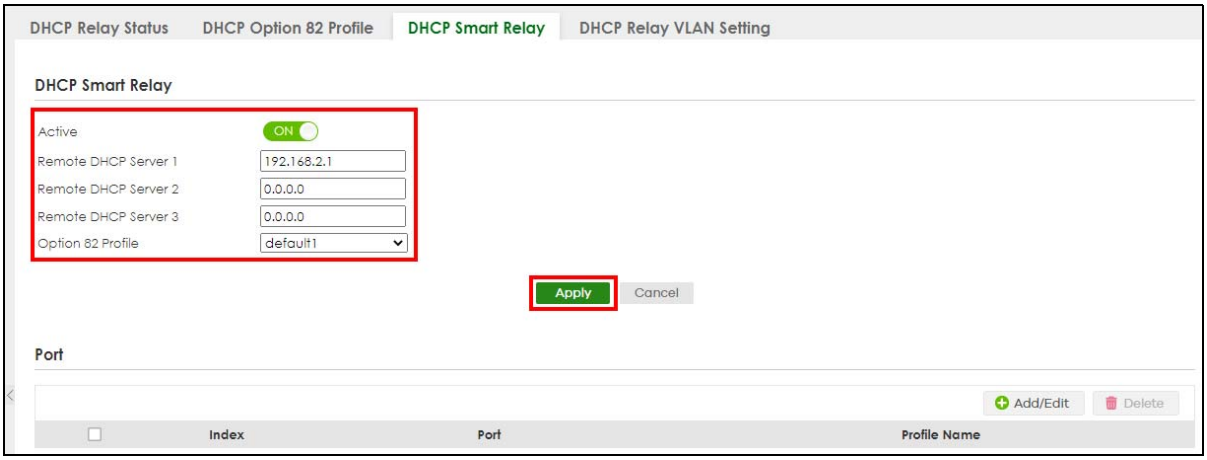
9 Click **Apply** to save your changes back to the run-time memory.

10 Click the **Save** link in the upper right of the Web Configurator to save your configuration permanently.

5.7.3 Configure DHCPv4 Relay

Follow the steps below to enable DHCP relay on the Switch and allow the Switch to add relay agent information (such as the VLAN ID) to DHCP requests.

1 Click **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Smart Relay**. Enable the **Active** switch button.



2 Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.

3 Select **default1** or **default2** in the **Option 82 Profile** field.

4 Click **Apply** to save your changes back to the run-time memory.

5 Click the **Save** link in the upper right of the Web Configurator to save your configuration permanently.

6 The DHCP server can then assign a specific IP address based on the DHCP request.

5.7.4 Troubleshooting

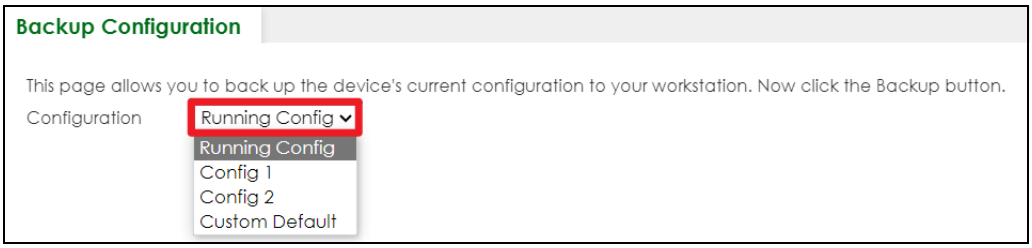
Check client **A**'s IP address. If it did not receive the IP address 172.16.1.18, make sure:

1. Client **A** is connected to the Switch's port 2 in VLAN 102.
2. You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.
3. You clicked the **Save** link on the Switch to have your settings take effect.

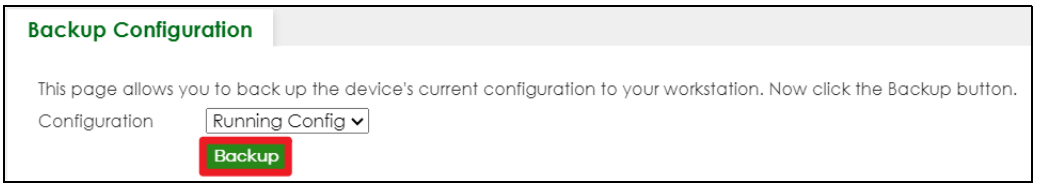
5.8 How to Back Up the Configuration

This section shows you how to back up the configuration. You should regularly back up your configuration especially before you make major configuration changes.

1. Log into the Web Configurator. Go to **MAINTENANCE** > **Configuration** > **Backup Configuration** > **Backup Configuration**.
2. Select the configuration you want to back up from the drop-down list. In this tutorial, you want to back up the currently running configuration, select **Running Config.**



3. Click **Backup**.



4. Save the downloaded file to your computer.

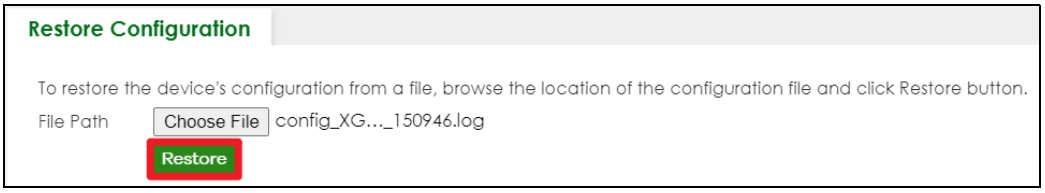
5.9 How to Restore the Configuration

This section shows you how to restore a previously saved configuration file from your computer to the Switch.

1. Log into the Web Configurator. Go to **MAINTENANCE** > **Configuration** > **Restore Configuration** > **Restore Configuration**.

2 Click **Choose File** and select the previously saved configuration file.

3 Click **Restore**.



4 Wait for the configuration to be restored. The screen will go to the login page. Log in with the default user name, **admin**, and default password, **1234**. Set up a new password to re-login.

5 The Switch is now running with the uploaded configuration.

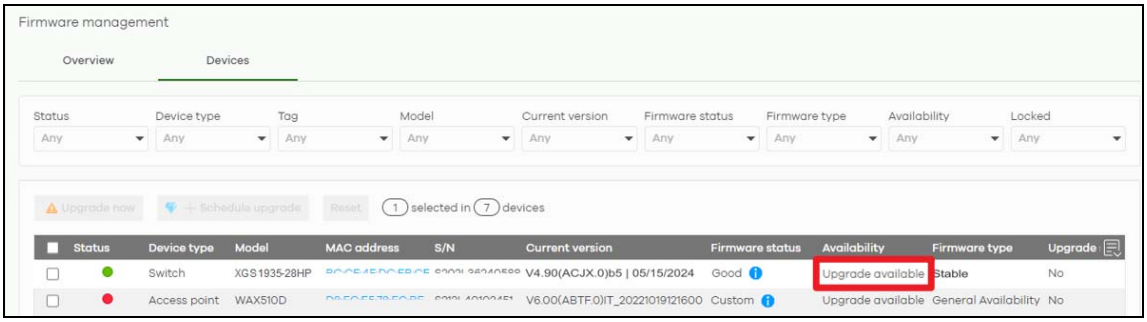
5.10 How to Upgrade the Firmware

This section shows you how to upgrade the Switch's firmware through NCC, the Web Configurator. You should always use the most recent firmware to get the latest features, improvements, and bug fixes.

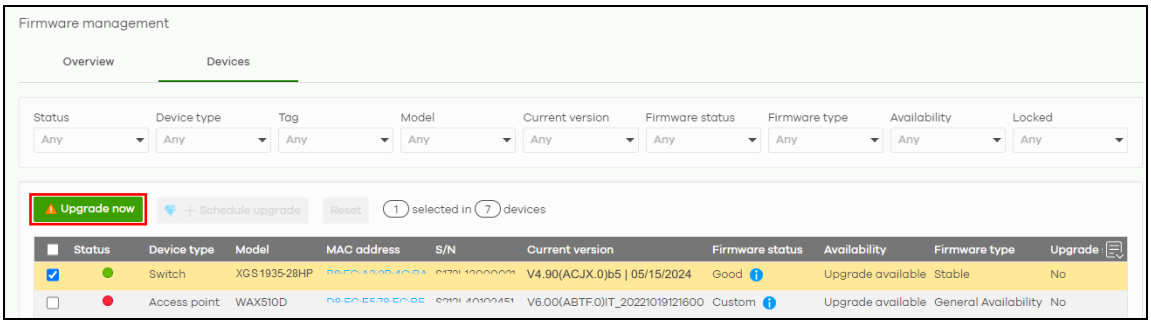
5.10.1 Firmware Upgrade Through NCC

Follow the steps below to upgrade the firmware to the Switch.

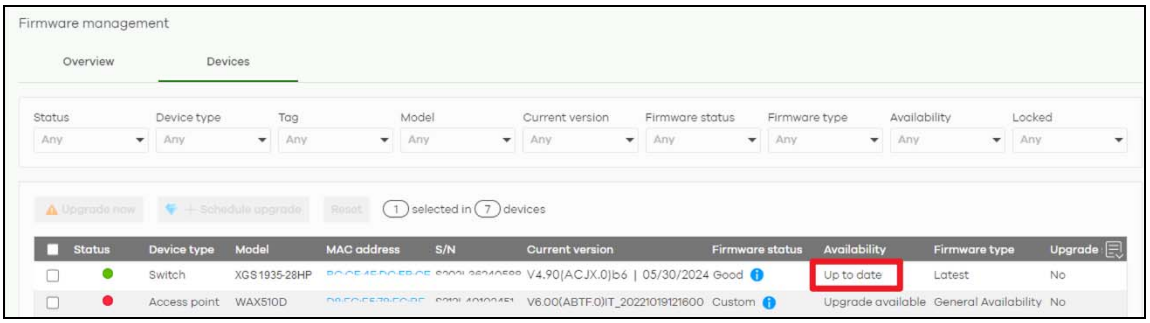
1 Log into the NCC. Go to **Site-wide** > **Configure** > **Firmware management** > **Devices.** Find the Switch in the device list. The **Availability** of the Switch is **Upgrade available** when a newer firmware is available.



2 Select the checkbox of the Switch, then click **Upgrade now**.



3 Check that the **Availability** of the Switch is **Up to date**.



5.10.2 Firmware Upgrade Through the Web Configurator

Follow the steps below to download the firmware from the Zyxel website first, then upgrade the Switch's firmware through the Web Configurator.

Download the Firmware

Follow the steps below to download the firmware.

1 Go to *https://www.zyxel.com/global/en/support* > **Support & Training** > **Download Library**.

2 Search for the model number of the Switch.

3 Download the firmware to your computer and then unzip it.

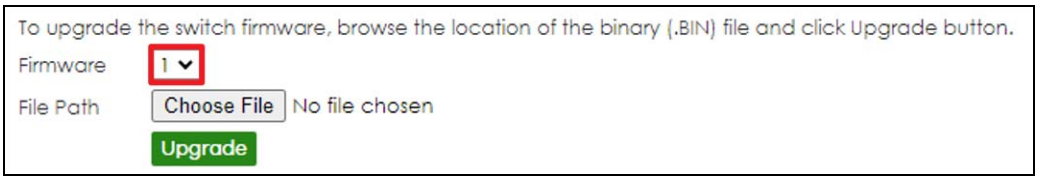
Upgrade the Firmware

The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. You can apply one of these images as an active image, and the other one as a backup image. Follow the steps below to upload and apply the firmware to the Switch.

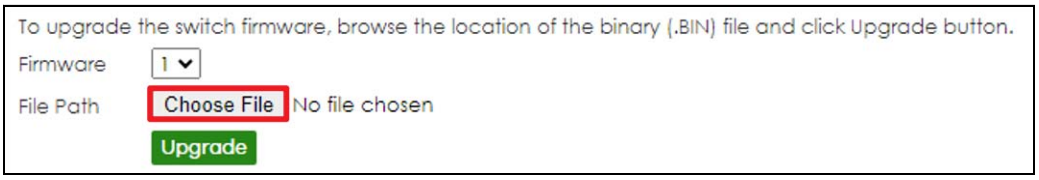
Note: Only the active image is loaded when the Switch starts up.

1 Log into the Web Configurator. Go to **MAINTENANCE** > **Firmware Upgrade** > **Firmware Upgrade**.

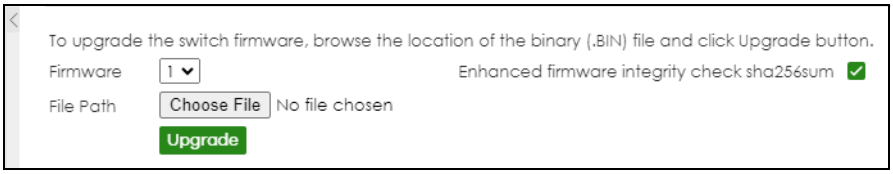
2 Select the firmware you want to upgrade from the drop-down list. In this tutorial, you want to upload the downloaded firmware to Firmware 1 on the Switch. Select **1**.



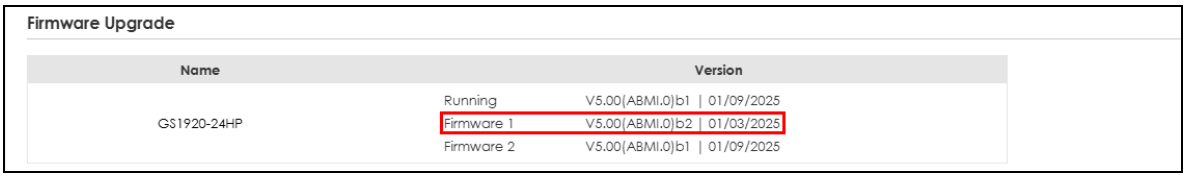
3 Click **Choose File** and select the downloaded, unzipped firmware file.



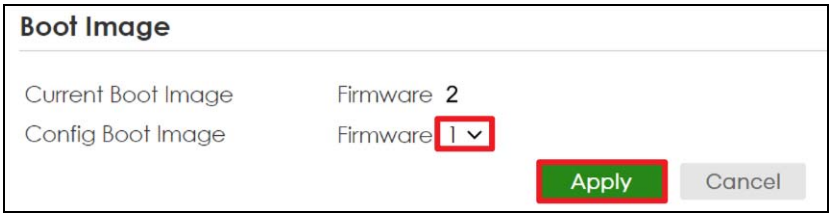
4 Click **Upgrade** to upload the new firmware.



5 The upgraded firmware will display in **Firmware Upgrade**. Check that the version is correct for **Firmware 1**.

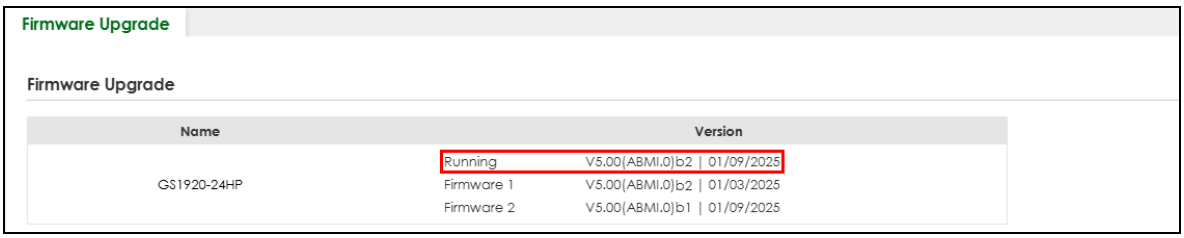


6 The Switch is currently using Firmware 2. To allow the Switch to use Firmware 1, select **1** from **Config Boot Image**, then click **Apply**.



7 Unplug the power cable and then plug it back into the Switch. Close the current window of the Web Configurator, then log into the Web Configurator with a new window.

8 Go to **MAINTENANCE** > **Firmware Upgrade** > **Firmware Upgrade**. Check that the **Running** firmware is the same as **Firmware 1** version.



CHAPTER 6
DASHBOARD

This chapter gives a quick introduction on the **DASHBOARD** screen.

The **DASHBOARD** screen automatically appears after you log into the Web Configurator.

6.1 User Interface

In the **DASHBOARD** screen, you can easily monitor the system status with the following tools (see DASHBOARD for more information):

- Visualized **Port Status** section with clickable port icons that provide information of that port, an ON/OFF switch button to enable/disable the port, and a **Power Cycle** button to turn the power off to the PoE port and then back on again (see Port Status).
- Visualized **Cloud Control Status** section that displays the NCC connection status using three connection-stage circles.
- Clickable hardware status monitoring sections that directly link to the **MONITOR** > **System Information** screen.
- Editable **Quick Link** section which provides shortcuts to configuration screens that you might frequently use (See Quick Links to Use).
- A **Search** tool on the upper right of the screen that you can use to search for the configuration screens you want to access (see Web Configurator Layout).

The left navigation panel is structured into a task-based UI. You can display the sub-menu in the **MONITOR**, **SYSTEM**, **PORT**, **SWITCHING**, **NETWORKING**, **SECURITY**, or the **MAINTENANCE** section by clicking their icons. See Web Configurator Layout for more information.

Find the latest release notes in: ***Download Library***.

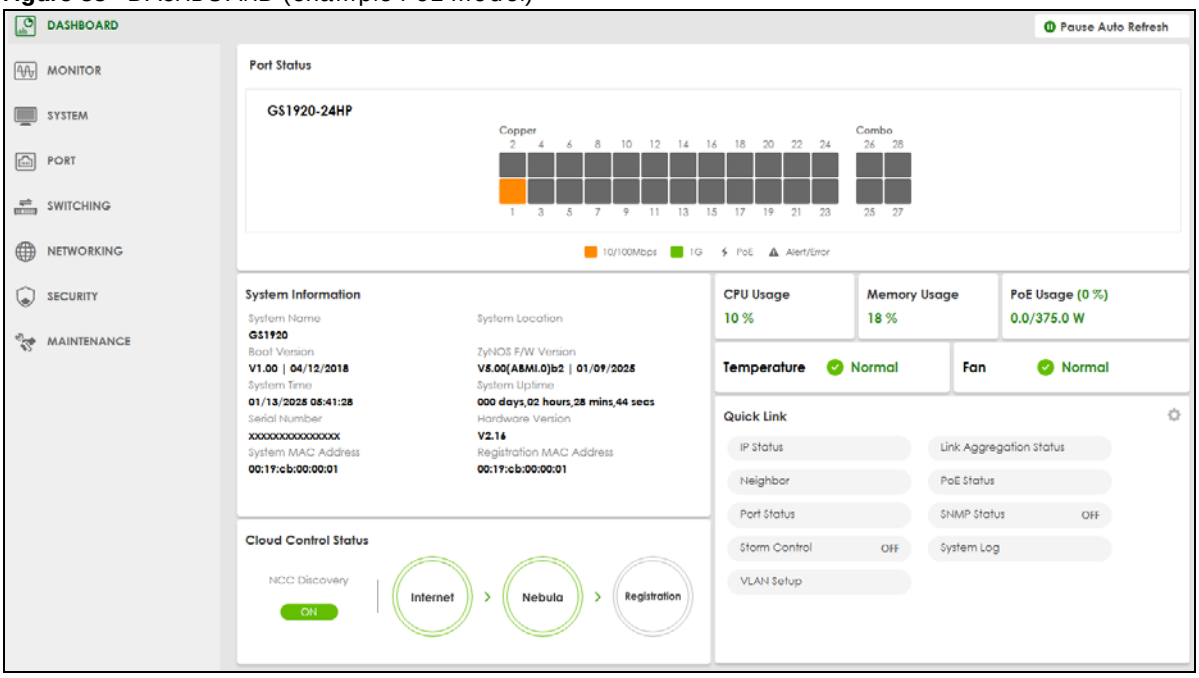
6.2 DASHBOARD

This screen displays general device information, system status, system resource usage, and port status.

This guide uses GS1920-8HP and GS1920-24HP screens as an example. The screens may vary slightly for different models.

Click **DASHBOARD** in the navigation panel to open the following screen.

Figure 55 DASHBOARD (example PoE model)



The following table describes the labels in this screen.

Table 13 DASHBOARD

LABEL	DESCRIPTION
Pause Auto Refresh	The **DASHBOARD** screen automatically refreshes every 30 seconds. Click this to disable the auto refresh. Click **Resume Auto Refresh** to enable.
Port Status	This displays individual port type, status, and connection speed of the Switch. Click on a port to open the port's status panel. Use the status panel to enable/disable a port, power cycle a PoE port, and view its basic information. For example, link speed and port utilization. Note: The port status may vary for non-PoE and PoE models.
System Information	
System Name	This field displays the name used to identify the Switch on any network.
System Location	This field displays the geographic location name you set for the Switch.
Boot Version	This field displays the version number and date of the boot module that is currently on the Switch.
ZyNOS F/W Version	This field displays the version number and date of the firmware the Switch is currently running.
System Time	This field displays the current date and time in the UAG. The format is mm/dd/yyyy hh:mm:ss.
System Uptime	This field displays how long the Switch has been running since it last restarted or was turned on.
Serial Number	This field displays the serial number of this Switch. The serial number is used for device tracking and control.
Hardware Version	This field displays the hardware version of the Switch.
System MAC Address	This field displays the MAC address of the Switch.

Table 13 DASHBOARD (continued)

LABEL	DESCRIPTION
Registration MAC Address	This is the MAC address reserved for NCC registration. Use this MAC address to register the Switch on NCC.
Cloud Control Status	This field displays: • The Switch Internet connection status. • The connection status between the Switch and NCC. • The Switch registration status on NCC. Mouse over the circles to display detailed information. To pass your Switch management to NCC, first make sure your Switch is connected to the Internet. Then go to NCC and register your Switch. Click **Cloud Control Status** or the switch button to go to the **SYSTEM** > **Cloud Management** screen. You can enable/disable NCC Discovery or view the NCC connection status in the **Cloud Management** screen. 1. **Internet** Green – The Switch is connected to the Internet. Orange – The Switch is not connected to the Internet. 2. **Nebula** Green – The Switch is connected to NCC. Gray – The Switch is not connected to NCC. 3. **Registration** Green – The Switch is registered on NCC. Gray – The Switch is not registered on NCC. Note: All circles will gray out if you disable Nebula Discovery. Note: If a circle displays orange or gray, hover the mouse over the circle to check the diagnostic message.
NCC Discovery	This displays if NCC discovery is enabled on the Switch. The Switch will connect to NCC and change to the NCC management mode if it: • is connected to the Internet. • has been registered on NCC.
CPU Usage	This displays the current CPU usage percentage. Click to go to the **MONITOR** > **System Information** > **System Information** screen to check the detailed information.
Memory Usage	This displays the current RAM usage percentage. Click to go to the **MONITOR** > **System Information** > **System Information** screen to check the detailed information.
PoE Usage	For PoE models. This field displays the amount of power the Switch is currently supplying to the connected PoE-enabled devices and the total power the Switch can provide to the connected PDs. It also shows the percentage of PoE power usage. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in **PORT** > **PoE Setup** > **PoE Setup**.

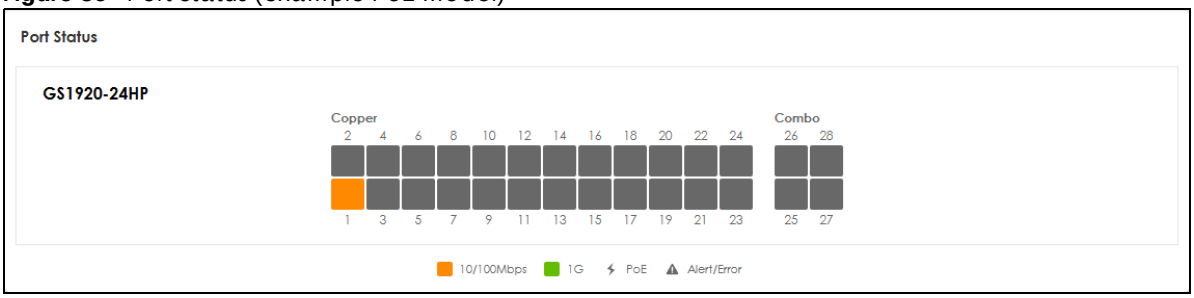
Table 13 DASHBOARD (continued)

LABEL	DESCRIPTION
Temperature	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. This displays the Switch's current device temperature level. Click to go to the **MONITOR** > **System Information** > **System Information** screen to check the detailed information.
Fan	Each fan of the Switch has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold. This displays the Switch's overall fan speed status. Click to go to the **MONITOR** > **System Information** > **System Information** screen to check the detailed information.
Quick Link	This section provides shortcut links to specific configuration screens. Click the edit button to choose the quick links to show.

6.2.1 Port Status

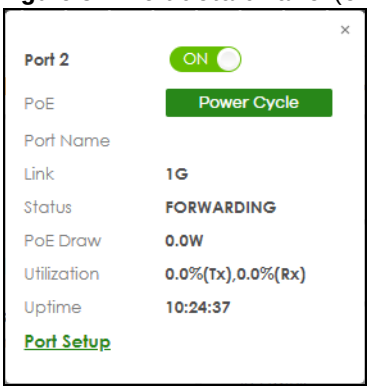
The **Port Status** section provides visualized port status for monitoring. Each port displays a status color determined by the their link speed.

Figure 56 Port Status (example PoE model)



Click on a port to display a port's status panel.

Figure 57 Port details Panel (example PoE model)

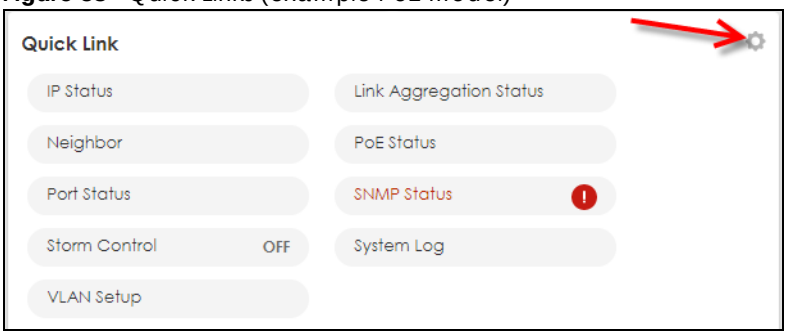


The port details pane includes the **Power Cycle** button for PoE models (turn the power off and then back on again), displays information such as link speed, status, PoE draw (for PoE models), port utilization, up time and has an ON/OFF switch button. Click the switch button to enable/disable the port.

6.2.2 Quick Links to Use

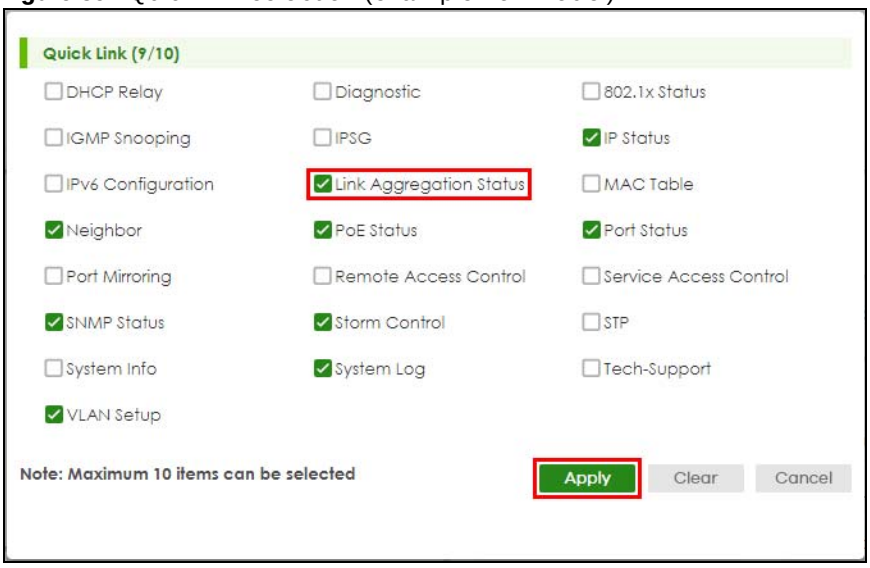
The quick links in the **Quick Link** section provide shortcuts to specific configuration screens. You can use the quick links to directly access the screens that you would frequently use. You can also decide which quick links to be put on the **DASHBOARD** screen using the **Edit** button.

Figure 58 Quick Links (example PoE model)



The setup panel displays after you click the **Edit** button.

Figure 59 Quick Link Selection (example PoE model)



Select the quick links you want and click **Apply**. The selected quick links will be displayed in the **Quick Link** section on the **DASHBOARD** screen.

CHAPTER 7 MONITOR

The following chapters introduces the configurations of the links under the **MONITOR** navigation panel.

Quick links to chapters:

CHAPTER 8
ARP Table

8.1 ARP Table Overview

This chapter introduces the ARP Table.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

8.1.1 What You Can Do

Use the **ARP Table** screen (Section 8.2 on page 91) to view IP-to-MAC address mappings.

8.1.2 What You Need to Know

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and if it finds the address, it sends it to the device.

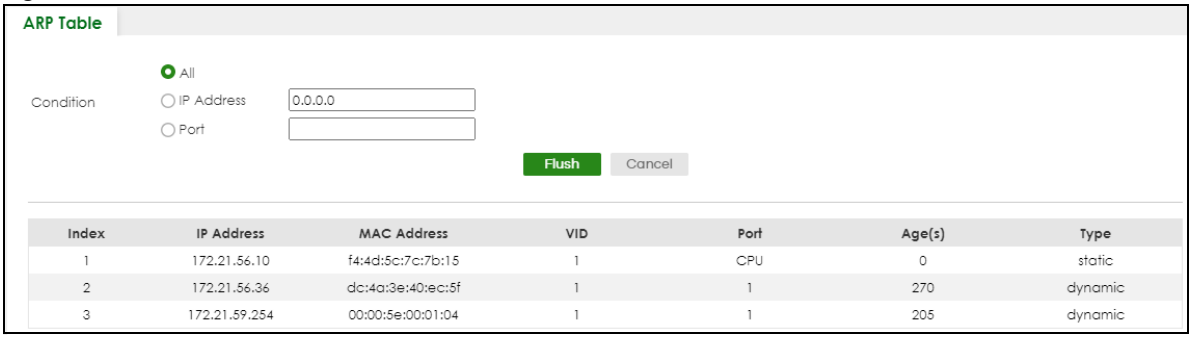
If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

8.2 Viewing the ARP Table

Use the ARP table to view IP-to-MAC address mappings and remove specific dynamic ARP entries.

Click **MONITOR** > **ARP Table** > **ARP Table** in the navigation panel to open the following screen.

Figure 60 MONITOR > ARP Table > ARP Table



The following table describes the labels in this screen.

Table 14 MONITOR > ARP Table > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the Switch to remove ARP entries when you click **Flush**. Select **All** to remove all of the dynamic entries from the ARP table. Select **IP Address** and enter an IP address to remove the dynamic entries learned with the specified IP address. Select **Port** and enter a port number to remove the dynamic entries learned on the specified port. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter “3-5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Flush	Click **Flush** to remove the ARP entries according to the condition you specified.
Cancel	Click **Cancel** to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. **CPU** means this IP address is the Switch’s management IP address.
Age(s)	This field displays how long (in seconds) an entry can still remain in the ARP table before it ages out and needs to be relearned. This shows **0** for a static entry.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (manually configured in **SYSTEM** > **IP Setup** > **IP Setup** or **NETWORKING** > **ARP Setup** > **Static ARP**).

CHAPTER 9
IPv6 Neighbor Table

9.1 IPv6 Neighbor Table Overview

This chapter introduces the IPv6 neighbor table.

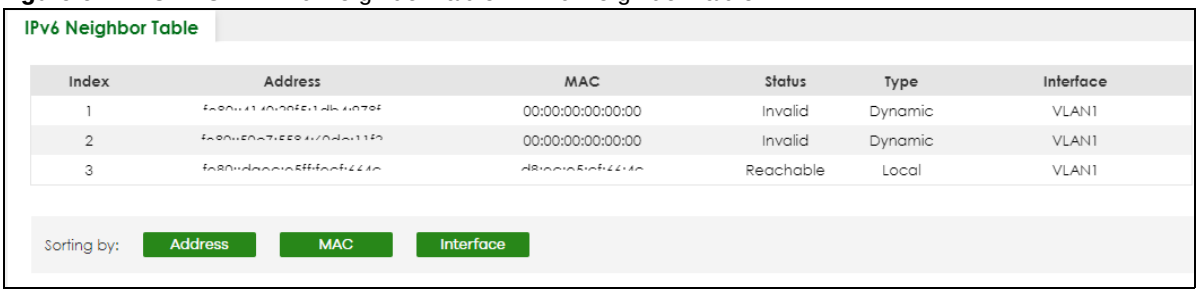
An IPv6 host is required to have a neighbor table. If there is an address to be resolved or verified, the Switch sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor table. You can also manually create a static IPv6 neighbor entry using the **SYSTEM** > **IPv6** > **IPv6 Neighbor Setup** screen.

When the Switch needs to send a packet, it first consults other table to determine the next hop. Once the next hop IPv6 address is known, the Switch looks into the neighbor table to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor table or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

9.2 Viewing the IPv6 Neighbor Table

Use this screen to view IPv6 neighbor information on the Switch. Click **MONITOR** > **IPv6 Neighbor Table** > **IPv6 Neighbor Table** in the navigation panel to display the screen as shown.

Figure 61 MONITOR > IPv6 Neighbor Table > IPv6 Neighbor Table



The following table describes the labels in this screen.

Table 15 MONITOR > IPv6 Neighbor Table > IPv6 Neighbor Table

LABEL	DESCRIPTION
Index	This field displays the index number of each entry in the table.
Address	This field displays the IPv6 address of the Switch or a neighboring device.
MAC	This field displays the MAC address of the IPv6 interface on which the IPv6 address is configured or the MAC address of the neighboring device.

Table 15 MONITOR > IPv6 Neighbor Table > IPv6 Neighbor Table (continued)

LABEL	DESCRIPTION
Status	This field displays whether the neighbor IPv6 interface is reachable. In IPv6, "reachable" means an IPv6 packet can be correctly forwarded to a neighbor node (host or router) and the neighbor can successfully receive and handle the packet. The available options in this field are: • Reachable (R): The interface of the neighboring device is reachable. (The Switch has received a response to the initial request.) • Stale (S): The last reachable time has expired and the Switch is waiting for a response to another initial request. The field displays this also when the Switch receives an unrequested response from the neighbor's interface. • Delay (D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The Switch delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • Probe (P): The Switch is sending request packets and waiting for the neighbor's response. • Invalid (IV): The neighbor address is with an invalid IPv6 address. • Unknown (?): The status of the neighboring interface cannot be determined for some reason. • Incomplete (I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. The interface of the neighboring device did not give a complete response.
Type	This field displays the type of an address mapping to a neighbor interface. The available options in this field are: • Other (O): none of the following type. • Local (L): A Switch interface is using the address. • Dynamic (D): The IP address to MAC address can be successfully resolved using IPv6 Neighbor Discovery protocol. Is it similar as IPv4 ARP (Address Resolution protocol). • Static (S): The interface address is statically configured.
Interface	This field displays the ID number of the IPv6 interface on which the IPv6 address is created or through which the neighboring device can be reached.
Sorting by	Click one of the following buttons to display and arrange the data according to that button type. The result is then displayed in the summary table above.
Address	Click this button to display and arrange the data according to IPv6 address.
MAC	Click this button to display and arrange the data according to MAC address.
Interface	Click this button to display and arrange the data according to IPv6 interface.

CHAPTER 10 MAC Table

10.1 MAC Table Overview

This chapter introduces the **MAC Table** screen.

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. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which ports and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **SWITCHING** > **Static MAC Forwarding** > **Static MAC Forwarding** screen).

10.1.1 What You Can Do

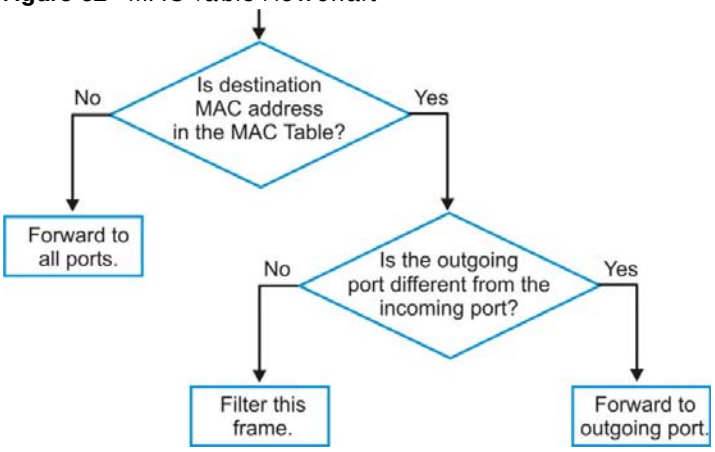
Use the **MAC Table** screen (Section 10.2 on page 96) to check whether the MAC address is dynamic or static.

10.1.2 What You Need to Know

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 on 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, then the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
   - 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 62 MAC Table Flowchart

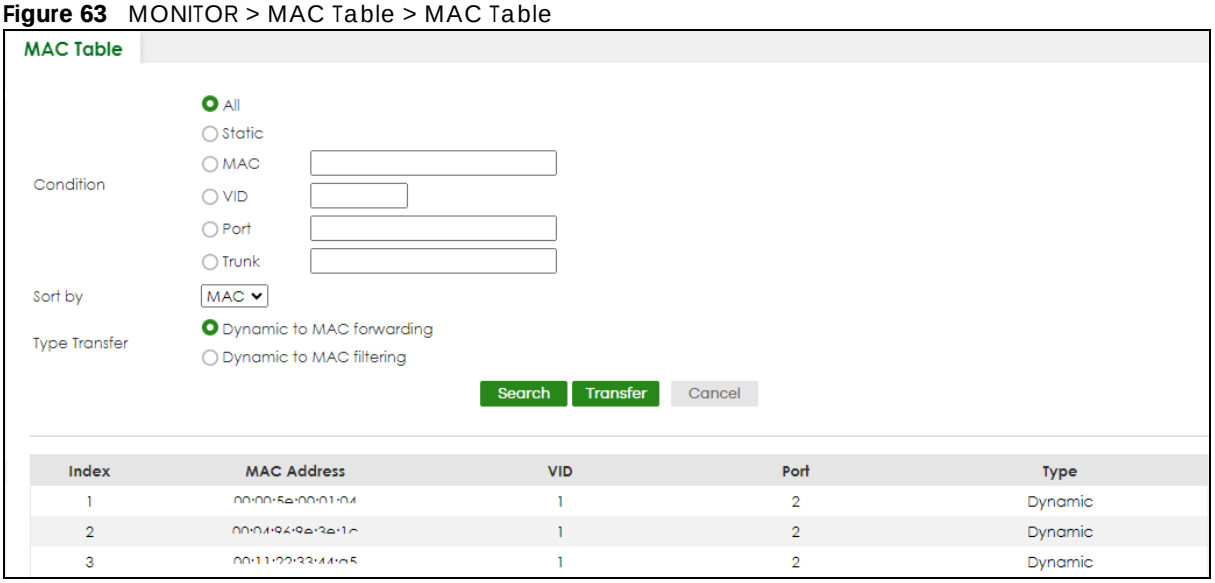


10.2 Viewing the MAC Table

Use this screen to search specific MAC addresses. You can also directly add dynamic MAC addresses into the static MAC forwarding table or MAC filtering table from the MAC table using this screen.

Click **MONITOR** > **MAC Table** > **MAC Table** in the navigation panel to display the following screen.

Figure 63 MONITOR > MAC Table > MAC Table



The following table describes the labels in this screen.

Table 16 MONITOR > MAC Table > MAC Table

LABEL	DESCRIPTION
Condition	Select one of the below search conditions and click **Search** to only display the data which matches the criteria you specified. Select **All** to display any entry in the MAC table of the Switch. Select **Static** to display the MAC entries manually configured on the Switch. Select **MAC** and enter a MAC address in the field provided to display a specified MAC entry. Select **VID** and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN. Select **Port** and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port. Select **Trunk** and type the ID of a trunk group to display all MAC addresses learned from the ports in the trunk group.
Sort by	Define how the Switch displays and arranges the data in the summary table below. Select **MAC** to display and arrange the data according to MAC address. Select **VID** to display and arrange the data according to VLAN group. Select **PORT** to display and arrange the data according to port number.
Type Transfer	Select **Dynamic to MAC forwarding** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into static entries. They also display in the **SWITCHING** > **Static MAC Forwarding** > **Static MAC Forwarding** screen. Select **Dynamic to MAC filtering** and click the **Transfer** button to change all dynamically learned MAC address entries in the summary table below into MAC filtering entries. These entries will then display only in the **SWITCHING** > **Static MAC Filtering** > **Static MAC Filtering** screen and the default filtering action is **Discard source**.
Search	Click this to search data in the MAC table according to your input criteria.
Transfer	Click this to perform the MAC address transferring you selected in the **Type Transfer** field.
Cancel	Click **Cancel** to change the fields back to their last saved values.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port where the above MAC address is forwarded.
Type	This shows whether the MAC address is **Dynamic** (learned by the Switch) or **Static** (manually entered in the **SWITCHING** > **Static MAC Forwarding** > **Static MAC Forwarding** screen).

CHAPTER 11
Neighbor

11.1 Neighbor Overview

The **Neighbor** screen allows you to view a summary and manage the Switch's neighboring devices. It uses Layer Link Discovery Protocol (LLDP) to discover all neighbor devices connected to the Switch including non-Zyxel devices. You can use this screen to perform tasks on the neighboring devices like login, power cycle (turn the power off and then back on again), and reset to factory default settings.

This screen shows the neighboring device first recognized on an Ethernet port of the Switch. Device information is displayed in gray when the neighboring device is offline.

11.1.1 What You Can Do

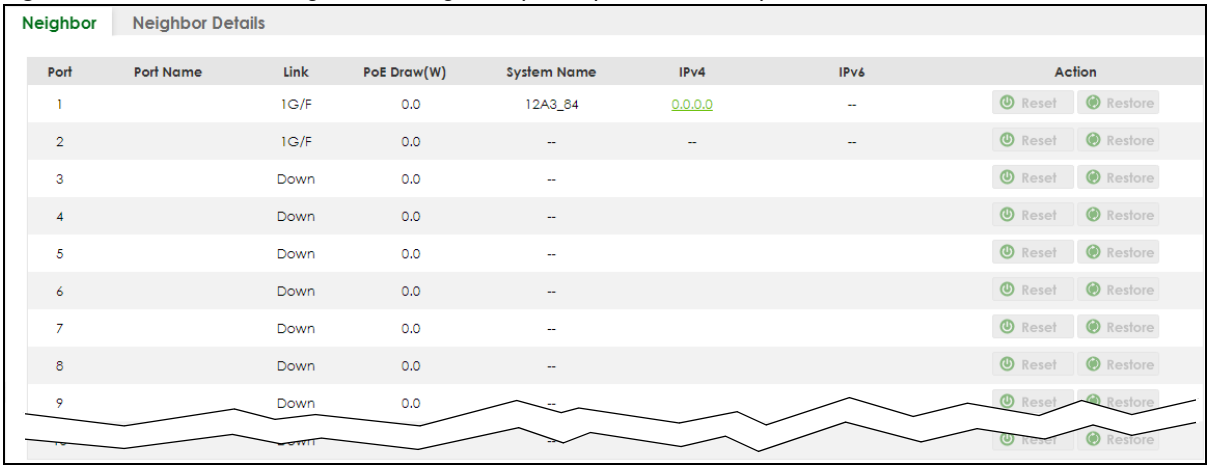
Use the **Neighbor** screen (Section 11.2 on page 98) to view a summary and manage the Switch's neighbor devices.

Use the **Neighbor Details** screen (Section 11.2.1 on page 99) to view more detailed information on the Switch's neighbor devices.

11.2 Neighbor

Click **MONITOR** > **Neighbor** > **Neighbor** to see the following screen.

Figure 64 MONITOR > Neighbor > Neighbor (example PoE model)



The following table describes the fields in the above screen.

Table 17 MONITOR > Neighbor > Neighbor

LABEL	DESCRIPTION
Port	This shows the port of the Switch, on which the neighboring device is discovered.
Port Name	This shows the port description of the Switch.
Link	This shows the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, **1G** for 1 Gbps, or **10G** for 10 Gbps) and the duplex (**F** for full duplex or **H** for half). This field displays **Down** if the port is not connected to any device.
PoE Draw (W)	For PoE models. This shows the consumption that the neighboring device connected to this port draws from the Switch. This allows you to plan and use within the power budget of the Switch.
System Name	This shows the system name of the neighbor device.
IPv4	This shows the IPv4 address of the neighbor device. The IPv4 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
IPv6	This shows the IPv6 address of the neighbor device. The IPv6 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
Action	For PoE models. Click the **Reset** button to turn OFF the power of the neighbor device and turn it back ON again. A count down button (from 5 to 0) starts. Note: The Switch must support power sourcing (PSE) or the network device is a powered device (PD). Click the **Restore** button to restore the neighboring device to its factory default settings. A warning message "**Are you sure you want to load factory default?**" appears prompting you to confirm the action. After confirming the action a count down button (from 5 to 0) starts. Note: • The Switch must support power sourcing (PSE) or the network device is a powered device (PD). • If multiple neighbor devices use the same port, the **Reset** button is not available. • You can only reset Zyxel powered devices that support the ZON utility.

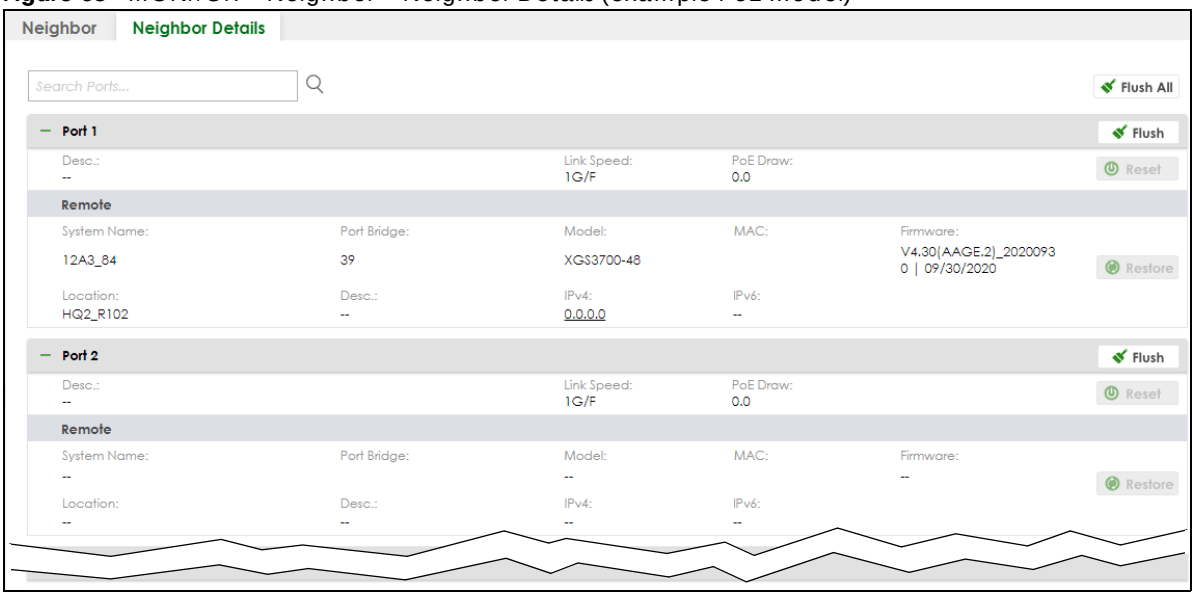
11.2.1 Neighbor Details

Use this screen to view detailed information about the neighboring devices. Device information is displayed in gray when the neighboring device is currently offline.

Up to 10 neighboring device records per Ethernet port can be retained in this screen even when the devices are offline. When the maximum number of neighboring device records per Ethernet port is reached, new device records automatically overwrite existing offline device records, starting with the oldest existing offline device record first.

Click **MONITOR** > **Neighbor** > **Neighbor Details** to see the following screen.

Figure 65 MONITOR > Neighbor > Neighbor Details (example PoE model)



The following table describes the fields in the above screen.

Table 18 MONITOR > Neighbor > Neighbor Details

LABEL	DESCRIPTION
Search Ports...	Enter the port number to search and display the ports you specified. The result will display in the below list. You can enter multiple ports separated by comma (",") or hyphen ("-") for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Port	This shows the port of the Switch, on which the neighboring device is discovered.
Desc.	This shows the port description of the Switch.
Link Speed	This shows the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, **1G** for 1 Gbps, **2.5G** for 2.5 Gbps, **5G** for 5 Gbps, or **10G** for 10 Gbps) and the duplex (**F** for full duplex or **H** for half). This field displays **Down** if the port is not connected to any device.
PoE Draw	For PoE models. This shows the consumption that the neighboring device connected to this port draws from the Switch. This allows you to plan and use within the power budget of the Switch.
Reset	Click this button to turn OFF the power of the neighbor device and turn it back ON again. A count down button (from 5 to 0) starts. Note: The Switch must support power sourcing (PSE) or the network device is a powered device (PD).
Remote	
System Name	This shows the system name of the neighbor device.
Port Bridge	This shows the neighboring device's MAC address or the port number connected to the Switch.
Model	This shows the model name of the neighbor device. This field will show "**–**" for devices that do not support the ZON utility.
MAC	This shows the MAC address of the neighbor device.
Firmware	This shows the firmware version of the neighbor device. This field will show "**–**" for devices that do not support the ZON utility.

Table 18 MONITOR > Neighbor > Neighbor Details (continued)

LABEL	DESCRIPTION
Location	This shows the geographic location of the neighbor device. This field will show "**–**" for devices that do not support the ZON utility.
Desc.	This shows the description of the neighbor device's port which is connected to the Switch.
IPv4	This shows the IPv4 address of the neighbor device. The IPv4 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
IPv6	This shows the IPv6 address of the neighbor device. The IPv6 address is a **hyper link** that you can click to log into and manage the neighbor device through its Web Configurator.
Restore	Click this button to restore the neighbor device to its factory default settings. A warning message "**Are you sure you want to load factory default?**" appears prompting you to confirm the action. After confirming the action a count down button (from 5 to 0) starts. Note: • The Switch must support power sourcing (PSE) or the network device is a powered device (PD). • If multiple neighbor devices use the same port, the **Reset** button is not available. • You can only reset Zyxel powered devices that support the ZON utility.
Flush	Click the **Flush** button on the port tab to remove information about neighbors learned on a specific ports.
Flush All	Click the **Flush All** button to remove information about neighbors learned on all ports.

CHAPTER 12
Path MTU Table

12.1 Path MTU Overview

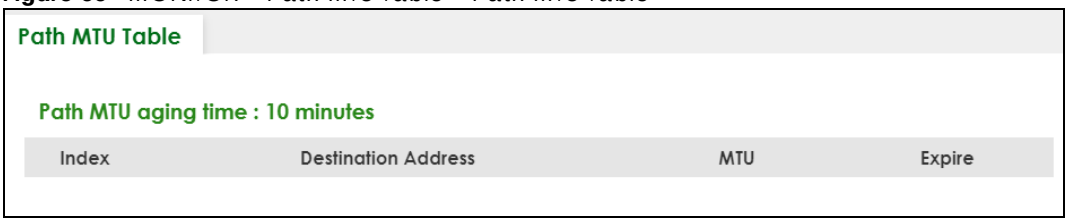
This chapter introduces the IPv6 Path MTU table.

The largest size (in bytes) of a packet that can be transferred over a data link is called the Maximum Transmission Unit (MTU). The Switch uses Path MTU Discovery to discover Path MTU (PMTU), that is, the minimum link MTU of all the links in a path to the destination. If the Switch receives an ICMPv6 Packet Too Big error message after sending a packet, it fragments the next packet according to the suggested MTU in the error message.

12.2 Viewing the Path MTU Table

Use this screen to view IPv6 path MTU information on the Switch. Click **MONITOR** > **Path MTU Table** > **Path MTU Table** in the navigation panel to display the screen as shown.

Figure 66 MONITOR > Path MTU Table > Path MTU Table



The following table describes the labels in this screen.

Table 19 MONITOR > Path MTU Table > Path MTU Table

LABEL	DESCRIPTION
Path MTU aging time	This field displays how long an entry remains in the Path MTU table before it ages out and needs to be relearned.
Index	This field displays the index number of each entry in the table.
Destination Address	This field displays the destination IPv6 address of each path or entry.
MTU	This field displays the maximum transmission unit of the links in the path.
Expire	This field displays how long (in minutes) an entry can still remain in the Path MTU table before it ages out and needs to be relearned.

CHAPTER 13
Port Status

This chapter introduces the **Port Status** screens.

13.0.1 What You Can Do

Use the **Port Status** screen (Section 13.1 on page 103) to view the port status of the Switch.

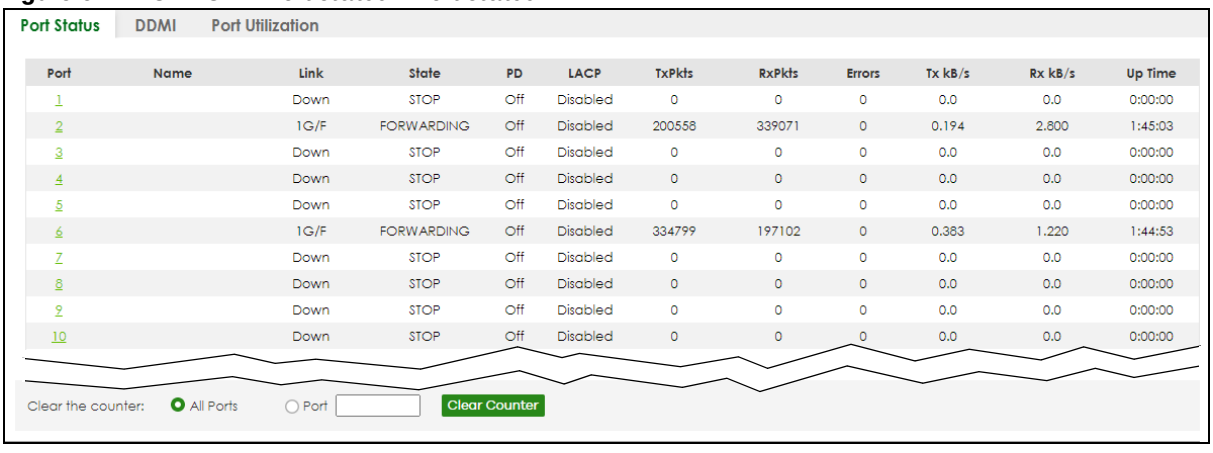
Use the **DDMI** screen (Section 13.2 on page 107) to view the DDMI (Digital Diagnostics Monitoring Interface) status of the SFP transceivers on the Switch.

Use the **Port Utilization** screen (Section 13.3 on page 109) to view the current data rate and utilization percentage of each port on the Switch.

13.1 Port Status

This screen displays a port statistical summary with links to each port showing statistical details. To view the port statistics, click **MONITOR** > **Port Status** > **Port Status** to display the **Port Status** screen as shown next. You can also click the **Port Status** link in the **Quick Link** section of the **DASHBOARD** screen to see the following screen.

Figure 67 MONITOR > Port Status > Port Status



The following table describes the labels in this screen.

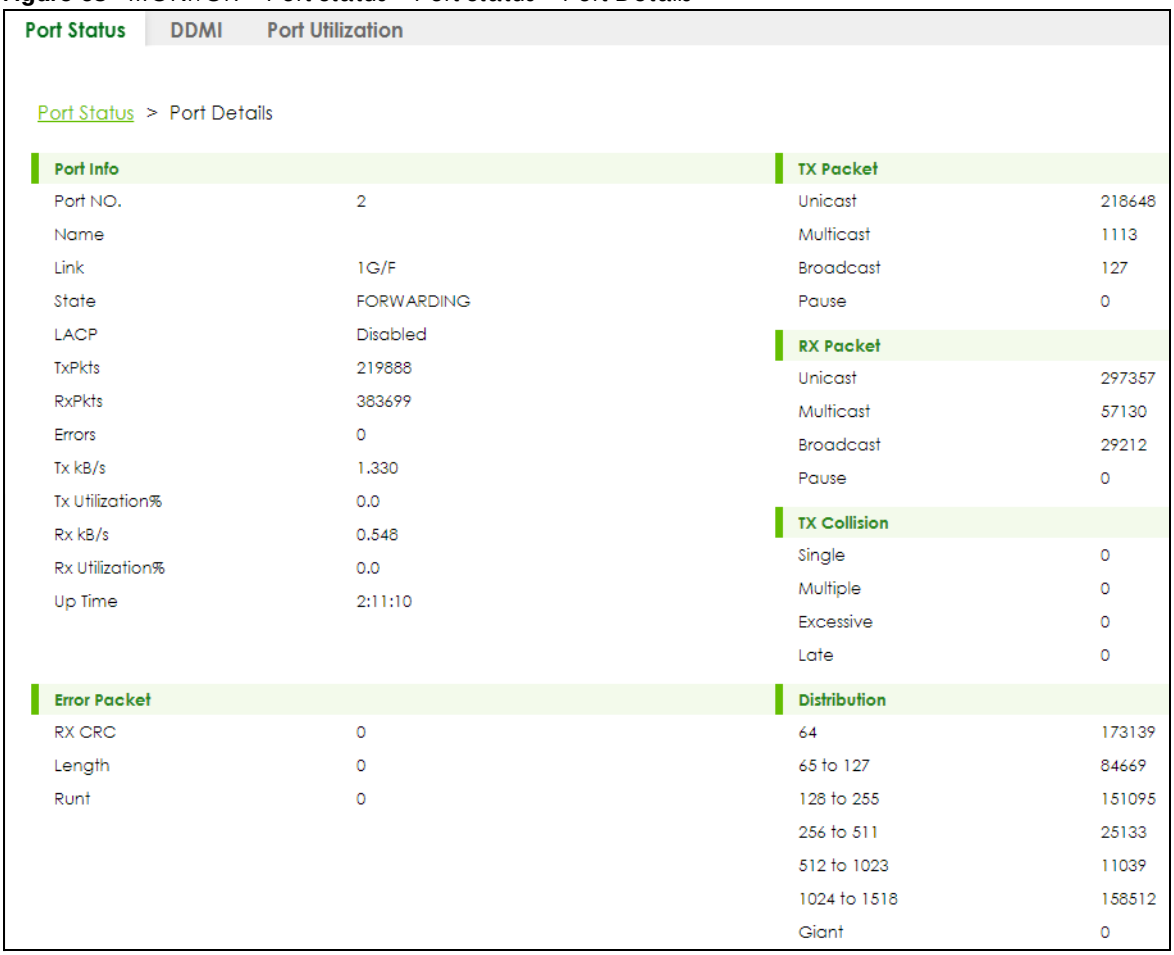
Table 20 MONITOR > Port Status > Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen.
Name	This is the name you assigned to this port in the **PORT** > **Port Setup** screen.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half). It also shows the cable type (**Copper** or **Fiber**) for the combo ports. This field displays **Down** if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**. When LACP (Link Aggregation Control Protocol) and STP are in blocking state, it displays **BLOCKING**.
PD	For PoE models only. This field displays whether or not a powered device (PD) is allowed to receive power from the Switch on this port.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx kB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx kB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear the counter	Select **Port**, enter a port number and then click **Clear Counter** to erase the recorded statistical information for that port, or select **ALL Ports** to clear statistics for all ports.

13.1.1 Port Details

Click an index in the **Port** column in the **MONITOR** > **Port Status** > **Port Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 68 MONITOR > Port Status > Port Status > Port Details



The following table describes the labels in this screen.

Table 21 MONITOR > Port Status > Port Status > Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**) for the combo ports. This field displays **Down** if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**. When LACP (Link Aggregation Control Protocol), STP, and dot1x are in blocking state, it displays **BLOCKING**.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx kB/s	This field shows the number of kilobytes per second transmitted on this port.

Table 21 MONITOR > Port Status > Port Status > Port Details (continued)

LABEL	DESCRIPTION
Tx Utilization%	This field shows the percentage of actual transmitted frames on this port as a percentage of the **Link** speed.
Rx kB/s	This field shows the number of kilobytes per second received on this port.
Rx Utilization%	This field shows the percentage of actual received frames on this port as a percentage of the **Link** speed.
Up Time	This field shows the total amount of time the connection has been up.
TX Packet The following fields display detailed information about packets transmitted.	
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good Multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x pause packets transmitted.
RX Packet The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good Multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x pause packets received.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet The following fields display detailed information about packets received that were in error.	
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) errors.
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65 to 127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128 to 255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256 to 511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.

Table 21 MONITOR > Port Status > Port Status > Port Details (continued)

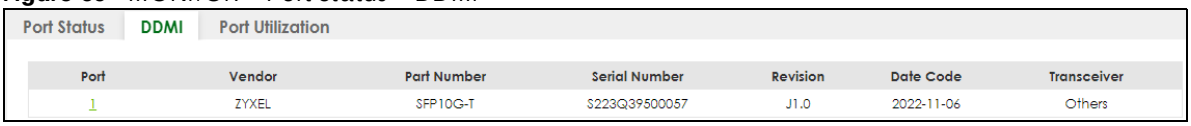
LABEL	DESCRIPTION
512 to 1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024 to 1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your switch model.

13.2 DDMI

The optical SFP transceiver's support for the Digital Diagnostics Monitoring Interface (DDMI) function lets you monitor the transceiver's parameters to perform component monitoring, fault isolation and failure prediction tasks. This allows proactive, preventative network maintenance to help ensure service continuity.

Use this screen to view the DDMI status of the Switch's SFP transceivers. Click **MONITOR** > **Port Status** > **DDMI** to see the following screen. Alternatively, click **DASHBOARD** from any Web Configurator screen and then the **Port Status** link in the **Quick Link** section of the **DASHBOARD** screen to display the **Port Status** screen and then click the **DDMI** link tab.

Figure 69 MONITOR > Port Status > DDMI



The following table describes the labels in this screen.

Table 22 MONITOR > Port Status > DDMI

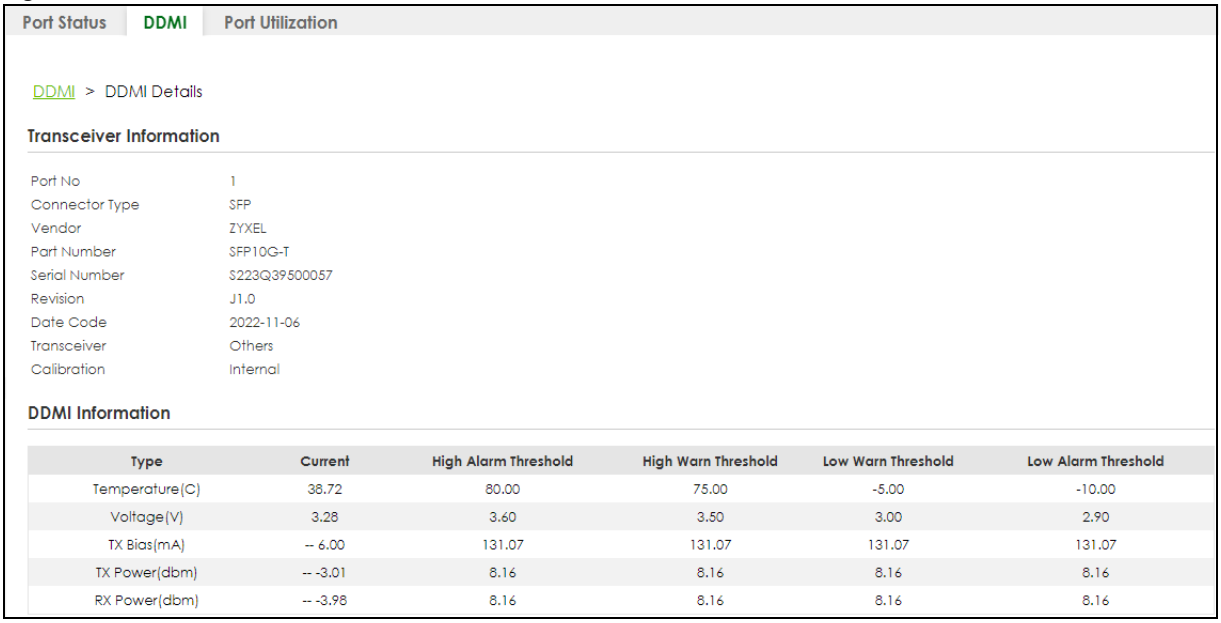
LABEL	DESCRIPTION
Port	This identifies the SFP port. Click a port number to display the **DDMI Details** screen.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays the type of optical transceiver installed in the SFP slot.

13.2.1 DDMI Details

Use this screen to view the real-time SFP (Small Form Factor Pluggable) transceiver information and operating parameters on the SFP port. The parameters include, for example, transmitting and receiving power, and module temperature.

Click an index in the **Port** column in the **DDMI** screen to view current transceivers' status.

Figure 70 MONITOR > Port Status > DDMI > DDMI Details



The following table describes the labels in this screen.

Table 23 MONITOR > Port Status > DDMI > DDMI Details

LABEL	DESCRIPTION
Transceiver Information	
Port No	This identifies the SFP port.
Connector Type	This displays the connector type of the optical transceiver.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays details about the type of transceiver installed in the SFP slot.
Calibration	This field is available only when an SFP transceiver is inserted into the SFP slot. **Internal** displays if the measurement values are calibrated by the transceiver. **External** displays if the measurement values are raw data which the Switch calibrates.
DDMI Information	
Type	This displays the DDMI parameter.
Temperature (C)	This displays the temperature inside the SFP transceiver in degrees Celsius.
Voltage (V)	This displays the level of voltage being supplied to the SFP transceiver.
TX Bias (mA)	This displays the milliamps (mA) being supplied to the SFP transceiver's Laser Diode Transmitter.
TX Power (dbm)	This displays the amount of power the SFP transceiver is transmitting.
RX Power (dbm)	This displays the amount of power the SFP transceiver is receiving from the fiber cable.
Current	This displays the current status for each monitored DDMI parameter.
High Alarm Threshold	This displays the high value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the Switch if the monitored DDMI parameter reaches this value.

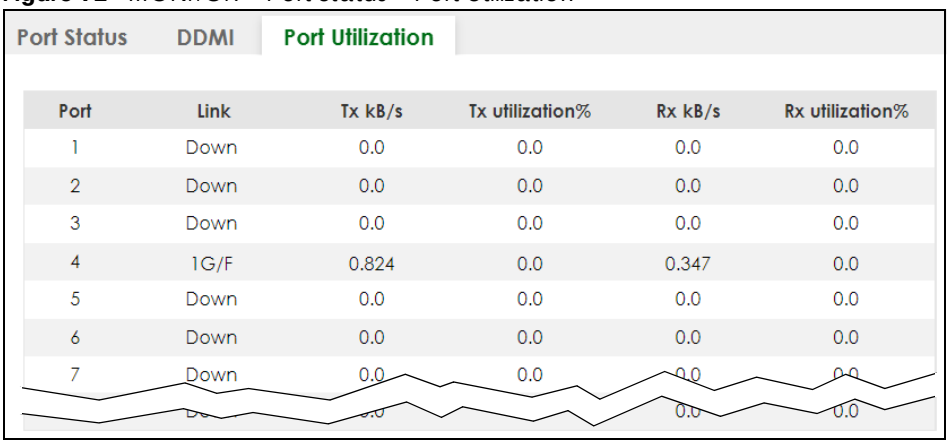
Table 23 MONITOR > Port Status > DDMI > DDMI Details (continued)

LABEL	DESCRIPTION
High Warn Threshold	This displays the high value warning threshold for each monitored DDMI parameter. A warning signal is reported to the Switch if the monitored DDMI parameter reaches this value.
Low Warn Threshold	This displays the low value warning threshold for each monitored DDMI parameter. A warning signal is reported to the Switch if the monitored DDMI parameter reaches this value.
Low Alarm Threshold	This displays the low value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the Switch if the monitored DDMI parameter reaches this value.

13.3 Port Utilization

This screen displays the percentage of actual transmitted or received frames on a port as a percentage of the **Link** speed. To view port utilization, click **MONITOR** > **Port Status** > **Port Utilization** to see the following screen. Alternatively, click **DASHBOARD** from any Web Configurator screen and then the **Port Status** link in the **Quick Link** section of the **DASHBOARD** screen to display the **Port Status** screen and then click the **Port Utilization** link tab.

Figure 71 MONITOR > Port Status > Port Utilization



The following table describes the labels in this screen.

Table 24 MONITOR > Port Status > Port Utilization

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Link	This field displays the speed (either **10M** for 10 Mbps, **100M** for 100 Mbps, or **1G** for 1 Gbps) and the duplex (**F** for full duplex). It also shows the cable type (**Copper** or **Fiber**) for the combo ports. This field displays **Down** if the port is not connected to any device.
Tx kB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Tx Utilization%	This field shows the percentage of actual transmitted frames on this port as a percentage of the **Link** speed.
Rx kB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Rx Utilization%	This field shows the percentage of actual received frames on this port as a percentage of the **Link** speed.

CHAPTER 14
System Information

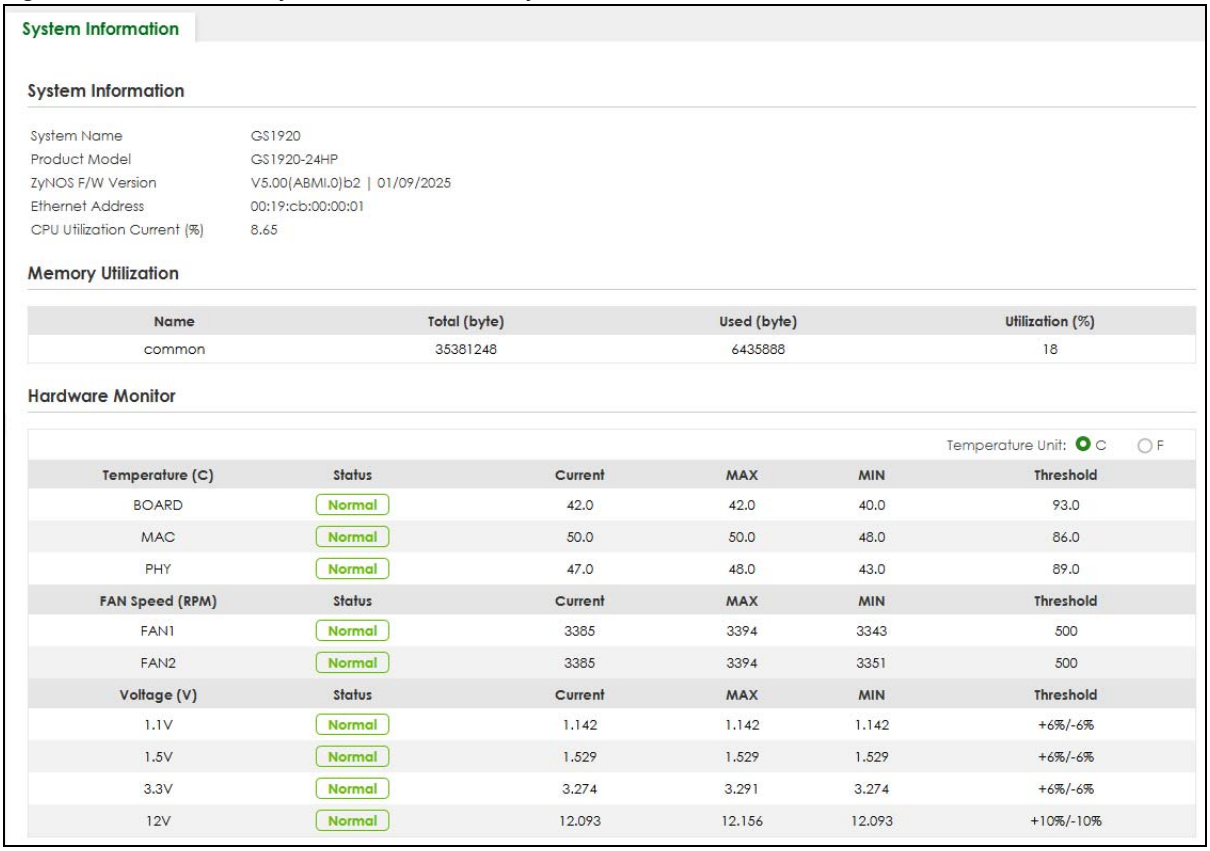
14.0.1 What You Can Do

Use the **System Information** screen (Section 14.1 on page 110) to view general system information and hardware status of the Switch.

14.1 System Information

In the navigation panel, click **MONITOR** > **System Information** > **System Information** to display the screen as shown. Use this screen to view general system information.

Figure 72 MONITOR > System Information > System Information



System Information

System Information

System Name	GS1920
Product Model	GS1920-24HP
ZyNOS F/W Version	V5.00(ABMI.0)b2 | 01/09/2025
Ethernet Address	00:19:cb:00:00:01
CPU Utilization Current (%)	8.65

Memory Utilization

Name	Total (byte)	Used (byte)	Utilization (%)
common	35381248	6435888	18

Hardware Monitor

Temperature Unit: C F

Temperature (C)	Status	Current	MAX	MIN	Threshold
BOARD	Normal	42.0	42.0	40.0	93.0
MAC	Normal	50.0	50.0	48.0	86.0
PHY	Normal	47.0	48.0	43.0	89.0
FAN Speed (RPM)	**Status**	**Current**	**MAX**	**MIN**	**Threshold**
FAN1	Normal	3385	3394	3343	500
FAN2	Normal	3385	3394	3351	500
Voltage (V)	**Status**	**Current**	**MAX**	**MIN**	**Threshold**
1.1V	Normal	1.142	1.142	1.142	+6%/-6%
1.5V	Normal	1.529	1.529	1.529	+6%/-6%
3.3V	Normal	3.274	3.291	3.274	+6%/-6%
12V	Normal	12.093	12.156	12.093	+10%/-10%

The following table describes the labels in this screen.

Table 25 MONITOR > System Information > System Information

LABEL	DESCRIPTION
System Information	
System Name	This displays the descriptive name of the Switch for identification purposes.
Product Model	This displays the product model of the Switch. Use this information when searching for firmware upgrade or looking for other support information in the website.
ZyNOS F/W Version	This displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This refers to the Ethernet MAC (Media Access Control) address of the Switch.
CPU Utilization Current (%)	This displays the current percentage of CPU utilization.
Memory Utilization Memory utilization shows how much DRAM memory is available and in use. It also displays the current percentage of memory utilization.	
Name	This displays the name of the memory pool.
Total (byte)	This displays the total number of bytes in this memory pool.
Used (byte)	This displays the number of bytes being used in this memory pool.
Utilization (%)	This displays the percentage (%) of memory being used in this memory pool.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature (C/F)	**BOARD** / **MAC** and **PHY**/**POWER** refers to the location of the temperature sensor on the Switch printed circuit board.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.

Table 25 MONITOR > System Information > System Information (continued)

LABEL	DESCRIPTION
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.

CHAPTER 15
System Log

15.1 System Log Overview

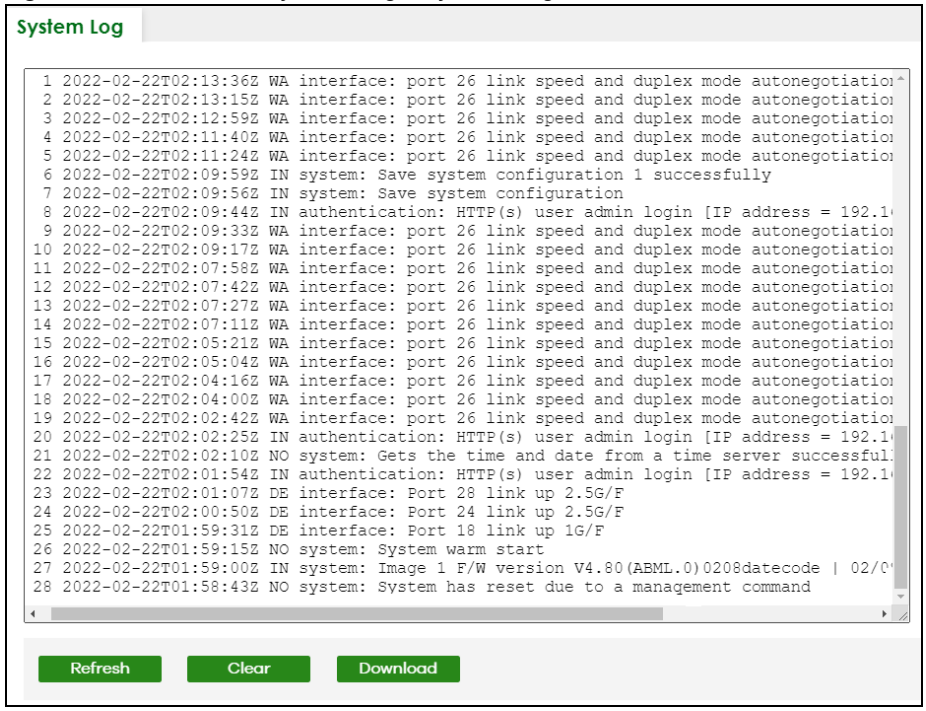
A log message stores the system history information for viewing.

15.2 System Log

Click **MONITOR** > **System Log** > **System Log** in the navigation panel to open this screen. Use this screen to check current system logs.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

Figure 73 MONITOR > System Log > System Log



The summary table shows the time the log message was recorded and the reason the log message was generated. Click **Refresh** to update this screen. Click **Clear** to clear the whole log, regardless of what is currently displayed on the screen. Click **Download** to save the log to your computer.

CHAPTER 16
SYSTEM

The following chapters introduces the configurations of the links under the **SYSTEM** navigation panel.

Quick links to chapters:

CHAPTER 17
Cloud Management

17.1 Cloud Management Overview

The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula APs, Ethernet switches and security gateways.

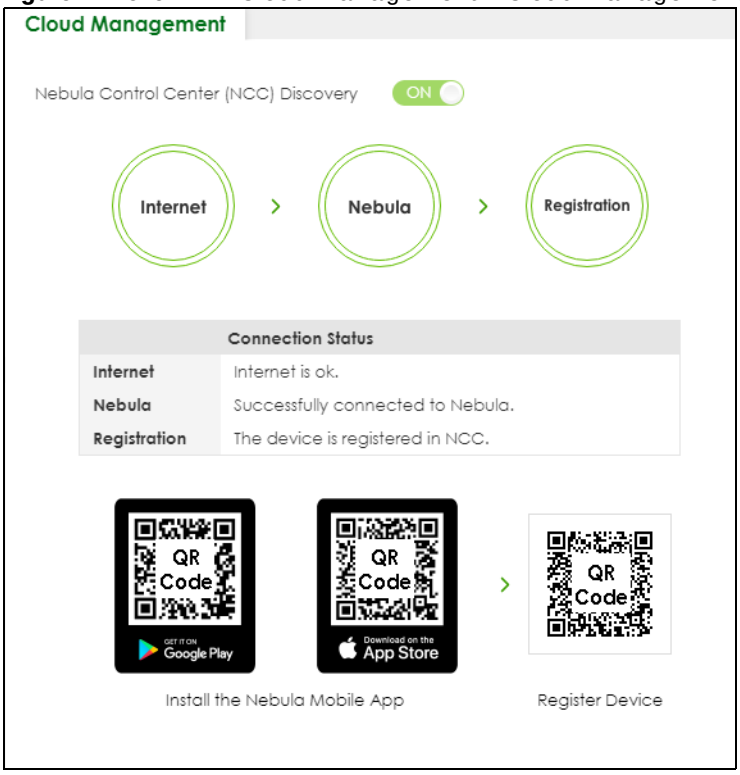
The Switch is managed and provisioned automatically by the NCC (Nebula Control Center) when:

- It is connected to the Internet.
- The **Nebula Control Center (NCC) Discovery** feature is enabled.
- It has been registered in the NCC.

17.2 Nebula Center Control Discovery

Click **SYSTEM** > **Cloud Management** > **Cloud Management** to display this screen.

Figure 74 SYSTEM > Cloud Management > Cloud Management



The following table describes the labels in this screen.

Table 26 SYSTEM > Cloud Management > Cloud Management

LABEL	DESCRIPTION
Nebula Control Center (NCC) Discovery	Enable the switch button to turn on Nebula Control Center (NCC) discovery on the Switch. This field displays: • The Switch Internet connection status. • The connection status between the Switch and NCC. • The Switch registration status on NCC. To pass your Switch management to NCC, first make sure your Switch is connected to the Internet. Then go to NCC and register your Switch. **1. Internet** Green – The Switch is connected to the Internet. Orange – The Switch is not connected to the Internet. **2. Nebula** Green – The Switch is connected to NCC. Orange – The Switch is not connected to NCC. **3. Registration** Green – The Switch is registered on NCC. Gray – The Switch is not registered on NCC. Note: All circles will gray out if you disable Nebula Discovery.
Connection Status	This table displays the NCC connection status information. Use status logs in the **Internet**, **Nebula**, and **Registration** fields for connection troubleshooting.

Cloud Management Mode

Enable the switch button to turn on NCC discovery on the Switch. If the Switch has Internet access and has been registered on the NCC, it will automatically go into cloud management mode. Follow the steps to register your Switch on NCC:

1 Download the Nebula Mobile App

First, download the app from the Google Play store for Android devices or the App Store for iOS devices and create an organization and site.

You can scan an app store QR code to open the app installation page on the app store.

2 Scan the Device QR code

The **Register Device** QR code in this screen contains the Switch's serial number and the registration MAC address for handy NCC registration of the Switch using the Nebula Mobile app.

Follow the wizard in the Nebula Mobile app to scan the QR code to register the Switch on NCC and add the Switch into a site.

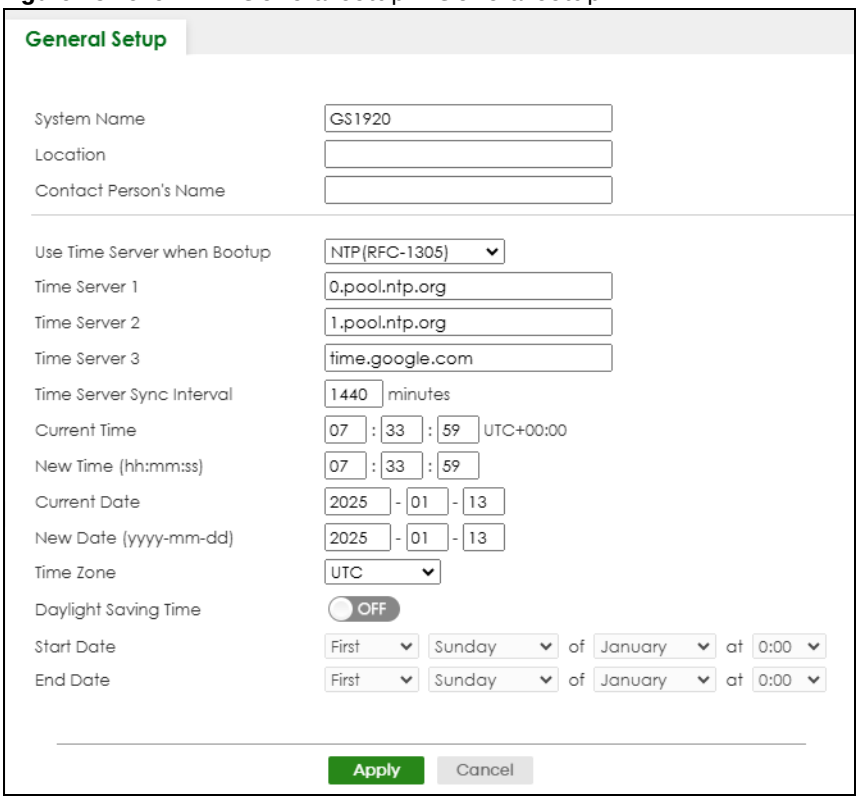
If **Nebula Control Center (NCC) Discovery** is disabled, the Switch will NOT discover the NCC and remain in Standalone mode.

CHAPTER 18
General Setup

18.1 General Setup

Use this screen to configure general settings such as the system name and time. Click **SYSTEM** > **General Setup** > **General Setup** in the navigation panel to display the screen as shown.

Figure 75 SYSTEM > General Setup > General Setup



Note: The input string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

Table 27 SYSTEM > General Setup > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable ASCII characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 128 printable ASCII characters; spaces are allowed.

Table 27 SYSTEM > General Setup > General Setup (continued)

LABEL	DESCRIPTION
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Enter the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC-867)** format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 00:00:00. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None** is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 2022-01-01 00:00:00.
Time Server 1/2/3	Enter the IPv4 / IPv6 address or domain name of your time server. The Switch searches for the first, then the second, then the third time server for around 60 seconds.
Time Server Sync Interval	Enter the period in minutes between each time server synchronization. The Switch checks the time server after every synchronization interval.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Enable the switch button if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 27 SYSTEM > General Setup > General Setup (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.

CHAPTER 19
Interface Setup

19.1 Interface Setup Overview

This chapter shows you how to create virtual interfaces for interface-based configurations. An IPv6 address is configured on a per-interface basis. The interface can be a physical interface (for example, an Ethernet port) or a virtual interface (for example, a VLAN).

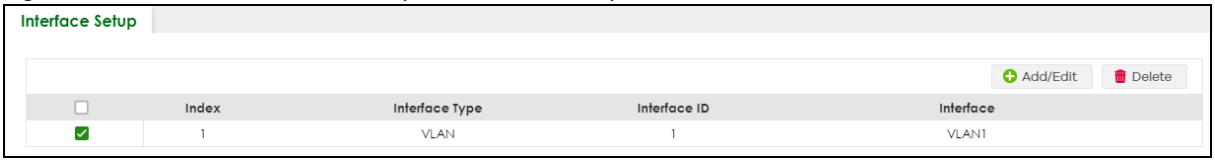
19.2 Interface Setup

Use this screen to view and set IPv6 interfaces on which you can configure an IPv6 address to access and manage the Switch.

The interfaces you create here will only take effect after you configure them in the **SYSTEM** > **IPv6** screens.

Click **SYSTEM** > **Interface Setup** > **Interface Setup** in the navigation panel to display the configuration screen.

Figure 76 SYSTEM > Interface Setup > Interface Setup



The following table describes the labels in this screen.

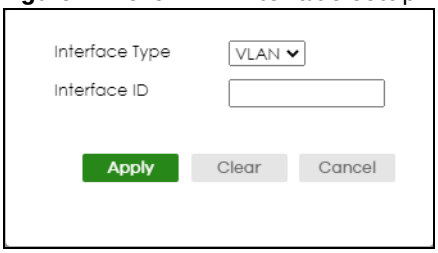
Table 28 SYSTEM > Interface Setup > Interface Setup

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Interface Type	This field displays the type of interface.
Interface ID	This field displays the identification number of the interface.
Interface	This field displays the interface's descriptive name which is generated automatically by the Switch. The name is from a combination of the interface type and ID number.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new interface or edit a selected one.
Delete	Click **Delete** to remove the selected interfaces.

19.2.1 Add/Edit Interfaces

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM** > **Interface Setup** > **Interface Setup** screen to display the configuration screen.

Figure 77 SYSTEM > Interface Setup > Interface Setup > Add/Edit



The following table describes the labels in this screen.

Table 29 SYSTEM > Interface Setup > Interface Setup > Add/Edit

LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **SWITCHING** > **VLAN** screens.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 20
IP Setup

20.1 IP Setup Overview

This chapter shows you how to configure IP settings and set up IP interfaces on the Switch using the **IP Setup** screens.

20.1.1 What You Can Do

- Use the **IP Status** screen (Section 20.2 on page 122) to view the current IP interfaces and DNS server settings on the Switch.
- Use the **IP Setup** screen (Section 20.3 on page 125) to configure the default gateway device, the default domain name server and add IP domains.
- Use the **Network Proxy Configuration** screen (Section 20.4 on page 127) to configure network proxy configurations.

20.1.2 IP Interfaces

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.

On the Switch, an IP address is not bound to any physical ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the Switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

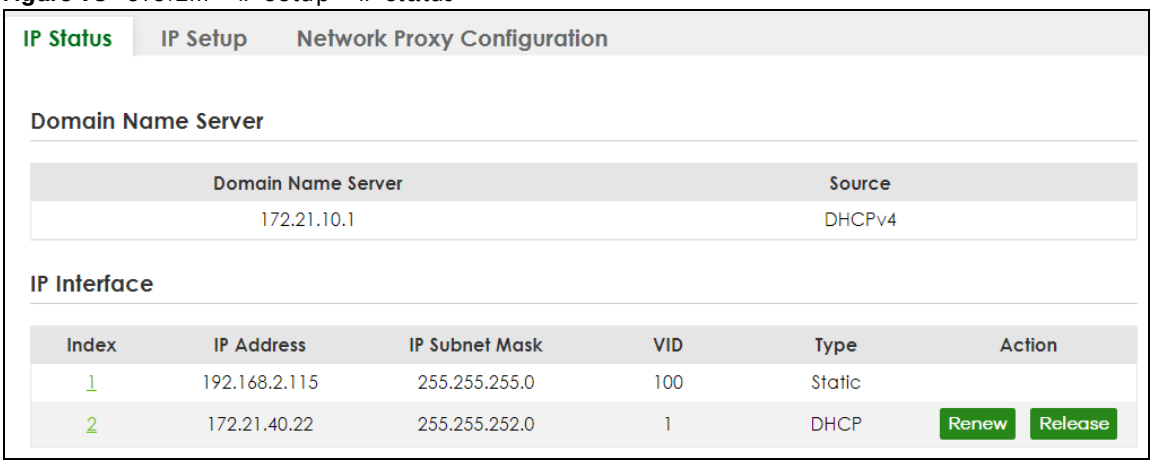
You can configure up to 64 IP domains which are used to access and manage the Switch from the ports belonging to the pre-defined VLANs.

Note: You must configure a VLAN first. Each VLAN can only have one management IP address.

20.2 IP Status

Click **SYSTEM** > **IP Setup** > **IP Status** to display the screen as shown.

Figure 78 SYSTEM > IP Setup > IP Status



The following table describes the labels in this screen.

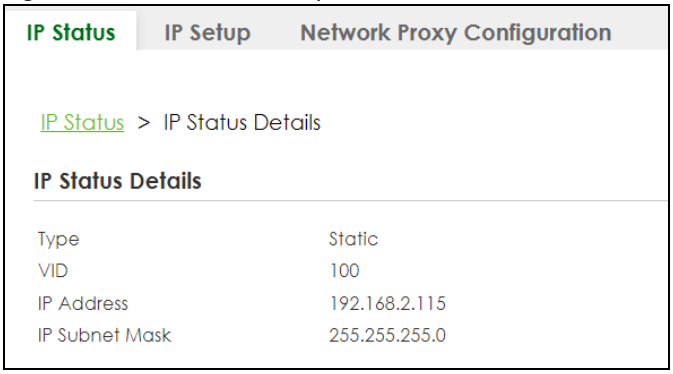
Table 30 SYSTEM > IP Setup > IP Status

LABEL	DESCRIPTION
Domain Name Server	
Domain Name Server	This field displays the IP address of the DNS server.
Source	This field displays whether the DNS server address is configured manually (**Static**) or obtained automatically using **DHCPv4**.
IP Interface	
Index	This field displays the index number of an entry.
IP Address	This field displays the IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Type	This shows whether this IP address is dynamically assigned from a DHCP server (**DHCP**) or manually assigned (**Static**).
Renew	Click this to renew the dynamic IP address.
Release	Click this to release the dynamic IP address.

20.2.1 IP Status Details

Use this screen to view IP status details. Click a number in the **Index** column in the **SYSTEM** > **IP Setup** > **IP Status** screen to display the screen as shown next.

Figure 79 SYSTEM > IP Setup > IP Status > IP Status Details: Static

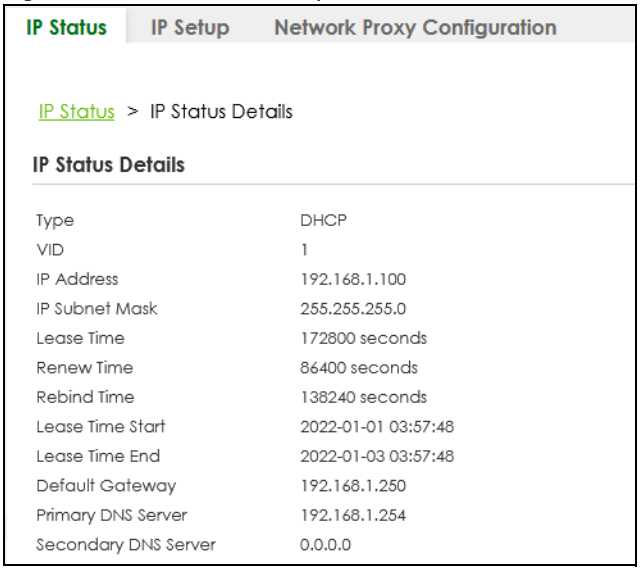


The following table describes the labels in this screen.

Table 31 SYSTEM > IP Setup > IP Status > IP Status Details: Static

LABEL	DESCRIPTION
Type	This shows the IP address is manually assigned (**Static**).
VID	This is the VLAN identification number to which an IP routing domain belongs.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.

Figure 80 SYSTEM > IP Setup > IP Status > IP Status Details: DHCP



The following table describes the labels in this screen.

Table 32 SYSTEM > IP Setup > IP Status > IP Status Details: DHCP

LABEL	DESCRIPTION
Type	This shows the IP address is dynamically assigned from a DHCP server (**DHCP**).
VID	This is the VLAN identification number to which an IP routing domain belongs.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Lease Time	This displays the length of time in seconds that this interface can use the current dynamic IP address from the DHCP server.

Table 32 SYSTEM > IP Setup > IP Status > IP Status Details: DHCP (continued)

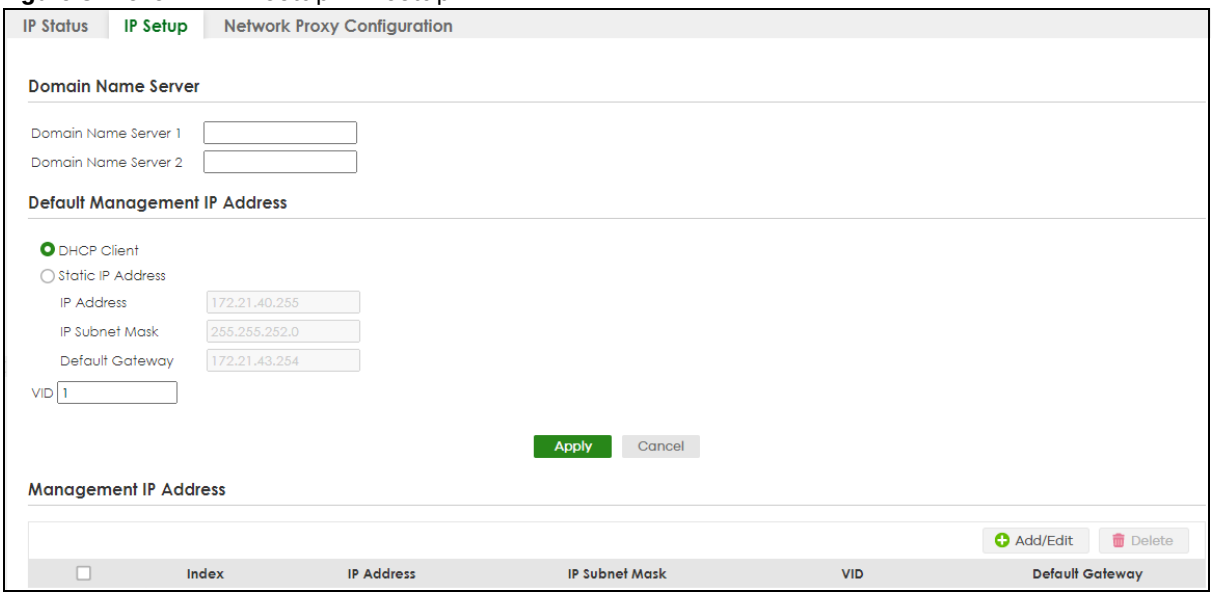
LABEL	DESCRIPTION
Renew Time	This displays the length of time from the lease start that the Switch will request to renew its current dynamic IP address from the DHCP server.
Rebind Time	This displays the length of time from the lease start that the Switch will request to get any dynamic IP address from the DHCP server.
Lease Time Start	This displays the date and time that the current dynamic IP address assignment from the DHCP server began. You should configure date and time in **SYSTEM** > **General Setup** > **General Setup**.
Lease Time End	This displays the date and time that the current dynamic IP address assignment from the DHCP server will end. You should configure date and time in **SYSTEM** > **General Setup** > **General Setup**.
Default Gateway	This displays the IP address of the default gateway assigned by the DHCP server. 0.0.0.0 means no gateway is assigned.
Primary / Secondary DNS Server	This displays the IP address of the primary and secondary DNS servers assigned by the DHCP server. 0.0.0.0 means no DNS server is assigned.

20.3 IP Setup

Use this screen to configure the default gateway device, the default domain name server and add IP domains. Click **SYSTEM** > **IP Setup** > **IP Setup** in the navigation panel to display the screen as shown.

Note: The Switch allows you to set a static IP interface in the same subnet that already has a DHCP-assigned IP interface on the Switch. The Switch will use the static IP you set and the DHCP-assigned IP will be set to 0.0.0.0.

Figure 81 SYSTEM > IP Setup > IP Setup



The following table describes the labels in this screen.

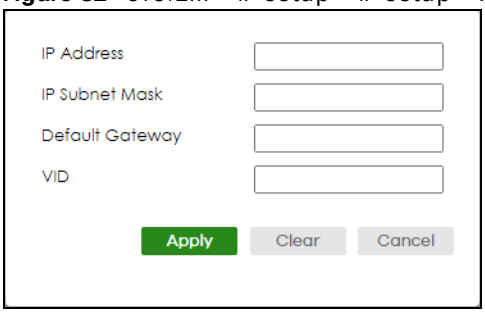
Table 33 SYSTEM > IP Setup > IP Setup

LABEL	DESCRIPTION
Domain Name Server	
Domain Name Server 1/2	Enter a domain name server IPv4 address in order to be able to use a domain name instead of an IP address.
Default Management IP Address Use these fields to create or edit IP routing domains on the Switch.	
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you do not have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 172.21.40.x. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.252.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 172.21.43.254.
VID	Enter the VLAN identification number associated with the Switch IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "Management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the Switch make sure the port that you are connected to is a member of Management VLAN. Note: Mis-configuring the management VLAN ID might cause the Switch to become inaccessible.
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.
Management IP Address	
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Default Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation.
Add/Edit	Click **Add/Edit** to add a new management port setting or edit a selected one.
Delete	Click **Delete** to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the Switch.

20.3.1 Add/Edit IP Interfaces

Use this screen to add or edit IP interfaces. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM** > **IP Setup** > **IP Setup** screen to display this screen.

Figure 82 SYSTEM > IP Setup > IP Setup > Add/Edit



The following table describes the labels in this screen.

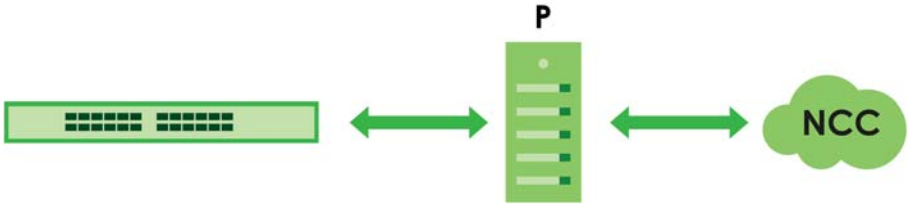
Table 34 SYSTEM > IP Setup > IP Setup > Add/Edit

LABEL	DESCRIPTION
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 172.21.40.x. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.252.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 172.21.43.254.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

20.4 Network Proxy Configuration

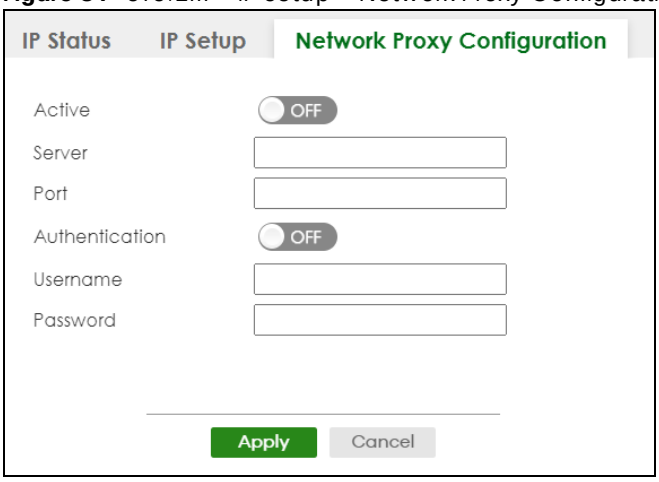
The proxy server of an organization may prohibit communication between the Switch and NCC (Nebula Control Center) (See Section 17.1 on page 115). Use this screen to enable communication between the Switch and NCC through the proxy server (**P**).

Figure 83 Network Proxy Configuration Application



As of this writing, this setting only allows communication between the Switch and the NCC.

Figure 84 SYSTEM > IP Setup > Network Proxy Configuration



The following table describes the labels in this screen.

Table 35 SYSTEM > IP Setup > Network Proxy Configuration

LABEL	DESCRIPTION
Active	Enable the switch button to enable communication between the Switch and NCC through a proxy server.
Server	Enter the IP address (dotted decimal notation) or host name of the proxy server. When entering the host name, up to 128 alphanumeric characters are allowed for the **Server** except [?], [|], ['], or ["].
Port	Enter the port number of the proxy server (1 – 65535).
Authentication	Enable the switch button to enable proxy server authentication using a **Username** and **Password**.
Username	Enter a login user name from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the **Username**. The string should not contain [?], [|], ['], ["], [,], [:], or space.
Password	Enter a login password from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the **Password** except [?], [|], ['], and ["].
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 21
IPv6

21.1 IPv6 Overview

This chapter introduces the **IPv6** screens.

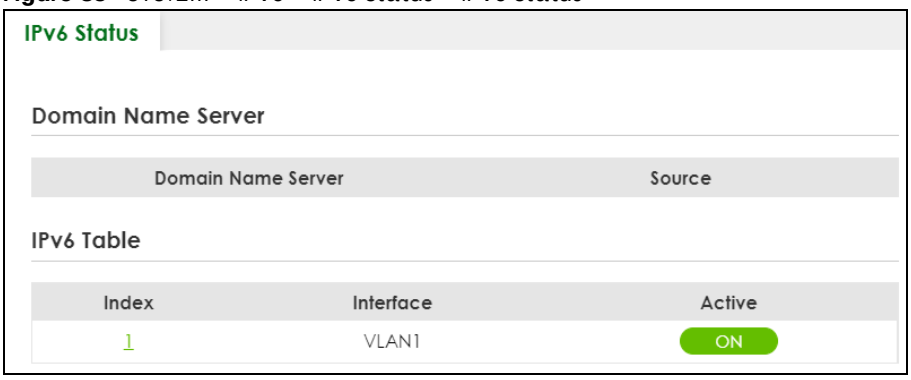
21.1.1 What You Can Do

- Use the **IPv6 Status** screen (Section 21.2 on page 129) to view the IPv6 table and DNS server information.
- Use the **IPv6 Global Setup** screen (Section 21.3 on page 132) to configure the global IPv6 settings.
- Use the **IPv6 Interface Setup** screen (Section 21.4 on page 133) to view and configure IPv6 interfaces.
- Use the **IPv6 Link-Local Address Setup** screen (Section 21.5 on page 134) to view and configure IPv6 link-local addresses.
- Use the **IPv6 Global Address Setup** screen (Section 21.6 on page 135) to view and configure IPv6 global addresses.
- Use the **IPv6 Neighbor Discovery Setup** screen (Section 21.7 on page 137) to view and configure neighbor discovery settings on each interface.
- Use the **IPv6 Neighbor Setup** screen (Section 21.8 on page 138) to configure static IPv6 neighbor entries in the Switch's IPv6 neighbor table.
- Use the**DHCPv6 Client Setup** screen (Section 21.9 on page 140) to configure the Switch's DHCP settings when it is acting as a DHCPv6 client.

21.2 IPv6 Status

Click **SYSTEM** > **IPv6** > **IPv6 Status** > **IPv6 Status** in the navigation panel to display the IPv6 status screen as shown next.

Figure 85 SYSTEM > IPv6 > IPv6 Status > IPv6 Status



The following table describes the labels in this screen.

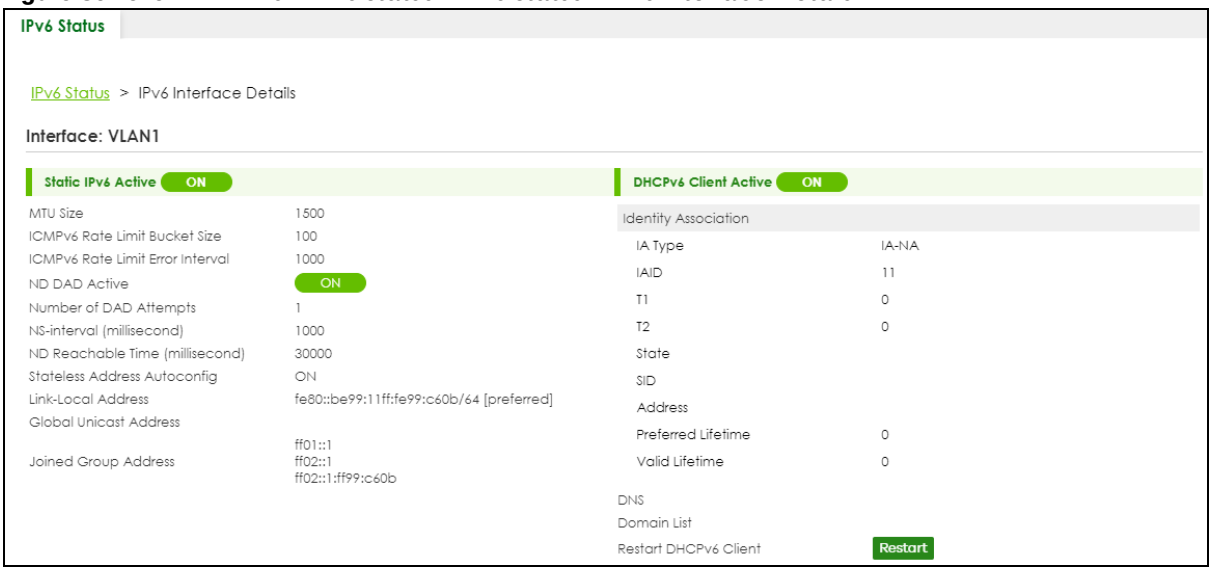
Table 36 SYSTEM > IPv6 > IPv6 Status > IPv6 Status

LABEL	DESCRIPTION
Domain Name Server	
Domain Name Server	This field displays the IP address of the DNS server.
Source	This field displays whether the DNS server address is configured manually (**Static**) or obtained automatically using **DHCPv6**.
IPv6 Table	
Index	This field displays the index number of an IPv6 interface. Click on an index number to view more interface details.
Interface	This is the name of the IPv6 interface you created.
Active	This field displays whether the IPv6 interface is activated or not.

21.2.1 IPv6 Interface Status Details

Use this screen to view a specific IPv6 interface status and detailed information. Click an interface index number in the **SYSTEM** > **IPv6** > **IPv6 Status** > **IPv6 Status** screen. The following screen opens.

Figure 86 SYSTEM > IPv6 > IPv6 Status > IPv6 Status > IPv6 Interface Details



The following table describes the labels in this screen.

Table 37 SYSTEM > IPv6 > IPv6 Status > IPv6 Status > IPv6 Interface Details

LABEL	DESCRIPTION
Static IPv6 Active This field displays whether the IPv6 interface is activated or not.	
MTU Size	This field displays the Maximum Transmission Unit (MTU) size for IPv6 packets on this interface.
ICMPv6 Rate Limit Bucket Size	This field displays the maximum number of ICMPv6 error messages which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.
ICMPv6 Rate Limit Error Interval	This field displays the time period (in milliseconds) during which ICMPv6 error messages of up to the bucket size can be transmitted. 0 means no limit.
ND DAD Active	This field displays whether Neighbor Discovery (ND) Duplicate Address Detection (DAD) is enabled on the interface.
Number of DAD Attempts	This field displays the number of consecutive neighbor solicitations the Switch sends for this interface.
NS-Interval (millisecond)	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
ND Reachable Time (millisecond)	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.
Stateless Address Autoconfig	This field displays whether the Switch's interface can automatically generate a link-local address through stateless auto-configuration.
Link-Local Address	This field displays the Switch's link-local IP address and prefix generated by the interface. It also shows whether the IP address is preferred, which means it is a valid address and can be used as a sender or receiver address.
Global Unicast Address	This field displays the Switch's global unicast address to identify this interface.
Joined Group Address	This field displays the IPv6 multicast addresses of groups the Switch's interface joins.
DHCPv6 Client Active This field displays whether the Switch acts as a DHCPv6 client to get an IPv6 address from a DHCPv6 server.	
Identity Association An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface.	
IA Type	The IA type is the type of address in the IA. Each IA holds one type of address. **IA_NA** means an identity association for non-temporary addresses and **IA_TA** is an identity association for temporary addresses.
IAID	Each IA consists of a unique IAID and associated IP information.
T1	This field displays the DHCPv6 T1 timer. After T1, the Switch sends the DHCPv6 server a Renew message. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire.
T2	This field displays the DHCPv6 T2 timer. If the time T2 is reached and the server does not respond, the Switch sends a Rebind message to any available server.

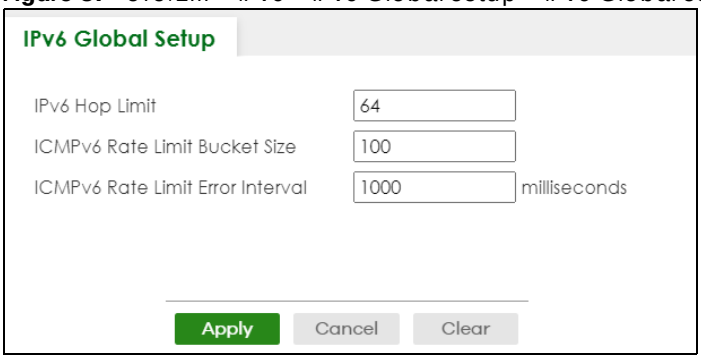
Table 37 SYSTEM > IPv6 > IPv6 Status > IPv6 Status > IPv6 Interface Details (continued)

LABEL	DESCRIPTION
State	This field displays the state of the TA. It shows **Active** when the Switch obtains addresses from a DHCpv6 server and the TA is created. **Renew** when the TA's address lifetime expires and the Switch sends out a Renew message. **Rebind** when the Switch does not receive a response from the original DHCPv6 server and sends out a Rebind message to another DHCPv6 server.
SID	This field displays the DHCPv6 server's unique ID.
Address	This field displays the Switch's global address which is assigned by the DHCPv6 server.
Preferred Lifetime	This field displays how long (in seconds) that the global address remains preferred.
Valid Lifetime	This field displays how long (in seconds) that the global address is valid.
DNS	This field displays the DNS server address assigned by the DHCPv6 server.
Domain List	This field displays the address record when the Switch queries the DNS server to resolve domain names.
Restart DHCPv6 Client	Click **Restart** to send a new DHCP request to the DHCPv6 server and update the IPv6 address and DNS information for this interface.

21.3 IPv6 Global Setup

Use this screen to configure the global IPv6 settings. Click **SYSTEM** > **IPv6** > **IPv6 Global Setup** > **IPv6 Global Setup** to display the screen as shown next.

Figure 87 SYSTEM > IPv6 > IPv6 Global Setup > IPv6 Global Setup



The following table describes the labels in this screen.

Table 38 SYSTEM > IPv6 > IPv6 Global Setup > IPv6 Global Setup

LABEL	DESCRIPTION
IPv6 Hop Limit	Specify the maximum number of hops (from 1 to 255) in router advertisements. This is the maximum number of hops on which an IPv6 packet is allowed to transmit before it is discarded by an IPv6 router, which is similar to the TTL field in IPv4.
ICMPv6 Rate Limit Bucket Size	Specify the maximum number of ICMPv6 error messages (from 1 to 200) which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.

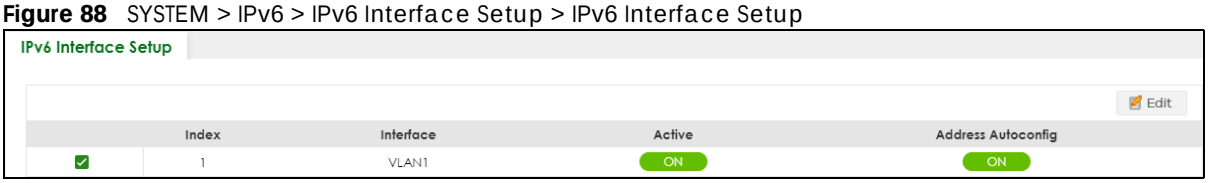
Table 38 SYSTEM > IPv6 > IPv6 Global Setup > IPv6 Global Setup (continued)

LABEL	DESCRIPTION
ICMPv6 Rate Limit Error Interval	Specify the time period (from 0 to 2147483647 milliseconds) during which ICMPv6 error messages of up to the bucket size can be transmitted. 0 means no limit.
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.
Clear	Click **Clear** to reset the fields to the factory defaults.

21.4 IPv6 Interface Setup

Use this screen to view and configure an IPv6 interface you create in the **SYSTEM** > **Interface Setup** screen. Click **SYSTEM** > **IPv6** > **IPv6 Interface Setup** > **IPv6 Interface Setup** to display the screen as shown next.

Figure 88 SYSTEM > IPv6 > IPv6 Interface Setup > IPv6 Interface Setup



The following table describes the labels in this screen.

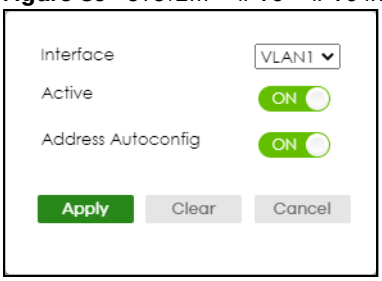
Table 39 SYSTEM > IPv6 > IPv6 Interface Setup > IPv6 Interface Setup

LABEL	DESCRIPTION
Index	This is the interface index number.
Interface	This is the name of the IPv6 interface you created.
Active	This field displays whether the IPv6 interface is activated or not.
Address Autoconfig	This field displays whether stateless auto-configuration is enabled on the interface.
	Select an entry's checkbox to select a specific entry.
Edit	Click **Edit** to edit the selected interface.

21.4.1 Edit an IPv6 Interface

Use this screen to turn on or off an IPv6 interface you create in the **SYSTEM** > **Interface Setup** > **Interface Setup** screen. Select an entry and click **Edit** in the **SYSTEM** > **IPv6** > **IPv6 Interface Setup** > **IPv6 Interface Setup** screen to display the screen as shown next.

Figure 89 SYSTEM > IPv6 > IPv6 Interface Setup > IPv6 Interface Setup > Edit



The following table describes the labels in this screen.

Table 40 SYSTEM > IPv6 > IPv6 Interface Setup > IPv6 Interface Setup > Edit

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Active	Enable the switch button to enable the interface.
Address Autoconfig	Select this option to allow the interface to automatically generate a link-local address through stateless auto-configuration.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

21.5 IPv6 Link-Local Address Setup

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10.

Use this screen to view and configure the interface's link-local address and default gateway. Click **SYSTEM** > **IPv6** > **IPv6 Addressing** > **IPv6 Link-Local Address Setup** to display the screen as shown next.

Note: You should first create an IPv6 interface in the **SYSTEM** > **Interface Setup** > **Interface Setup** screen.

Figure 90 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Link-Local Address Setup

The following table describes the labels in this screen.

Table 41 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Link-Local Address Setup

LABEL	DESCRIPTION
Index	This is the interface index number.
Interface	This is the name of the IPv6 interface you created.

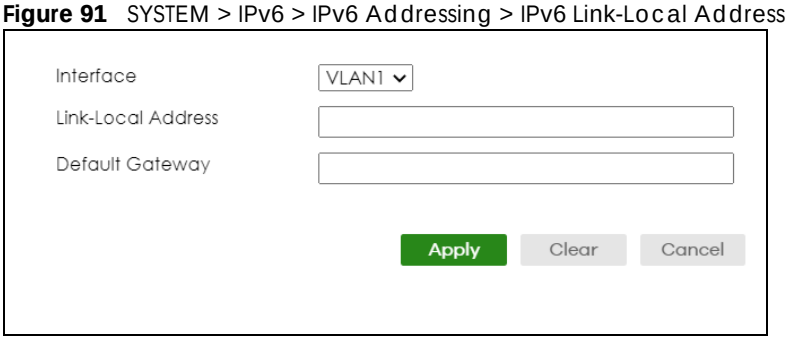
Table 41 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Link-Local Address Setup (continued)

LABEL	DESCRIPTION
IPv6 Link-Local Address	This is the static IPv6 link-local address for the interface.
IPv6 Default Gateway	This is the default gateway IPv6 address for the interface.
	Select an entry's checkbox to select a specific entry.
Edit	Click **Edit** to edit the selected entry.

21.5.1 Edit an IPv6 Link-Local Address

Use this screen to configure the link-local address and default gateway of an IPv6 interface you create in the **SYSTEM** > **Interface Setup** screen. Select an entry and click **Edit** in the **SYSTEM** > **IPv6** > **IPv6 Addressing** > **IPv6 Link-Local Address Setup** screen to display this screen.

Figure 91 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Link-Local Address Setup > Edit



The following table describes the labels in this screen.

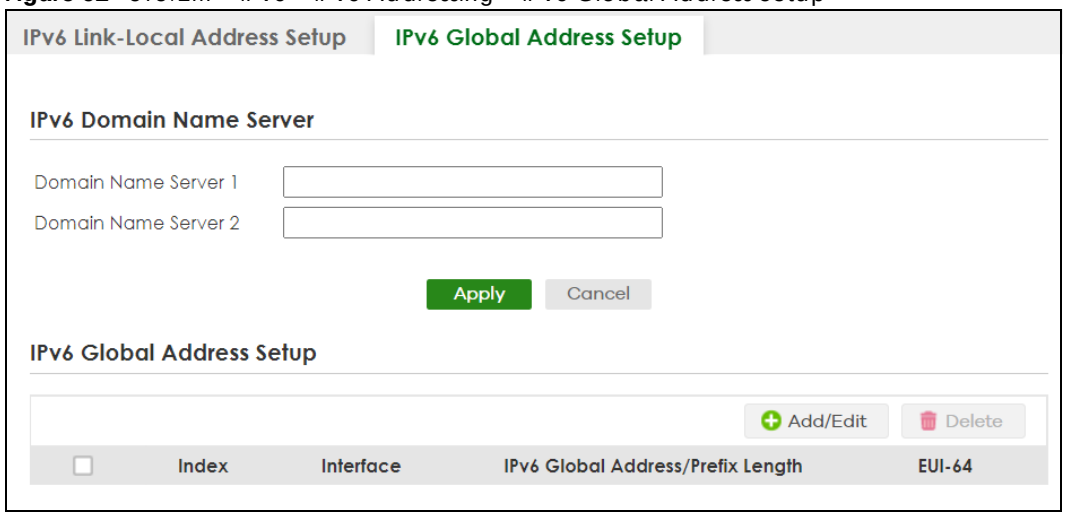
Table 42 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Link-Local Address Setup > Edit

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Link-Local Address	Manually configure a static IPv6 link-local address for the interface.
Default Gateway	Set the default gateway IPv6 address for the interface. When an interface cannot find a routing information for a frame's destination, it forwards the packet to the default gateway.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

21.6 IPv6 Global Address Setup

Use this screen to view and configure the interface's IPv6 global address. Click **SYSTEM** > **IPv6 Addressing** > **IPv6 Global Address Setup** to display the screen as shown next.

Figure 92 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Global Address Setup



The following table describes the labels in this screen.

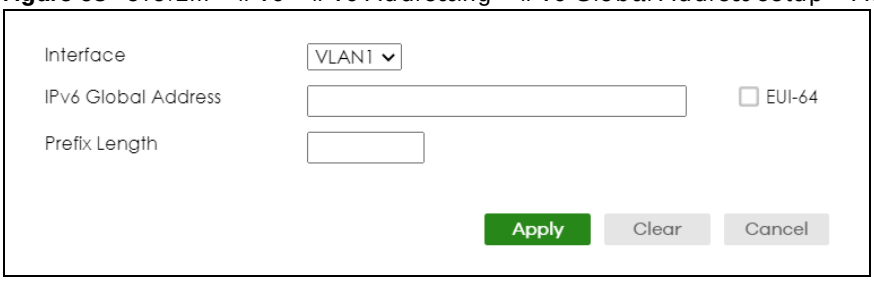
Table 43 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Global Address Setup

LABEL	DESCRIPTION
IPv6 Domain Name Server	
Domain Name Server 1/2	Enter a domain name server IPv6 address in order to be able to use a domain name instead of an IP address.
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 this to reset the **Domain Name Server** values in this screen to their last-saved values.
IPv6 Global Address Setup	
Index	This is the interface index number.
Interface	This is the name of the IPv6 interface you created.
IPv6 Global Address/Prefix Length	This field displays the IPv6 global address and prefix length for the interface.
EUI-64	This shows whether the interface ID of the global address is generated using the EUI-64 format.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

21.6.1 Add/Edit an IPv6 Global Address

Use this screen to configure the interface's IPv6 global address. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM** > **IPv6** > **IPv6 Addressing** > **IPv6 Global Address Setup** screen to display this screen.

Figure 93 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Global Address Setup > Add/Edit



The following table describes the labels in this screen.

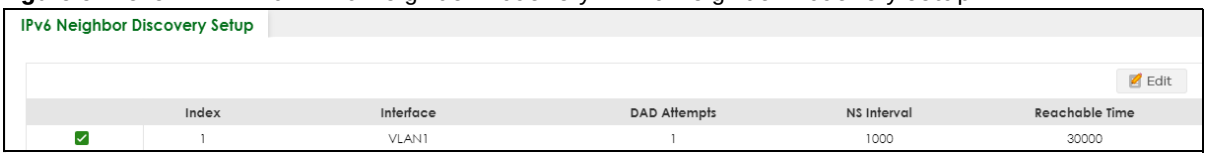
Table 44 SYSTEM > IPv6 > IPv6 Addressing > IPv6 Global Address Setup > Add/Edit

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IPv6 Global Address	Manually configure a static IPv6 global address for the interface.
Prefix Length	Specify an IPv6 prefix length that specifies how many most significant bits (start from the left) in the address compose the network address.
EUI-64	Select this option to have the interface ID be generated automatically using the EUI-64 format.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

21.7 IPv6 Neighbor Discovery Setup

Use this screen to configure neighbor discovery settings for each interface. Click **SYSTEM** > **IPv6** > **IPv6 Neighbor Discovery** > **IPv6 Neighbor Discovery Setup** to display the screen as shown next.

Figure 94 SYSTEM > IPv6 > IPv6 Neighbor Discovery > IPv6 Neighbor Discovery Setup



The following table describes the labels in this screen.

Table 45 SYSTEM > IPv6 > IPv6 Neighbor Discovery > IPv6 Neighbor Discovery Setup

LABEL	DESCRIPTION
Index	This is the interface index number.
Interface	This is the name of the IPv6 interface you created.
DAD Attempts	This field displays the number of consecutive neighbor solicitations the Switch sends for this interface.
NS Interval	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.

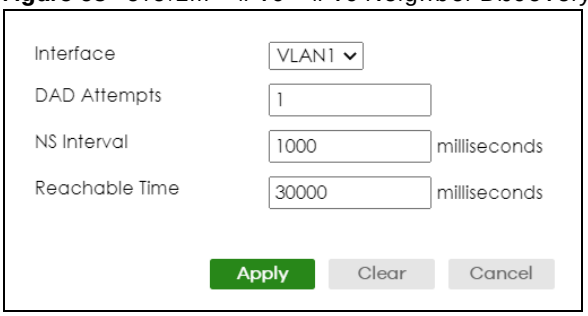
Table 45 SYSTEM > IPv6 > IPv6 Neighbor Discovery > IPv6 Neighbor Discovery Setup (continued)

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry.
Edit	Click **Edit** to edit the selected entry.

21.7.1 Edit an IPv6 Neighbor Discovery

Use this screen to configure neighbor discovery settings for each interface. Select an entry and click **Edit** in the **SYSTEM** > **IPv6** > **IPv6 Neighbor Discovery** > **IPv6 Neighbor Discovery Setup** screen to display this screen.

Figure 95 SYSTEM > IPv6 > IPv6 Neighbor Discovery > IPv6 Neighbor Discovery Setup > Edit



The following table describes the labels in this screen.

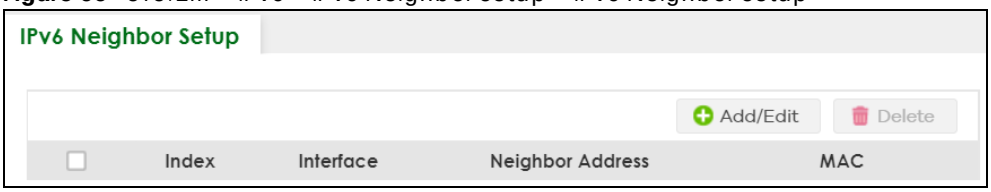
Table 46 SYSTEM > IPv6 > IPv6 Neighbor Discovery > IPv6 Neighbor Discovery Setup > Edit

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
DAD Attempts	The Switch uses Duplicate Address Detection (DAD) with neighbor solicitation and advertisement messages to check whether an IPv6 address is already in use before assigning it to an interface. Specify the number of consecutive neighbor solicitations (from 0 to 600) the Switch sends for this interface. Enter 0 to turn off DAD.
NS Interval	Specify the time interval (from 1000 to 3600000 milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	Specify how long (from 1000 to 3600000 milliseconds) a neighbor is considered reachable for this interface.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

21.8 IPv6 Neighbor Setup

Use this screen to view and configure static IPv6 neighbor entries in the Switch's IPv6 neighbor table to store the neighbor information permanently. Click **SYSTEM** > **IPv6** > **IPv6 Neighbor Setup** > **IPv6 Neighbor Setup** to display the screen as shown next.

Figure 96 SYSTEM > IPv6 > IPv6 Neighbor Setup > IPv6 Neighbor Setup



The following table describes the labels in this screen.

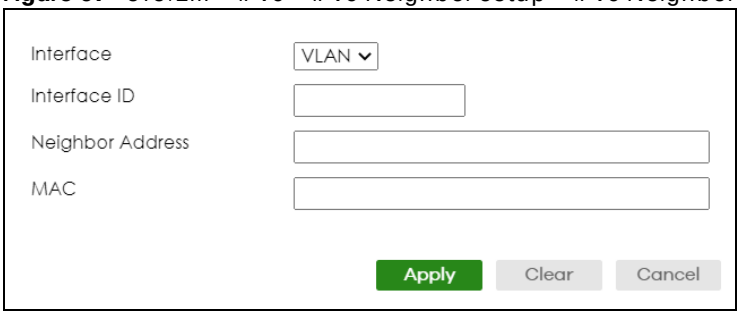
Table 47 SYSTEM > IPv6 > IPv6 Neighbor Setup > IPv6 Neighbor Setup

LABEL	DESCRIPTION
Index	This is the interface index number.
Interface	This is the name of the IPv6 interface you created.
Neighbor Address	This field displays the IPv6 address of the neighboring device which can be reached through the interface.
MAC	This field displays the MAC address of the neighboring device which can be reached through the interface.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

21.8.1 Add/Edit IPv6 Neighbor

Use this screen to create a static IPv6 neighbor entry. Click **Add/Edit,** or select an entry and click **Add/Edit** in the **SYSTEM** > **IPv6** > **IPv6 Neighbor Setup** > **IPv6 Neighbor Setup** screen to display this screen.

Figure 97 SYSTEM > IPv6 > IPv6 Neighbor Setup > IPv6 Neighbor Setup > Add/Edit



The following table describes the labels in this screen.

Table 48 SYSTEM > IPv6 > IPv6 Neighbor Setup > IPv6 Neighbor Setup > Add/Edit

LABEL	DESCRIPTION
Interface	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. A static IPv6 neighbor entry displays in the **MONITOR** > **IPv6 Neighbor Table** > **IPv6 Neighbor Table** screen only when the interface ID is also created in the **SYSTEM** > **Interface Setup** > **Interface Setup** screen. To have IPv6 function properly, you should configure a static VLAN with the same ID number in the **SWITCHING** > **VLAN** screens.

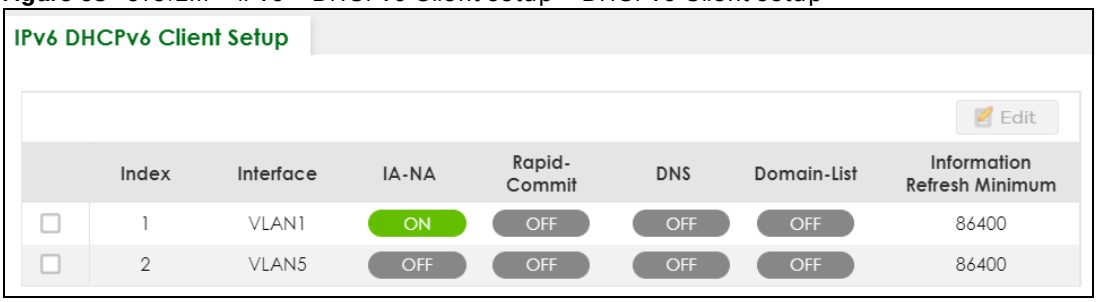
Table 48 SYSTEM > IPv6 > IPv6 Neighbor Setup > IPv6 Neighbor Setup > Add/Edit (continued)

LABEL	DESCRIPTION
Neighbor Address	Specify the IPv6 address of the neighboring device which can be reached through the interface.
MAC	Specify the MAC address of the neighboring device which can be reached through the interface.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

21.9 DHCPv6 Client Setup

Use this screen to configure the Switch's DHCP settings when it is acting as a DHCPv6 client. Click **SYSTEM** > **IPv6** > **DHCPv6 Client Setup** > **DHCPv6 Client Setup** to display the screen as shown next.

Figure 98 SYSTEM > IPv6 > DHCPv6 Client Setup > DHCPv6 Client Setup



The following table describes the labels in this screen.

Table 49 SYSTEM > IPv6 > DHCPv6 Client Setup > DHCPv6 Client Setup

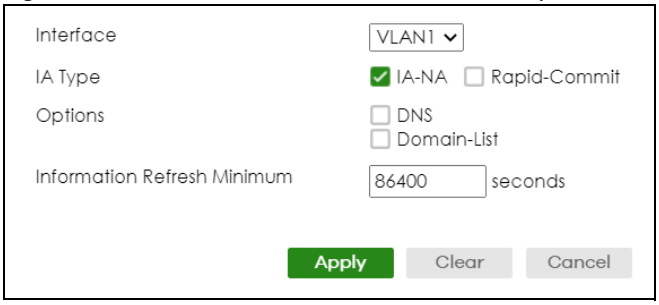
LABEL	DESCRIPTION
Index	This is the interface index number.
Interface	This is the name of the IPv6 interface you created.
IA-NA	This field displays whether the Switch obtains a non-temporary IP address from the DHCPv6 server.
Rapid-Commit	This field displays whether the Switch obtains information from the DHCPv6 server by a rapid two-message exchange.
DNS	This field displays whether the Switch obtains DNS server IPv6 addresses from the DHCPv6 server.
Domain-List	This field displays whether the Switch obtains a list of domain names from the DHCP server.
Information Refresh Minimum	This field displays the time interval (in seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.
	Select an entry's checkbox to select a specific entry.
Edit	Click **Edit** to edit the selected entry.

21.9.1 Edit DHCPv6 Client

Use this screen to configure the Switch's DHCP settings when it is acting as a DHCPv6 client. Select an

entry and click **Edit** in the **SYSTEM** > **IPv6** > **DHCPv6 Client Setup** > **DHCPv6 Client Setup** screen to display this screen.

Figure 99 SYSTEM > IPv6 > DHCPv6 Client Setup > DHCPv6 Client Setup > Edit



The following table describes the labels in this screen.

Table 50 SYSTEM > IPv6 > DHCPv6 Client Setup > DHCPv6 Client Setup > Edit

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IA Type	Select **IA-NA** to set the Switch to get a non-temporary IP address from the DHCPv6 server for this interface. Optionally, you can also select **Rapid-Commit** to have the Switch send its DHCPv6 Solicit message with a Rapid Commit option to obtain information from the DHCPv6 server by a rapid two-message exchange. The Switch discards any Reply messages that do not include a Rapid Commit option. The DHCPv6 server should also support the Rapid Commit option to have it work well.
Options	Select **DNS** to have the Switch obtain DNS server IPv6 addresses and/or select **Domain-List** to have the Switch obtain a list of domain names from the DHCP server.
Information Refresh Minimum	Specify the time interval (from 600 to 4294967295 seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 22
Logins

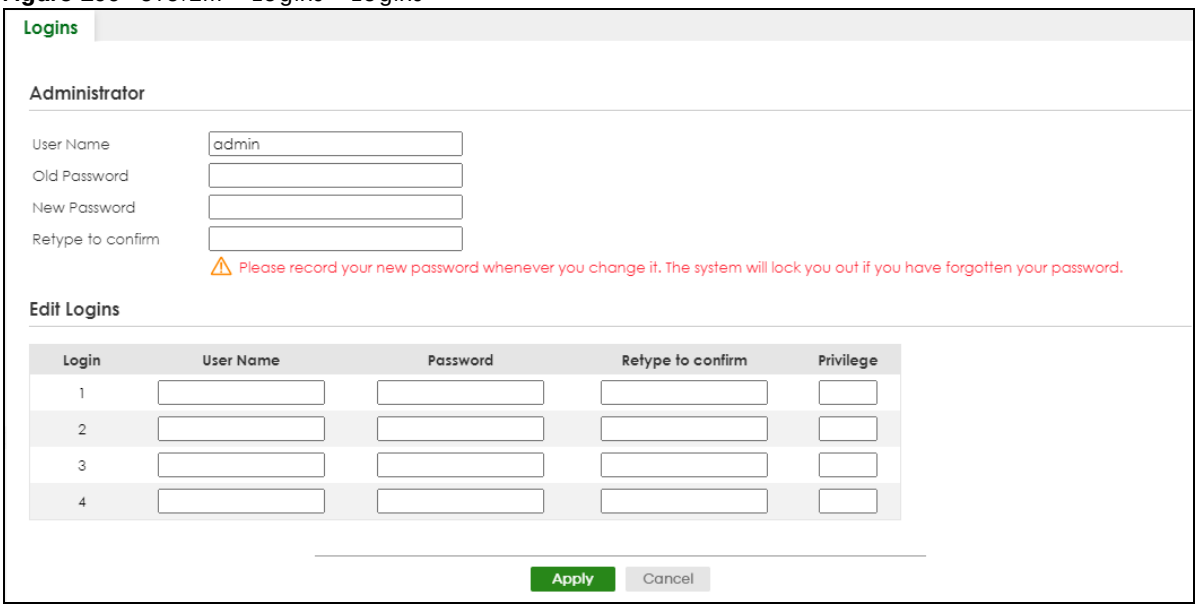
22.1 Set Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch through Web Configurator at any one time.

- An administrator is someone who can both view and configure Switch changes. The default user name for the Administrator is **admin**. The default administrator password is **1234**.
- A non-administrator (user name is something other than **admin**) is someone who can view and/or configure Switch settings. The configuration right varies depending on the user's privilege level.

Click **SYSTEM** > **Logins** > **Logins** to view the screen as shown.

Figure 100 SYSTEM > Logins > Logins



The following table describes the labels in this screen.

Table 51 SYSTEM > Logins > Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the "admin" user name. You can change the default administrator user name.	
User Name	Change the default "admin" system user name (up to 32 printable ASCII characters except [?], [|], ['], ["], [space], [,], or [:].

Table 51 SYSTEM > Logins > Logins (continued)

LABEL	DESCRIPTION
Old Password	Enter the existing system password (**1234** is the default password).
New Password	Enter your new system password. The password rule when **Password Complexity** is disabled in **SECURITY** > **Access Control** > **Account Security** > **Account Security** is: • 4 to 32 characters in length The password rule when **Password Complexity** is enabled are: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether **Password Complexity** is enabled or disabled.
Retype to confirm	Retype your new system password for confirmation. You can enter up to 32 printable ASCII characters.
Edit Logins You may configure passwords for up to four users. These users can have read-only or read/write access.	
Login	This is the index of an user account.
User Name	Specify the user name (up to 32 printable ASCII characters except [?], [|], ['], ["], [space], [,], or [:]).
Password	Enter your new system password. The password rule when **Password Complexity** is disabled in **SECURITY** > **Access Control** > **Account Security** > **Account Security** is: • 4 to 32 characters in length The password rule when **Password Complexity** is enabled are: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether **Password Complexity** is enabled or disabled.
Retype to confirm	Retype your new system password for confirmation.

Table 51 SYSTEM > Logins > Logins (continued)

LABEL	DESCRIPTION
Privilege	Type the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown below. • 0 – Display basic system information. • 3 – Display configuration or status. • 13 – Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. • 14 – Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he or she can run commands that requires privilege level of 5 or less but not more.
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.

CHAPTER 23
SNMP

23.1 SNMP Overview

This chapter introduces the SNMP screens and shows you how to setup SNMP settings for management.

23.1.1 What You Can Do

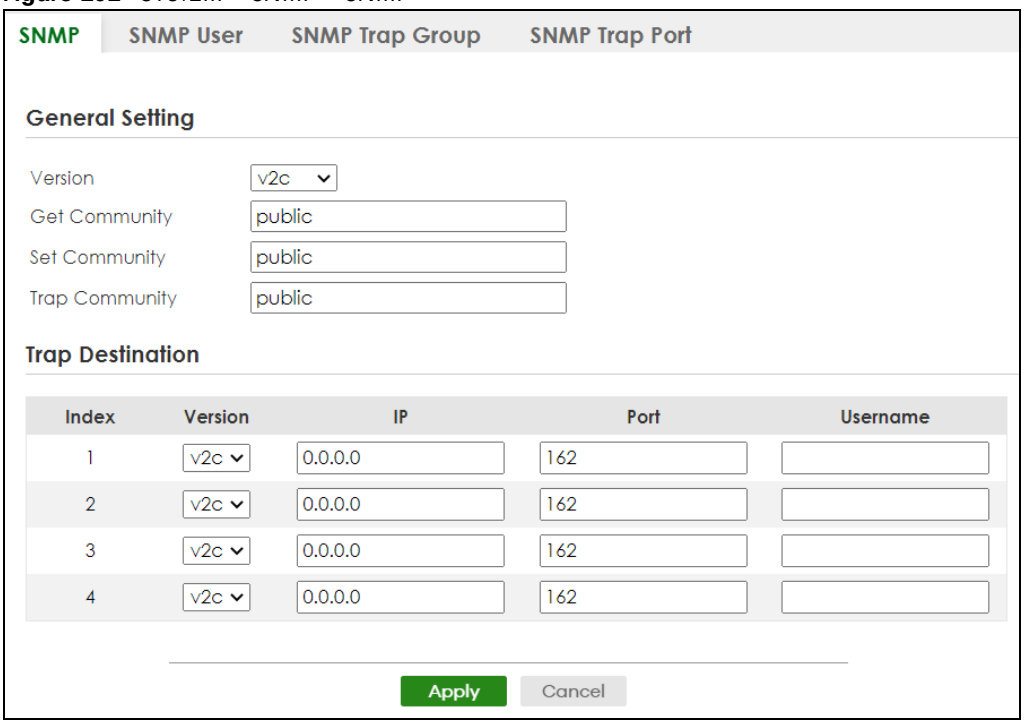
- Use the **SNMP** screen (Section 23.2 on page 145) to configure general SNMP settings.
- Use the **SNMP User** screen (Section 23.3 on page 147) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **SNMP Trap Group** screen (Section 23.4 on page 150) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **SNMP Trap Port** screen (Section 23.5 on page 151) to enable/disable sending SNMP traps on a port.

23.2 Configure SNMP

Use this screen to configure your SNMP settings.

Click **SYSTEM** > **SNMP** > **SNMP** to view the screen as shown.

Figure 101 SYSTEM > SNMP > SNMP



Note: The string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

Table 52 SYSTEM > SNMP > SNMP

LABEL	DESCRIPTION
General Setting Use this section to specify the SNMP version and community (password) values.	
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (**v2c**), SNMP version 3 (**v3**) or both (**v3v2c**). SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNext-requests from the management station. The **Get Community** string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the **Set Community** string, which is the password for incoming Set- requests from the management station. The **Set Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the **Trap Community** string, which is the password sent with each trap to the SNMP manager. The **Trap Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination Use this section to configure where to send SNMP traps from the Switch.	
Index	This is the index of a trap destination.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.

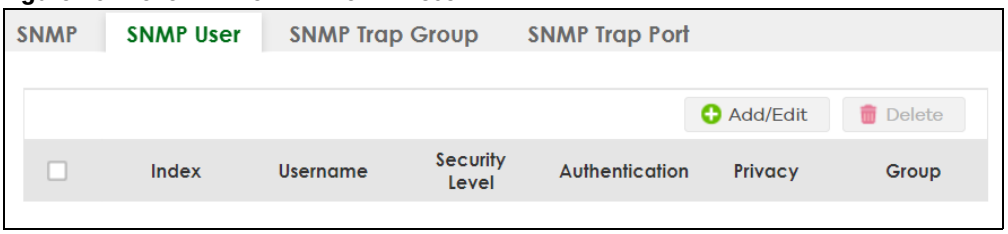
Table 52 SYSTEM > SNMP > SNMP (continued)

LABEL	DESCRIPTION
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the user name to be sent to the SNMP manager along with the SNMP v3 trap. The string should not contain [?], [|], ['], ["], [,], [:], or space. This user name must match an existing account on the Switch (configured in the **SYSTEM** > **SNMP** > **SNMP User** screen).
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.

23.3 Configure SNMP User

Use this screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager. Click **SYSTEM** > **SNMP** > **SNMP User** to view the screen as shown.

Figure 102 SYSTEM > SNMP > SNMP User



The following table describes the labels in this screen.

Table 53 SYSTEM > SNMP > SNMP User

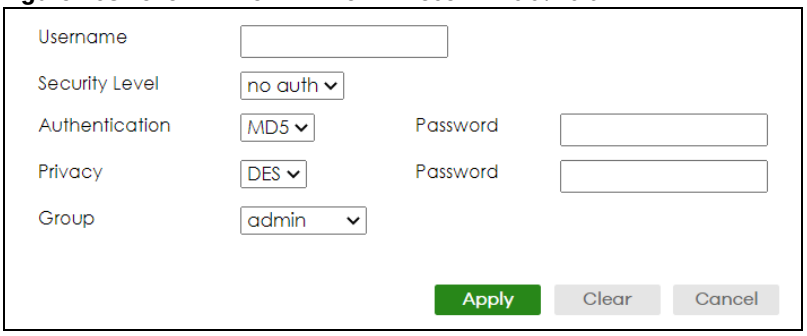
LABEL	DESCRIPTION
Index	This is a read-only number identifying a login account on the Switch.
Username	This field displays the user name of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

23.3.1 Add/Edit SNMP User

Use this screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM** > **SNMP** > **SNMP User** screen to view the screen.

Note: Use the user name and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.

Figure 103 SYSTEM > SNMP > SNMP User > Add/Edit



The following table describes the labels in this screen.

Table 54 SYSTEM > SNMP > SNMP User > Add/Edit

LABEL	DESCRIPTION
Username	Specify the user name (up to 32 printable ASCII characters) of a login account on the Switch. The string should not contain [?], [|], ['], ["], [space], [,], or [:].
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • **no auth** – to use the user name as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • **auth** – to implement an authentication algorithm for SNMP messages sent by this user. • **priv** – to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.

Table 54 SYSTEM > SNMP > SNMP User > Add/Edit (continued)

LABEL	DESCRIPTION
Password	When you select **no auth** in **Security Level**, enter the password of up to 32 printable ASCII characters (except [?], [|], ['], ["], [space], [,], [[ ] , or [ ]]). When you select **auth** or **priv** in **Security Level**, the password rule when **Password Complexity** is disabled in **SECURITY** > **Access Control** > **Account Security** > **Account Security** for SNMP user authentication is: • 4 to 32 characters in length The password rule when **Password Complexity** is enabled are: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether **Password Complexity** is enabled or disabled.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • **DES** – Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** – Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	When you select **no auth** or **auth** in **Security Level**, enter the password of up to 32 printable ASCII characters (except [?], [|], ['], ["], [space], [,], [[ ] , or [ ]]). When you select **priv** in **Security Level**, the password rule when **Password Complexity** is disabled in **SECURITY** > **Access Control** > **Account Security** > **Account Security** for encrypting SNMP packets is: • 4 to 32 characters in length The password rule when **Password Complexity** is enabled are: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether **Password Complexity** is enabled or disabled.

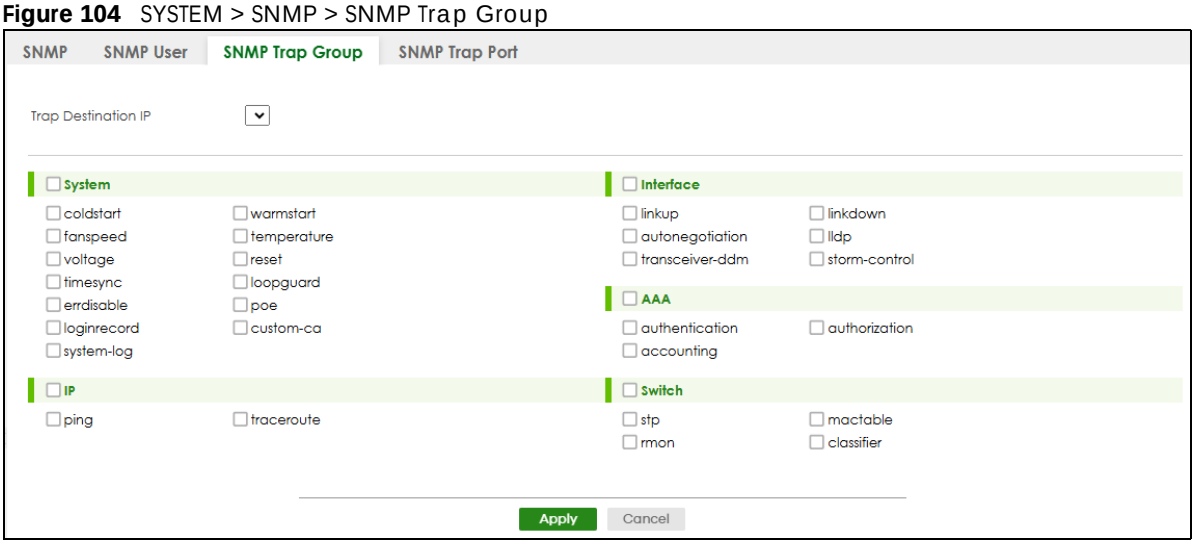
Table 54 SYSTEM > SNMP > SNMP User > Add/Edit (continued)

LABEL	DESCRIPTION
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. **admin** – Members of this group can perform all types of system configuration, including the management of administrator accounts. **read-write** – Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. **read-only** – Members of this group have read rights only, meaning the user can collect information from the Switch.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

23.4 SNMP Trap Group

Use this screen to specify the types of SNMP traps that should be sent to each SNMP manager. Click **SYSTEM** > **SNMP** > **SNMP Trap Group** to view the screen as shown.

Figure 104 SYSTEM > SNMP > SNMP Trap Group



The following table describes the labels in this screen.

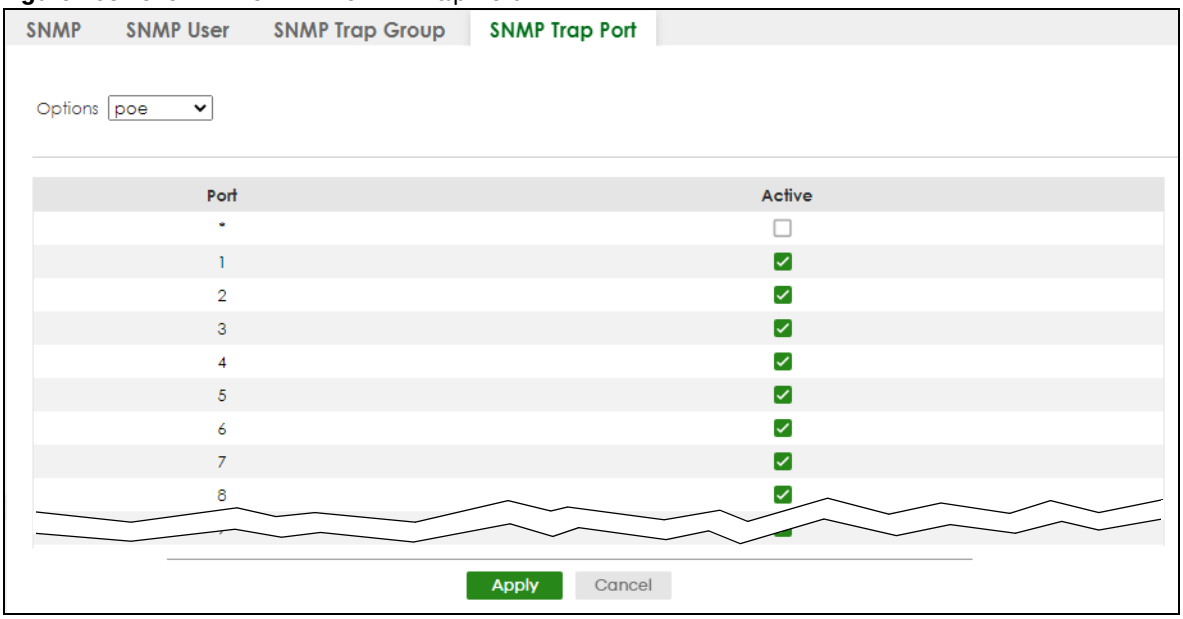
Table 55 SYSTEM > SNMP > SNMP Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the **SYSTEM** > **SNMP** > **SNMP** screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. The traps are grouped by category. Selecting a category in the heading row automatically selects all of the SNMP traps under that category. Clear the checkboxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's checkbox automatically clears all of the category's trap checkboxes (the Switch only sends traps from selected categories).
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.

23.5 Enable or Disable Sending of SNMP Traps on a Port

Click **SYSTEM** > **SNMP** > **SNMP Trap Port** to view the screen as shown. Use this screen to set whether a trap received on the ports would be sent to the SNMP manager.

Figure 105 SYSTEM > SNMP > SNMP Trap Port



The following table describes the labels in this screen.

Table 56 SYSTEM > SNMP > SNMP Trap Port

LABEL	DESCRIPTION
Options	Select the trap type you want to configure here.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the trap type of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. Clear this checkbox to disable the sending of SNMP traps on this port.
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.

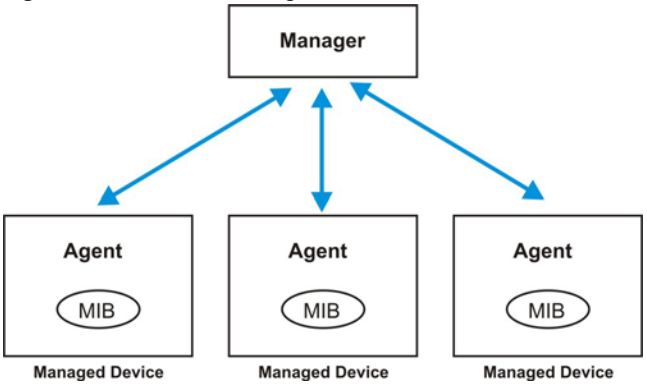
23.6 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

23.6.1 About 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 through SNMP version 1 (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 106 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with

SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables or managed objects that define each piece of information to be collected about a Switch. Examples of variables include number of packets received, node port status, and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request or response protocol based on the manager or agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 57 SNMP Commands

LABEL	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Supported MIBs

A MIB is a collection of managed objects that is organized according to hierarchy. The objects define the attributes of the managed device, which includes the names, status, access rights, and data types. Each object can be addressed through an object identifier (OID). An OID that begins with "**1.3.6.1.4.1.890.1.15**" is a Zyxel-defined private MIB. Otherwise, it is a standard MIB OID.

MIBs let administrators collect statistics and monitor status and performance. The Switch uses both standard public (RFC-defined) MIBs for standard functionality, and private MIBs that support additional Switch functionality. Private MIBs contain Switch specific managed objects.

To view a list of standard MIBs supported by your Switch, see the product datasheet at *www.zyxel.com* (**Support** > **Download Library** > **Datasheet**).

To get the private MIBs supported by your Switch, download (and unzip) the correct model MIB from *www.zyxel.com* (**Support** > **Download Library** > **MIB File**).

SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

Table 58 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
custom-ca	zySysMgmtReloadCustomCAFail	1.3.6.1.4.1.890.1.15.3.49.2.4	This trap is sent when the uploaded HTTPS certificate fails to load during the Switch restart.

Table 59 SNMP Interface Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. 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.

Table 61 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

Table 62 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.

CHAPTER 24
Switch Setup

24.1 Switch Setup Overview

Use this screen to do the Switch's basic setup configuration, for example, VLAN (Virtual Local Area Network) type, enabling switching protocols, and MAC learning aging time setup.

24.1.1 Introduction to VLANs

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 groups; 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 in the same building.

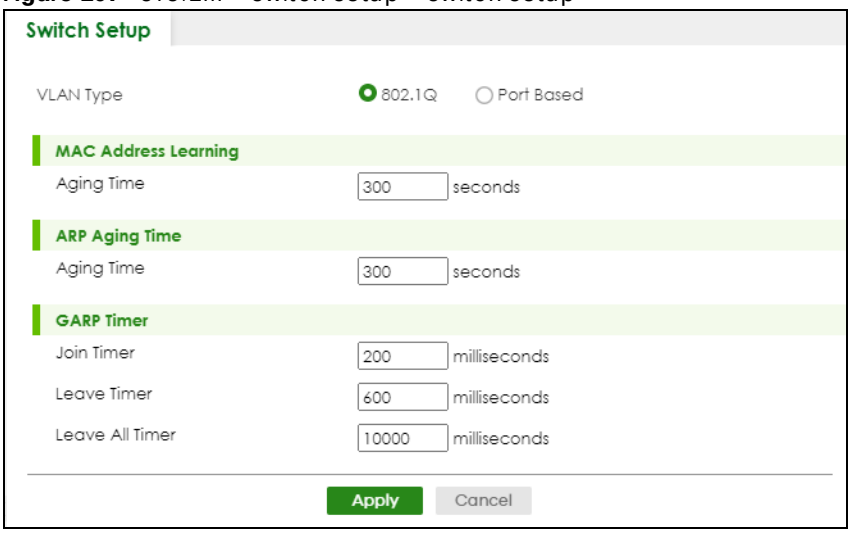
VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note: VLAN is unidirectional; it only governs outgoing traffic.

24.2 Switch Setup

Click **SYSTEM** > **Switch Setup** > **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen.

Figure 107 SYSTEM > Switch Setup > Switch Setup



The following table describes the labels in this screen.

Table 63 SYSTEM > Switch Setup > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose **802.1Q** or **Port Based**. The **SWITCHING** > **VLAN** link and its sub-links only appears when you choose **802.1Q** VLAN type in this screen.
MAC Address Learning MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.	
Aging Time	Enter a time from 10 to 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
ARP Aging Time	
Aging Time	Enter a time from 60 to 1000000 seconds. This is how long dynamically learned ARP entries remain in the ARP table before they age out (and must be relearned). The setting here applies to ARP entries which are newly added in the ARP table after you click **Apply**.
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	**Join Timer** sets the duration of the **Join Period** timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	**Leave Timer** sets the duration of the **Leave Period** timer for GVRP in milliseconds. Each port has a single **Leave Period** timer. **Leave Time** must be two times larger than **Join Timer**; the default is 600 milliseconds.
Leave All Timer	**Leave All Timer** sets the duration of the **Leave All Period** timer for GVRP in milliseconds. Each port has a single **Leave All Period** timer. **Leave All Timer** must be larger than **Leave Timer**.
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.

CHAPTER 25
Syslog Setup

25.1 Syslog Overview

This chapter explains the **Syslog** screens.

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.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 64 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

25.1.1 What You Can Do

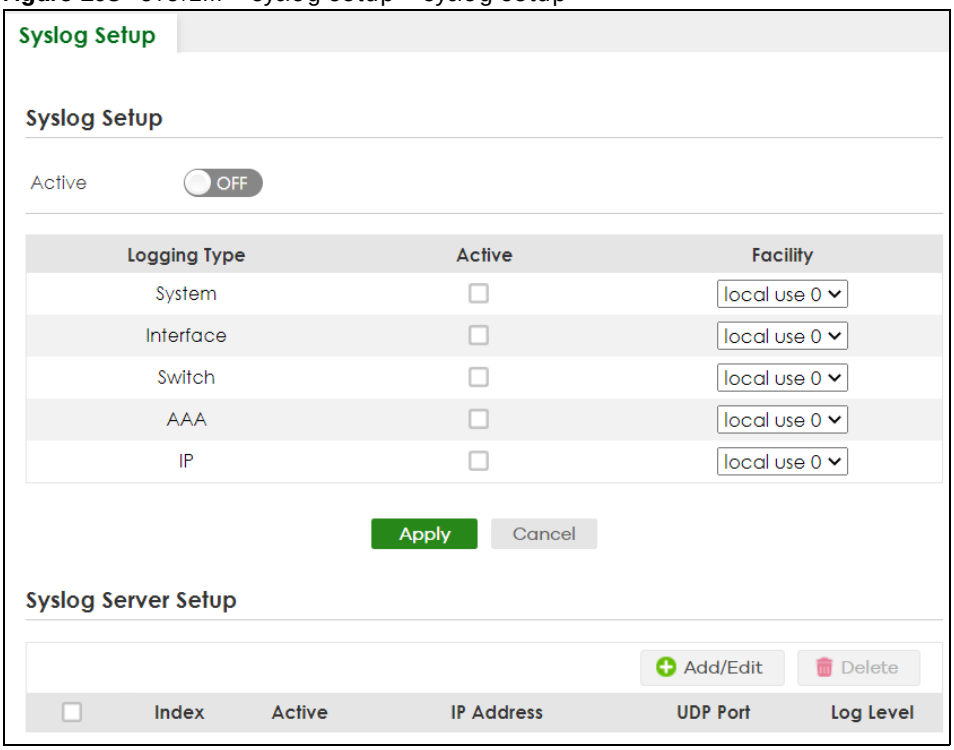
Use the **Syslog Setup** screen (Section 25.2 on page 157) to configure the device's system logging settings and configure a list of external syslog servers.

25.2 Syslog Setup

The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings and configure a list of external syslog servers.

Click **SYSTEM** > **Syslog Setup** > **Syslog Setup** in the navigation panel to display this screen.

Figure 108 SYSTEM > Syslog Setup > Syslog Setup



The following table describes the labels in this screen.

Table 65 SYSTEM > Syslog Setup > Syslog Setup

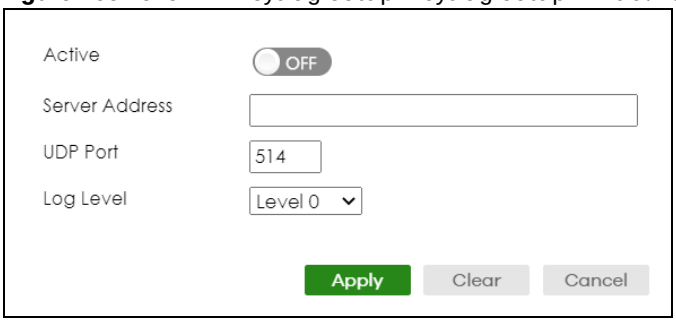
LABEL	DESCRIPTION
Syslog Setup	
Active	Enable the switch button to turn on syslog (system logging) and then configure the syslog setting.
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	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 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.
Syslog Server Setup	
Index	This is the index number of a syslog server entry.
Active	This field displays if the device is activated to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
UDP Port	This field displays the port of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

25.2.1 Add/Edit a Syslog Server

Use this screen to configure an external syslog server.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM** > **Syslog Setup** > **Syslog Setup** screen to display this screen.

Figure 109 SYSTEM > Syslog Setup > Syslog Setup > Add/Edit



The following table describes the labels in this screen.

Table 66 SYSTEM > Syslog Setup > Syslog Setup > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to have the device send logs to this syslog server. Clear the checkbox if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IPv4 or IPv6 address of the syslog server.
UDP Port	The default syslog server port is 514. If your syslog server uses a different port, configure the one it uses here.
Log Level	Select the severity levels of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 26
Time Range

26.1 Time Range Overview

You can set up one-time and recurring schedules for time-oriented features, such as PoE and classifier. The UAG 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.

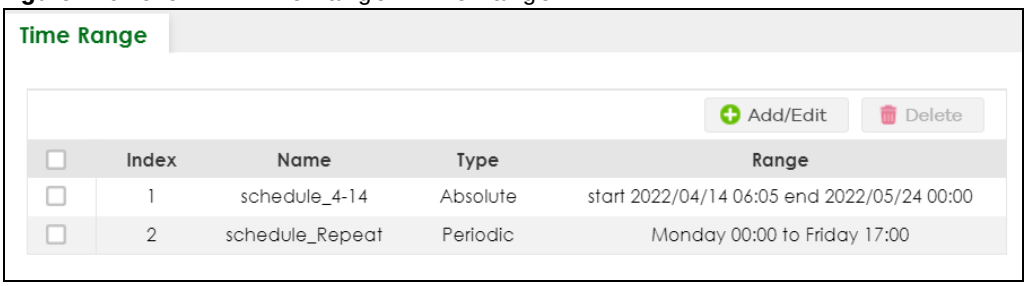
26.1.1 What You Can Do

Use the **Time Range** screen (Section 26.2 on page 160) to view or define a schedule on the Switch.

26.2 Configure a Time Range

Click **SYSTEM** > **Time Range** > **Time Range** in the navigation panel to display the screen as shown.

Figure 110 SYSTEM > Time Range > Time Range



The following table describes the labels in this screen.

Table 67 SYSTEM > Time Range > Time Range

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
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. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].

Table 67 SYSTEM > Time Range > Time Range (continued)

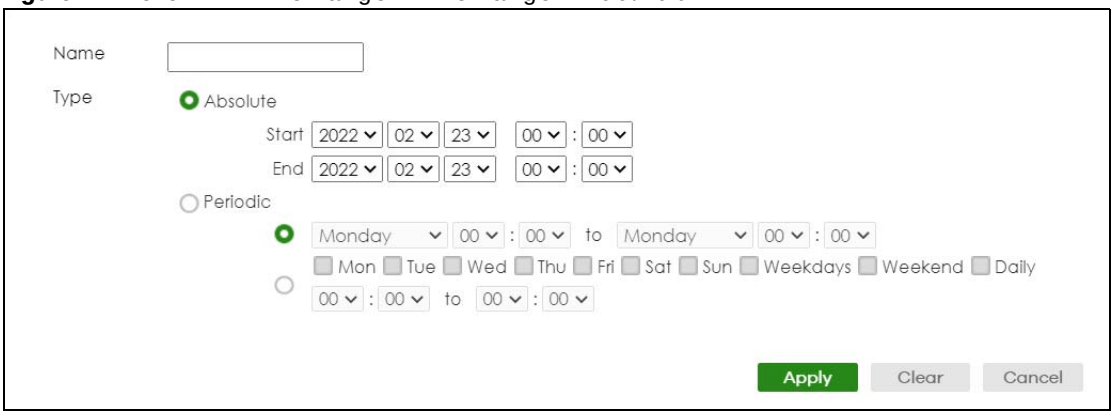
LABEL	DESCRIPTION
Type	This displays the schedule type of the time range rule. **Absolute** An one-time schedule. One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods. **Periodic** A recurring 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.
Range	This field displays the time periods to which this schedule applies.
Add/Edit	Click **Add/Edit** to add a new schedule rule or edit a selected one.
Delete	Click **Delete** to remove the selected rules.

26.2.1 Add/Edit Time Range

This screen allows you to create a new time range or edit an existing one.

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 111 SYSTEM > Time Range > Time Range > Add/Edit



The following table describes the labels in this screen.

Table 68 SYSTEM > Time Range > Time Range > Add/Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for this rule for identifying purposes. The string should not contain [?], [|], ['], ["], or [,].
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. 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.

Table 68 SYSTEM > Time Range > Time Range > Add/Edit (continued)

LABEL	DESCRIPTION
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**. 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.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 27
PORT

The following chapters introduces the configurations of the links under the **PORT** navigation panel.

Quick links to chapters:

- Green Ethernet
- Link Aggregation
- Link Layer Discovery Protocol (LLDP)
- OAM
- PoE Setup (for PoE models only)
- Port Setup

CHAPTER 28
Green Ethernet

This chapter shows you how to configure the Switch to reduce the power consumed by switch ports.

28.1 Green Ethernet Overview

Green Ethernet reduces switch port power consumption in the following ways.

IEEE 802.3az Energy Efficient Ethernet (EEE)

If EEE is enabled, both sides of a link support EEE and there is no traffic, the port enters Low Power Idle (LPI) mode. LPI mode turns off some functions of the physical layer (becomes quiet) to save power. Periodically the port transmits a REFRESH signal to allow the link partner to keep the link alive. When there is traffic to be sent, a WAKE signal is sent to the link partner to return the link to active mode.

Auto Power Down

Auto Power Down turns off almost all functions of the port's physical layer functions when the link is down, so the port only uses power to check for a link up pulse from the link partner. After the link up pulse is detected, the port wakes up from **Auto Power Down** and operates normally.

Short Reach

Traditional Ethernet transmits all data with enough power to reach the maximum cable length. Shorter cables lose less power, so **Short Reach** saves power by adjusting the transmit power of each port according to the length of cable attached to that port.

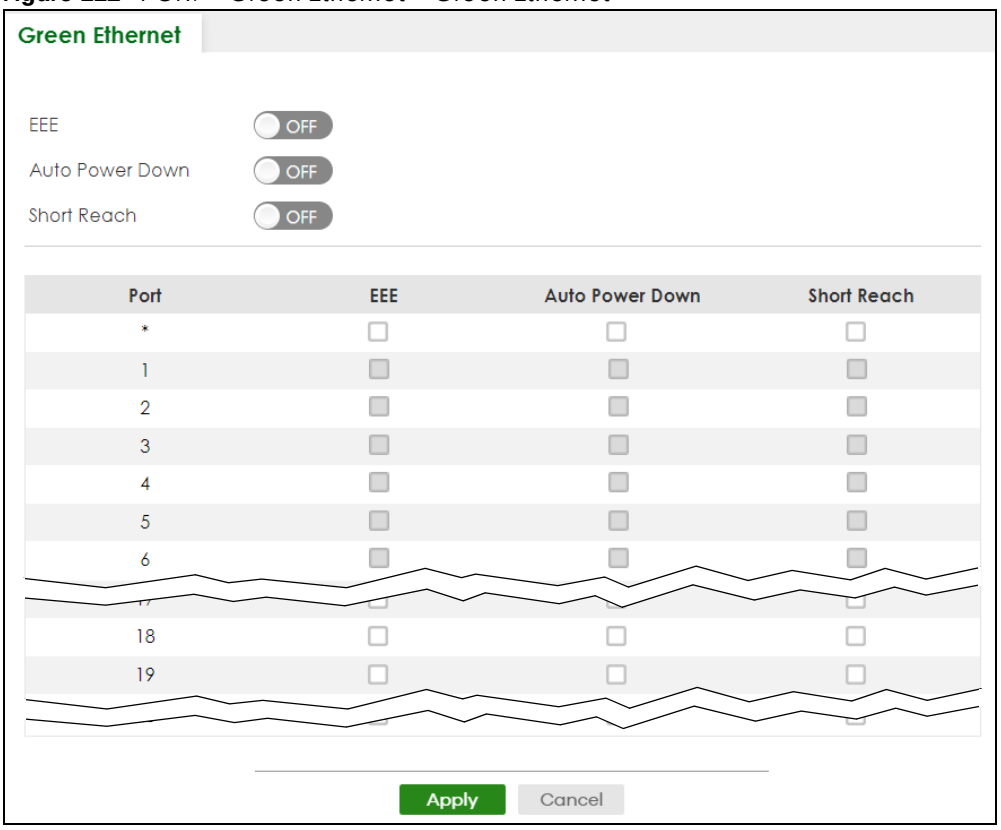
28.2 Configure Green Ethernet

Click **PORT** > **Green Ethernet** > **Green Ethernet** in the navigation panel to display the screen as shown.

Note: This feature is only available on copper ports. Checkboxes of SFP ports are grayed out and cannot be selected.

Note: EEE, Auto Power Down and Short Reach are NOT supported on an uplink port.

Figure 112 PORT > Green Ethernet > Green Ethernet



The following table describes the labels in this screen.

Table 69 PORT > Green Ethernet > Green Ethernet

LABEL	DESCRIPTION
EEE	Enable the switch button to activate Energy Efficient Ethernet globally.
Auto Power Down	Enable the switch button to activate Auto Power Down globally.
Short Reach	Enable the switch button to activate Short Reach globally.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
EEE	Select this to activate Energy Efficient Ethernet on this port.
Auto Power Down	Select this to activate Auto Power Down on this port.
Short Reach	Select this to activate Short Reach on this port.
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.

CHAPTER 29
Link Aggregation

29.1 Link Aggregation Overview

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

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 beginning port of each trunk group must be physically connected to form a trunk group.

29.1.1 What You Can Do

- Use the **Link Aggregation Status** screen (Section 29.2 on page 167) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen (Section 29.3 on page 169) to configure static link aggregation.
- Use the **Link Aggregation Control Protocol** screen (Section 29.4 on page 170) to enable Link Aggregation Control Protocol (LACP).

29.1.2 What You Need to Know

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.

See Section 29.5.1 on page 172 for a static port trunking example.

Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an

operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

Link Aggregation ID

LACP aggregation ID consists of the following information[1]:

Table 70 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Table 71 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Algorithm Types Limitation

The maximum number of link aggregation algorithm types (**Criteria**) that can link up at the same time depends on your Switch model. See Table 73 on page 168 for the list of **Criteria** that your Switch currently supports.

The following table shows the maximum number of link aggregation algorithm types that can link up at the same time.

Table 72 Link Aggregation Algorithm Types Limitation

MODEL	LINK AGGREGATION ALGORITHM TYPES (MAXIMUM)
GS1920v2 Series	4

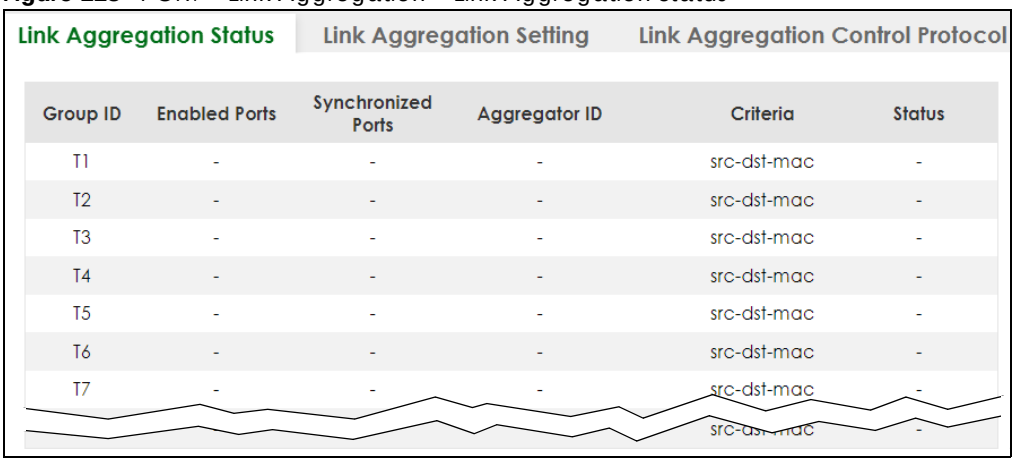
For example, if your Switch has four link aggregation algorithm types that are currently linked up, the fifth link aggregation algorithm type can only link up when link down occurs on one of the link aggregation algorithm type.

29.2 Link Aggregation Status

Click **PORT** > **Link Aggregation > Link Aggregation Status** in the navigation panel to display the screen as shown. See Section 29.1 on page 166 for more information.

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

Figure 113 PORT > Link Aggregation > Link Aggregation Status



The following table describes the labels in this screen.

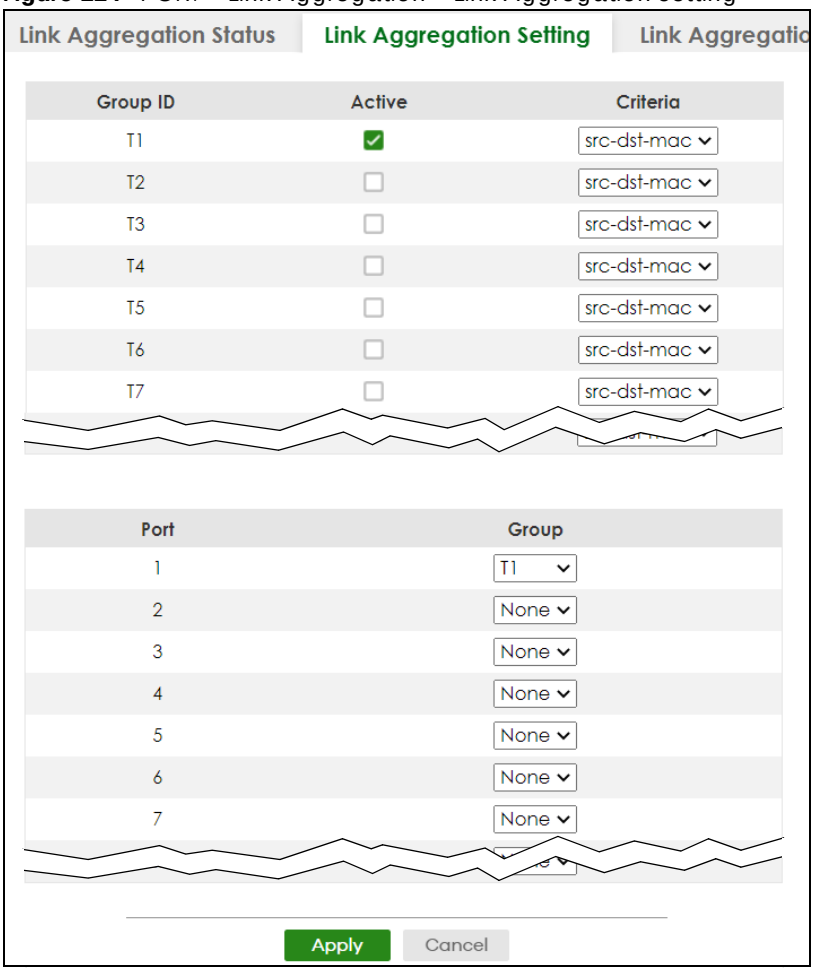
Table 73 PORT > Link Aggregation > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the **Link Aggregation Setting** screen to be in the trunk group. The port numbers displays only when this trunk group is activated and there is a port belonging to this group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm types used in this trunk group. Sending of packets are from the same source and/or to the same destination over the same link within the trunk. **src-mac** means the Switch distributes traffic based on the packet's source MAC address. **dst-mac** means the Switch distributes traffic based on the packet's destination MAC address. **src-dst-mac** means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. **src-ip** means the Switch distributes traffic based on the packet's source IP address. **dst-ip** means the Switch distributes traffic based on the packet's destination IP address. **src-dst-ip** means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses. Note: To find the number of link aggregation algorithm types that can link up at the same time, see Algorithm Types Limitation on page 167.
Status	This field displays how these ports were added to the trunk group. It displays: • **Static** – if the ports are configured as static members of a trunk group. • **LACP** – if the ports are configured to join a trunk group through LACP.

29.3 Link Aggregation Setting

Click **PORT** > **Link Aggregation** > **Link Aggregation Setting** to display the screen shown next. See Section 29.1 on page 166 for more information on link aggregation.

Figure 114 PORT > Link Aggregation > Link Aggregation Setting



The following table describes the labels in this screen.

Table 74 PORT > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
This is the only screen you need to configure to enable static link aggregation.	
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this to activate a trunk group.

Table 74 PORT > Link Aggregation > Link Aggregation Setting (continued)

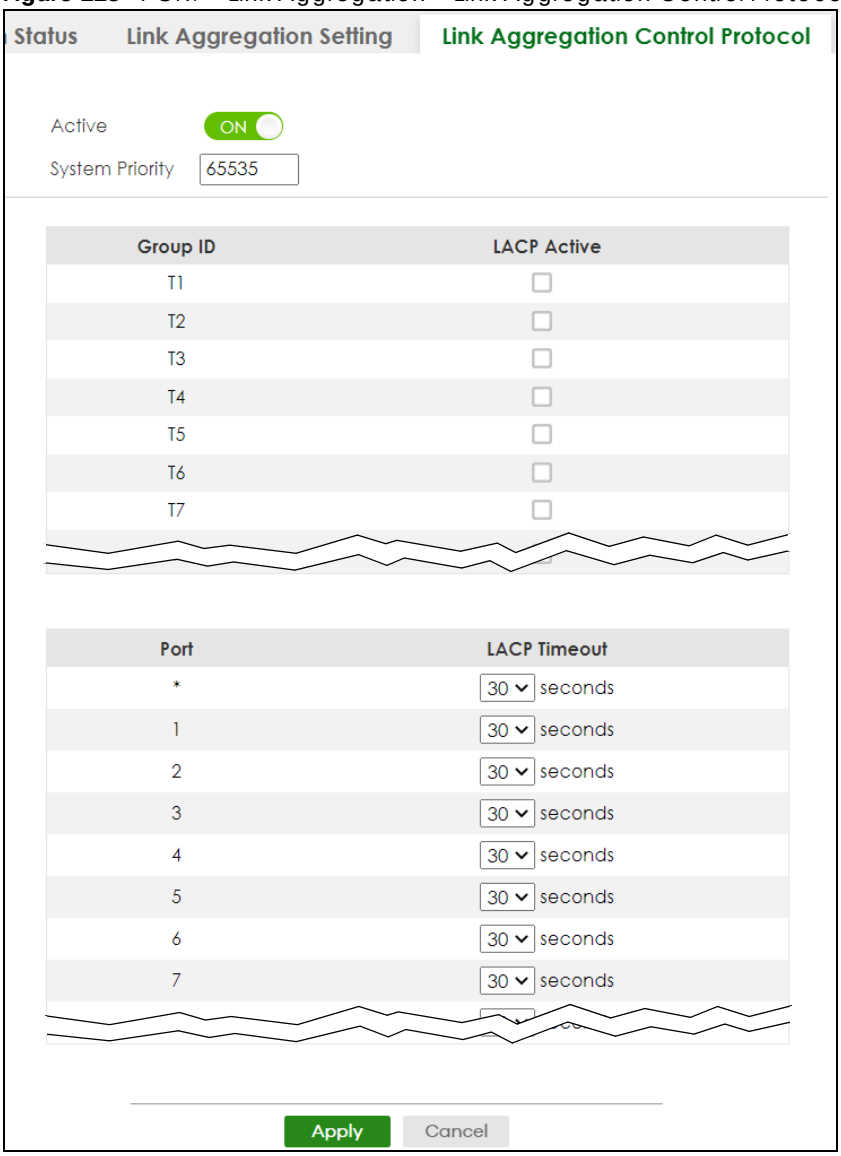
LABEL	DESCRIPTION
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **src-dst-mac** distribution type. If the Switch is behind a router, the packet's destination or source MAC address will be changed. In this case, set the Switch to distribute traffic based on its IP address to make sure port trunking can work properly. Select **src-mac** to distribute traffic based on the packet's source MAC address. Select **dst-mac** to distribute traffic based on the packet's destination MAC address. Select **src-dst-mac** to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select **src-ip** to distribute traffic based on the packet's source IP address. Select **dst-ip** to distribute traffic based on the packet's destination IP address. Select **src-dst-ip** to distribute traffic based on a combination of the packet's source and destination IP addresses.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs. Note: When you enable the port security feature on the Switch and configure port security settings for a port, you cannot include the port in an active trunk group.
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.

29.4 Link Aggregation Control Protocol

Click **PORT** > **Link Aggregation** > **Link Aggregation Control Protocol** to display the screen shown next. See Dynamic Link Aggregation on page 166 for more information on dynamic link aggregation.

Note: Do NOT configure this screen unless you want to enable dynamic link aggregation.

Figure 115 PORT > Link Aggregation > Link Aggregation Control Protocol



The following table describes the labels in this screen.

Table 75 PORT > Link Aggregation > Link Aggregation Control Protocol

LABEL	DESCRIPTION
Active	Enable the switch button to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65535. 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.
Use this section to enable LACP on trunks.	
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Use this section to configure LACP timeout on ports.	
Port	This field displays the port number.

Table 75 PORT > Link Aggregation > Link Aggregation Control Protocol (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	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 (1 second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
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.

29.5 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

29.5.1 Static Trunking Example

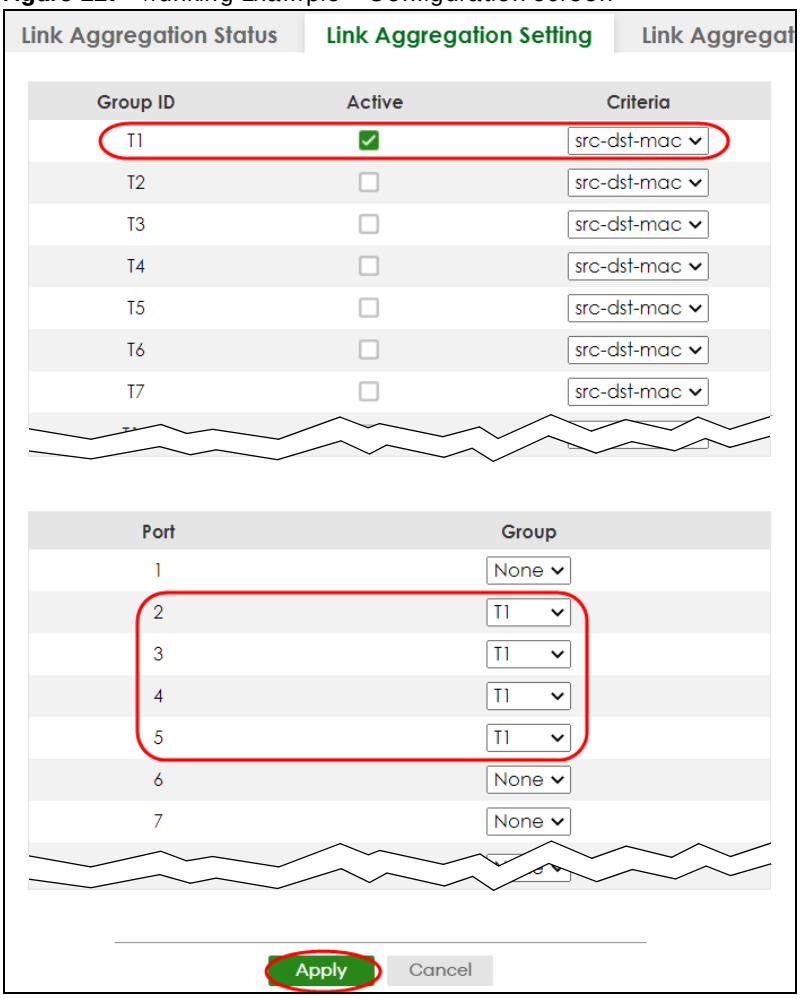
This example shows you how to create a static port trunk group for ports 2 – 5.

1 **Make your physical connections** – make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2 – 5 on switch **A** connected to switch **B**.

Figure 116 Trunking Example – Physical Connections

2 **Configure static trunking** – Click **PORT** > **Link Aggregation** > **Link Aggregation Setting**. In this screen activate trunk group **T1**, select the traffic distribution algorithm used by this group and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 117 Trunking Example – Configuration Screen



Your trunk group 1 (**T1**) configuration is now complete.

CHAPTER 30
Link Layer Discovery Protocol (LLDP)

30.1 LLDP Overview

The LLDP (Link Layer Discovery Protocol) is a layer 2 protocol. It 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. This helps an administrator discover network changes and perform necessary network reconfiguration and management. The device information is encapsulated in the LLDPDUs (LLDP data units) in the form of TLV (Type, Length, Value). Device information carried in the received LLDPDUs is stored in the standard MIB.

The Switch supports these basic management TLVs.

- End of LLDPDU (mandatory)
- Chassis ID (mandatory)
- Port ID (mandatory)
- Time to Live (mandatory)
- Port Description (optional)
- System Name (optional)
- System Description (optional)
- System Capabilities (optional)
- Management Address (optional)

The Switch also supports the IEEE 802.1 and IEEE 802.3 organizationally-specific TLVs.

IEEE 802.1 specific TLVs:

- Port VLAN ID TLV (optional)
- Port and Protocol VLAN ID TLV (optional)

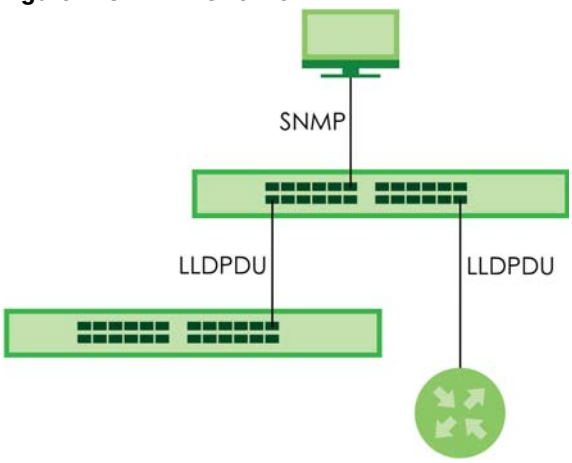
IEEE 802.3 specific TLVs:

- MAC/PHY Configuration/Status TLV (optional)
- Power via MDI TLV (optional, For PoE models only)
- Link Aggregation TLV (optional)
- Maximum Frame Size TLV (optional)

The optional TLVs are inserted between the Time To Live TLV and the End of LLDPDU TLV.

The next figure demonstrates that the network devices Switches and Routers (S and R) transmit and receive device information through LLDPDU and the network manager can query the information using Simple Network Management Protocol (SNMP).

Figure 118 LLDP Overview



30.2 LLDP-MED Overview

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension to the standard LLDP developed by the Telecommunications Industry Association (TIA) TR-41.4 subcommittee which defines the enhanced discovery capabilities, such as VoIP applications, to enable network administrators manage their network topology application more efficiently. Unlike the traditional LLDP, which has some limitations when handling multiple application devices, the LLDP-MED offers display of accurate physical topology, interoperability of devices, and easy trouble shooting for mis-configured IP addresses. There are three classes of endpoint devices that the LLDP-MED supports:

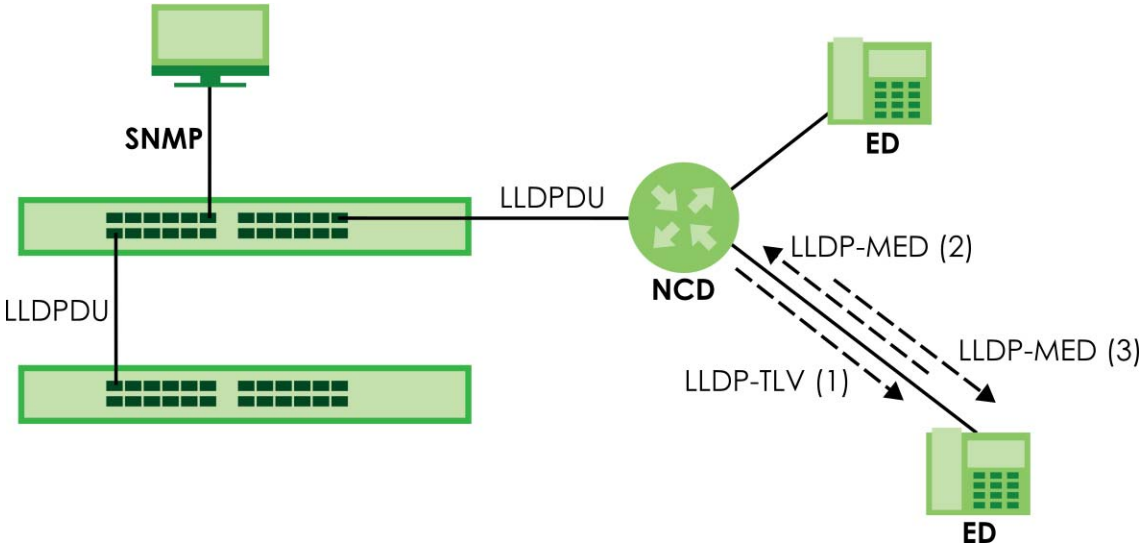
Class I: IP Communications Controllers or other communication related servers

Class II: Voice Gateways, Conference Bridges or Media Servers

Class III: IP-Phones, PC-based Softphones, End user Communication Appliances supporting IP Media

The following figure shows that with the LLDP-MED, network connectivity devices (NCD) like Switches and Routers will transmit LLDP TLV to endpoint device (ED) like IP Phone first (1), to get its device type and capabilities information, then it will receive that information in LLDP-MED TLV back from endpoint devices (2), after that the network connectivity devices will transmit LLDP-MED TLV (3) to provision the endpoint device to such that the endpoint device's network policy and location identification information is updated. Since LLDPDU updates status and configuration information periodically, network managers may check the result of provision through remote status. The remote status is updated by receiving LLDP-MED TLVs from endpoint devices.

Figure 119 LLDP-MED Overview



30.2.1 What You Can Do – LLDP

- Use the **LLDP Local Status** screen (Section 30.3 on page 176) to view the Switch's LLDP information.
- Use the **LLDP Remote Status** screen (Section 30.4 on page 181) to view LLDP information from the neighboring devices.
- Use the **LLDP Setup** screen (Section 30.5 on page 186) to configure LLDP on the Switch.
- Use the **Basic TLV Setting** screen (Section 30.6 on page 188) to configure basic TLV settings on each port.
- Use the **Org-specific TLV Setting** screen (Section 30.7 on page 189) to configure organization-specific TLV settings on each port.

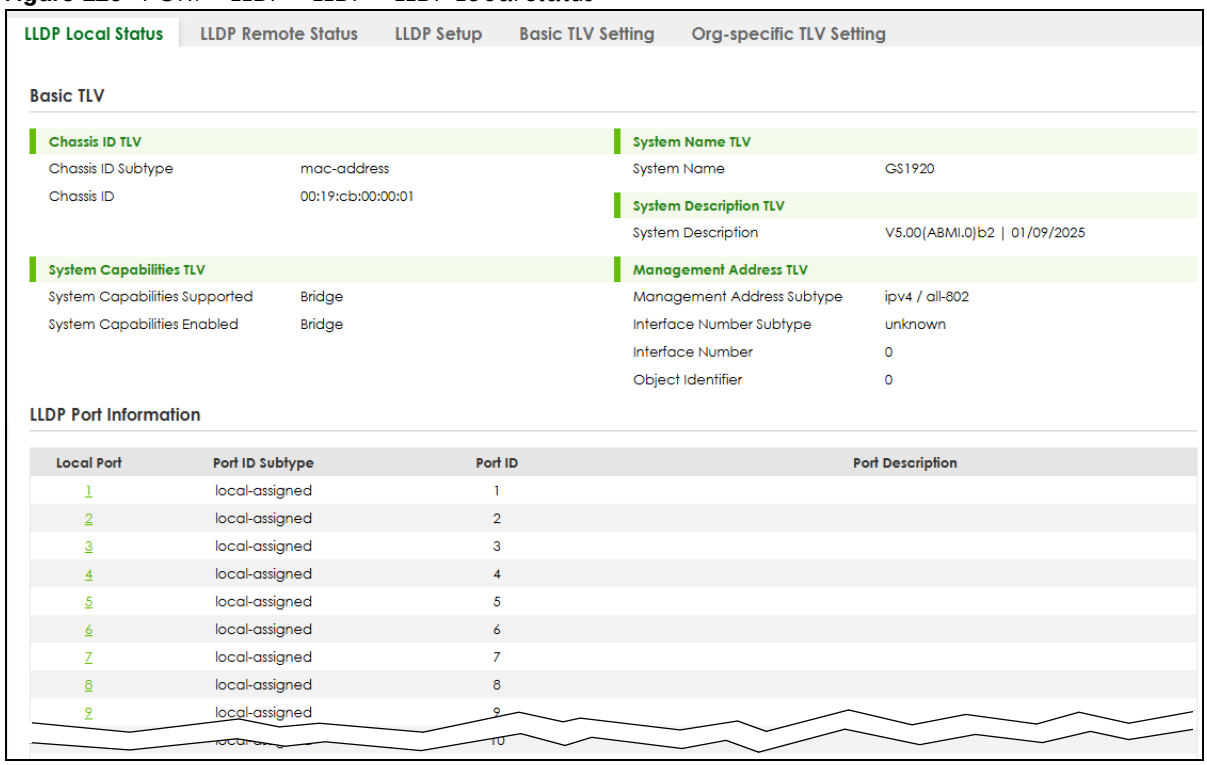
30.2.2 What You Can Do – LLDP MED

- Use the **LLDP-MED Setup** screen (Section 30.8 on page 190) to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) parameters.
- Use the **LLDP-MED Network Policy** screen (Section 30.9 on page 191) to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) network policy parameters.
- Use the **LLDP-MED Location** screen (Section 30.10 on page 192) to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) location parameters.

30.3 LLDP Local Status

This screen displays a summary of LLDP status on this Switch. Click **PORT** > **LLDP** > **LLDP** > **LLDP Local Status** to display the screen as shown next.

Figure 120 PORT > LLDP > LLDP > LLDP Local Status



The following table describes the labels in this screen.

Table 76 PORT > LLDP > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	This displays the chassis ID of the local Switch, that is the Switch you are configuring. The chassis ID is identified by the chassis ID subtype. • **Chassis ID Subtype** – This displays how the chassis of the Switch is identified. • **Chassis ID** – This displays the chassis ID of the local Switch.
System Name TLV	**System Name** – This shows the host name of the Switch.
System Description TLV	**System Description** – This shows the firmware version of the Switch.
System Capabilities TLV	This shows the System Capabilities enabled and supported on the local Switch. • **System Capabilities Supported** – Bridge • **System Capabilities Enabled** – Bridge
Management Address TLV	The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher layer entities to assist discovery by network management. The TLV may also include the system interface number and an object identifier (OID) that are associated with this management address. This field displays the Management Address settings on the specified ports. • **Management Address Subtype** – ipv4 or all-802 • **Interface Number Subtype** – unknown • **Interface Number** – 0 (not supported) • **Object Identifier** – 0 (not supported)

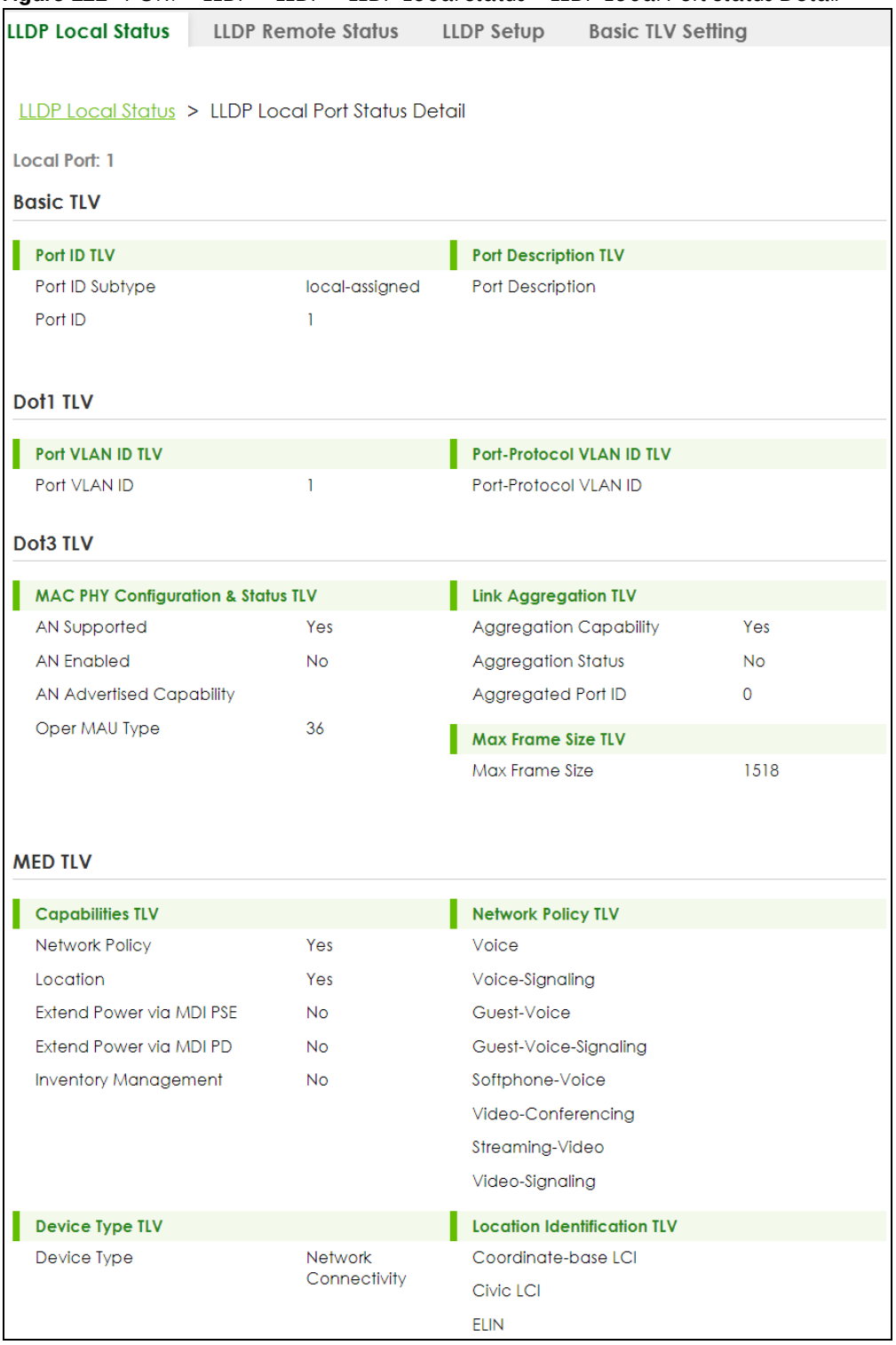
Table 76 PORT > LLDP > LLDP > LLDP Local Status (continued)

LABEL	DESCRIPTION
LLDP Port Information This displays the local port information.	
Local Port	This displays the number of the Switch port which receives the LLDPDU from the remote device. Click a port number to view the detailed LLDP status on this port in the **LLDP Local Port Status Details** screen.
Port ID Subtype	This indicates how the port ID field is identified.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted.
Port Description	This shows the port description that the Switch will advertise from this port.

30.3.1 LLDP Local Port Status Details

This screen displays detailed LLDP status for each port on this Switch. Click **PORT** > **LLDP** > **LLDP** > **LLDP Local Status** and then, click a port number, for example 1 in the local port column to display the screen as shown next.

Figure 121 PORT > LLDP > LLDP > LLDP Local Status > LLDP Local Port Status Detail



The following table describes the labels in this screen.

Table 77 PORT > LLDP > LLDP > LLDP Local Status > LLDP Local Port Status Details

LABEL	DESCRIPTION
Local Port	This displays the number of the Switch's port.
Basic TLV These are the Basic TLV flags	
Port ID TLV	The port ID TLV identifies the specific port that transmitted the LLDP frame. • **Port ID Subtype** – This shows how the port is identified. • **Port ID** – This is the ID of the port.
Port Description TLV	**Port Description** – This displays the local port description.
Dot1 TLV	
Port VLAN ID TLV	**Port VLAN ID** – This displays the VLAN ID sent by the IEEE 802.1 Port VLAN ID TLV.
Port-Protocol VLAN ID TLV	**Port-Protocol VLAN ID** – This displays the IEEE 802.1 Port Protocol VLAN ID TLVs, which indicates whether the VLAN is enabled and supported.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. • **AN Supported** – Displays if the port supports or does not support auto-negotiation. • **AN Enabled** – The current auto-negotiation status of the port. • **AN Advertised Capability** – The auto-negotiation capabilities of the port. • **Oper MAU Type** – The current Medium Attachment Unit (MAU) type of the port.
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. • **Aggregation Capability** – The current aggregation capability of the port. • **Aggregation Status** – The current aggregation status of the port. • **Aggregation Port ID** – The aggregation ID of the current port.
Max Frame Size TLV	This displays the maximum supported frame size in octets.
MED TLV LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.	
Capabilities TLV	This field displays which LLDP-MED TLV are capable to transmit on the Switch. • **Network Policy** • **Location** • **Extend Power via MDI PSE** • **Extend Power via MDI PD** • **Inventory Management**

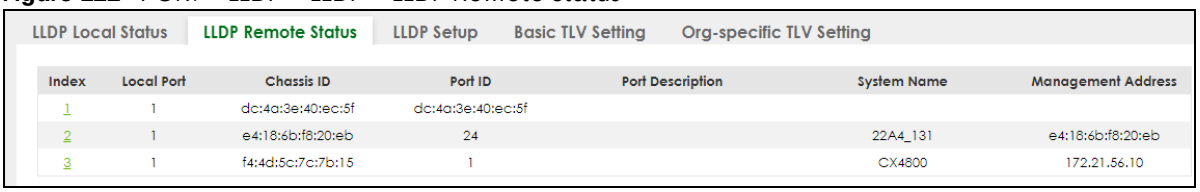
Table 77 PORT > LLDP > LLDP > LLDP Local Status > LLDP Local Port Status Details (continued)

LABEL	DESCRIPTION
Network Policy TLV	This displays a network policy for the specified application. • **Voice** • **Voice-Signaling** • **Guest-Voice** • **Guest-Voice-Signaling** • **Softphone-Voice** • **Video-Conferencing** • **Streaming-Video** • **Video-Signaling**
Device Type TLV	**Device Type** – This is the LLDP-MED device class. The Zyxel Switch device type is: • Network Connectivity
Location Identification TLV	This shows the location information of a caller by its ELIN (Emergency Location Identifier Number) or the IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). • **Coordinate-based LCI** – Latitude, longitude and altitude coordinates of the location Configuration Information (LCI) • **Civic LCI** – IETF Geopriv Civic Address based Location Configuration Information • **ELIN** – (Emergency Location Identifier Number)

30.4 LLDP Remote Status

This screen displays a summary of LLDP status for each LLDP connection to a neighboring Switch. Click **PORT** > **LLDP** > **LLDP** > **LLDP Remote Status** to display the screen as shown next.

Figure 122 PORT > LLDP > LLDP > LLDP Remote Status



The following table describes the labels in this screen.

Table 78 PORT > LLDP > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
Index	The index number shows the number of remote devices that are connected to the Switch. Click on an index number to view the detailed LLDP status for this remote device in the **LLDP Remote Port Status Details** screen.
Local Port	This is the number of the Switch's port that received LLDPDU from the remote device.
Chassis ID	This displays the chassis ID of the remote device associated with the transmitting LLDP agent. The chassis ID is identified by the chassis ID subtype. For example, the MAC address of the remote device.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted. The port ID is identified by the port ID subtype.
Port Description	This displays a description for the port from which this LLDPDU was transmitted.

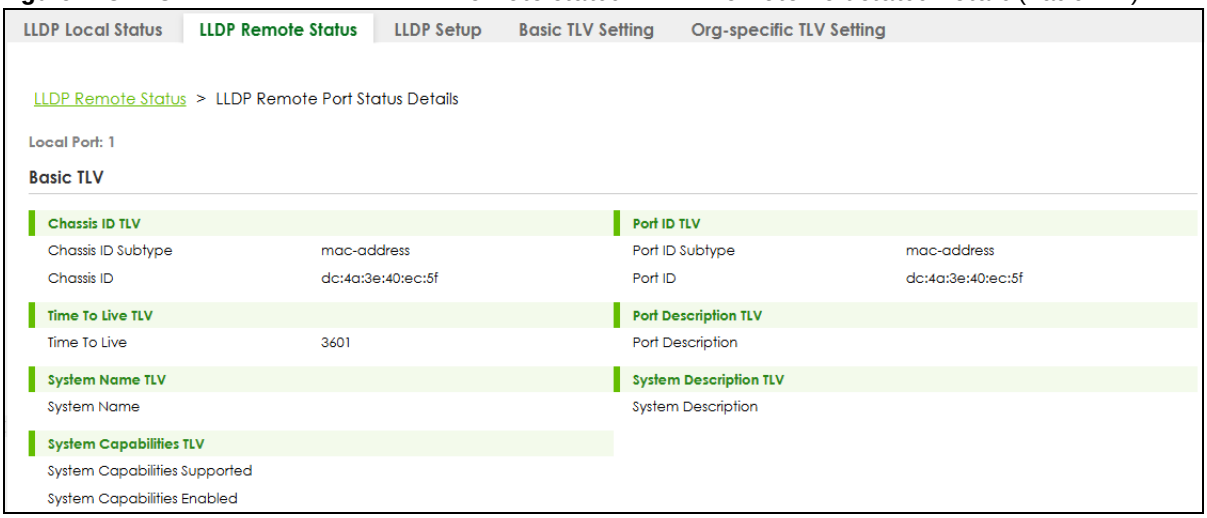
Table 78 PORT > LLDP > LLDP > LLDP Remote Status (continued)

LABEL	DESCRIPTION
System Name	This displays the system name of the remote device.
Management Address	This displays the management address of the remote device. It could be the MAC address or IP address.

30.4.1 LLDP Remote Port Status Details

This screen displays detailed LLDP status of the remote device connected to the Switch. Click **PORT** > **LLDP** > **LLDP** > **LLDP Remote Status** and then click an index number, for example 1, in the **Index** column in the **LLDP Remote Status** screen to display the screen as shown next.

Figure 123 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Basic TLV)



The following table describes the labels in Basic TLV part of the screen.

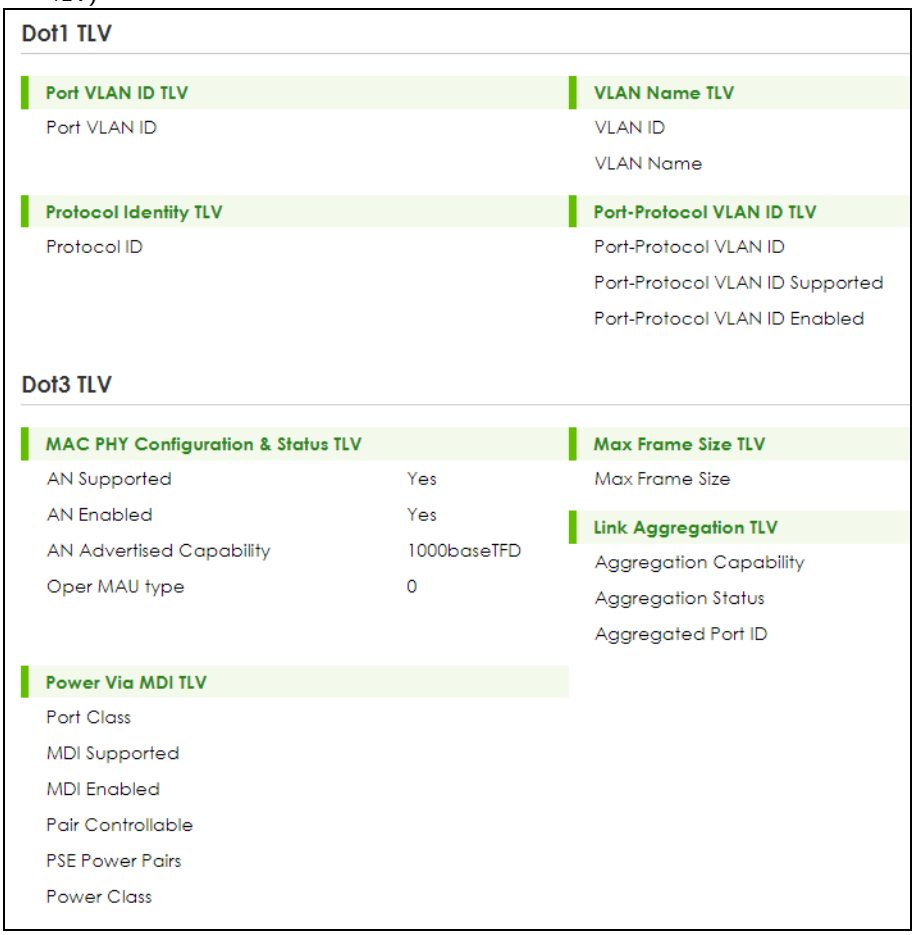
Table 79 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Basic TLV)

LABEL	DESCRIPTION
Local Port	This displays the number of the Switch's port to which the remote device is connected.
Basic TLV	
Chassis ID TLV	• **Chassis ID Subtype** – This displays how the chassis of the remote device is identified. • **Chassis ID** – This displays the chassis ID of the remote device. The chassis ID is identified by the chassis ID subtype.
Port ID TLV	• **Port ID Subtype** – This displays how the port of the remote device is identified. • **Port ID** – This displays the port ID of the remote device. The port ID is identified by the port ID subtype.
Time To Live TLV	**Time To Live** – This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP frames transmitting interval.
Port Description TLV	**Port Description** – This displays the remote port description.
System Name TLV	**System Name** – This displays the system name of the remote device.

Table 79 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Basic TLV)

LABEL	DESCRIPTION
System Description TLV	**System Description** – This displays the system description of the remote device.
System Capabilities TLV	This displays whether the system capabilities are enabled and supported on the remote device. • **System Capabilities Supported** • **System Capabilities Enabled**

Figure 124 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Dot1 and Dot3 TLV)



The following table describes the labels in the Dot1 and Dot3 parts of the screen.

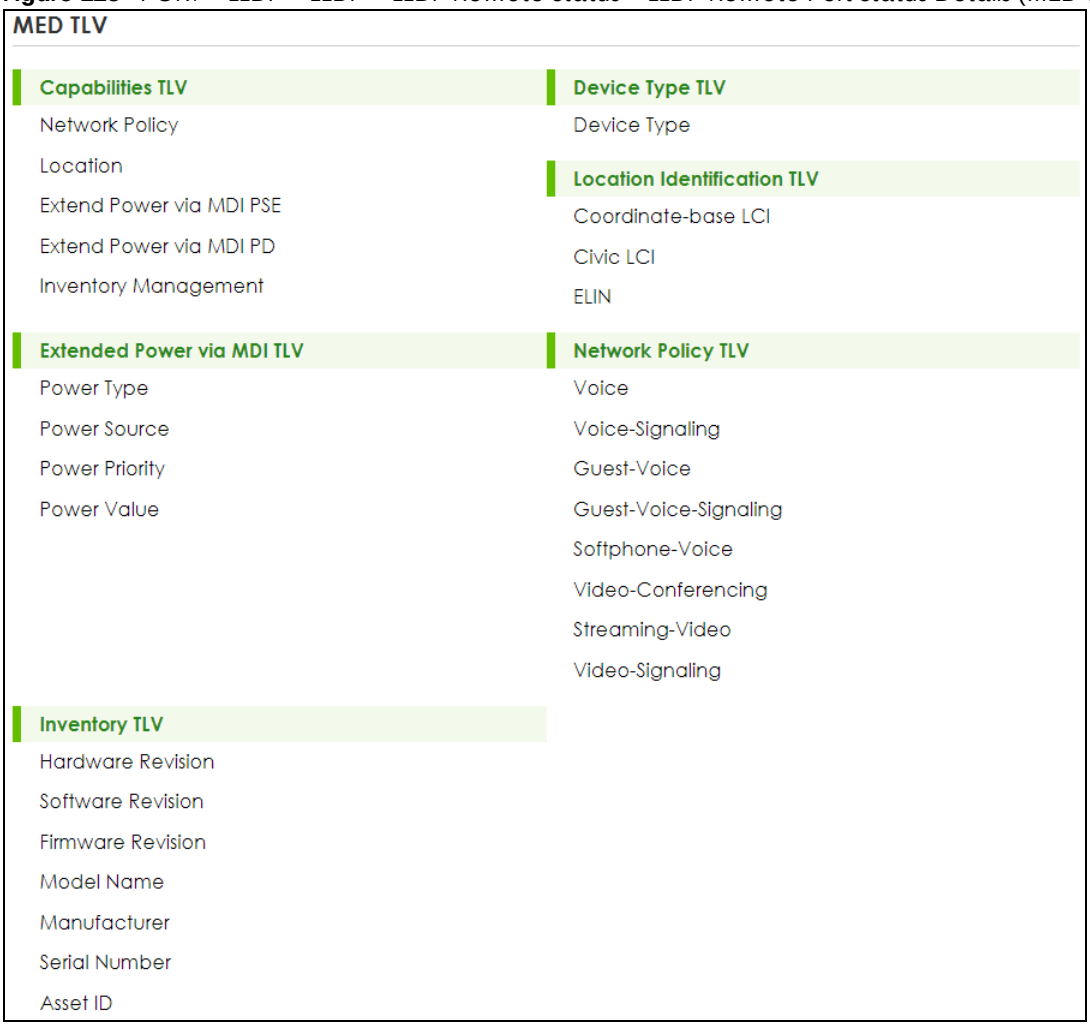
Table 80 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Dot1 TLV	
Port VLAN ID TLV	**Port VLAN ID** – This displays the VLAN ID of this port on the remote device.
Vlan Name TLV	This shows the VLAN ID and name for remote device port. • **VLAN ID** • **VLAN Name**

Table 80 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Dot1 and Dot3 TLV) (continued)

LABEL	DESCRIPTION
Protocol Identity TLV	**Protocol ID** – The Protocol Identity TLV allows the Switch to advertise the particular protocols that are accessible through its port.
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLV, which indicates whether the VLAN ID and whether it is enabled and supported on the port of remote Switch which sent the LLDPDU. • **Port-Protocol VLAN ID** • **Port-Protocol VLAN ID Supported** • **Port-Protocol VLAN ID Enabled**
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. • **AN Supported** – Displays if the port supports or does not support auto-negotiation. • **AN Enabled** – The current auto-negotiation status of the port. • **AN Advertised Capability** – The auto-negotiation capabilities of the port. • **Oper MAU Type** – The current Medium Attachment Unit (MAU) type of the port.
Max Frame Size TLV	**Max Frame Size** – This displays the maximum supported frame size in octets.
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. • **Aggregation Capability** – The current aggregation capability of the port. • **Aggregation Status** – The current aggregation status of the port. • **Aggregated Port ID** – The aggregation ID of the current port.
Power Via MDI TLV	The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. • **Port Class** • **MDI Supported** • **MDI Enabled** • **Pair Controllable** • **PSE Power Pairs** • **Power Class**

Figure 125 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (MED TLV)



The following table describes the labels in the MED TLV part of the screen.

Table 81 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (MED TLV)

LABEL	DESCRIPTION
MED TLV LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.	
Capabilities TLV	This displays the MED capabilities the remote port supports. • **Network Policy** • **Location** • **Extend Power via MDI PSE** • **Extend Power via MDI PD** • **Inventory Management**
Device Type TLV	LLDP-MED endpoint device classes: • **Endpoint Class I** • **Endpoint Class II** • **Endpoint Class III** • **Network Connectivity**

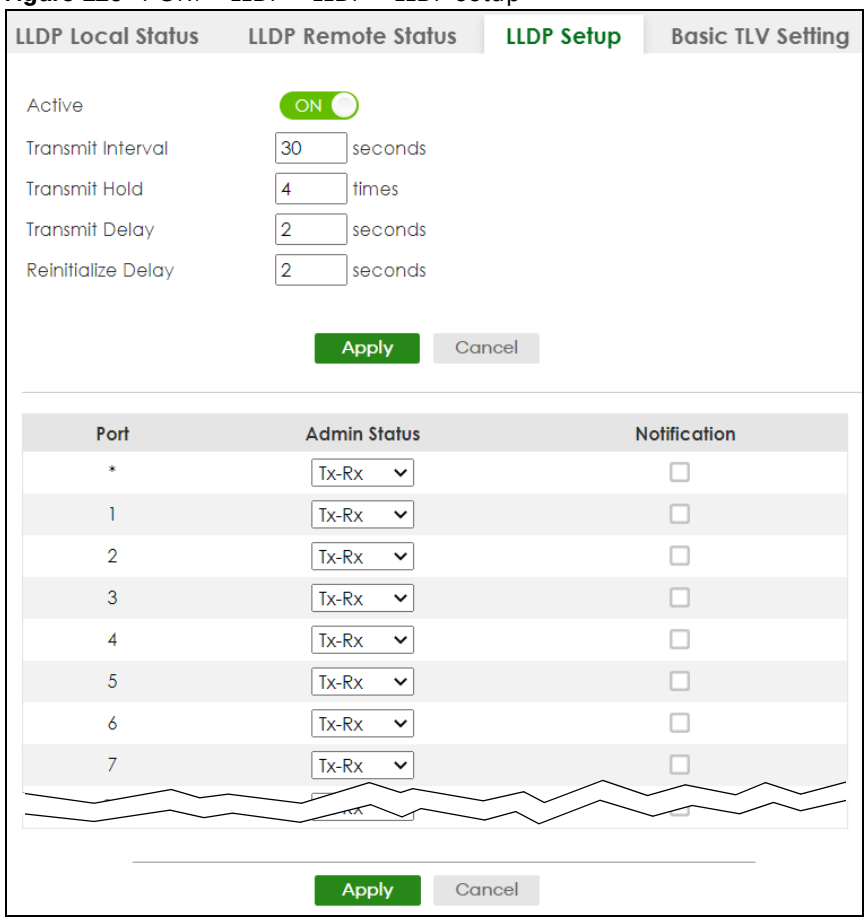
Table 81 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (MED TLV)

LABEL	DESCRIPTION
Location Identification TLV	This shows the location information of a caller by its: • **Coordinate-base LCI** – Latitude and longitude coordinates of the Location Configuration Information (LCI) • **Civic LCI** – IETF Geopriv Civic Address based Location Configuration Information • **ELIN** – (Emergency Location Identifier Number)
Extended Power via MDI TLV	Extended Power Via MDI Discovery enables detailed power information to be advertised by Media Endpoints, such as IP phones and Network Connectivity Devices such as the Switch. • **Power Type** – Whether it is currently operating from primary power or is on backup power (backup power may indicate to the Endpoint Device that it should move to a power conservation mode). • **Power Source** – Whether or not the Endpoint is currently operating from an external power source. • **Power Priority** – The Endpoint Device's power priority (which the Network Connectivity Device may use to prioritize which devices will remain in service during power shortages). • **Power Value** – Power requirement, in fractions of Watts, in current configuration.
Network Policy TLV	This displays a network policy for the specified application. • **Voice** • **Voice-Signaling** • **Guest-Voice** • **Guest-Voice-Signaling** • **Softphone-Voice** • **Video-Conferencing** • **Streaming-Video** • **Video-Signaling**
Inventory TLV	The majority of IP Phones lack support of management protocols such as SNMP, so LLDP-MED inventory TLVs are used to provide their inventory information to the Network Connectivity Devices such as the Switch. The Inventory TLV may contain the following information. • **Hardware Revision** • **Software Revision** • **Firmware Revision** • **Model Name** • **Manufacturer** • **Serial Number** • **Asset ID**

30.5 LLDP Setup

Use this screen to configure global LLDP settings on the Switch. Click **PORT** > **LLDP** > **LLDP** > **LLDP Setup** to display the screen as shown next.

Figure 126 PORT > LLDP > LLDP > LLDP Setup



The following table describes the labels in this screen.

Table 82 PORT > LLDP > LLDP > LLDP Setup

LABEL	DESCRIPTION
Active	Select to enable LLDP on the Switch. It is enabled by default.
Transmit Interval	Enter how many seconds the Switch waits before sending LLDP packets.
Transmit Hold	Enter the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP packets transmitting interval.
Transmit Delay	Enter the delay (in seconds) between successive LLDPDU transmissions initiated by value or status changes in the Switch MIB.
Reinitialize Delay	Enter the number of seconds for LLDP to wait before initializing on a port.
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.
Port	This displays the Switch's port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.

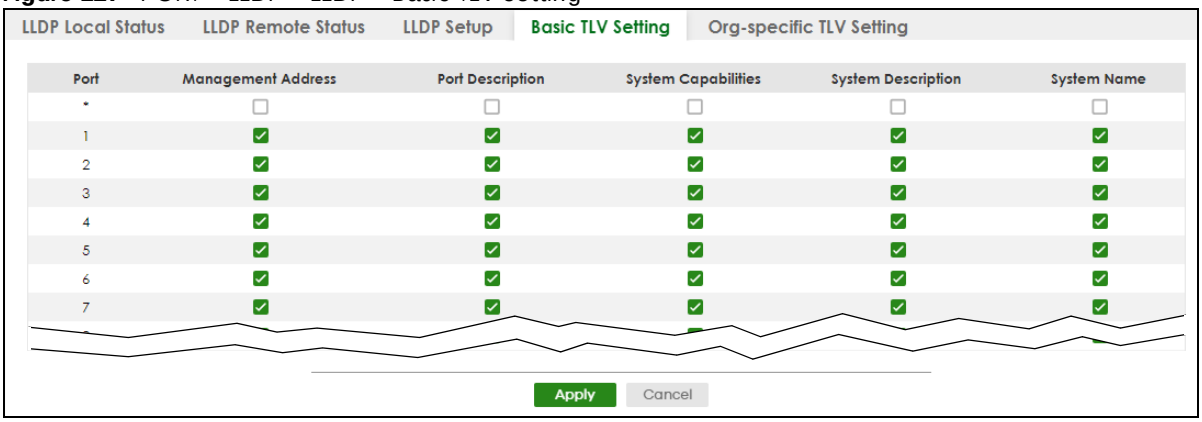
Table 82 PORT > LLDP > LLDP > LLDP Setup (continued)

LABEL	DESCRIPTION
Admin Status	Select whether LLDP transmission and/or reception is allowed on this port. • **Disable** – not allowed • **Tx-Only** – transmit only • **Rx-Only** – receive only • **Tx-Rx** – transmit and receive
Notification	Select whether LLDP notification is enabled on this port.
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.

30.6 Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **PORT** > **LLDP** > **LLDP** > **Basic TLV Setting** to display the screen as shown next.

Figure 127 PORT > LLDP > LLDP > Basic TLV Setting



The following table describes the labels in this screen.

Table 83 PORT > LLDP > LLDP > Basic TLV Setting

LABEL	DESCRIPTION
Port	This displays the Switch's port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Management Address	Select the checkboxes to enable or disable the sending of Management Address TLVs on the ports.
Port Description	Select the checkboxes to enable or disable the sending of Port Description TLVs on the ports.
System Capabilities	Select the checkboxes to enable or to disable the sending of System Capabilities TLVs on the ports.
System Description	Select the checkboxes to enable or to disable the sending of System Description TLVs on the ports.
System Name	Select the checkboxes to enable or to disable the sending of System Name TLVs on the ports.

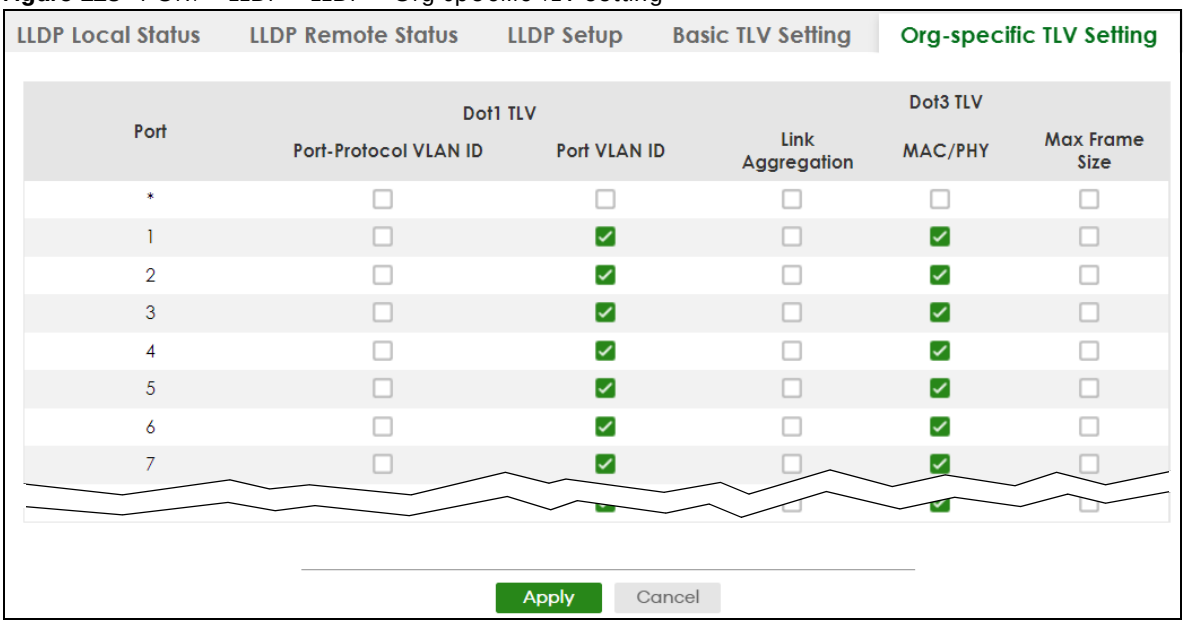
Table 83 PORT > LLDP > LLDP > Basic TLV Setting (continued)

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.

30.7 Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **PORT** > **LLDP** > **LLDP** > **Org-specific TLV Setting** to display the screen as shown next.

Figure 128 PORT > LLDP > LLDP > Org-specific TLV Setting



The following table describes the labels in this screen.

Table 84 PORT > LLDP > LLDP > Org-specific TLV Setting

LABEL	DESCRIPTION
Port	This displays the Switch's port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Dot1 TLV	
Port-Protocol VLAN ID	Select the checkboxes to enable or disable the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs on the ports.
Port VLAN ID	Select the checkboxes to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the ports. All checkboxes in this column are enabled by default.
Dot3 TLV	
Link Aggregation	Select the checkboxes to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the ports.

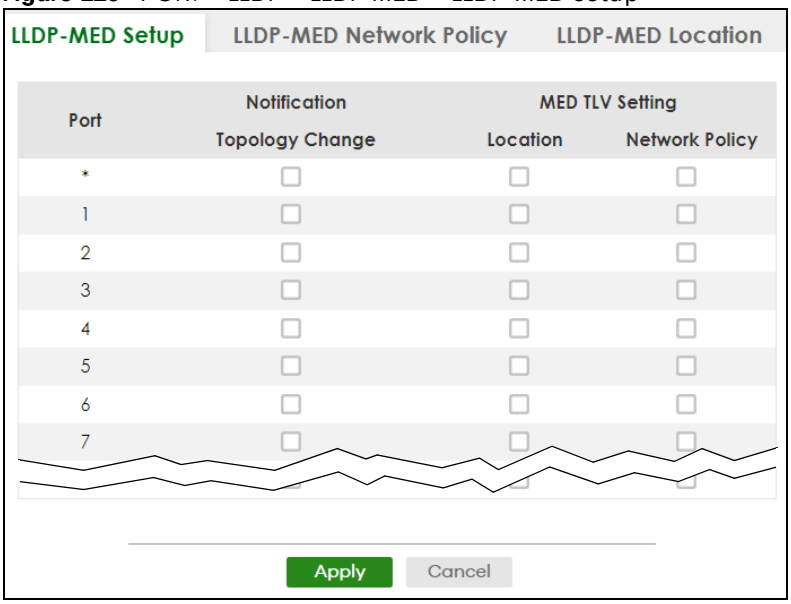
Table 84 PORT > LLDP > LLDP > Org-specific TLV Setting (continued)

LABEL	DESCRIPTION
MAC/PHY	Select the checkboxes to enable or disable the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the ports. All checkboxes in this column are enabled by default.
Max Frame Size	Select the checkboxes to enable or disable the sending of IEEE 802.3 Max Frame Size TLVs on the ports.
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.

30.8 LLDP-MED Setup

Click **PORT** > **LLDP** > **LLDP MED** > **LLDP-MED Setup** to display the screen as shown next.

Figure 129 PORT > LLDP > LLDP MED > LLDP-MED Setup



The following table describes the labels in this screen.

Table 85 PORT > LLDP > LLDP MED > LLDP-MED Setup

LABEL	DESCRIPTION
Port	This displays the Switch's port number. Select * to configure all ports simultaneously.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Notification	
Topology Change	Select to enable LLDP-MED topology change traps on this port.
MED TLV Setting	
Location	Select to enable transmitting LLDP-MED location TLV.

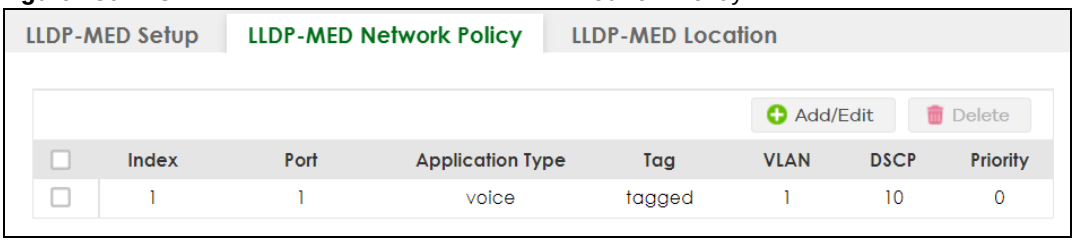
Table 85 PORT > LLDP > LLDP MED > LLDP-MED Setup (continued)

LABEL	DESCRIPTION
Network Policy	Select to enable transmitting LLDP-MED Network Policy TLV.
Apply	Click **Apply** to save the 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.

30.9 LLDP-MED Network Policy

Click **PORT** > **LLDP** > **LLDP MED** > **LLDP-MED Network Policy** to display the screen as shown next.

Figure 130 PORT > LLDP > LLDP MED > LLDP-MED Network Policy



The following table describes the labels in this screen.

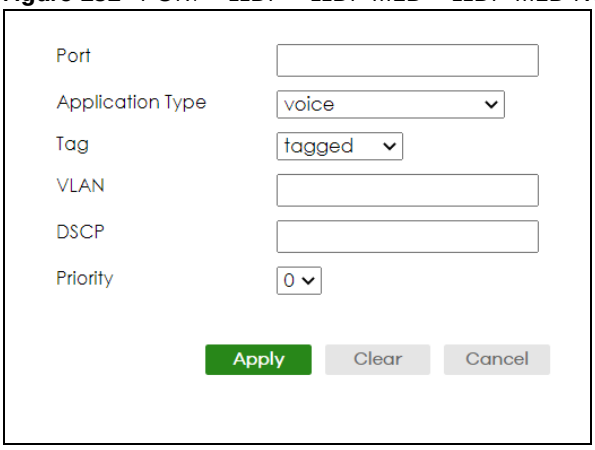
Table 86 PORT > LLDP > LLDP MED > LLDP-MED Network Policy

LABEL	DESCRIPTION
Index	This field displays the of index number of the network policy. Click an index number to edit the rule.
Port	This field displays the port number of the network policy.
Application Type	This field displays the application type of the network policy.
Tag	This field displays the Tag Status of the network policy.
VLAN	This field displays the VLAN ID of the network policy.
DSCP	This field displays the DSCP value of the network policy.
Priority	This field displays the priority value of the network policy.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new schedule rule or edit a selected one.
Delete	Select the rules that you want to remove, then click **Delete**.

30.9.1 Add/Edit LLDP-MED Network Policy

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 131 PORT > LLDP > LLDP MED > LLDP-MED Network Policy > Add/Edit



The following table describes the labels in this screen.

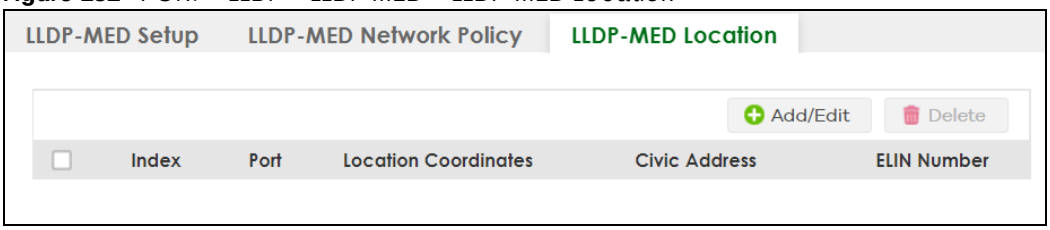
Table 87 PORT > LLDP > LLDP MED > LLDP-MED Network Policy > Add/Edit

LABEL	DESCRIPTION
Port	Enter the port number to set up the LLDP-MED network policy. You can enter multiple ports separated by (no space) comma (“,”) or hyphen (“-”) for a range. For example, enter “3-5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Application Type	Select the type of application used in the network policy. • **voice** • **voice-signaling** • **guest-voice** • **guest-voice-signaling** • **softphone-voice** • **video-conferencing** • **streaming-video** • **video-signaling**
Tag	Select to tag or untag in the network policy. • **tagged** • **untagged**
VLAN	Enter the VLAN ID number. It should be from 1 to 4094. For priority tagged frames, enter “0”.
DSCP	Enter the DSCP value of the network policy. The value is defined from 0 through 63 with the 0 representing use of the default DSCP value.
Priority	Enter the priority value for the network policy.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

30.10 LLDP-MED Location

Click **PORT** > **LLDP** > **LLDP MED** > **LLDP-MED Location** to display the screen as shown next.

Figure 132 PORT > LLDP > LLDP MED > LLDP-MED Location



The following table describes the labels in this screen.

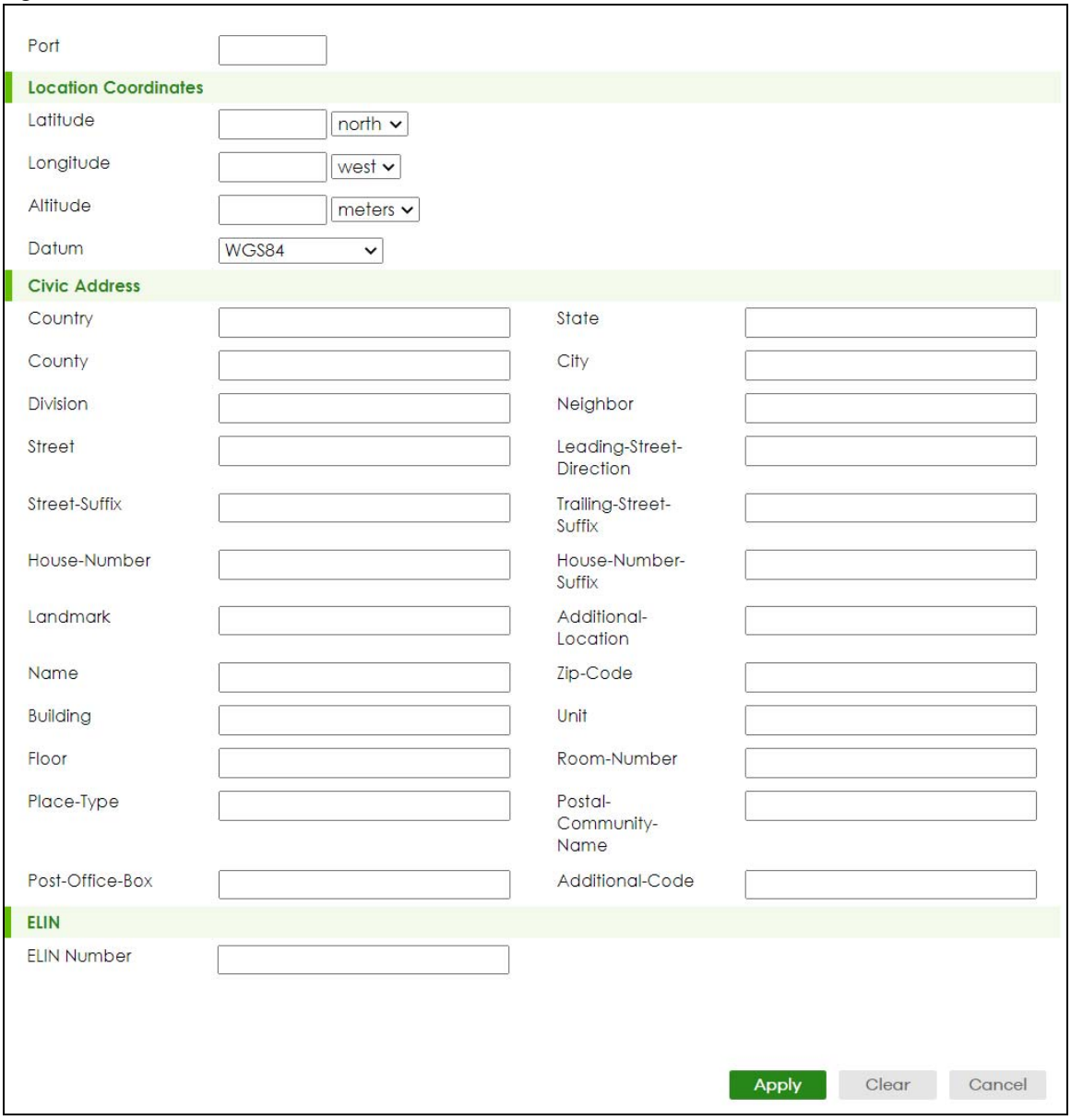
Table 88 PORT > LLDP > LLDP MED > LLDP-MED Location

LABEL	DESCRIPTION
Index	This lists the index number of the location configuration. Click an index number to view or edit the location.
Port	This lists the port number of the location configuration.
Location Coordinates	This field displays the location configuration information based on geographical coordinates that includes longitude, latitude, altitude and datum.
Civic Address	This field displays the Civic Address for the remote device using information such as Country, State, County, City, Street, Number, ZIP code and additional information.
ELIN Number	This field shows the Emergency Location Identification Number (ELIN), which is used to identify endpoint devices when they issue emergency call services. The valid length is form 10 to 25 characters.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new location or edit a selected one.
Delete	Select the locations that you want to remove, then click **Delete**.

30.10.1 Add/Edit LLDP-MED Location

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 133 PORT > LLDP > LLDP MED > LLDP-MED Location > Add/Edit



The following table describes the labels in this screen.

Table 89 PORT > LLDP > LLDP MED > LLDP-MED Location > Add/Edit

LABEL	DESCRIPTION
Port	Enter the port number you want to set up the location within the LLDP-MED network.
Location Coordinates The LLDP-MED uses geographical coordinates and Civic Address to set the location information of the remote device. Geographical based coordinates includes latitude, longitude, altitude and datum. Civic Address includes Country, State, County, City, Street and other related information.	
Latitude	Enter the latitude information. The value should be from 0º to 90º. • **north** • **south**

Table 89 PORT > LLDP > LLDP MED > LLDP-MED Location > Add/Edit (continued)

LABEL	DESCRIPTION
Longitude	Enter the longitude information. The value should be from 0º to 180º. • **west** • **east**
Altitude	Enter the altitude information. The value should be from –2097151 to 2097151 in meters or in floors. • **meters** • **floor**
Datum	Select the appropriate geodetic datum used by GPS. • **WGS84** • **NAD83-NAVD88** • **NAD83-MLLW**
Civic Address	Enter the Civic Address by providing information such as Country, State, County, City, Street, Number, ZIP code and other additional information. Enter at least 2 fields in this configuration including the Country. The valid length of the Country field is 2 characters and all other fields are up to 32 characters. • **Country** • **State** • **County** • **City** • **Division** • **Neighbor** • **Street** • **Leading-Street-Direction** • **Street-Suffix** • **Trailing-Street-Suffix** • **House-Number** • **House-Number-Suffix** • **Landmark** • **Additional-Location** • **Name** • **Zip-Code** • **Building** • **Unit** • **Floor** • **Room-Number** • **Place-Type** • **Postal-Community-Name** • **Post-Office-Box** • **Additional-Code**
ELIN Number	Enter a numerical digit string, corresponding to the ELIN identifier which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The valid length is from 10 to 25 characters.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 31 OAM

31.1 OAM Overview

Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units or OAM PDUs to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah. Because link layer Ethernet OAM operates at layer two of the OSI (Open Systems Interconnection Basic Reference) model, neither IP or SNMP are necessary to monitor or troubleshoot network connection problems.

The Switch supports the following IEEE 802.3ah features:

- Discovery – this identifies the devices on each end of the Ethernet link and their OAM configuration.
- Remote Loopback – this can initiate a loopback test between Ethernet devices.

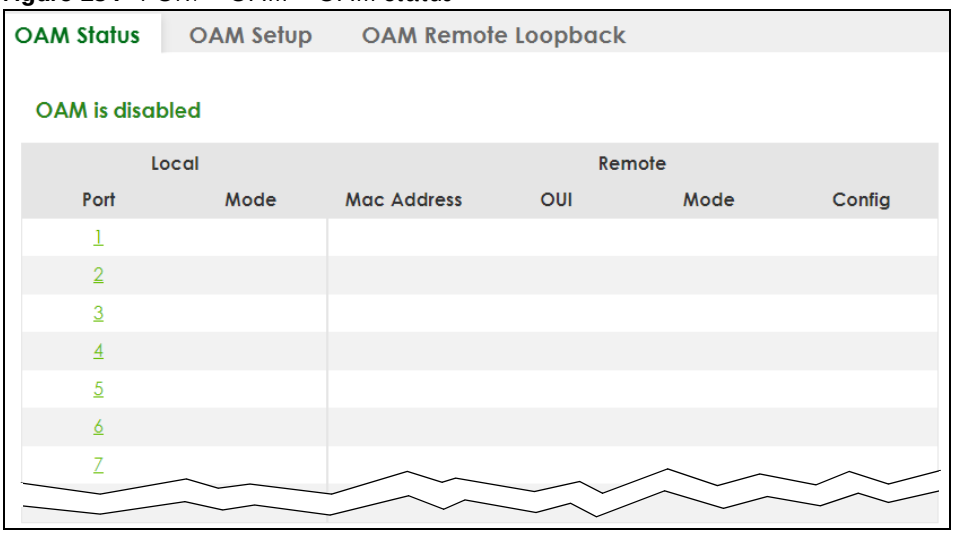
31.1.1 What You Can Do

- Use the **OAM Status** screen (Section 31.2 on page 196) to view the configuration of ports on which Ethernet OAM is enabled.
- Use the **OAM Setup** screen (Section 31.3 on page 201) to enable Ethernet OAM on the Switch.
- Use the **OAM Remote Loopback** screen (Section 31.4 on page 202) to perform remote-loopback tests.

31.2 OAM Status

Use this screen to view the configuration of ports on which Ethernet OAM is enabled. Click **PORT** > **OAM** > **OAM Status** in the navigation panel.

Figure 134 PORT > OAM > OAM Status



The following table describes the fields in the above screen.

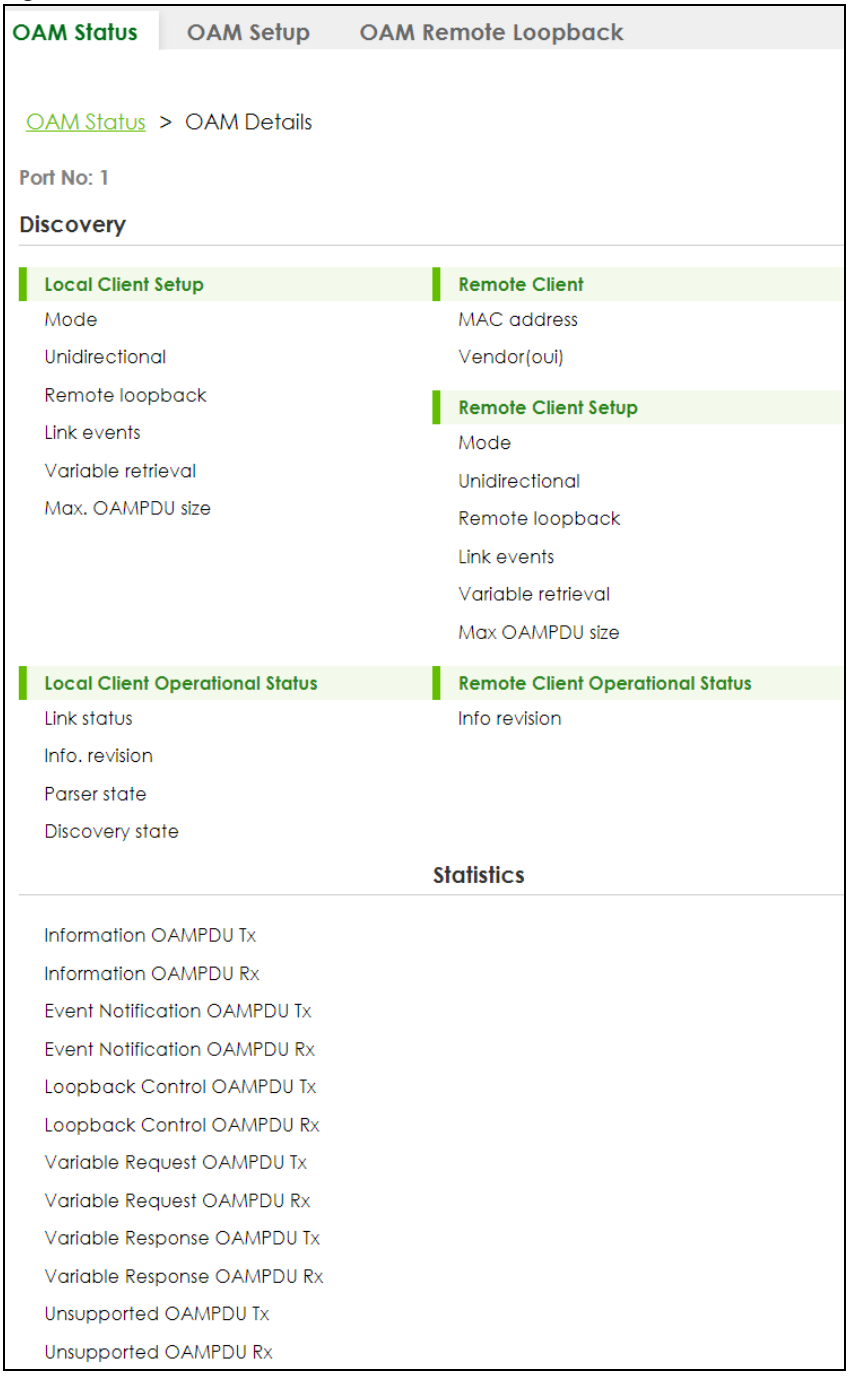
Table 90 PORT > OAM > OAM Status

LABEL	DESCRIPTION
Local This section displays information about the ports on the Switch.	
Port	This field displays the port number.
Mode	This field displays the operational state of the port when OAM is enabled on the port. **Active** – Allows the port to issue and respond to Ethernet OAM commands. **Passive** – Allows the port to respond to Ethernet OAM commands.
Remote This section displays information about the remote device.	
Mac Address	This field displays the MAC address of the remote device.
OUI	This field displays the OUI (first 3 bytes of the MAC address) of the remote device.
Mode	This field displays the operational state of the port when OAM is enabled on the port. **Active** – Allows the port to issue and respond to Ethernet OAM commands. **Passive** – Allows the port to respond to Ethernet OAM commands.
Config	This field displays the capabilities of the Switch and remote device.

31.2.1 OAM Details

Use this screen to view OAM configuration details and operational status of a specific port. Click a number in the **Port** column in the **PORT** > **OAM** > **OAM Status** screen to display the screen as shown next.

Figure 135 PORT > OAM > OAM Status > OAM Details



The following table describes the fields in the above screen.

Table 91 PORT > OAM > OAM Status > OAM Details

LABEL	DESCRIPTION
Port No	This field displays the port number.
Discovery This section displays OAM configuration details and operational status of the port on the Switch and/or the remote device.	

Table 91 PORT > OAM > OAM Status > OAM Details (continued)

LABEL	DESCRIPTION
Local Client/Remote Client Setup	
Mode	This field displays the OAM mode. The device in active mode (typically the service provider's device) controls the device in passive mode (typically the subscriber's device). **Active**: The port initiates OAM discovery; sends information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs. **Passive**: The port waits for the remote device to initiate OAM discovery; sends information PDUs; may send event notification PDUs; and may respond to variable request PDUs or loopback control PDUs. The Switch might not support some types of PDUs, as indicated in the fields below.
Unidirectional	This field indicates whether or not the port can send information PDUs to transmit fault information when the receive path is non-operational.
Remote loopback	This field indicates whether or not the port can use loopback control PDUs to put the remote device into loopback mode.
Link events	This field indicates whether or not the port can interpret link events, such as link fault and dying gasp. Link events are sent in event notification PDUs and indicate when the number of errors in a given interval (time, number of frames, number of symbols, or number of error frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well.
Variable retrieval	This field indicates whether or not the port can respond to requests for more information, such as requests for Ethernet counters and statistics, about link events.
Max. OAMPDU size	This field displays the maximum size of PDU for receipt and delivery.
Local Client/Remote Client Operational status	
Link status	This field indicates that the link between the Switch port and a connected IEEE 802.3ah-enabled remote Ethernet device is up or down.
Info. revision	This field displays the current version of local state and configuration. This two-octet value starts at zero and increments every time the local state or configuration changes.
Parser state	This field indicates the current state of the parser. **Forward**: The port is forwarding packets normally. **Loopback**: The port is in loopback mode. **Discard**: The port is discarding non-OAM PDUs because it is trying to or has put the remote device into loopback mode.

Table 91 PORT > OAM > OAM Status > OAM Details (continued)

LABEL	DESCRIPTION
Discovery state	This field indicates the state in the OAM discovery process. OAM-enabled devices use this process to detect each other and to exchange information about their OAM configuration and capabilities. OAM discovery is a handshake protocol. **Fault**: One of the devices is transmitting OAM PDUs with link fault information, or the interface is not operational. **Active Send Local**: The port is in active mode and is trying to see if the remote device supports OAM. **Passive Wait**: The port is in passive mode and is waiting for the remote device to begin OAM discovery. **Send Local Remote**: This state occurs in the following circumstances. • The port has discovered the remote device but has not accepted or rejected the connection yet. • The port has discovered the remote device and rejected the connection. **Send Local Remote OK**: The port has discovered the remote device and has accepted the connection. In addition, the remote device has not accepted or rejected the connection yet, or the remote device has rejected the connected. **Send Any**: The port and the remote device have accepted the connection. This is the operating state for OAM links that are fully operational.
Remote Client	
MAC Address	This field displays the MAC address of the IEEE 802.3ah-enabled remote Ethernet device that is connected to the Switch.
Vendor(oui)	This field displays the Organizationally Unique Identifiers (OUI) representing the vendor of the IEEE 802.3ah-enabled remote Ethernet device that is connected to the Switch.
Statistics This section displays the number of OAM packets transferred on the port of the Switch.	
Information OAMPDU Tx	This field displays the number of OAM PDUs sent on the port.
Information OAMPDU Rx	This field displays the number of OAM PDUs received on the port.
Event Notification OAMPDU Tx	This field displays the number of unique or duplicate OAM event notification PDUs sent on the port.
Event Notification OAMPDU Rx	This field displays the number of unique or duplicate OAM event notification PDUs received on the port.
Loopback Control OAMPDU Tx	This field displays the number of loopback control OAM PDUs sent on the port.
Loopback Control OAMPDU Rx	This field displays the number of loopback control OAM PDUs received on the port.
Variable Request OAMPDU Tx	This field displays the number of OAM PDUs sent to request MIB objects on the remote device.
Variable Request OAMPDU Rx	This field displays the number of OAM PDUs received requesting MIB objects on the Switch.
Variable Response OAMPDU Tx	This field displays the number of OAM PDUs sent by the Switch in response to requests.
Variable Response OAMPDU Rx	This field displays the number of OAM PDUs sent by the remote device in response to requests.

Table 91 PORT > OAM > OAM Status > OAM Details (continued)

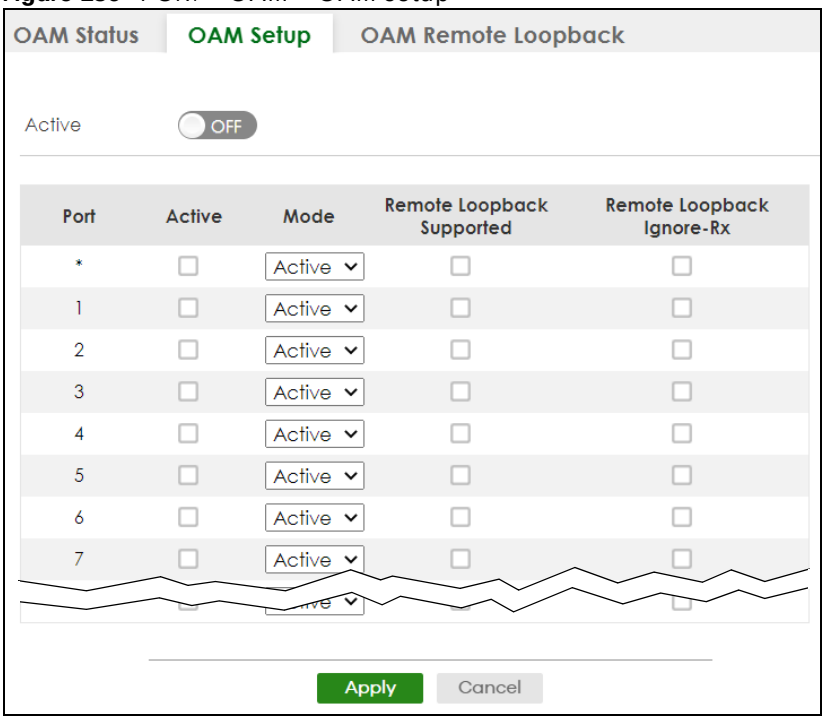
LABEL	DESCRIPTION
Unsupported OAMPDU Tx	This field displays the number of unsupported OAM PDUs sent on the port.
Unsupported OAMPDU Rx	This field displays the number of unsupported OAM PDUs received on the port.

31.3 OAM Setup

Use this screen to turn on Ethernet OAM on the Switch and ports and configure the related settings.

Click **PORT** > **OAM** > **OAM Setup** to display the configuration screen as shown.

Figure 136 PORT > OAM > OAM Setup



The following table describes the fields in the above screen.

Table 92 PORT > OAM > OAM Setup

LABEL	DESCRIPTION
Active	Enable the switch button to enable Ethernet OAM on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

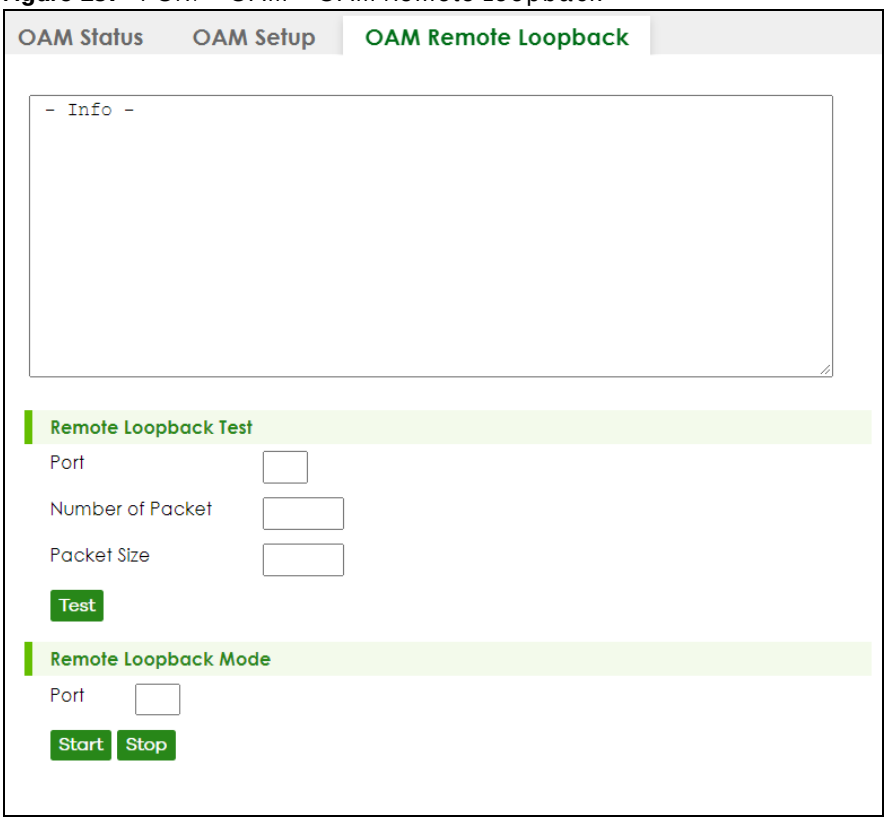
Table 92 PORT > OAM > OAM Setup (continued)

LABEL	DESCRIPTION
Active	Select this checkbox to enable Ethernet OAM on this port. Clear this checkbox to disable Ethernet OAM on the port.
Mode	Specify the OAM mode on the port. Select **Active** to allow the port to issue and respond to Ethernet OAM commands. Select **Passive** to allow the port to respond to Ethernet OAM commands.
Remote Loopback Supported	Select this checkbox to enable the remote loopback feature on the port. Otherwise, clear the checkbox to disable it.
Remote Loopback Ignore-Rx	Select this checkbox to set the Switch to process loopback commands received on the port. Otherwise, clear the checkbox to have the Switch ignore loopback commands received on the port.
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.

31.4 OAM Remote Loopback

Use this screen to perform a remote loopback test. Click **PORT** > **OAM** > **OAM Remote Loopback** to display the screen as shown.

Figure 137 PORT > OAM > OAM Remote Loopback



The following table describes the fields in the above screen.

Table 93 PORT > OAM > OAM Remote Loopback

LABEL	DESCRIPTION
Remote Loopback Test	
Port	Enter the number of the port from which the Switch performs a remote-loopback test.
Number of Packet	Define the allowable packet number of the loopback test frames.
Packet Size	Define the allowable packet size of the loopback test frames.
Test	Click **Test** to begin the test.
Remote Loopback Mode	
Port	Enter the number of the port from which the Switch sends loopback control PDUs to initiate or terminate a remote-loopback test.
Start	Click **Start** to initiate a remote-loopback test from the specified port by sending Enable Loopback Control PDUs to the remote device.
Stop	Click **Stop** to terminate a remote-loopback test from the specified port by sending Disable Loopback Control PDUs to the remote device.

CHAPTER 32
PoE Setup

32.1 PoE Status (for PoE models only)

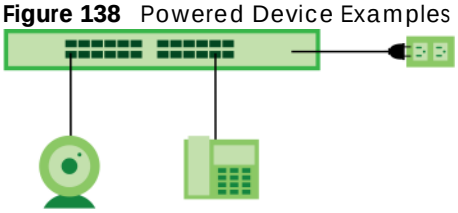
Note: The following screens are available for the PoE models only. Some features are only available for the Ethernet ports (1 to 8 for GS1920-8HPv2, 1 to 24 for GS1920-24HPv2, and 1 to 48 for GS1920-48HPv2).

The PoE models supports the IEEE 802.3at High Power over Ethernet (PoE) standard.

A powered device (PD) is a device such as an access point or a switch, that supports PoE (Power over Ethernet) so that it can receive power from another device through an Ethernet port.

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 138 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 (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

PoE-Disabled Mechanism for GS1920-8HPv2

The GS1920-8HPv2 is a compact and fanless Switch capable of supplying Power over Ethernet (PoE). Certain action will be taken when the temperature of the GS1920-8HPv2 reaches the temperature thresholds. Please see the table below for how the mechanism works.

Table 94 Temperature and Action

TEMPERATURE	ACTION
74°C/165.2.°F	When the temperature of the GS1920-8HPv2 reaches this temperature threshold, the **SYS** LED will become steady red. To cool down the GS1920-8HPv2, make sure there is enough clearance for ventilation. You can also relocate the GS1920-8HPv2 to a cooler place.

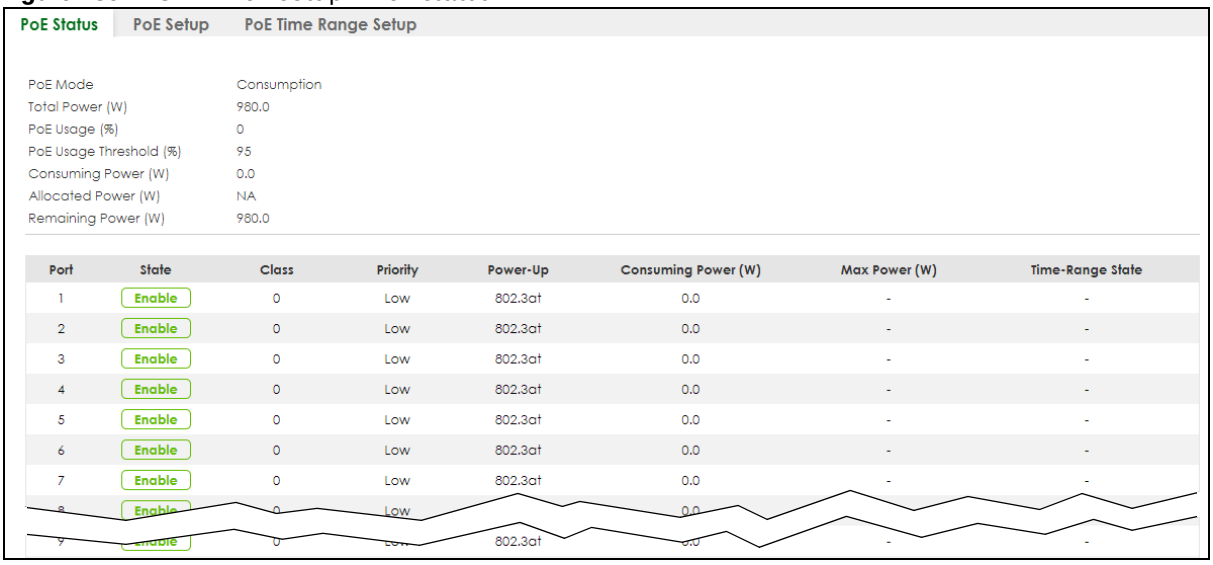
Table 94 Temperature and Action

TEMPERATURE	ACTION
79°C/174.2.°F	If the temperature keeps climbing and reaches this temperature threshold, PoE will be turned off automatically.
Below 74°C/165.2.°F	PoE will be turned on again when the temperature drops and remains below this temperature threshold for a 30-minute period.

Note: The GS1920-8HPv2 will generate logs messages for the situations listed in the **System Log** screen. They will also be sent to the syslog server.

To view the current amount of power that PDs are receiving from the Switch, click **PORT** > **PoE Setup** > **PoE Status**.

Figure 139 PORT > PoE Setup > PoE Status



The following table describes the labels in this screen.

Table 95 PORT > PoE Setup > PoE Status

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.
PoE Usage (%)	This field displays the amount of power currently being supplied to connected PoE devices (PDs) as a percentage of the total PoE power the Switch can supply. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in **PORT** > **PoE Setup** > **PoE Setup**.
PoE Usage Threshold (%)	This field displays the percentage of PoE usage. The Switch will generate a trap and/or a log when the usage exceeds the specified threshold.
Consuming Power (W)	This field displays the 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 devices. It shows **NA** when the Switch is in consumption mode. **Consuming Power (W)** can be less than or equal but not more than the **Allocated Power (W)**.

Table 95 PORT > PoE Setup > PoE Status (continued)

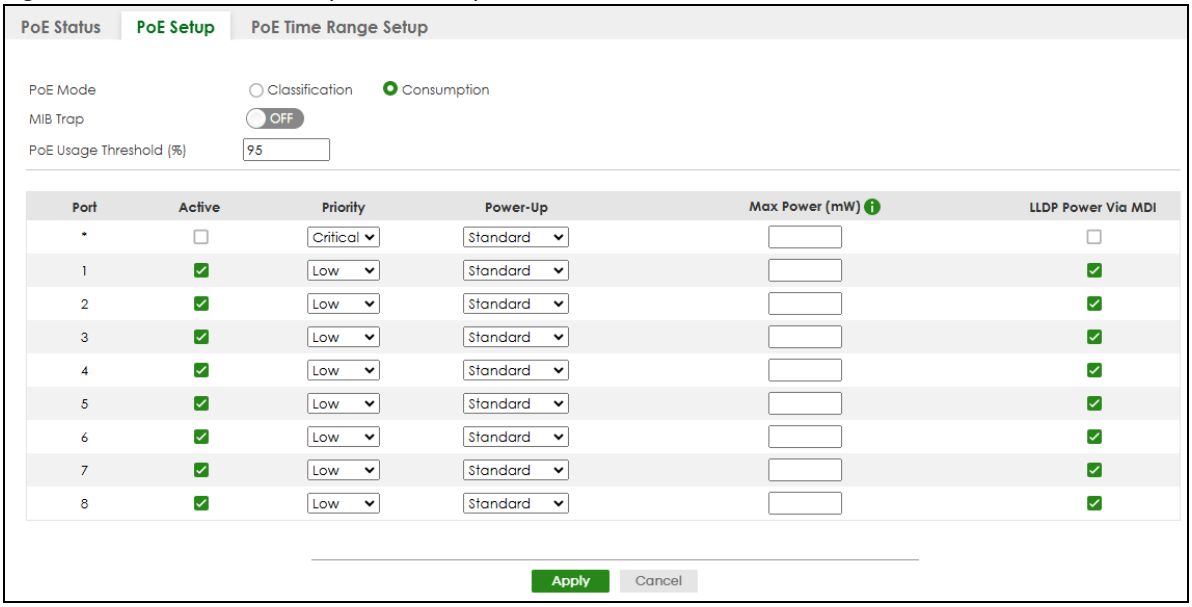
LABEL	DESCRIPTION
Remaining Power (W)	This field displays the amount of power the Switch can still provide for PoE.
Port	This is the port index number.
State	This field shows which ports can receive power from the Switch. • **Disable** – The PD connected to this port cannot get power supply. • **Enable** – The PD connected to this port can receive power.
Class	This shows the power classification of the PD. Each PD has a specified maximum power that fall under one of the classes. The **Class** is a number from 0 to 4, where each value represents the range of power that the Switch provides to the PD. Each class corresponds to a default maximum power that can be extended in **PORT** > **PoE Setup** > **PoE Setup** to the following values. • **Class 0** – default: 0.44 W to 15.4 W, can be extended to 17.8 W. • **Class 1** – default: 0.44 W to 4 W, can be extended to 5.8 W. • **Class 2** – default: 0.44 W to 7 W, can be extended to 9 W. • **Class 3** – default: 0.44 W to 15.4 W, can be extended to 17.8 W. • **Class 4** – default: 0.44 W to 30 W, can be extended to 32.8 W.
Priority	When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the priority to allow the Switch to provide power to ports with higher priority first. • **Critical** has the highest priority. • **High** has the Switch assign power to the port after all critical priority ports are served. • **Low** has the Switch assign power to the port after all critical and high priority ports are served.
Power-Up	This field displays the PoE setting the Switch uses to provide power on this port.
Consuming Power (W)	This field displays the current amount of power consumed by the PD from the Switch on this port.
Max Power (W)	This field displays the maximum amount of power the PD could use from the Switch on this port. This field displays "–" if the maximum power is not specified in **PORT** > **PoE Setup** > **PoE Setup**.
Time-Range State	This field shows whether or not the port currently receives power from the Switch according to its schedule. • It shows "**In**" followed by the time range name if PoE is currently enabled on the port. • It shows "**Out**" if PoE is currently disabled on the port. • It shows **"–"** if no schedule is applied to the port. PoE is enabled by default.

32.2 PoE Setup

Use this screen to set the PoE power management mode, priority levels, power-up mode and the maximum amount of power for the connected PDs.

Click the **PoE Setup** tab in the **PORT** > **PoE Setup** screen. The following screen opens.

Figure 140 PORT > PoE Setup > PoE Setup



The following table describes the labels in this screen.

Table 96 PORT > PoE Setup > PoE Setup

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the Switch to use. • **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. • **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 30 W (IEEE 802.3at Class 4) or 22 W (IEEE 802.3af Classes 0 to 3).
MIB Trap	The Switch sends traps (monitoring event notification) to an SNMP (Simple Network Management Protocol) manager when an event occurs. Select **ON** to allow sending of MIB Trap when the following situations occur: • Situation 1 – Trap sent whenever a PoE port status change occurs (PoE port delivers power or delivers no power to a PD (powered device) • Situation 2 – Trap sent in cases where the total power usage exceeds the PoE usage threshold • Situation 3 – Trap sent if total usage power decreases below the PoE usage threshold (only if previous total power usage exceeded the PoE usage threshold and a trap was sent). Note: If the **MIB Trap** is **ON**, you must also configure: • SNMP trap destination (**SYSTEM** > **SNMP** > **SNMP**), SNMP trap group (**SYSTEM** > **SNMP** > **SNMP Trap Group**) and SNMP trap port (**SYSTEM** > **SNMP** > **SNMP Trap Port**) for Situation 1 • SNMP trap destination and SNMP trap group for Situation 2 and Situation 3. See Section 23.1 on page 145 for more information on configuring SNMP.
PoE Usage Threshold (%)	Enter a number ranging from 1 to 99 to set the threshold. The Switch will generate a trap and/or log when the actual PoE usage is higher than the specified threshold.
Port	This is the port index number.

Table 96 PORT > PoE Setup > PoE Setup (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to provide power to a PD connected to the port. If left unchecked, the PD connected to the port cannot receive power from the Switch.
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. Select **Critical** to give the highest PD priority on the port. Select **High** to set the Switch to assign the remaining power to the port after all critical priority ports are served. Select **Low** to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.
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. Inrush current is the maximum, instantaneous input current drawn by the PD when first turned on. **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 30 W 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. **Force-802.3at** – the Switch offers power of up to 30 W on the port without performing PoE hardware classification. Select this option if the connected PD does not comply with any PoE standard and requests power higher than a standard power limit. Note: Wide Range Detection (WRD) is integrated into Force-802.3at mode. Your previous WRD configuration will be retained if you upgrade firmware to ZyNOS 4.70(xxxx.7) ('xxxx' refers to the Switch's model code) or later with WRD enabled. If you now want to disable WRD, you need to use **Maintenance** > **Erase Running-Configuration** to reset the Switch to its default settings. Note you will lose all current settings.
Max Power (mW)	Specify the maximum amount of power the PD could use from the Switch on this port. If you leave this field blank, the Switch refers to the standard or default maximum power for each class.

Table 96 PORT > PoE Setup > PoE Setup (continued)

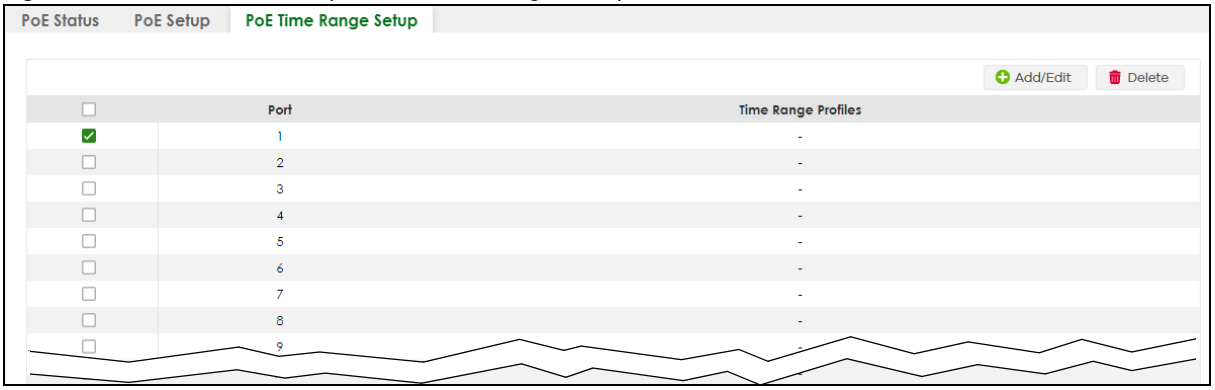
LABEL	DESCRIPTION
LLDP Power Via MDI	Select this to have the Switch negotiate PoE power with the PD connected to the port by transmitting LLDP Power Via MDI TLV frames. This helps the Switch allocate less power to the PD on this port. The connected PD must be able to request PoE power through LLDP. The Power Via MDI TLV allows PoE devices to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controllable • PSE Power Pairs • Power Class
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.

32.3 PoE Time Range Setup

Use this screen to apply a schedule to the ports on the Switch. You must first configure a schedule in the **SYSTEM** > **Time Range** > **Time Range** screen.

Click the **PoE Time Range Setup** tab in the **PORT** > **PoE Setup** screen. The following screen opens.

Figure 141 PORT > PoE Setup > PoE Time Range Setup



The following table describes the labels in this screen.

Table 97 PORT > PoE Setup > PoE Time Range Setup

LABEL	DESCRIPTION
Port	This field displays the index number of the port. Click a port number to change the schedule settings.
Time Range Profiles	This field displays the name of the schedule which is applied to the port. PoE is enabled at the specified time or date.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

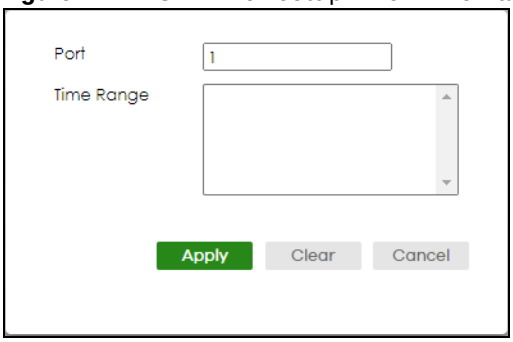
Table 97 PORT > PoE Setup > PoE Time Range Setup (continued)

LABEL	DESCRIPTION
Add/Edit	Click **Add/Edit** to add a new rule or edit a selected one.
Delete	Check the rules that you want to remove and then click the **Delete** button.

32.3.1 Add/Edit PoE Time Range

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 142 PORT > PoE Setup > PoE Time Range Setup > Add/Edit



The following table describes the labels in this screen.

Table 98 PORT > PoE Setup > PoE Time Range Setup > Add/Edit

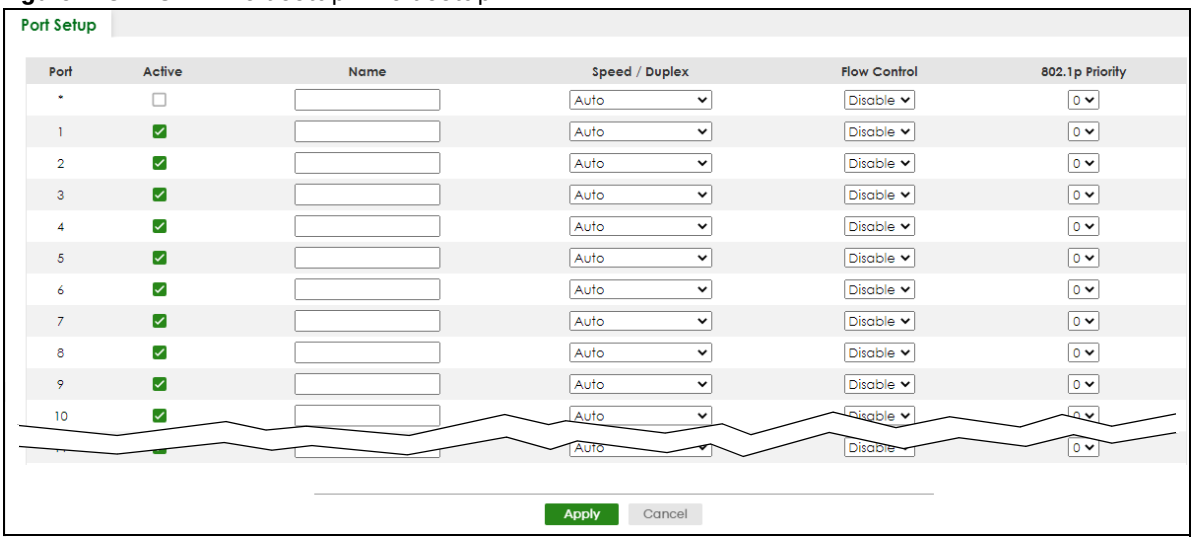
LABEL	DESCRIPTION
Port	Enter the number of the port to which you want to apply a schedule.
Time Range	This field displays the name of the schedule that you have created using the **SYSTEM** > **Time Range** > **Time Range** screen. Select a pre-defined schedule to control when the Switch enables PoE to provide power on the port. To select more than one schedule, press [SHIFT] and select the choices at the same time.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 33
Port Setup

33.1 Port Setup

Use this screen to configure Switch port settings. Click **PORT** > **Port Setup** > **Port Setup** in the navigation panel to display the configuration screen.

Figure 143 PORT > Port Setup > Port Setup



The following table describes the labels in this screen.

Table 99 PORT > Port Setup > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can enter up to 128 printable ASCII characters except [?], [|], ['] or ["]. Note: Due to space limitation, the port name may be truncated in some Web Configurator screens.

Table 99 PORT > Port Setup > Port Setup (continued)

LABEL	DESCRIPTION
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10-an** (10M/auto-negotiation), **10M/Half Duplex**, **10M/Full Duplex**, **100-an** (100M/auto-negotiation), **100M/Half Duplex**, **100M/Full Duplex** and **1G/Full Duplex** (Gigabit connections only). Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, therefore requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	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. The Switch uses IEEE802.3x flow control in full duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Select **Flow Control** to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Section 43.2 on page 268 for more information.
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.

CHAPTER 34
SWITCHING

The following chapters introduces the configurations of the links under the **SWITCHING** navigation panel.

Quick links to chapters:

CHAPTER 35
Layer 2 Protocol Tunneling

35.1 Layer 2 Protocol Tunneling Overview

This chapter shows you how to configure layer 2 protocol tunneling on the Switch.

35.1.1 What You Can Do

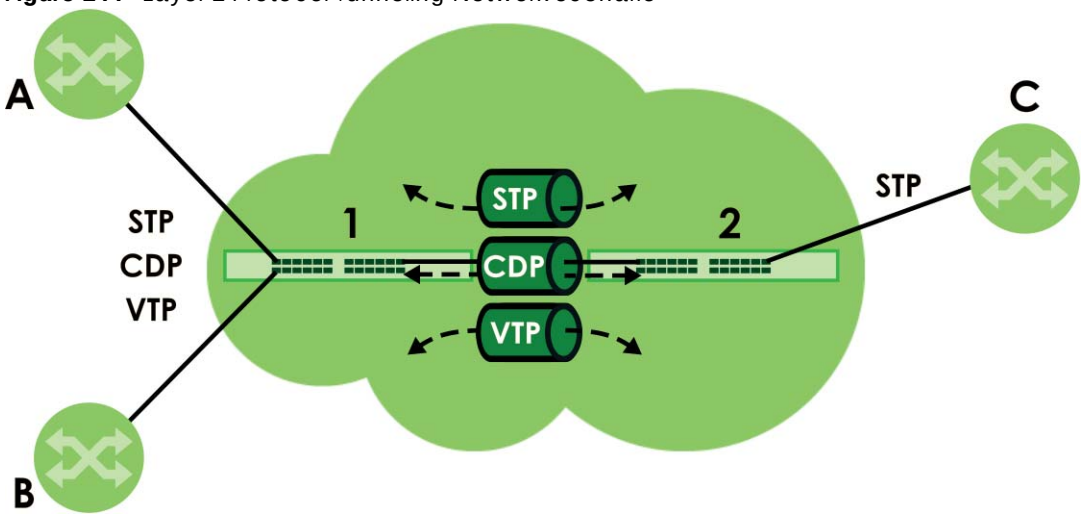
Use the **Layer 2 Protocol Tunneling** screen (Section 35.2 on page 215) to enable layer 2 protocol tunneling on the Switch and specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets.

35.1.2 What You Need to Know

Layer 2 protocol tunneling (L2PT) is used on the service provider's edge devices.

L2PT allows edge switches (**1** and **2** in the following figure) to tunnel layer 2 **STP** (Spanning Tree Protocol), **CDP** (Cisco Discovery Protocol) and **VTP** (VLAN Trunking Protocol) packets between customer switches (**A**, **B** and **C** in the following figure) connected through the service provider's network. The edge switch encapsulates layer 2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

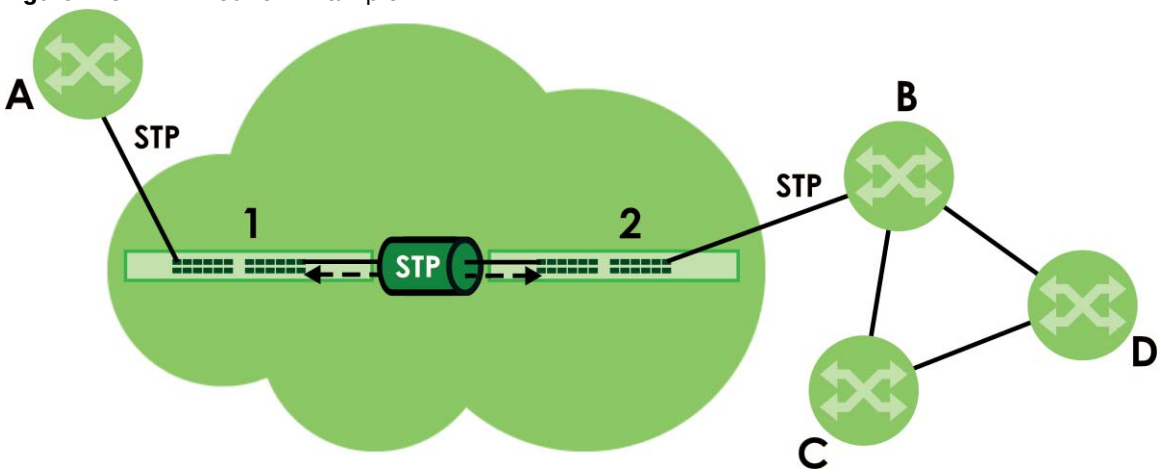
Figure 144 Layer 2 Protocol Tunneling Network Scenario



In the following example, if you enable L2PT for STP, you can have switches **A**, **B**, **C** and **D** in the same spanning tree, even though switch **A** is not directly connected to switches **B**, **C** and **D**. Topology change information can be propagated throughout the service provider's network.

To emulate a point-to-point topology between two customer switches at different sites, such as **A** and **B**, you can enable protocol tunneling on edge switches **1** and **2** for PAgP (Port Aggregation Protocol), LACP or UDLD (Uni-Directional Link Detection).

Figure 145 L2PT Network Example



35.1.2.1 Layer 2 Protocol Tunneling Mode

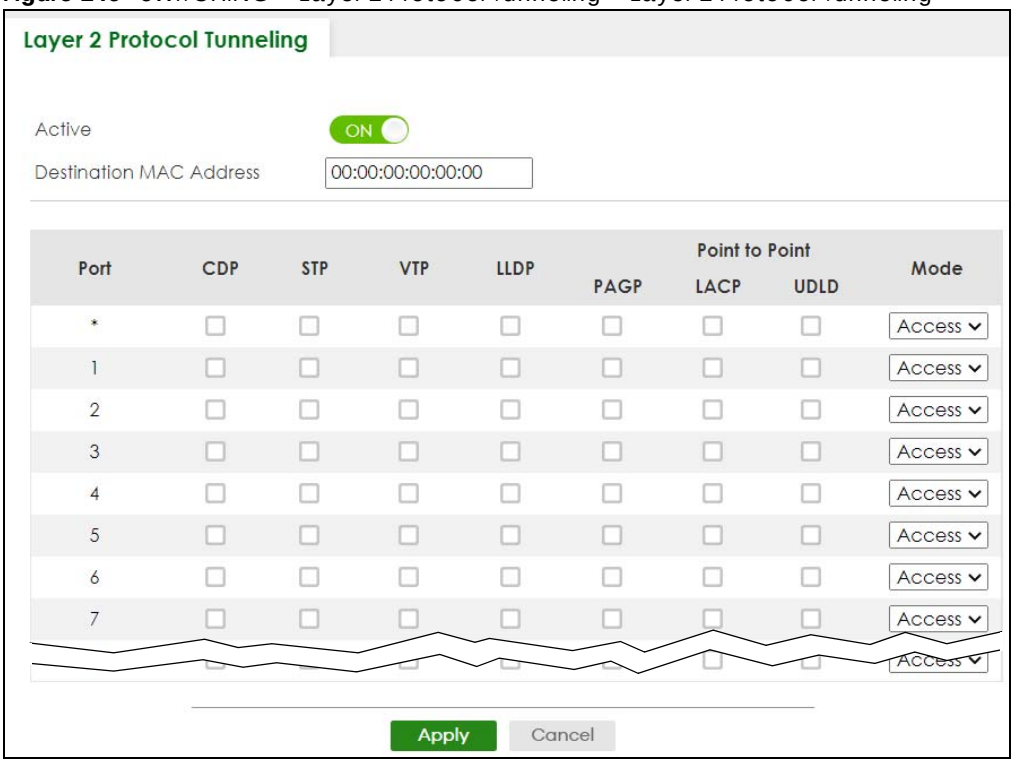
Each port can have two layer 2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in Figure 145 on page 215) and connected to a customer switch (**A** or **B**). Incoming layer 2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- The **Tunnel** port is an egress port at the edge of the service provider's network and connected to another service provider's switch. Incoming encapsulated layer 2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

35.2 Configuring Layer 2 Protocol Tunneling

Click **SWITCHING** > **Layer 2 Protocol Tunneling** > **Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 146 SWITCHING > Layer 2 Protocol Tunneling > Layer 2 Protocol Tunneling



The following table describes the labels in this screen.

Table 100 SWITCHING > Layer 2 Protocol Tunneling > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Enable the switch button to enable layer 2 protocol tunneling on the Switch.
Destination MAC Address	Specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.

Table 100 SWITCHING > Layer 2 Protocol Tunneling > Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
LLDP	Select this option to have the Switch tunnel LLDP (Link Layer Discovery Protocol) packets so that all network devices can advertise its identity and capabilities through the service provider's network.
Point to Point	The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAgP and UDLD are Cisco's proprietary data link layer protocols. PAgP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.
PAGP	Select this option to have the Switch send PAgP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically create and manage trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	Select **Access** to have the Switch encapsulate the incoming layer 2 protocol packets and forward them to the tunnel ports. Select **Access** for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, PAgP, and LLDP on the access ports only. Select **Tunnel** for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer 2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the services is not enabled on an access port, the protocol packets are dropped.
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.

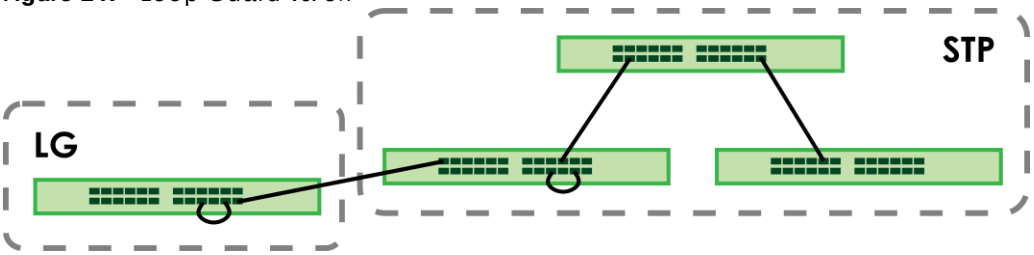
CHAPTER 36
Loop Guard

36.1 Loop Guard Overview

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

Loop guard (**LG**) 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.

Figure 147 Loop Guard vs. STP



Refer to Section 36.1.2 on page 218 for more information.

36.1.1 What You Can Do

Use the **Loop Guard** screen (Section 36.2 on page 219) to enable loop guard on the Switch and in specific ports.

36.1.2 What You Need to Know

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.

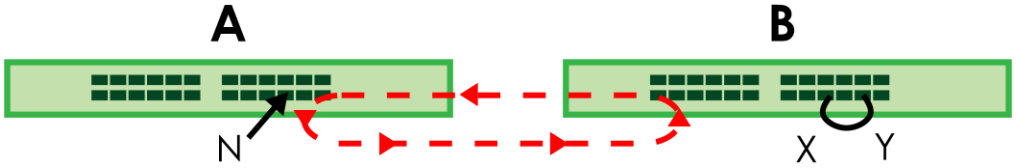
If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- The switch (not in loop state) will receive broadcast messages sent out from the switch in loop state.
- The switch (not in loop state) 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** has two ports, **X** and **Y**, mistakenly connected to each other. It forms a loop. 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**.

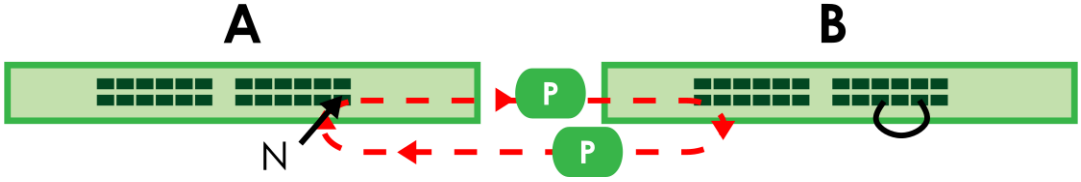
Figure 148 Switch in Loop State



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.

Loop guard can be enabled on both Ethernet ports. 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.

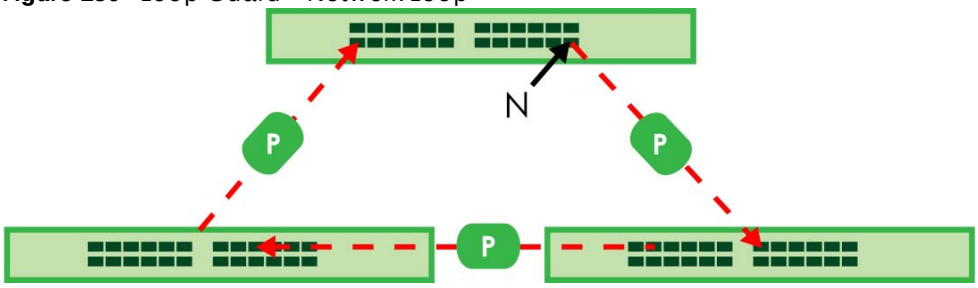
Figure 149 Loop Guard – Probe Packet



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 150 Loop Guard – Network Loop



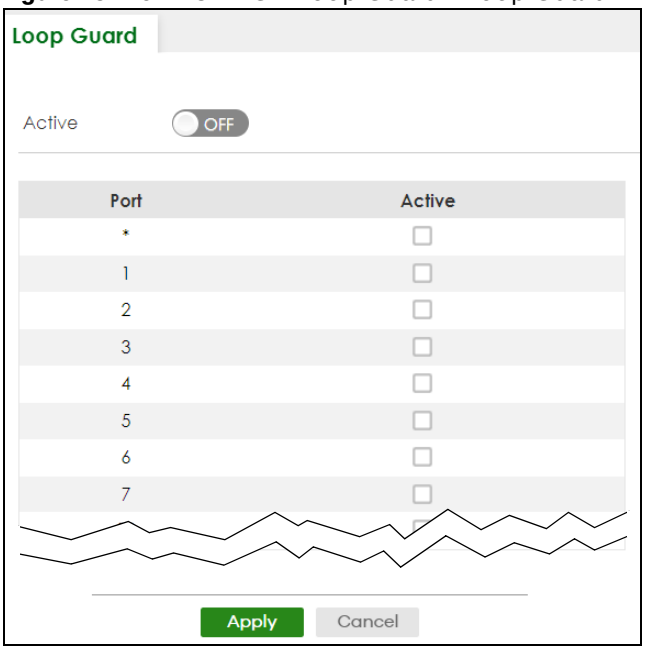
Note: After resolving the loop problem on your network you can re-activate the disabled port through the Web Configurator.

36.2 Loop Guard Setup

Click **SWITCHING** > **Loop Guard** > **Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 151 SWITCHING > Loop Guard > Loop Guard



The following table describes the labels in this screen.

Table 101 SWITCHING > Loop Guard > Loop Guard

LABEL	DESCRIPTION
Active	Enable the switch button to activate loop guard function on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port through the loop guard feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the loop guard feature on this port. The Switch sends broadcast and multicast probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port. Clear this checkbox to disable the loop guard feature.
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.

CHAPTER 37
Mirroring

37.1 Mirroring Overview

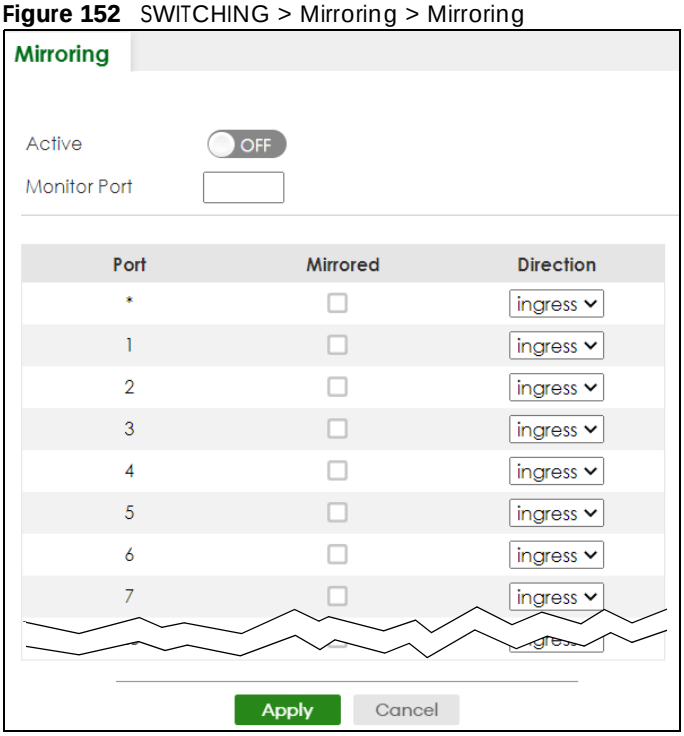
This chapter discusses port mirroring setup screens.

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.

37.2 Port Mirroring Setup

Click **SWITCHING** > **Mirroring** > **Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 152 SWITCHING > Mirroring > Mirroring



The following table describes the labels in this screen.

Table 102 SWITCHING > Mirroring > Mirroring

LABEL	DESCRIPTION
Active	Enable the switch button to activate port mirroring on the Switch. Disable the switch 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 ports. Enter the port number of the monitor port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are **Egress** (outgoing), **Ingress** (incoming) and **Both**.
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.

CHAPTER 38
Multicast

38.1 Multicast Overview

This chapter shows you how to configure various multicast features.

Traditionally, IP packets are transmitted in one of either two ways – Unicast (one sender to one recipient) or Broadcast (one 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 a 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.

38.1.1 What You Can Do – IPv4 Multicast

- Use the **IPv4 Multicast Status** screen (Section 38.2 on page 227) to view IPv4 multicast group information.
- Use the **IGMP Snooping** screen (Section 38.3 on page 228) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IGMP Snooping VLAN** screen (Section 38.4 on page 231) to perform IGMP snooping on VLANs.
- Use the **IGMP Filtering Profile** (Section 38.5 on page 232) to specify a range of multicast groups that clients connected to the Switch are able to join.

38.1.2 What You Can Do – IPv6 Multicast

- Use the **IPv6 Multicast Status** screen (Section 38.6 on page 235) to view IPv6 multicast group information.
- Use the **MLD Snooping-proxy** screen (Section 38.7 on page 235) to enable the upstream port to report group changes to a connected multicast router and forward MLD messages to other upstream ports.
- Use the **MLD Snooping-proxy VLAN** screen (Section 38.8 on page 236) to enable and configure MLD snooping-proxy settings on the VLANs you specified.
- Use the **MLD Snooping-proxy Port Role Setting** screen (Section 38.9 on page 238) to assign MLD snooping-proxy port roles and configure Leave settings for each port.
- Use the **MLD Snooping-proxy Filtering** screen (Section 38.10 on page 240) to enable and configure MLD snooping-proxy filtering.
- Use the **MLD Snooping-proxy Filtering Profile** screen (Section 38.11 on page 241) to create/edit MLD snooping-proxy filtering profiles.

38.1.3 What You Can Do – MVR

- Use the **MVR** screen (Section 38.12 on page 243) to create multicast VLANs and select the receiver ports and a source port for each multicast VLAN.
- Use the **Group Setup** screen (Section 38.12 on page 243) to configure MVR IP multicast group addresses.

38.1.4 What You Need to Know

Read on for concepts on Multicasting that can help you configure the screens in this chapter.

IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA website for more information).

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group. Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8.

IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the Switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers or switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed

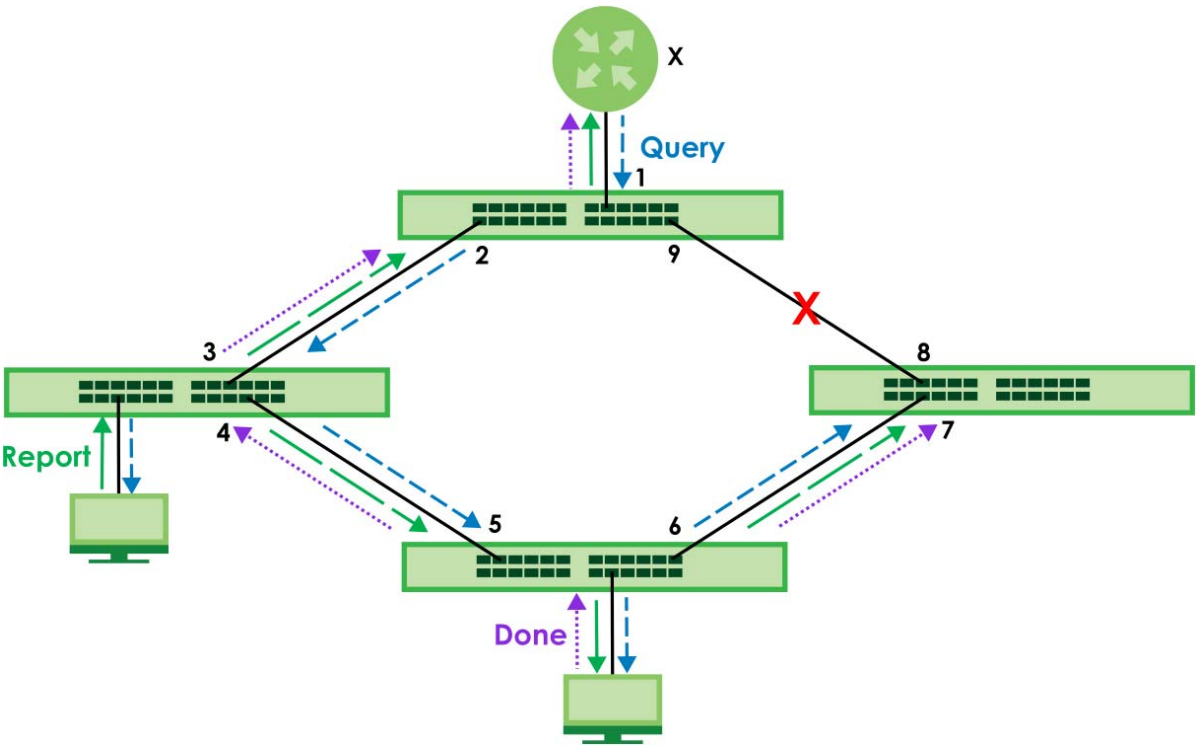
mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

MLD Snooping-proxy

MLD snooping-proxy is a Zyxel-proprietary feature. IPv6 MLD proxy allows only one upstream interface on a switch, while MLD snooping-proxy supports more than one upstream port on a switch. The upstream port in MLD snooping-proxy can report group changes to a connected multicast router and forward MLD messages to other upstream ports. This helps especially when you want to have a network that uses STP to provide backup links between switches and also performs MLD snooping and proxy functions. MLD snooping-proxy, like MLD proxy, can minimize MLD control messages and allow better network performance.

In MLD snooping-proxy, if one upstream port is learned through snooping, all other upstream ports on the same device will be added to the same group. If one upstream port requests to leave a group, all other upstream ports on the same device will also be removed from the group.

In the following MLD snooping-proxy example, all connected upstream ports (**1** – **7**) are treated as one interface. The connection between ports **8** and **9** is blocked by STP to break the loop. If there is one **Query** from a router (**X**) or MLD **Done** or **Report** message from any upstream port, it will be broadcast to all connected upstream ports.



MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is similar to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. If the leave mode is not set to **Immediate**, the router or switch sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

MVR Overview

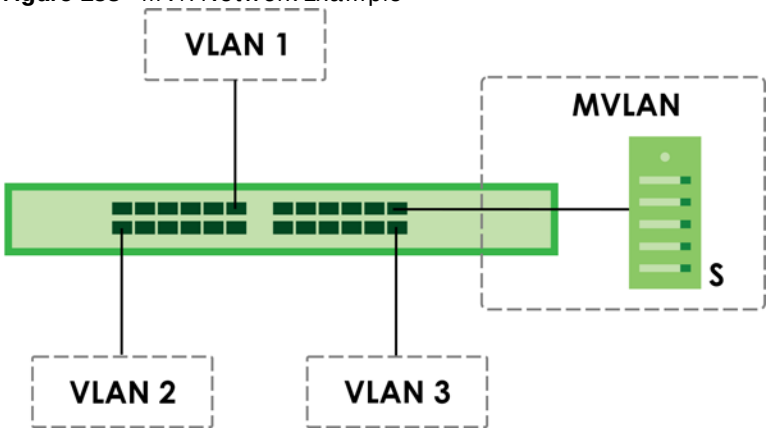
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server (**S**). In addition, the multicast VLAN (**MVLAN**) information is only visible to the Switch and **S**.

Figure 153 MVR Network Example



Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

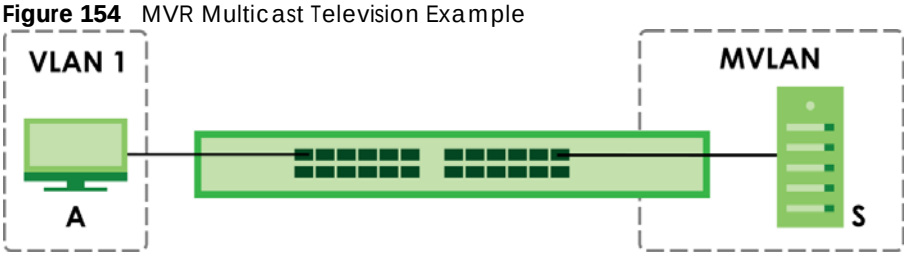
How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in **VLAN 1** receives multicast traffic from the streaming media server (**S**), through the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, an uplink port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

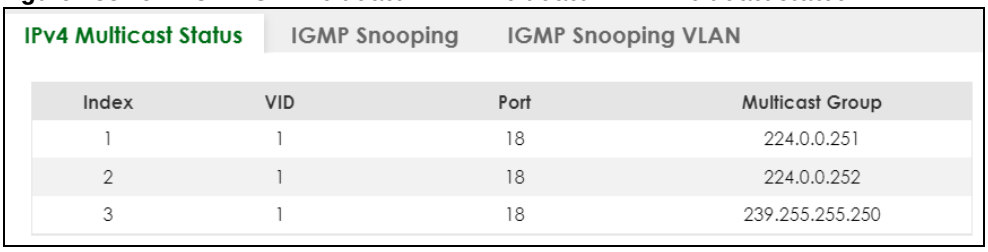
Figure 154 MVR Multicast Television Example



38.2 IPv4 Multicast Status

Click **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IPv4 Multicast Status** to display the screen as shown. This screen shows the IPv4 multicast group information. See Section 38.1 on page 223 for more information on multicasting.

Figure 155 SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status



The following table describes the labels in this screen.

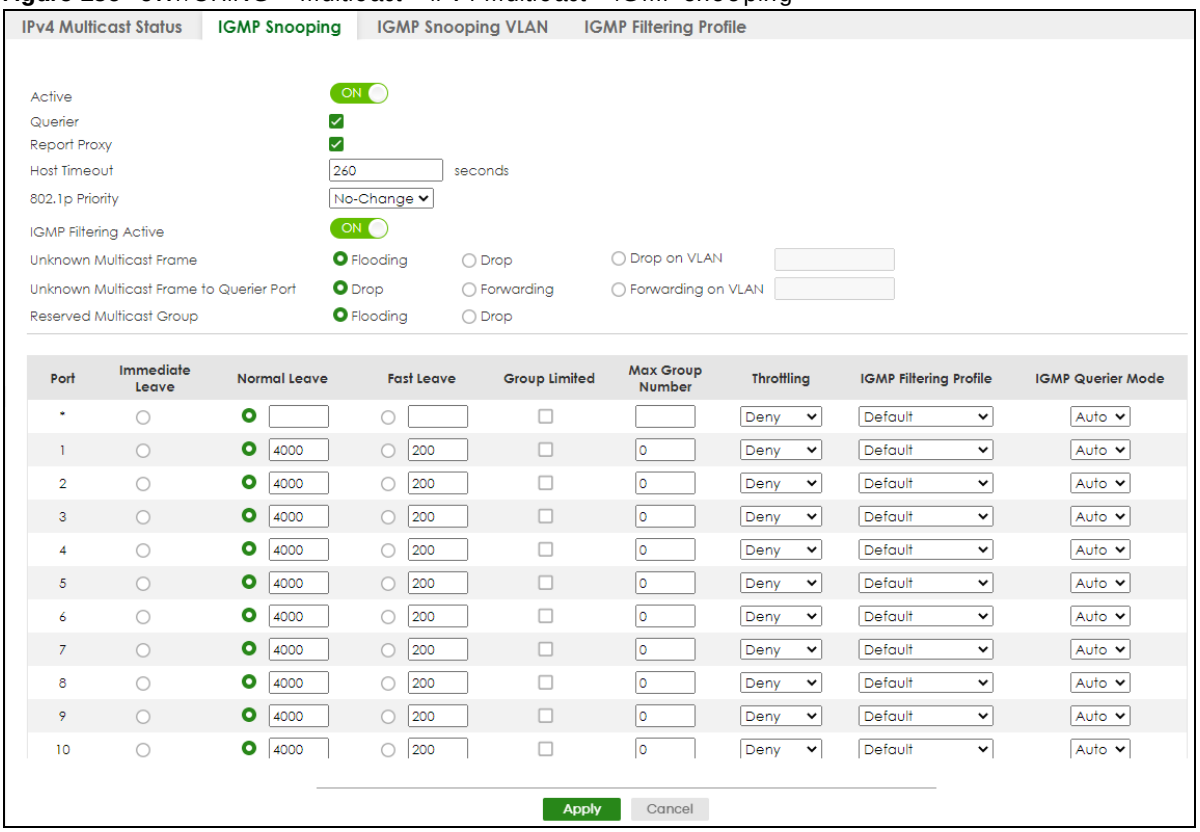
Table 103 SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

38.3 IGMP Snooping

Click **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Snooping** to display the screen as shown. See Section 38.1 on page 223 for more information on multicasting.

Figure 156 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping



The following table describes the labels in this screen.

Table 104 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping

LABEL	DESCRIPTION
Active	Enable the switch button to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Report Proxy	Select this to allow the Switch to act as the IGMP report proxy and leave proxy. It will report group changes to a connected multicast router. The Switch not only checks IGMP packets between multicast routers or switches and multicast hosts to learn the multicast group membership, but also replaces the source MAC address in an IGMP v1/v2 report with its own MAC address before forwarding to the multicast router or switch. When the Switch receives more than one IGMP v1/v2 join report that requests to join the same multicast group, it only sends a new join report with its MAC address. This helps reduce the number of multicast join reports passed to the multicast router or switch. The Switch sends a leave message with its MAC address to the multicast router or switch only when it receives the leave message from the last host in a multicast group.
Host Timeout	Specify the time (from 1 to 16711450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.

Table 104 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
802.1p Priority	Select a priority level (0 – 7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering Active	Enable the switch button to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. • Select **Flooding** to send the frames to all ports. • Select **Drop** to discard the frames. • Select **Drop on VLAN** and enter the VLAN ID numbers to discard the frames on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
Unknown Multicast Frame to Querier Port	Specify the action to perform when **Unknown Multicast Frame** is set to **Drop**. • Select **Drop** to discard the frames. • Select **Forwarding** to send the frames to all querier ports. • Select **Forwarding on VLAN** and enter the VLAN ID numbers to send the frames to the ports which are used as an IGMP query port on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. • Select **Flooding** to send the frames to all ports. • Select **Drop** to discard the frames.
Use this section to configure IGMP Snooping on each port.	
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Immediate Leave	Select this to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.

Table 104 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping (continued)

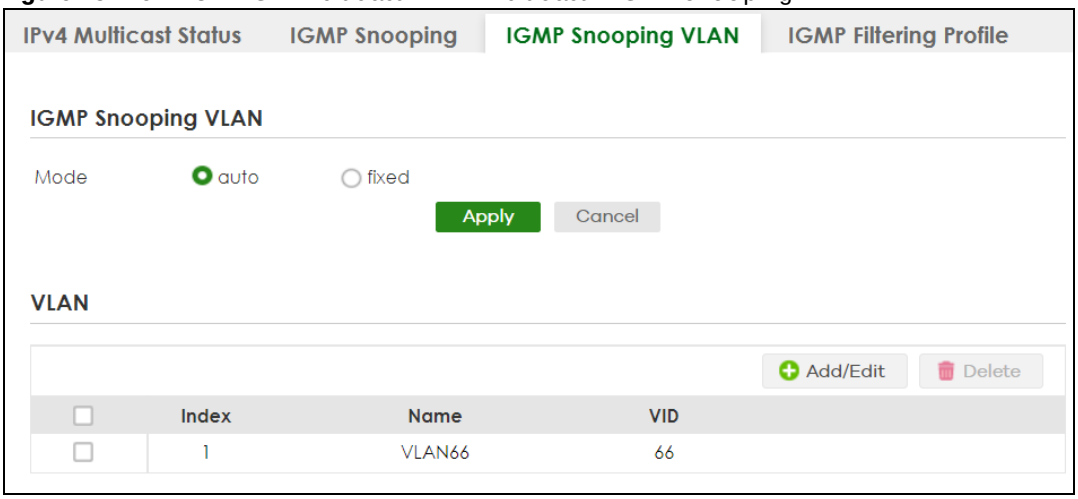
LABEL	DESCRIPTION
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6348800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In normal leave mode, when the Switch receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6348800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In fast leave mode, right after receiving an IGMP leave message from a host on a port, the Switch itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Number	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frames is dropped on this port.
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select **Deny** to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select **Replace** to replace an existing entry in the multicast forwarding table with the new IGMP reports received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Filtering Profile** screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
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.

38.4 IGMP Snooping VLAN

Click **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Snooping VLAN** to display the screen as shown. See IGMP Snooping and VLANs on page 224 for more information on IGMP Snooping VLAN.

Note: You can perform IGMP snooping on up to 16 VLANs.

Figure 157 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN



The following table describes the labels in this screen.

Table 105 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN

LABEL	DESCRIPTION
IGMP Snooping VLAN	
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLANs that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs (including up to five VLANs you configured in the **MVR** screen). For example, if you have configured one multicast VLAN in the **SWITCHING** > **Multicast** > **MVR** screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. You must also enable IGMP snooping in the **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Snooping** screen first.
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.
VLAN Use this section of the screen to add VLANs on which the Switch is to perform IGMP snooping.	
Index	This is the index number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 105 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN (continued)

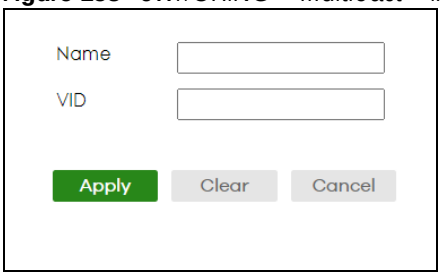
LABEL	DESCRIPTION
Add/Edit	Click **Add/Edit** to create a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

38.4.1 Add/Edit IGMP Snooping VLANs

This screen allows you to add an IGMP snooping VLAN or edit an existing one.

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 158 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN > Add/Edit



The following table describes the labels in this screen.

Table 106 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN > Add/Edit

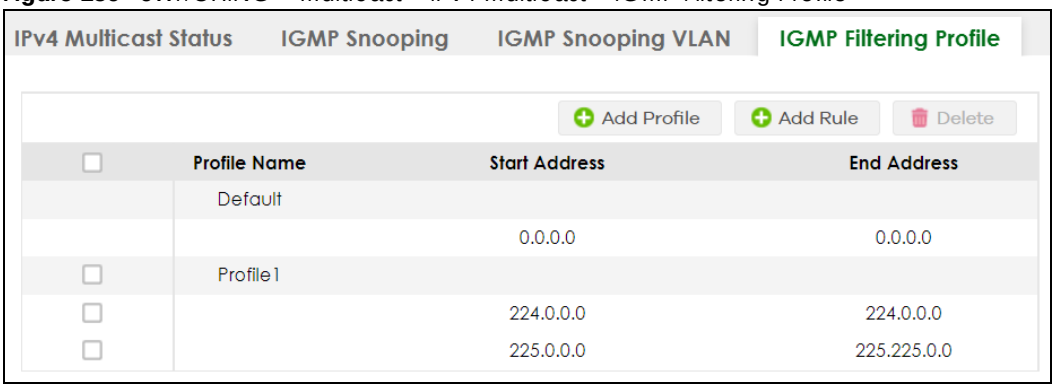
LABEL	DESCRIPTION
Name	Enter the descriptive name of the VLAN for identification purposes. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["] or [,].
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. Note: You cannot configure the same VLAN ID as in the **SWITCHING** > **Multicast** > **MVR** screen.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

38.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Snooping** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Filtering Profile** link to display the screen as shown.

Figure 159 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile



The following table describes the labels in this screen.

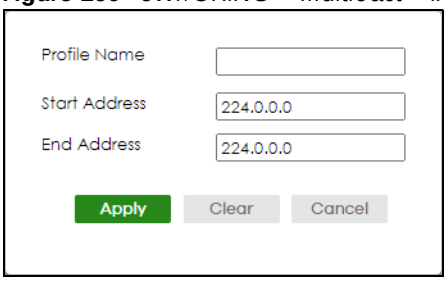
Table 107 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add Profile	Click this to add a new IGMP filtering profile.
Add Rule	Click **Add Rule** to add a new rule and specify the profile it belongs to in the **Add Rule** screen. You can also select a profile entry and click **Add Rule** to add an additional rule for the selected profile.
Delete	Select a profile and click **Delete** to remove the selected profile and the accompanying rules. Select a rule from a profile and click **Delete** to remove the selected rule.

38.5.1 Add IGMP Filtering Profile

To access this screen, click the **Add Profile** button in the **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Filtering Profile** screen.

Figure 160 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Profile



The following table describes the labels in this screen.

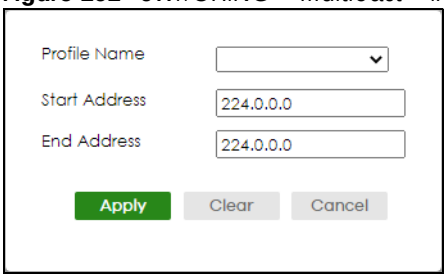
Table 108 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].
Start Address	Enter the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Enter the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

38.5.2 Add IGMP Filtering Rule

Click **Add Rule** in the **SWITCHING** > **Multicast** > **IPv4 Multicast** > **IGMP Filtering Profile** screen to access this screen.

Figure 161 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Rule



The following table describes the labels in this screen.

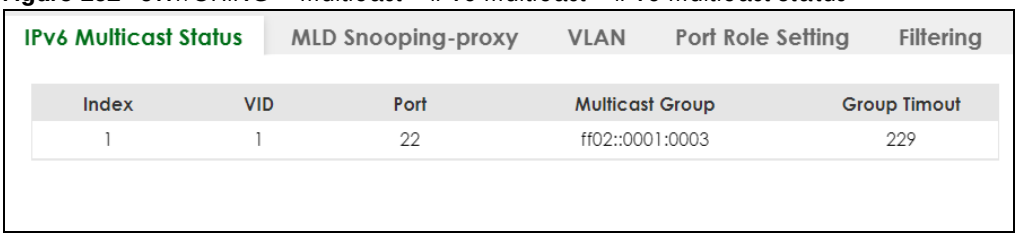
Table 109 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Rule

LABEL	DESCRIPTION
Profile Name	Select a profile from the drop-down list to add a additional rule for the existing profile.
Start Address	Enter the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Enter the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

38.6 IPv6 Multicast Status

Click **SWITCHING** > **Multicast** > **IPv6 Multicast** > **IPv6 Multicast Status** to display the screen as shown. This screen shows the IPv6 multicast group information. See Section 38.1 on page 223 for more information on multicasting.

Figure 162 SWITCHING > Multicast > IPv6 Multicast > IPv6 Multicast Status



The following table describes the fields in the above screen.

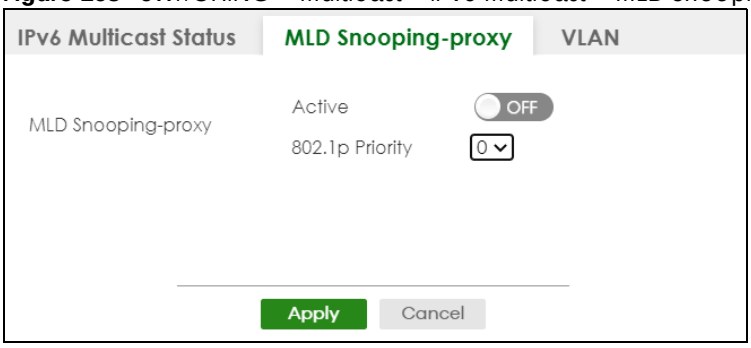
Table 110 SWITCHING > Multicast > IPv6 Multicast > IPv6 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.
Group Timeout	This field displays the time (in seconds) that elapses before the Switch removes a MLD group membership entry if it does not receive report messages from the port.

38.7 MLD Snooping-proxy

Click **SWITCHING** > **Multicast** > **IPv6 Multicast** > **MLD Snooping-proxy** to display the screen as shown. See Section 38.1 on page 223 for more information on multicasting.

Figure 163 SWITCHING > Multicast > IPv6 Multicast > MLD Snooping-proxy



The following table describes the fields in the above screen.

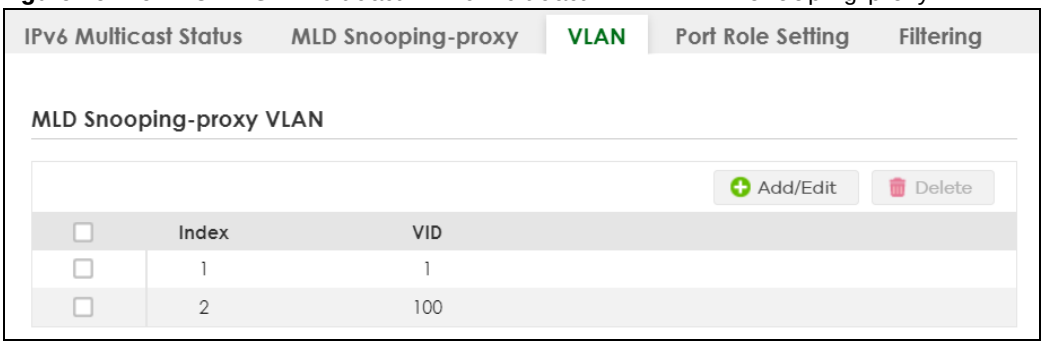
Table 111 SWITCHING > Multicast > IPv6 Multicast > MLD Snooping-proxy

LABEL	DESCRIPTION
MLD Snooping-proxy Use these settings to configure MLD snooping-proxy.	
Active	Enable the switch button to enable MLD snooping-proxy on the Switch to minimize MLD control messages and allow better network performance.
802.1p Priority	Select a priority level (0 – 7) to which the Switch changes the priority in outgoing MLD messages.
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.

38.8 MLD Snooping-proxy VLAN

Click **SWITCHING** > **Multicast** > **IPv6 Multicast** > **VLAN** screen to display the screen as shown. See Section 38.1 on page 223 for more information on multicasting.

Figure 164 SWITCHING > Multicast > IPv6 Multicast > VLAN: MLD Snooping-proxy VLAN



The following table describes the fields in the above screen.

Table 112 SWITCHING > Multicast > IPv6 Multicast > VLAN: MLD Snooping-proxy VLAN

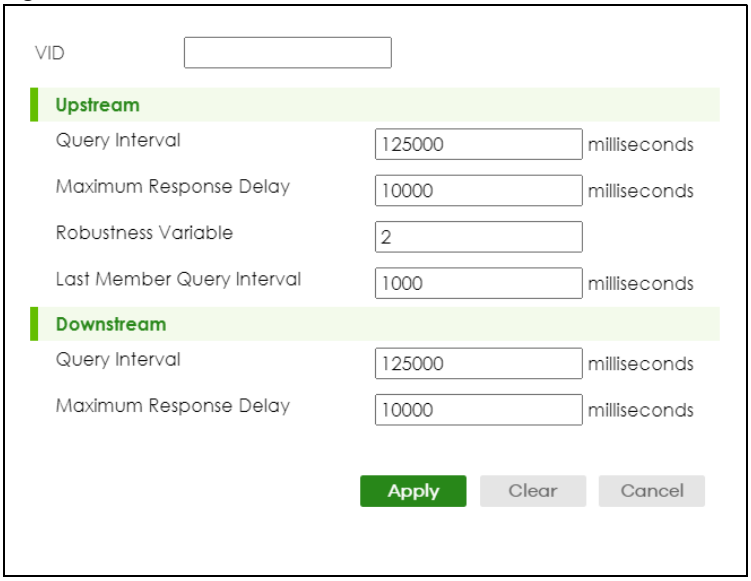
LABEL	DESCRIPTION
MLD Snooping-proxy VLAN	
Index	This is the index number of the MLD snooping-proxy VLAN entry in the table.
VID	This field displays the ID number of the VLAN group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entry.

38.8.1 Add/Edit MLD Snooping-proxy VLAN

The screen allows you to enable and configure MLD Snooping-proxy settings on a VLAN you specified.

Click **Add/Edit** in the **SWITCHING** > **Multicast** > **IPv6 Multicast** > **VLAN** screen to display this screen.

Figure 165 SWITCHING > Multicast > IPv6 Multicast > VLAN > Add/Edit



The following table describes the fields in the above screen.

Table 113 SWITCHING > Multicast > IPv6 Multicast > VLAN > Add/Edit

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN on which you want to enable MLD snooping-proxy and configure related settings.
Upstream	
Query Interval	Enter the amount of time (in miliseconds) between general query messages sent by the router connected to the upstream port. This value should be exactly the same as what is configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be T = (QI*RV) + MRD, where T = Timeout, QI = Query Interval, RV = Robustness Variable, and MRD = Maximum Response Delay.
Maximum Response Delay	Enter the amount of time (in miliseconds) the router connected to the upstream port waits for a response to an MLD general query message. This value should be exactly the same as what is configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table. When an MLD Report message is received, the Switch sets the timeout period of the entry to be T = (QI*RV) + MRD, where T = Timeout, QI = Query Interval, RV = Robustness Variable, and MRD = Maximum Response Delay. When an MLD Done message is received, the Switch sets the entry's lifetime to be the product of **Last Member Query Interval** and **Robustness Variable**.

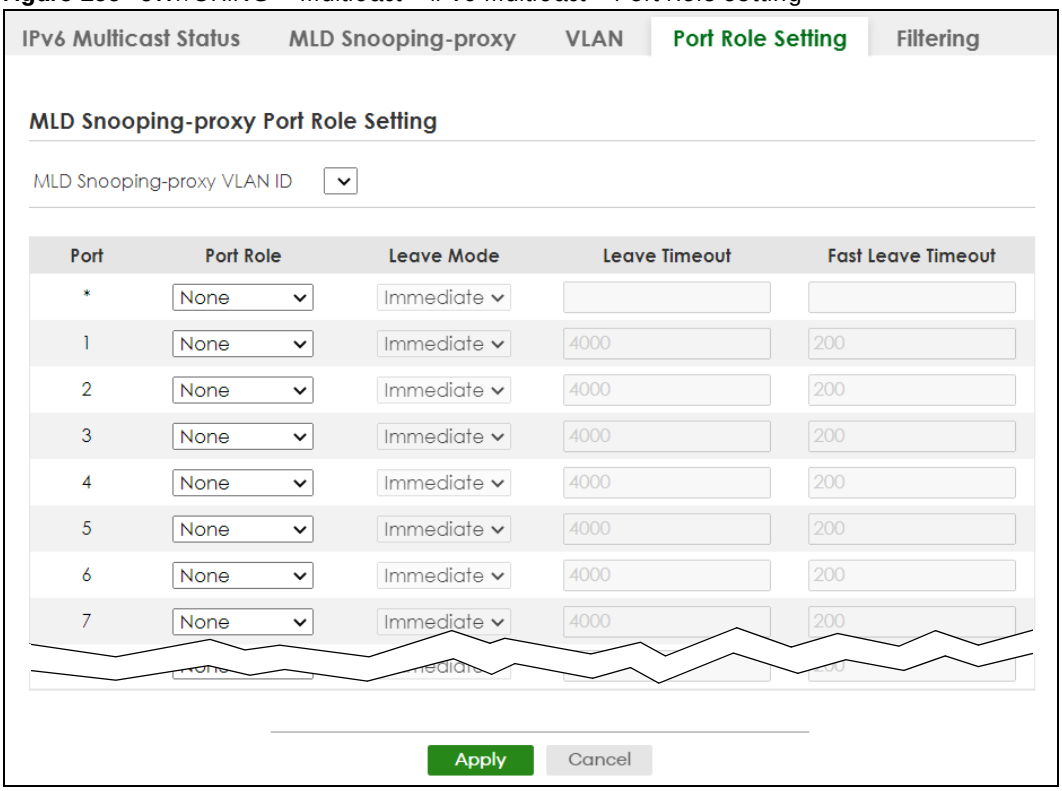
Table 113 SWITCHING > Multicast > IPv6 Multicast > VLAN > Add/Edit (continued)

LABEL	DESCRIPTION
Robustness Variable	Enter the number of queries. A multicast address entry (learned only on an upstream port by snooping) is removed from the forwarding table when there is no response to the configured number of queries sent by the router connected to the upstream port. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table.
Last Member Query Interval	Enter the amount of time (in miliseconds) between the MLD group-specific queries sent by an upstream port when an MLD Done message is received. This value should be exactly the same as what's configured in the connected multicast router. This value is used to calculate the amount of time an MLD snooping membership entry (learned only on the upstream port) can remain in the forwarding table after a Done message is received. When an MLD Done message is received, the Switch sets the entry's lifetime to be the product of **Last Member Query Interval** and **Robustness Variable**.
Downstream	
Query Interval	Enter the amount of time (in miliseconds) between general query messages sent by the downstream port.
Maximum Response Delay	Enter the maximum time (in miliseconds) that the Switch waits for a response to a general query message sent by the downstream port.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

38.9 MLD Snooping-proxy Port Role Setting

Click **SWITCHING** > **Multicast** > **IPv6 Multicast** > **Port Role Setting** to display the screen as shown. See Section 38.1 on page 223 for more information on multicasting.

Figure 166 SWITCHING > Multicast > IPv6 Multicast > Port Role Setting



The following table describes the fields in the above screen.

Table 114 SWITCHING > Multicast > IPv6 Multicast > Port Role Setting

LABEL	DESCRIPTION
MLD Snooping-proxy Port Role Setting	
MLD Snooping-proxy VLAN ID	Select the VLAN ID for which you want to configure a port's MLD snooping-proxy settings.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Port Role	A port on the Switch can be either a **Downstream** port or **Upstream** port in MLD. A downstream port connects to MLD hosts and acts as a multicast router to send MLD queries and listen to the MLD host's Report and Done messages. An upstream port connects to a multicast router and works as a host to send Report or Done messages when receiving queries from a multicast router. Otherwise, select **None** if the port is not joining a multicast group or does not belong to this VLAN.
Leave Mode	This is configurable only when you select **Downstream** in the previous **Port Role** field. Select the leave mode for the specified downstream ports in this VLAN. This specifies whether the Switch removes an MLD snooping membership entry (learned on a downstream port) immediately (**Immediate**) or wait for an MLD report before the leave timeout (**Normal**) or fast leave timeout (**Fast**) when an MLD leave message is received on this port from a host.

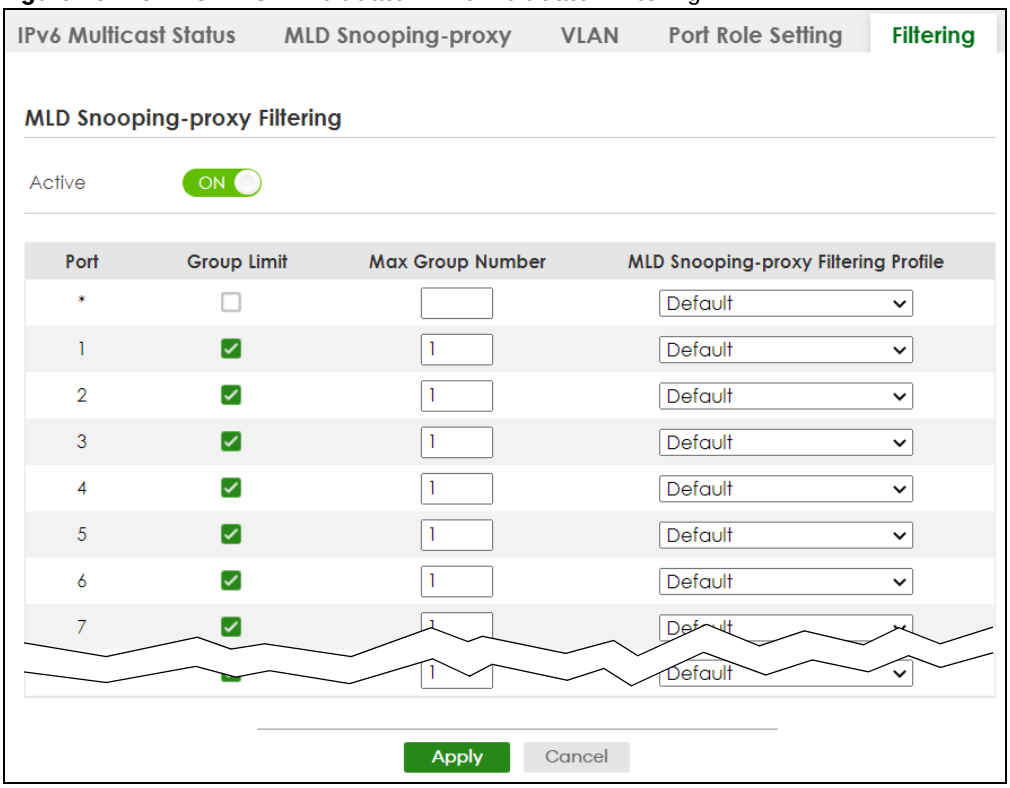
Table 114 SWITCHING > Multicast > IPv6 Multicast > Port Role Setting (continued)

LABEL	DESCRIPTION
Leave Timeout	Enter the MLD snooping normal leave timeout (in milliseconds) the Switch uses to update the forwarding table for the specified downstream ports. This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.
Fast Leave Timeout	Enter the fast leave timeout (in milliseconds) for the specified downstream ports. This defines how many seconds the Switch waits for an MLD report before removing an MLD snooping membership entry (learned on a downstream port) when an MLD Done message is received on this port from a host.
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.

38.10 MLD Snooping-proxy Filtering

Use this screen to configure the Switch's MLD filtering settings. Click the **SWITCHING** > **Multicast** > **IPv6 Multicast** > **Filtering** screen to display the screen as shown.

Figure 167 SWITCHING > Multicast > IPv6 Multicast > Filtering



The following table describes the fields in the above screen.

Table 115 SWITCHING > Multicast > IPv6 Multicast > Filtering

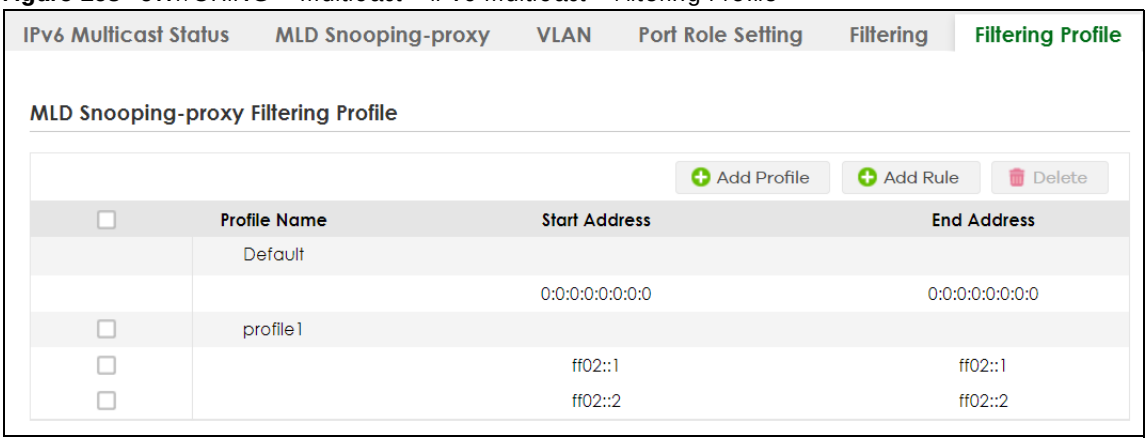
LABEL	DESCRIPTION
MLD Snooping-proxy Filtering	
Active	Enable the switch button to enable MLD filtering on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Group Limit	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Number	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new MLD Report message is dropped on this port.
MLD Snooping-proxy Filtering Profile	Select the name of the MLD filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create MLD filtering profiles in the **SWITCHING** > **Multicast** > **IPv6 Multicast** > **Filtering Profile** screen.
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.

38.11 MLD Snooping-proxy Filtering Profile

Use this screen to view and create MLD filtering profiles.

Click **SWITCHING** > **Multicast** > **IPv6 Multicast** > **Filtering Profile** to display the screen as shown.

Figure 168 SWITCHING > Multicast > IPv6 Multicast > Filtering Profile



The following table describes the fields in the above screen.

Table 116 SWITCHING > Multicast > IPv6 Multicast > Filtering Profile

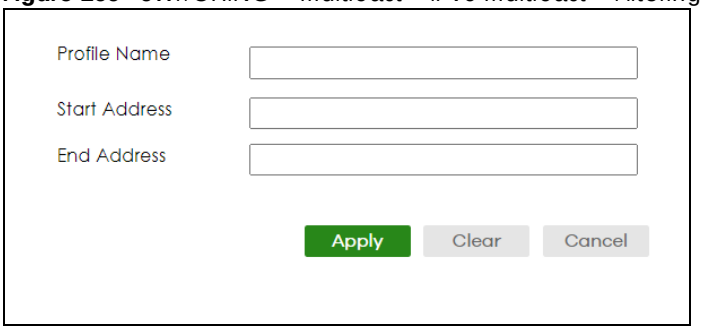
LABEL	DESCRIPTION
MLD Snooping-proxy Filtering Profile	
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast IPv6 address range.
End Address	This field displays the end of the multicast IPv6 address range.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add Profile	Click this to add a new MLD Snooping-proxy filtering profile.
Add Rule	Click **Add Rule** to add a new rule and specify the profile it belongs to in the **Add Rule** screen. You can also select a profile entry and click **Add Rule** to add an additional rule for the selected profile.
Delete	Select a profile and click **Delete** to remove the selected profile and the accompanying rules. Select a rule from a profile and click **Delete** to remove the selected rule.

38.11.1 Add MLD Snooping-proxy Filtering Profile

Use this screen to create an MLD filtering profile and set the range of the multicast addresses.

Click **Add Profile** in the **SWITCHING** > **Multicast** > **IPv6 Multicast** > **Filtering Profile** to display the screen as shown.

Figure 169 SWITCHING > Multicast > IPv6 Multicast > Filtering Profile > Add Profile



The following table describes the fields in the above screen.

Table 117 SWITCHING > Multicast > IPv6 Multicast > Filtering Profile > Add Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [|], ['], ["], or [,]) for the profile for identification purposes. To configure additional rules for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Enter the starting multicast IPv6 address for a range of multicast IPv6 addresses that you want to belong to the MLD filtering profile.

Table 117 SWITCHING > Multicast > IPv6 Multicast > Filtering Profile > Add Profile (continued)

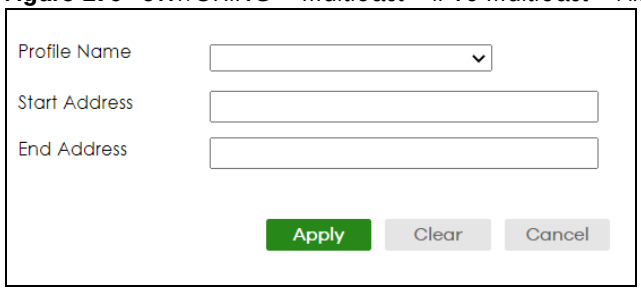
LABEL	DESCRIPTION
End Address	Enter the ending multicast IPv6 address for a range of IPv6 addresses that you want to belong to the MLD filtering profile. If you want to add a single multicast IPv6 address, enter it in both the **Start Address** and **End Address** fields.
Apply	Click **Apply** to save 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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

38.11.2 Add MLD Snooping-proxy Filtering Rule

Use this screen to create a multicast addresses range rule of the MLD filtering profile.

Click **Add Rule** in the **SWITCHING** > **Multicast** > **IPv6 Multicast** > **Filtering Profile** to display this screen.

Figure 170 SWITCHING > Multicast > IPv6 Multicast > Filtering Profile > Add Rule



The following table describes the fields in the above screen.

Table 118 SWITCHING > Multicast > IPv6 Multicast > Filtering Profile > Add Rule

LABEL	DESCRIPTION
Profile Name	Select a profile from the drop-down list to add a additional rule for the existing profile.
Start Address	Enter the starting multicast IPv6 address for a range of multicast IPv6 addresses that you want to belong to the MLD filtering profile.
End Address	Enter the ending multicast IPv6 address for a range of IPv6 addresses that you want to belong to the MLD filtering profile. If you want to add a single multicast IPv6 address, enter it in both the **Start Address** and **End Address** fields.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

38.12 MVR Configuration

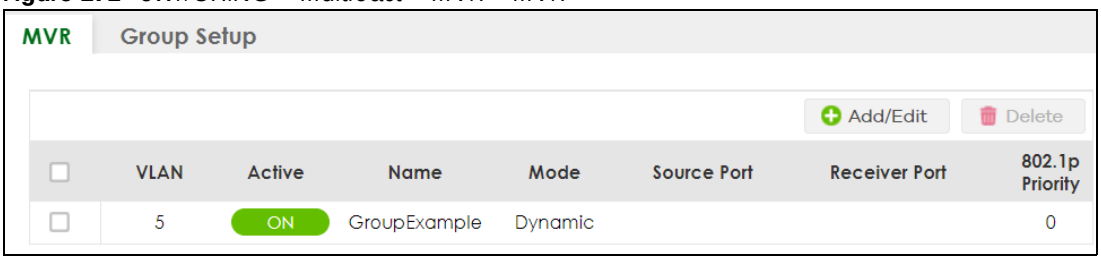
Use this screen to view and create multicast VLANs.

Click **SWITCHING** > **Multicast** > **MVR** > **MVR** to display the screen as shown next.

Note: You can create up to five multicast VLANs and up to 256 multicast rules on the Switch.

Note: Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 171 SWITCHING > Multicast > MVR > MVR



The following table describes the related labels in this screen.

Table 119 SWITCHING > Multicast > MVR > MVR

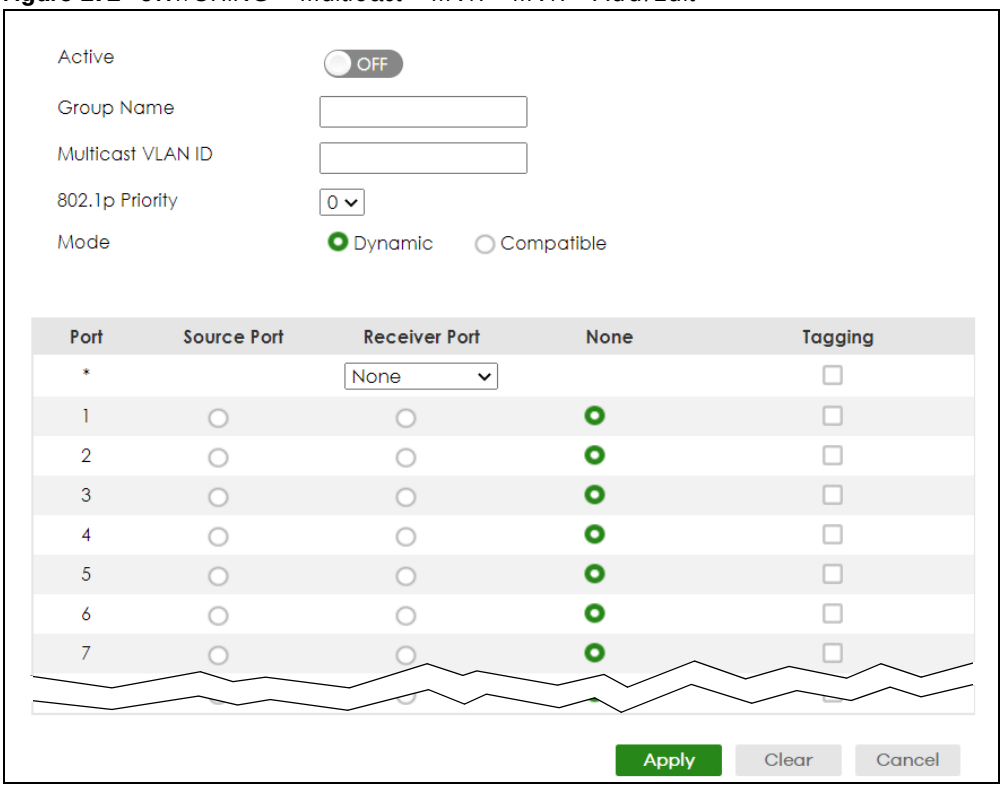
LABEL	DESCRIPTION
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port numbers.
Receiver Port	This field displays the receiver port numbers.
802.1p Priority	This field displays the priority level.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new multicast VLAN or edit a selected one.
Delete	Select the entries that you want to remove, then click **Delete** to delete multicast VLANs.

38.12.1 Add/Edit MVR

Use this screen to create or edit multicast VLANs and select the receiver ports and a source port for each multicast VLAN.

To access this screen, click **Add/Edit** or select an existing entry and click **Add/Edit** in the **SWITCHING** > **Multicast** > **MVR** > **MVR** screen.

Figure 172 SWITCHING > Multicast > MVR > MVR > Add/Edit



The following table describes the related labels in this screen.

Table 120 SWITCHING > Multicast > MVR > MVR > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Group Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [|], ['], ["], or [,]) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0 – 7) with which the Switch replaces the priority in outgoing IGMP or MLD control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports or MLD messages to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports or MLD messages.
Use this section to configure MVR settings on each port.	
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.

Table 120 SWITCHING > Multicast > MVR > MVR > Add/Edit (continued)

LABEL	DESCRIPTION
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

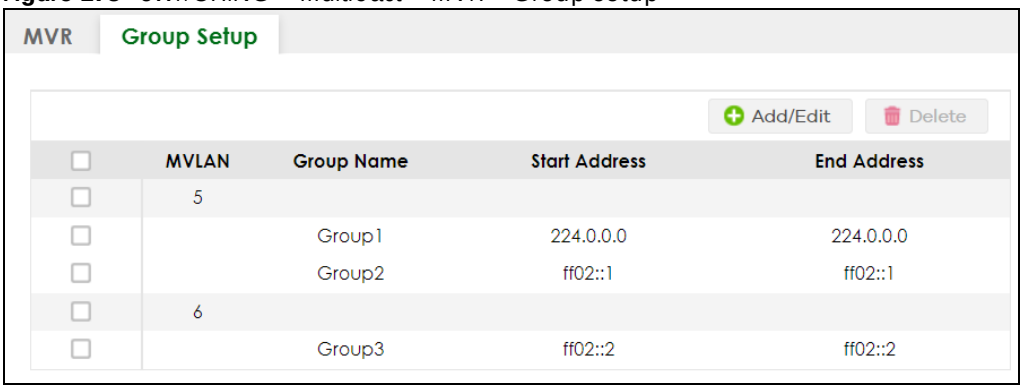
38.13 MVR Group Setup

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Use this screen to view and configure MVR IP multicast group settings. Click **SWITCHING** > **Multicast** > **MVR** > **Group Setup** to access this screen.

Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 173 SWITCHING > Multicast > MVR > Group Setup



The following table describes the labels in this screen.

Table 121 SWITCHING > Multicast > MVR > Group Setup

LABEL	DESCRIPTION
MVLAN	This field displays the multicast VLAN ID.
Group Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

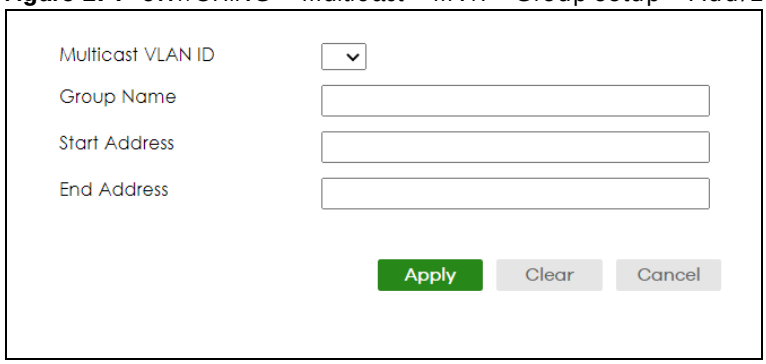
Table 121 SWITCHING > Multicast > MVR > Group Setup (continued)

LABEL	DESCRIPTION
Add/Edit	Click **Add/Edit** to add a new multicast group or edit a selected one.
Delete	Select the group entries that you want to remove, then click **Delete** to delete the selected multicast groups. If you delete a multicast VLAN, all multicast groups in this VLAN will also be removed.

38.13.1 Add/Edit MVR Group

Use this screen to configure MVR IP multicast group addresses. To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 174 SWITCHING > Multicast > MVR > Group Setup > Add/Edit



The following table describes the labels in this screen.

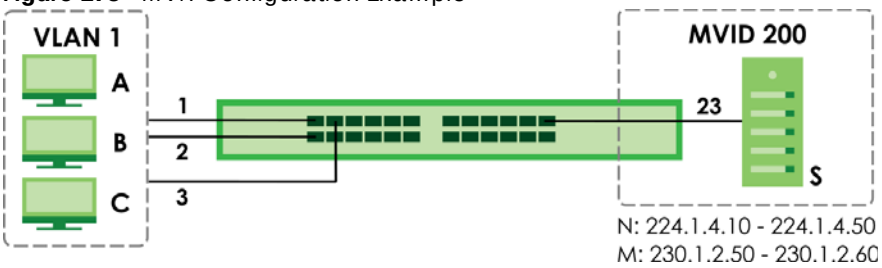
Table 122 SWITCHING > Multicast > MVR > Group Setup > Add/Edit

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Group Name	Enter a descriptive name for identification purposes. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

38.13.2 MVR Configuration Example

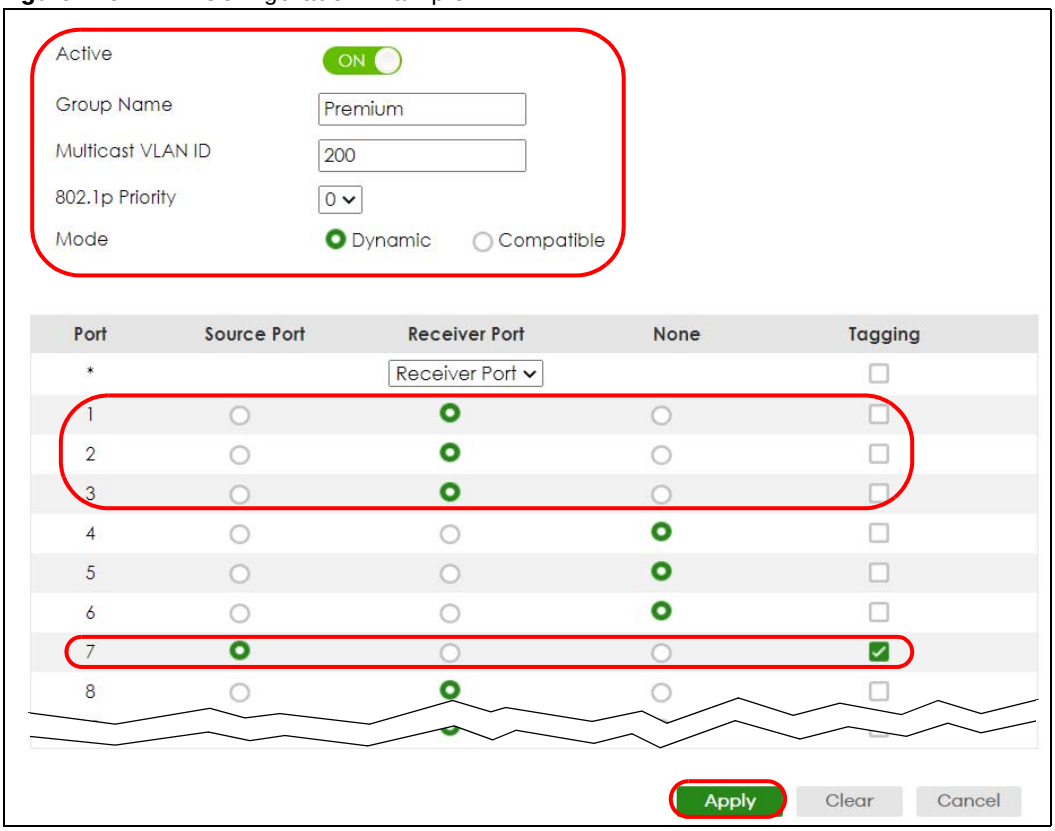
The following figure shows a network example where ports **1**, **2** and **3** on the Switch belong to **VLAN 1**. In addition, port **23** belongs to the multicast group with **VID 200** (**MVID 200**) to receive multicast traffic (the News (**N**) and Movie (**M**) channels) from the remote streaming media server (**S**). Computers **A**, **B** and **C** in **VLAN 1** are able to receive the traffic.

Figure 175 MVR Configuration Example



To configure the MVR settings on the Switch, click the **Add/Edit** button in the **SWITCHING** > **Multicast** > **MVR** > **MVR** screen. Create a multicast VLAN and set the receiver and source ports.

Figure 176 MVR Configuration Example



To set the Switch to forward the multicast group traffic to the subscribers, click **Add/Edit** in the **SWITCHING** > **Multicast** > **MVR** > **Group Setup** screen and configure multicast group settings. The following figure shows an example where two IPv4 multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 177 MVR Group Configuration Example – Add

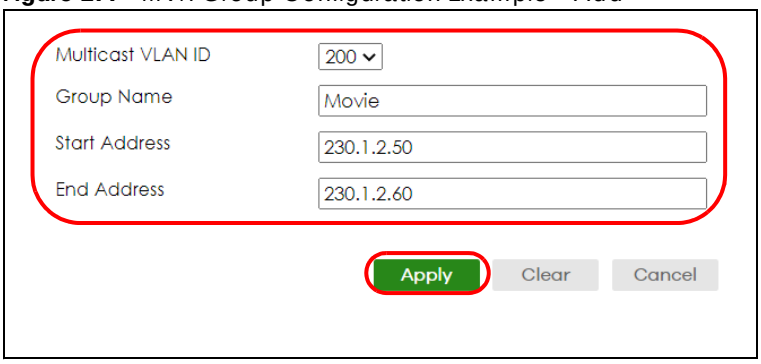
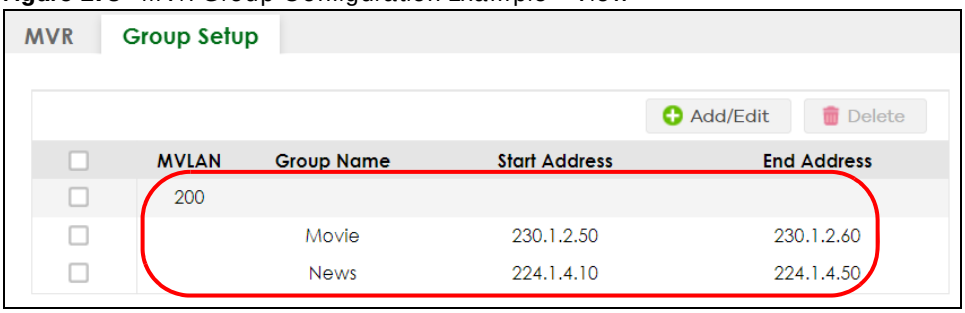


Figure 178 MVR Group Configuration Example – View



CHAPTER 39
Static Multicast Forwarding

39.1 Static Multicast Forwarding Overview

This chapter discusses how to configure static multicast forwarding rules based on multicast MAC addresses or multicast IPv4 addresses.

Use these screens to configure static multicast address forwarding by defining the ports and VLANs that multicast traffic can pass through the Switch. If a subscriber is on a different port or VLAN, then the subscriber will not get the multicast.

39.1.1 What You Can Do

Use the **Static Multicast Forwarding By MAC** screen (Section 39.2 on page 251) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific ports.

39.1.2 What You Need To Know

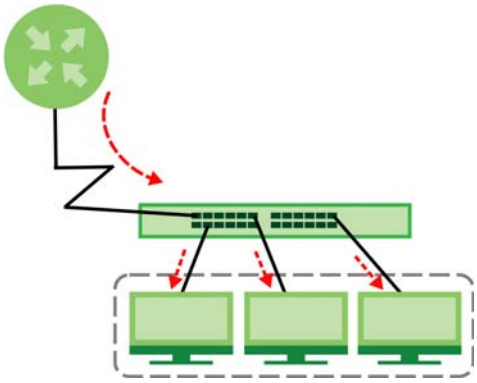
A multicast MAC address or multicast IP address is the MAC address or IP address of a multicast group, and not a receiving device.

A static multicast address is a multicast MAC address or multicast IPv4 address that has been manually entered in the multicast table. This identifies the destination of the multicast content. Multicast IPv4 addresses uses the Class D IP addresses range 224.0.0.0 to 239.255.255.255. Multicast MAC addresses have a “1” as the last binary bit of the first octet pair (for example, 01:00:5e:00:00:0A). Static multicast addresses do not age out. See IP Multicast Addresses on page 224 for more information on IP multicast addresses.

Note: Static (manual) multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the Switch cannot forward to specific ports unless you configure static (manual) multicast entries. The Switch will either flood the multicast frames to all ports (default) or drop them. Figure 179 on page 251 shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to ports within a VLAN group.

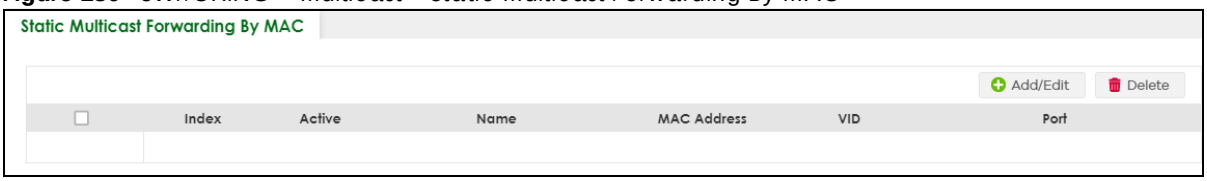
Figure 179 No Multicast Forwarding



39.2 Static Multicast Forwarding By MAC

Use this screen to view and configure static multicast MAC addresses for ports to receive the multicast stream. Click **SWITCHING** > **Multicast** > **Static Multicast Forwarding By MAC** to display the screen as shown next.

Figure 180 SWITCHING > Multicast > Static Multicast Forwarding By MAC



The following table describes the labels in this screen.

Table 123 SWITCHING > Multicast > Static Multicast Forwarding By MAC

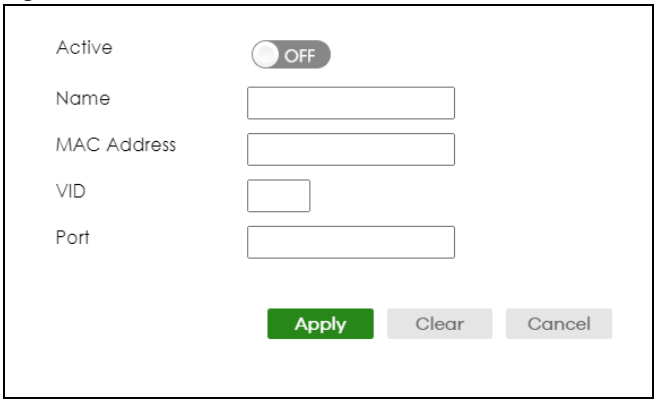
LABEL	DESCRIPTION
Index	This is the index number of the static multicast MAC address rule.
Active	This field displays whether a static multicast MAC address forwarding rule is active or not. You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the ports within an identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new rule or edit a selected one.
Delete	Click **Delete** to remove the selected rules.

39.2.1 Add/Edit Static Multicast Forwarding By MAC

Use this screen to add a static multicast MAC address rule for ports to receive the multicast stream.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **Multicast** > **Static Multicast Forwarding By MAC** to display this screen.

Figure 181 SWITCHING > Multicast > Static Multicast Forwarding By MAC > Add/Edit



The following table describes the labels in this screen

Table 124 SWITCHING > Multicast > Static Multicast Forwarding By MAC > Add/Edit

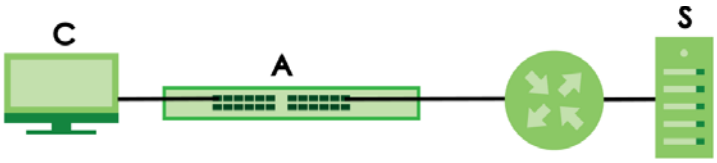
LABEL	DESCRIPTION
Active	Enable the switch button to activate your rule. You may temporarily deactivate a rule without deleting it by disabling the switch.
Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [|], ['], ["], or [,]) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 in hexadecimal, so 01:00:5e:00:00:0A and 01:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination multicast MAC address to ports within a VLAN group. Enter the ID that identifies the VLAN group here. If you do NOT have a specific target VLAN, enter 1.
Port	Enter the ports where frames with destination multicast MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter “3-5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 40
PPPoE

40.1 PPPoE Intermediate Agent Overview

This chapter describes how the Switch gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

A PPPoE Intermediate Agent (PPPoE IA) (**A**) is deployed between a PPPoE server (**S**) and PPPoE clients (**C**). It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



40.1.1 What You Can Do

- Use the **PPPoE Intermediate Agent** screen (Section 40.2 on page 255) to enable the PPPoE Intermediate Agent on the Switch.
- Use the **PPPoE IA Port** screen (Section 40.3 on page 257) to set the port state and configure PPPoE intermediate agent sub-options on a per-port basis.
- Use the **PPPoE IA Port VLAN** screen (Section 40.4 on page 258) to configure PPPoE IA settings that apply to a specific VLAN on a port.
- Use the **PPPoE IA VLAN** (Section 40.5 on page 260) to enable the PPPoE Intermediate Agent on a VLAN.

40.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

40.1.2.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients.

This tag is defined in RFC 2516 and has the following format for this feature.

Table 125 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the "ADSL Forum" IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.

40.1.2.2 Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

Table 126 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 127 PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (63 bytes)

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, the Switch puts the PPPoE client's MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-option example is "Switch/07/0123" and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch's port 7 and belong to VLAN 123.

Table 128 PPPoE IA Circuit ID Sub-option Format: Using Identifier String and Variables

SubOpt	Length	Value						
0x01 (1 byte)	N (1 byte)	Identifier String (53 byte)	delimiter (1 byte)	Slot ID (1 byte)	delimiter (1 byte)	Port No (2 byte)	delimiter (1 byte)	VLAN ID (4 bytes)

WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE** > **Intermediate Agent** screen, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates “Ethernet”.

Table 129 PPPoE IA Circuit ID Sub-option Format: Defined in WT-101

SubOpt	Length	Value								
0x01 (1 byte)	N (1 byte)	Access Node Identifier (20 byte)	Space (1 byte)	eth (3 byte)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port No (2 byte)	: (1 byte)	VLAN ID (4 bytes)

40.1.2.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted or untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted ports.

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

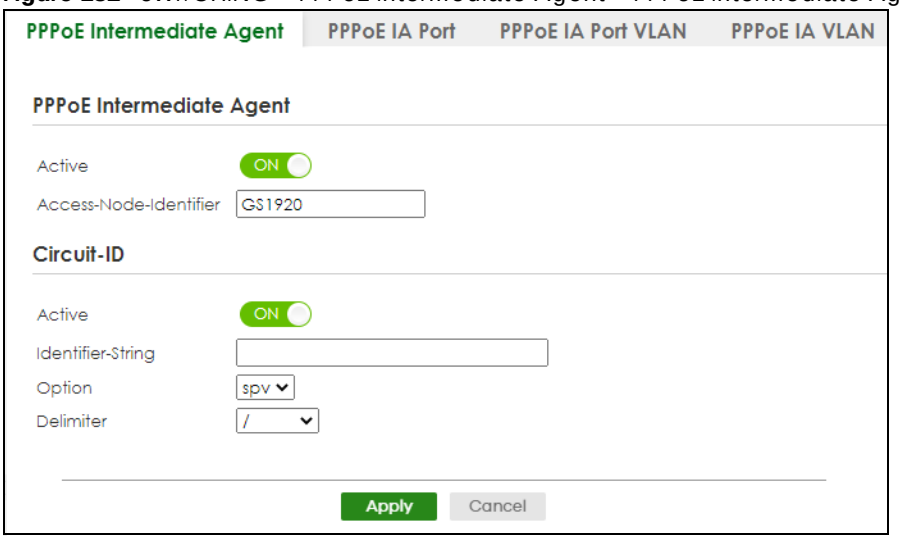
- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted ports.
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

40.2 PPPoE Intermediate Agent

Use this screen to configure the Switch to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE Intermediate Agent** to display the screen as shown.

Figure 182 SWITCHING > PPPoE Intermediate Agent > PPPoE Intermediate Agent



The following table describes the labels in this screen.

Table 130 SWITCHING > PPPoE Intermediate Agent > PPPoE Intermediate Agent

LABEL	DESCRIPTION
PPPoE Intermediate Agent	
Active	Enable the switch button to enable the PPPoE intermediate agent globally on the Switch.
Access-Node-Identifier	Enter up to 20 ASCII printable characters (except [?], [|], ['], ["], or [,]) to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.
Circuit-ID Use this section to configure the Circuit ID field in the PADI and PADR packets. The Circuit ID you configure for a specific port (in the **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE IA Port** screen) or for a specific VLAN on a port (in the **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE IA Port VLAN** screen) has priority over this. That means, if you also want to configure PPPoE IA Per-Port or Per-Port Per-VLAN setting, leave the fields here empty and configure circuit-id and remote-id in the Per-Port or Per-Port Per-VLAN screen.	
Active	Enable the switch button to have the Switch add the user-defined identifier string and variables (specified in the **Option** field) to PADI or PADR packets from PPPoE clients. If you leave this option unselected and do not configure any Circuit ID string (using CLI commands) on the Switch, the Switch will use the string specified in the **Access-Node-Identifier** field.
Identifier-String	Specify a string that the Switch adds in the Agent Circuit ID sub-option. You can enter up to 53 printable ASCII characters (except [?], [|], ['], ["], or [,]). Spaces are allowed.
Option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include **sp**, **sv**, **pv** and **spv** which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value.
Delimiter	Select a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. You can use a pound key (**#**), semi-colon (**;**), period (**.**), comma (**,**), forward slash (**/**) or space.
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.

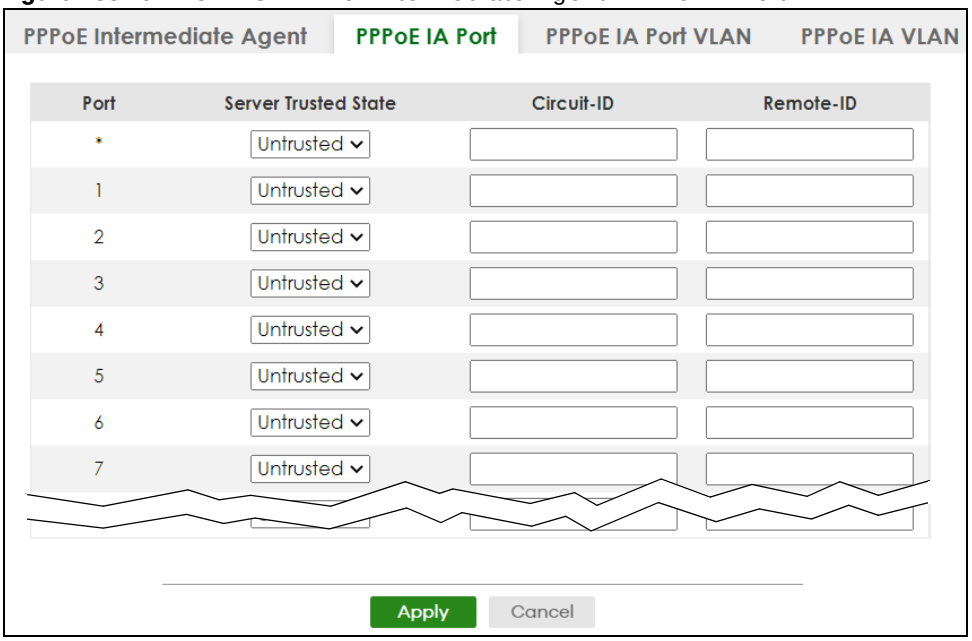
40.3 PPPoE IA Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The Switch will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the Switch and there are no trusted ports.

Click the **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE IA Port** screen to display the screen as shown.

Figure 183 SWITCHING > PPPoE Intermediate Agent > PPPoE IA Port



The following table describes the labels in this screen.

Table 131 SWITCHING > PPPoE Intermediate Agent > PPPoE IA Port

LABEL	DESCRIPTION
Port	This field displays the port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.

Table 131 SWITCHING > PPPoE Intermediate Agent > PPPoE IA Port (continued)

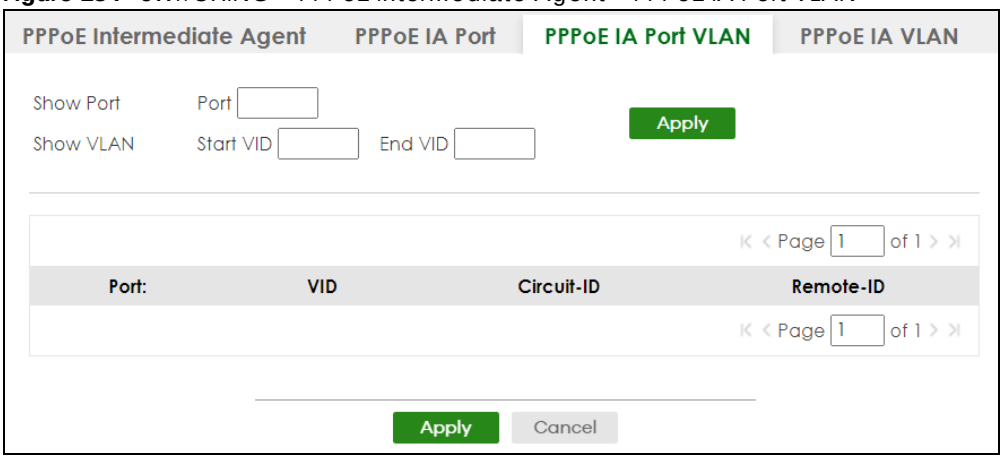
LABEL	DESCRIPTION
Server Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are uplink ports connected to PPPoE servers. If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted ports. Untrusted ports are downlink ports connected to subscribers. If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted ports. The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-ID	Enter a string of up to 63 ASCII characters (except [?], [|], ['], ["], or [,]) that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE IA Port VLAN** screen) has the highest priority.
Remote-ID	Enter a string of up to 63 ASCII characters (except [?], [|], ['], ["], or [,]) that the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. If you do not specify a string here or in the **Remote-ID** field for a VLAN on a port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure for a specific VLAN on a port (in the **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE IA Port VLAN** screen) has the highest priority.
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.

40.4 PPPoE IA Port VLAN

Use this screen to configure PPPoE IA settings that apply to a specific VLAN on a port.

Click **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE IA Port VLAN** to display the screen as shown.

Figure 184 SWITCHING > PPPoE Intermediate Agent > PPPoE IA Port VLAN



The following table describes the labels in this screen.

Table 132 SWITCHING > PPPoE Intermediate Agent > PPPoE IA Port VLAN

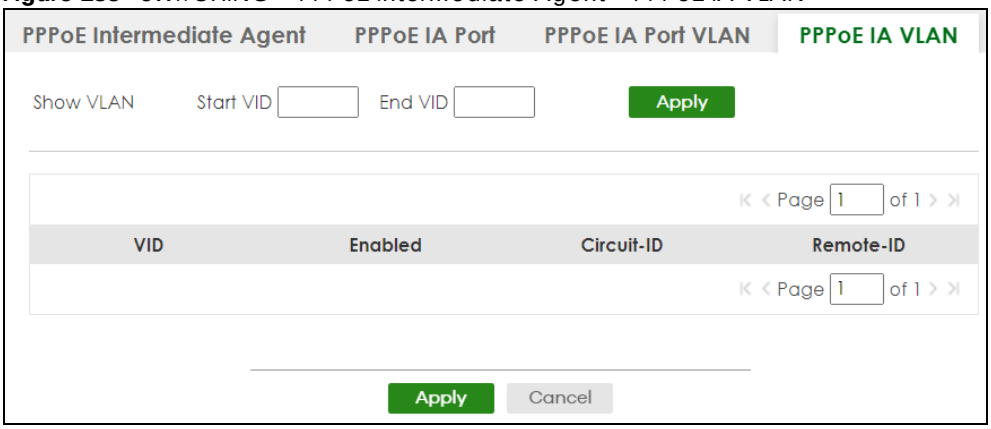
LABEL	DESCRIPTION
Show Port	
Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLANs on the port.
Show VLAN Use this section to specify the VLANs you want to configure in the section below.	
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
Port:	This field displays the port number specified above.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-ID	Enter a string of up to 63 ASCII characters (except [?], [|], ['], ["], or [,]) that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.
Remote-ID	Enter a string of up to 63 ASCII characters (except [?], [|], ['], ["], or [,]) that the Switch adds into the Agent Remote ID sub-option for this VLAN on the specified port. Spaces are allowed. If you do not specify a string here or in the **Remote-ID** field for a specific port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure here has the highest priority.
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.

40.5 PPPoE IA VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the Switch appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click **SWITCHING** > **PPPoE Intermediate Agent** > **PPPoE IA VLAN** to display the screen as shown.

Figure 185 SWITCHING > PPPoE Intermediate Agent > PPPoE IA VLAN



The following table describes the labels in this screen.

Table 133 SWITCHING > PPPoE Intermediate Agent > PPPoE IA VLAN

LABEL	DESCRIPTION
Show VLAN Use this section to specify the VLANs you want to configure in the section below.	
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-ID	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-ID	Select this option to make the Remote ID settings for a specific VLAN take effect.
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.

CHAPTER 41
Differentiated Services

41.1 DiffServ Overview

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

41.1.1 What You Can Do

- Use the **Diffserv** screen (Section 41.1 on page 261) to activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.
- Use the **DSCP Setting** screen (Section 41.3.1 on page 264) to change the DSCP-IEEE 802.1p mapping.

41.1.2 What You Need to Know

Read on for concepts on Differentiated Services that can help you configure the screens in this chapter.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Figure 186 DiffServ: Differentiated Service Field

DSCP (6 bits)	CU (2 bits)

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

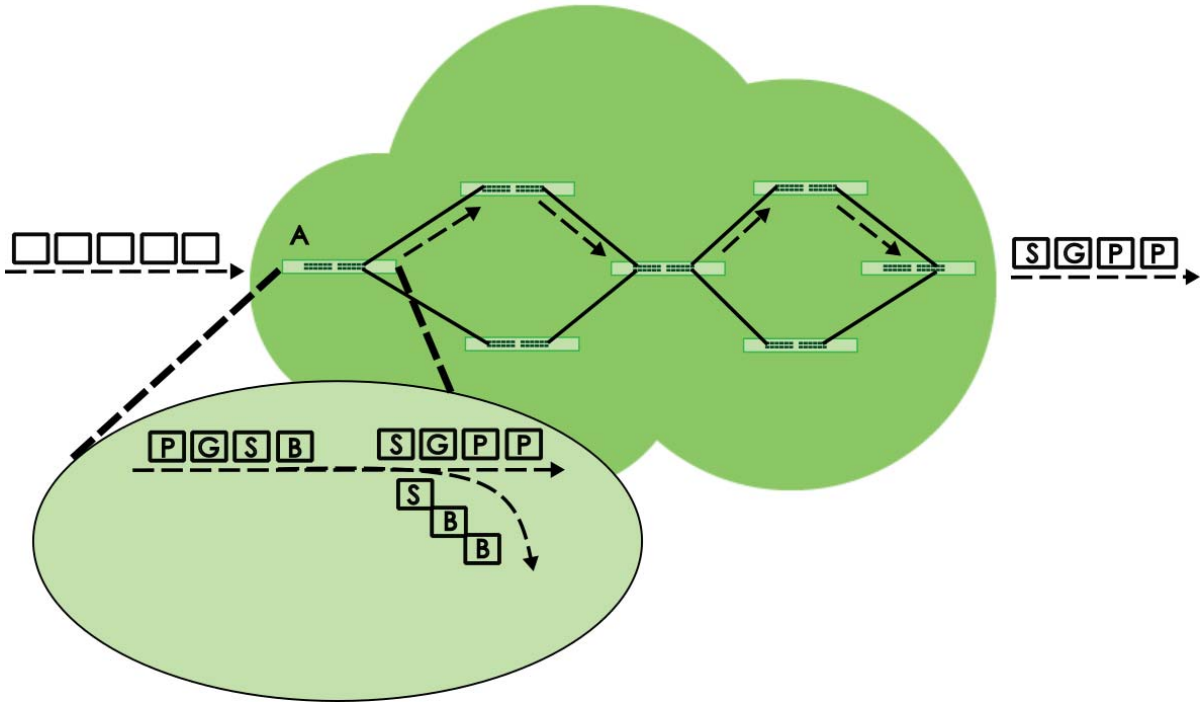
The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different

priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in Figure 187) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 187 DiffServ Network

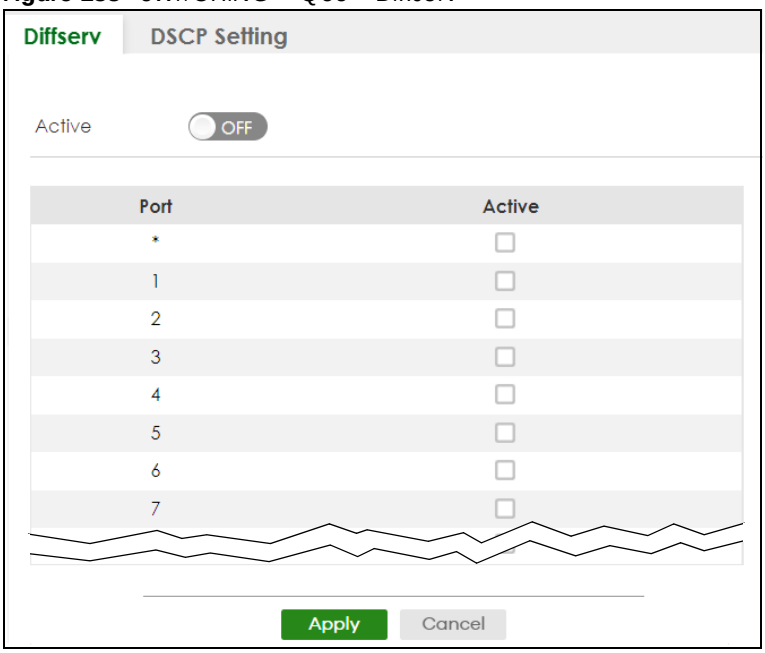


41.2 Activate DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected ports.

Click **SWITCHING** > **QoS** > **Diffserv** to display the screen as shown.

Figure 188 SWITCHING > QoS > Diffserv



The following table describes the labels in this screen.

Table 134 SWITCHING > QoS > Diffserv

LABEL	DESCRIPTION
Active	Enable the switch button to enable Diffserv on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select **Active** to enable Diffserv on the port.
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.

41.3 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

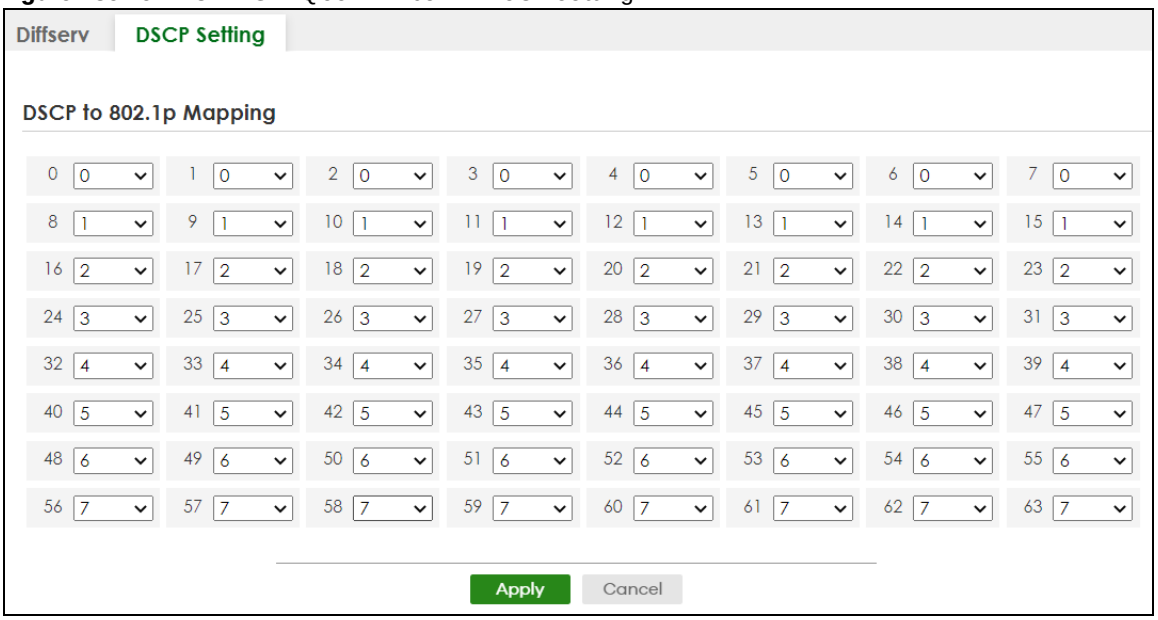
Table 135 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

41.3.1 Configure DSCP Settings

To change the DSCP-IEEE 802.1p mapping click **SWITCHING** > **QoS** > **Diffserv** > **DSCP Setting** to display the screen as shown next.

Figure 189 SWITCHING > QoS > Diffserv > DSCP Setting



The following table describes the labels in this screen.

Table 136 SWITCHING > QoS > Diffserv > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
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.

CHAPTER 42
Queuing Method

42.1 Queuing Method Overview

This section introduces the queuing methods supported.

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in the **SWITCHING** > **QoS** > **Priority Queue** screen and **802.1p Priority** in the **PORT** > **Port Setup** > **Port Setup** screen for related information.

42.1.1 What You Can Do

Use the **Queuing Method** screen (Section 42.2 on page 266) to set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

42.1.2 What You Need to Know

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SPQ does not automatically adapt to changing network requirements.

Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (portion) (the number you configure in the Weight field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic

on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

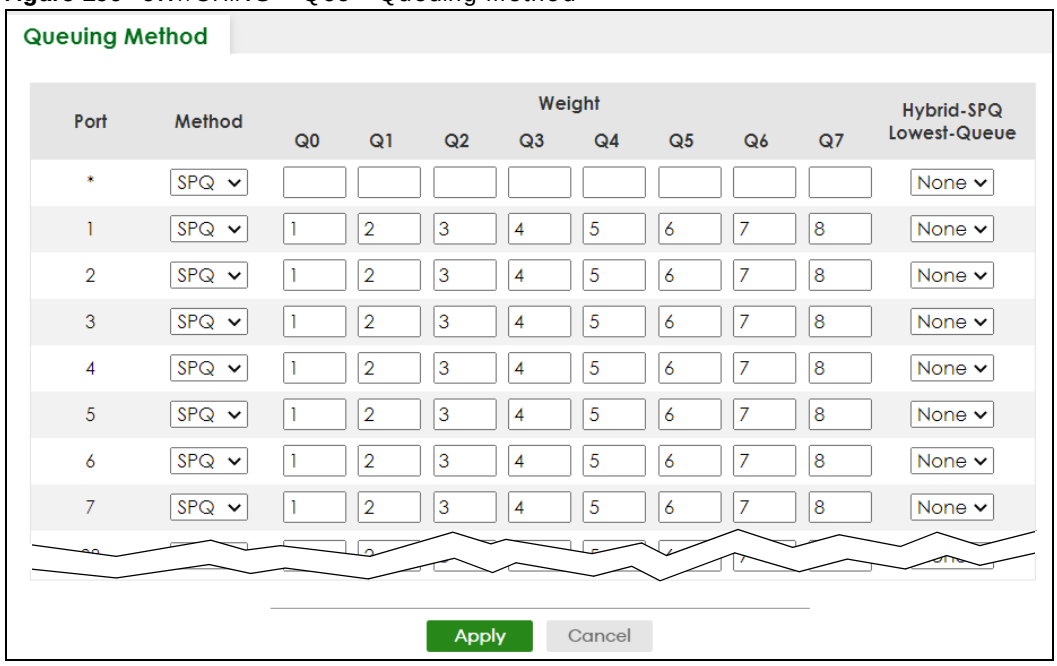
Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

42.2 Configure Queuing

Use this screen to set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

Click **SWITCHING** > **QoS** > **Queuing Method** to display the screen as shown below.

Figure 190 SWITCHING > QoS > Queuing Method



The following table describes the labels in this screen.

Table 137 SWITCHING > QoS > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 137 SWITCHING > QoS > Queuing Method (continued)

LABEL	DESCRIPTION
Method	Select **SPQ** (Strictly Priority Queuing), **WFQ** (Weighted Fair Queuing) or **WRR** (Weighted Round Robin). Strictly Priority Queuing services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the **Weight** field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Weight	When you select **WFQ** or **WRR**, enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select **WFQ** or **WRR**. Select a queue (**Q0** to **Q7**) to have the Switch use **SPQ** to service the subsequent queues after and including the specified queue for the port. For example, if you select **Q5**, the Switch services traffic on **Q5**, **Q6** and **Q7** using **SPQ**. Select **None** to always use **WFQ** or **WRR** for the port.
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.

CHAPTER 43
Priority Queue

43.1 Priority Queue Overview

IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use this screen to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the eight priority levels.

On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.

43.1.1 What You Can Do

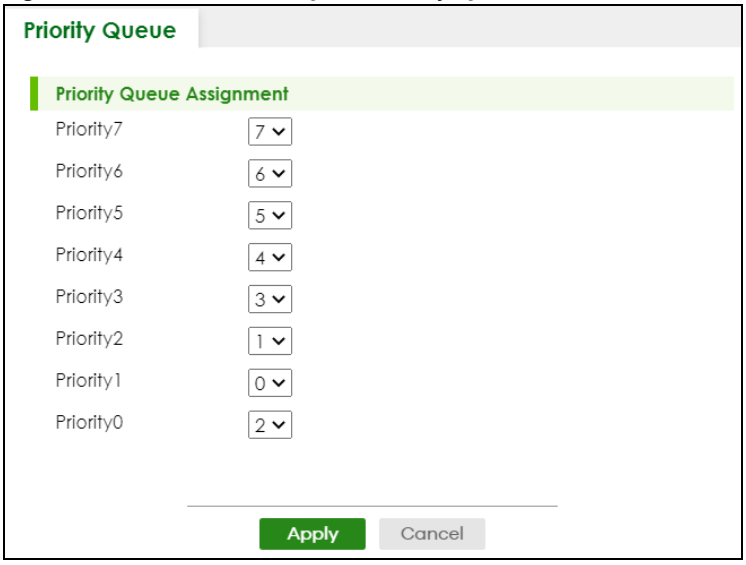
Use the **Priority Queue** screen (Section 43.2 on page 268) to configure the priority level-to-physical queue mapping.

43.2 Assign Priority Queue

Use this screen to assign priority level to each queue.

Click **SWITCHING** > **QoS** > **Priority Queue** to open this screen.

Figure 191 SWITCHING > QoS > Priority Queue



The following table describes the related labels in this screen.

Table 138 SWITCHING > QoS > Priority Queue

LABEL	DESCRIPTION
Priority Queue Assignment The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p). To map a priority level to a physical queue, select a physical queue from the drop-down menu on the right.	
Priority 7	Typically used for network control traffic such as router configuration messages.
Priority 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Priority 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Priority 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Priority 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Priority 2	This is for "spare bandwidth".
Priority 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Priority 0	Typically used for best-effort traffic.
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.

CHAPTER 44
Bandwidth Control

44.1 Bandwidth Control Overview

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

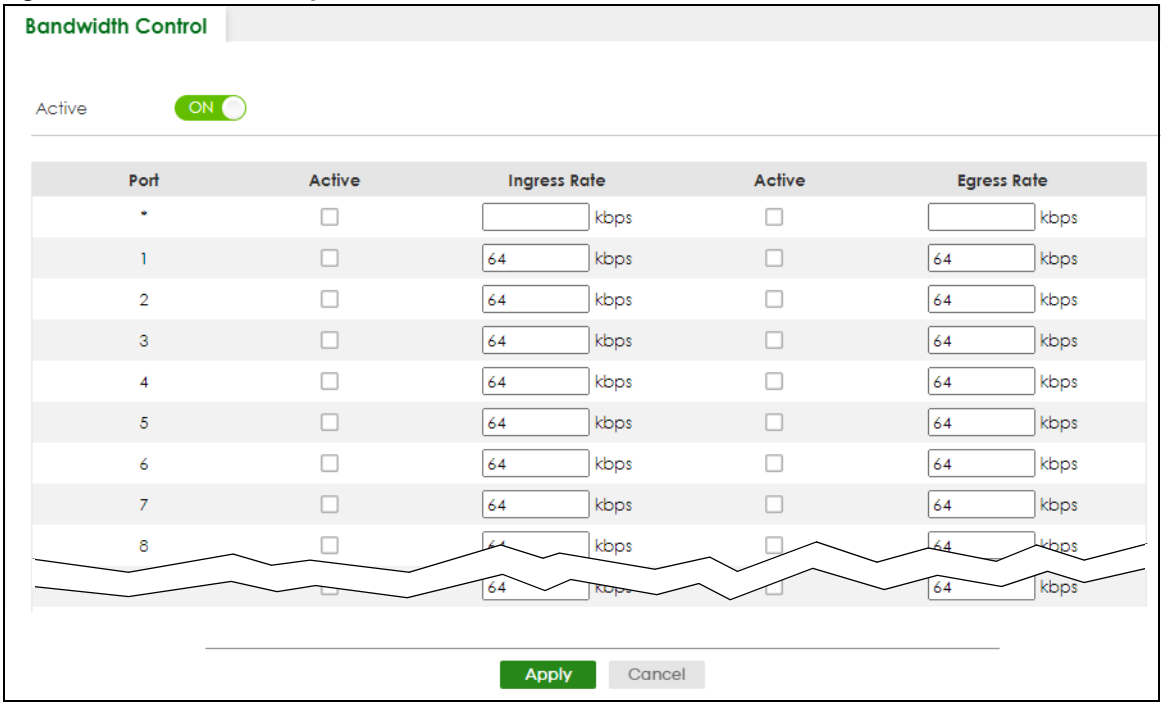
44.1.1 What You Can Do

Use the **Bandwidth Control** screen (Section 44.2 on page 270) to limit the bandwidth for traffic going through the Switch.

44.2 Bandwidth Control Setup

Click **SWITCHING** > **QoS** > **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 192 SWITCHING > QoS > Bandwidth Control



The following table describes the related labels in this screen.

Table 139 SWITCHING > QoS > Bandwidth Control

LABEL	DESCRIPTION
Active	Enable the switch button to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to activate ingress rate limits on this port.
Ingress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. Note: Ingress rate bandwidth control applies to layer 2 traffic only.
Active	Select this checkbox to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
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.

CHAPTER 45
Spanning Tree Protocol

45.1 Spanning Tree Protocol Overview

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.

45.1.1 What You Can Do

- Use the **Spanning Tree Protocol Status** screen (Section 45.2 on page 275) to view the STP status in the different STP modes (RSTP, MRSTP or MSTP) you can configure on the Switch.
- Use the **Spanning Tree Setup** screen (Section 45.3 on page 275) to activate one of the STP modes on the Switch.
- Use the **Rapid Spanning Tree Protocol Status** screen (Section 45.4 on page 276) to view the RSTP status.
- Use the **Rapid Spanning Tree Protocol** screen (Section 45.5 on page 278) to configure RSTP settings.
- Use the **Multiple Rapid Spanning Tree Protocol Status** screen (Section 45.6 on page 280) to view the MRSTP status.
- Use the **Multiple Rapid Spanning Tree Protocol** screen (Section 45.7 on page 282) to configure MRSTP.
- Use the **Multiple Spanning Tree Protocol Status** screen (Section 45.8 on page 284) to view the MSTP status.
- Use the **Multiple Spanning Tree Protocol** screen (Section 45.9 on page 287) to configure MSTP.
- Use the **Multiple Spanning Tree Protocol Port Setup** screen (Section 45.10 on page 290) to configure MSTP ports.

45.1.2 What You Need to Know

Read on for concepts on STP that can help you configure the screens in this chapter.

(Rapid) Spanning Tree Protocol

(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 that then 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.

STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 140 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4 Mbps	250	100 to 1000	1 to 65535
Path Cost	10 Mbps	100	50 to 600	1 to 65535
Path Cost	16 Mbps	62	40 to 400	1 to 65535
Path Cost	100 Mbps	19	10 to 60	1 to 65535
Path Cost	1 Gbps	4	3 to 10	1 to 65535
Path Cost	10 Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It 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.

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.

How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from

blocking state to forwarding state so as to eliminate transient loops.

Table 141 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does NOT exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

Multiple RSTP

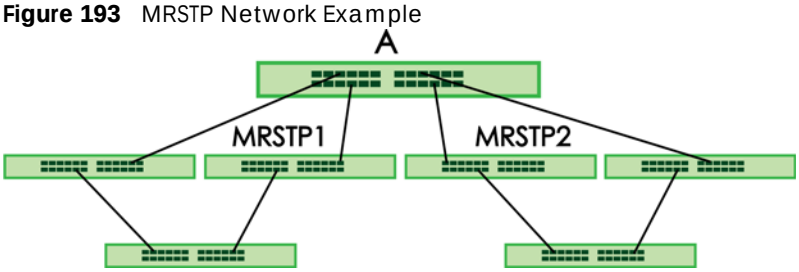
MRSTP (Multiple RSTP) is Zyxel's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign ports to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

To set up MRSTP, activate MRSTP on the Switch and specify which ports belong to which spanning tree.

Note: Each port can belong to one STP tree only.

Figure 193 MRSTP Network Example



Multiple STP

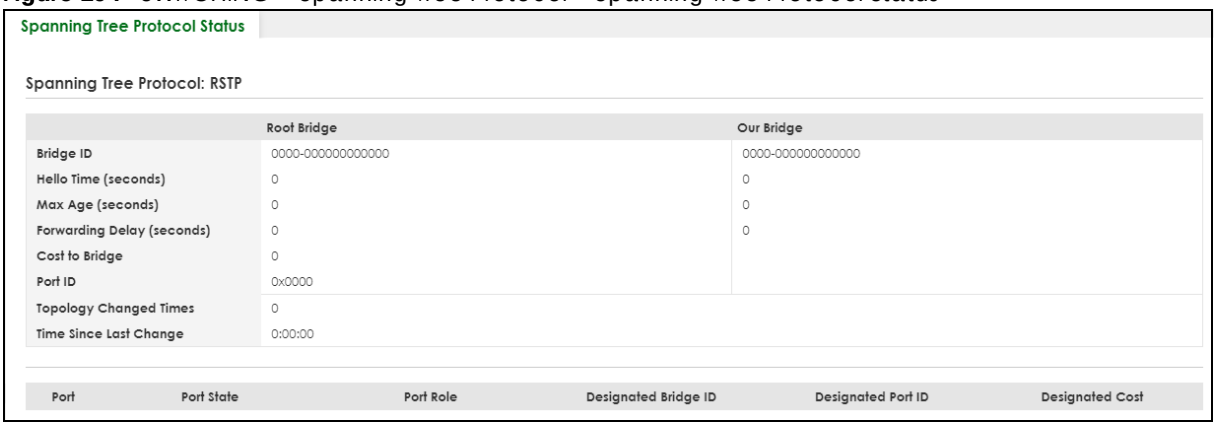
Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

45.2 Spanning Tree Protocol Status

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Protocol Status** to see the screen as shown.

Figure 194 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status

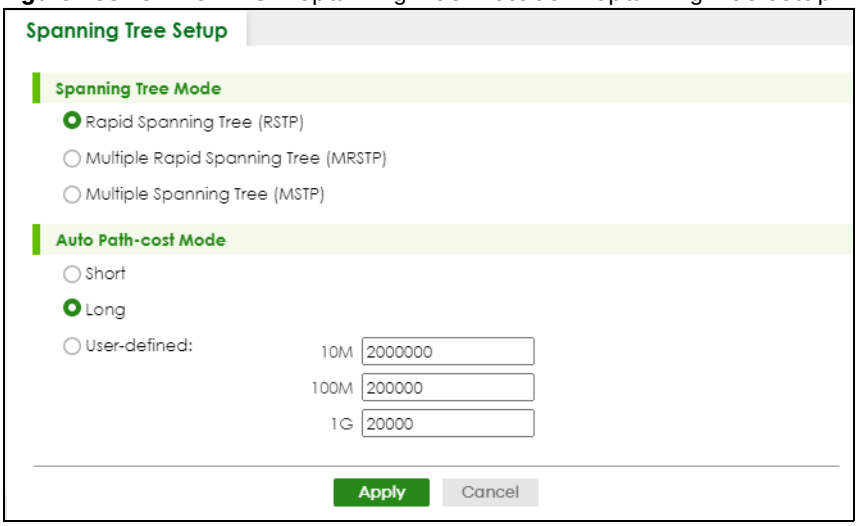


This screen differs depending on which STP mode (RSTP, MRSTP or MSTP) you configure on the Switch. This screen is described in detail in the section (Section 45.4 on page 276, Section 45.6 on page 280, and Section 45.8 on page 284) that follows the configuration section for each STP mode. Use the **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Setup** screen to activate one of the STP standards on the Switch.

45.3 Spanning Tree Setup

Use the this screen to activate one of the STP modes on the Switch. Click **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Setup** to display the screen as shown.

Figure 195 SWITCHING > Spanning Tree Protocol > Spanning Tree Setup



The following table describes the labels in this screen.

Table 142 SWITCHING > Spanning Tree Protocol > Spanning Tree Setup

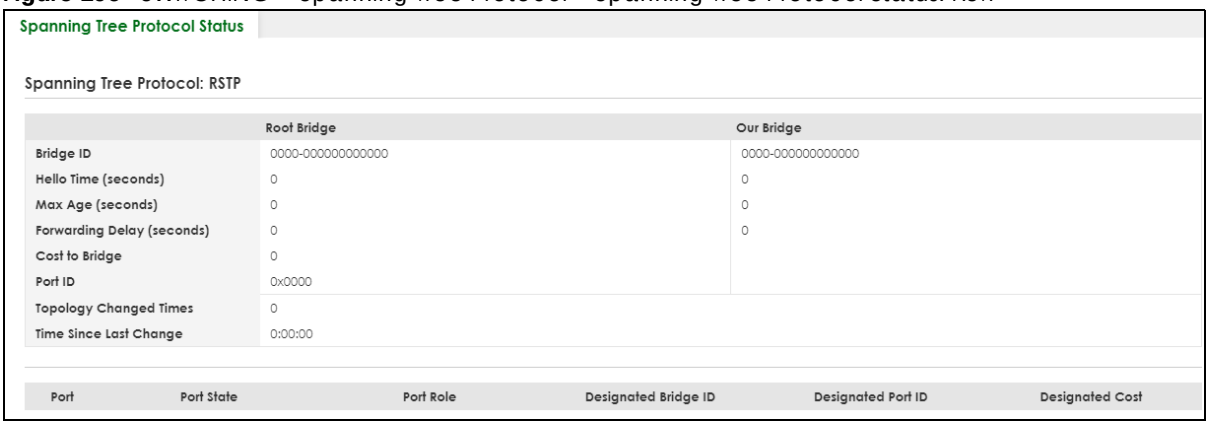
LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree (RSTP)**, **Multiple Rapid Spanning Tree (MRSTP)** or **Multiple Spanning Tree (MSTP)**.
Auto Path-cost Mode **Auto Path-cost Mode** allows you to have the Switch automatically set the path cost for each port according to their link speed. The Switch uses the path costs to determine the best path to the root bridge in a spanning tree. There are three **Auto Path-cost Mode**s that supports different path cost lengths: • **Short** (16-bit) • **Long** (32-bit) • **User-defined** (32-bit). The auto path cost values of each mode are described in Section 45.3 on page 275. Note: It is recommended to use the same **Auto Path-cost Mode** on all switches within the spanning tree network system. To use the auto path-cost feature, select the **Auto Path-cost mode** (**Short**, **Long**, **User-defined**), set a port's **Path Cost** (in the **SWITCHING** > **Spanning Tree Protocol** > **RSTP**, **MRSTP**, and **MSTP** screens) to "0". The Switch will automatically set the port's path cost to the auto path cost value defined by the **Auto Path-cost Mode** you select.	
Short	Select this mode if you want to use the 16-bit auto path cost values the Switch defines.
Long	Select this mode if you want to use the 32-bit auto path cost values the Switch defines.
User-defined	Select this mode to manually set the auto path costs for each link speed. Enter the path cost value for each link speed. The range is from 1 – 200000000. It is recommended to assign this value according to link speeds. The slower the speed, the higher the cost.
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.

45.4 Rapid Spanning Tree Protocol Status

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Protocol Status** in the navigation panel to display the status screen as shown next. See Section 45.1 on page 272 for more information on RSTP.

Note: This screen is only available after you activate RSTP on the Switch.

Figure 196 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: RSTP



The following table describes the labels in this screen.

Table 143 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: RSTP

LABEL	DESCRIPTION
Spanning Tree Protocol: RSTP	
Bridge	**Root Bridge** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root Bridge** and **Our Bridge** if the Switch is the root switch.
Hello Time (seconds)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time**, **Max Age** and **Forwarding Delay**.
Max Age (seconds)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (seconds)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does NOT exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Port	This field displays the number of the port on the Switch.
Port State	This field displays the port state in STP. • **DISCARDING** – The port does not forward or process received frames or learn MAC addresses, but still listens for BPDUs. • **LEARNING** – The port learns MAC addresses and processes BPDUs, but does NOT forward frames yet. • **FORWARDING** – The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.

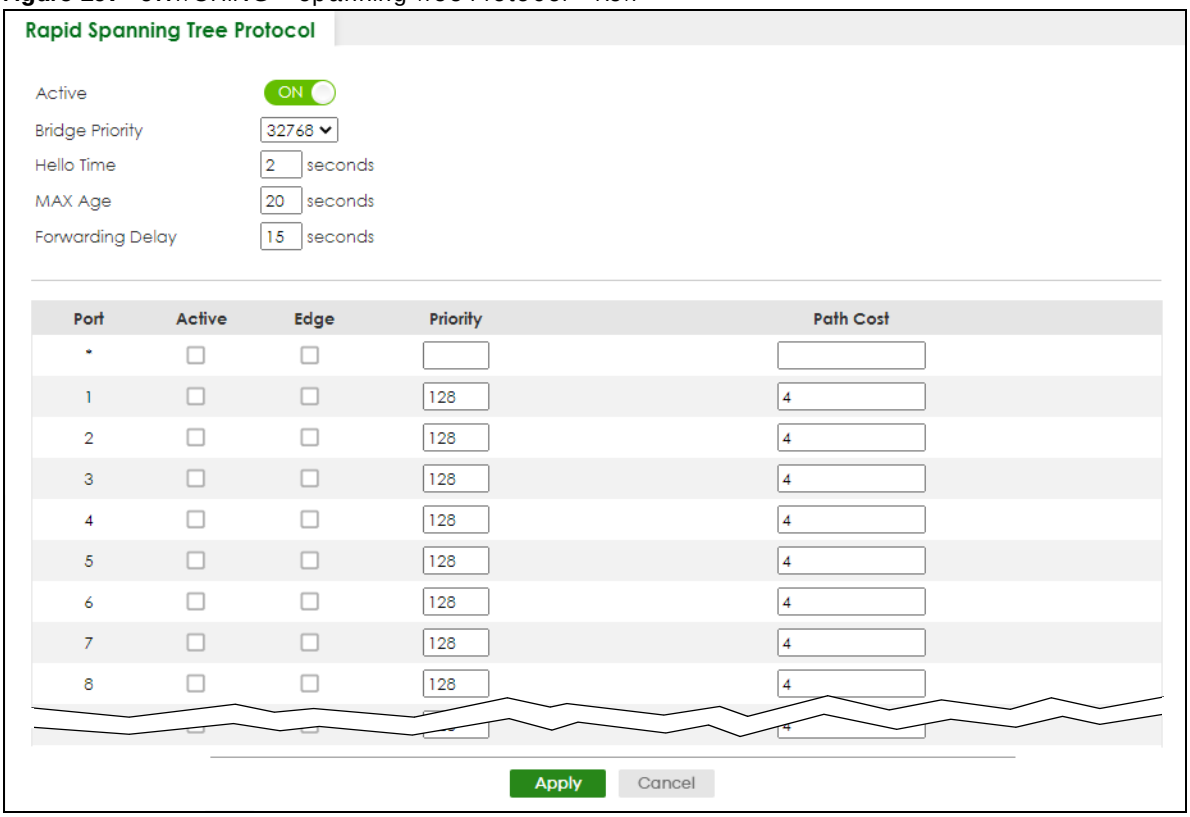
Table 143 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: RSTP (continued)

LABEL	DESCRIPTION
Port Role	This field displays the role of the port in STP. • **Root** – A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does NOT have a root port. • **Designated** – A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • **Alternate** – A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • **Backup** – A blocked port, which has a backup or redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • **Disabled** – Not strictly part of STP. The port can be disabled manually.
Designated Bridge ID	This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected.
Designated Port ID	This field displays the priority and number of the bridge port (on the designated bridge), through which the designated bridge transmits the stored configuration messages.
Designated Cost	This field displays the path cost to the LAN segment to which the port is connected when the port is a designated port. Otherwise, it displays the path cost to the root bridge from the designated port for the LAN segment to which this port is connected.

45.5 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 45.1 on page 272 for more information on RSTP. Click **SWITCHING** > **Spanning Tree Protocol** > **RSTP** in the navigation panel to display the screen as shown.

Figure 197 SWITCHING > Spanning Tree Protocol > RSTP



The following table describes the labels in this screen.

Table 144 SWITCHING > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Active	Enable the switch button to activate RSTP. Disable the switch to disable RSTP. Note: You must also activate **Rapid Spanning Tree (RSTP)** in the **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Setup** screen to enable RSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The Switch with the highest priority (lowest numeric value) becomes the STP root switch. If all Switches have the same priority, the Switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines **Hello Time**, **Max Age** and **Forwarding Delay**.
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.
Max Age	This is the maximum time (in seconds) the 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.

Table 144 SWITCHING > Spanning Tree Protocol > RSTP (continued)

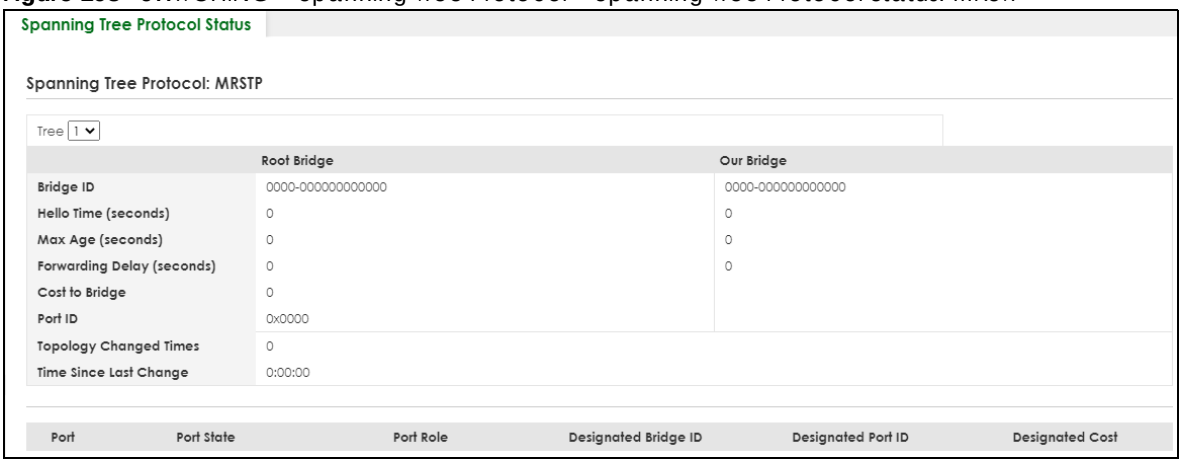
LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every Switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to activate RSTP on this port.
Edge	Select this checkbox to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
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.
Path Cost	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.
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.

45.6 Multiple Rapid Spanning Tree Protocol

Click **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Protocol Status** in the navigation panel to display the status screen as shown next. See Section 45.6 on page 280 for more information on MRSTP.

Note: This screen is only available after you activate MRSTP on the Switch.

Figure 198 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MRSTP



The following table describes the labels in this screen.

Table 145 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MRSTP

LABEL	DESCRIPTION
Tree	Select which STP tree configuration you want to view.
Bridge	**Root Bridge** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root Bridge** and **Our Bridge** if the Switch is the root switch.
Hello Time (seconds)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time**, **Max Age** and **Forwarding Delay**.
Max Age (seconds)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (seconds)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Port	This field displays the number of the port on the Switch.
Port State	This field displays the port state in STP. • **DISCARDING** – The port does not forward or process received frames or learn MAC addresses, but still listens for BPDUs. • **LEARNING** – The port learns MAC addresses and processes BPDUs, but does not forward frames yet. • **FORWARDING** – The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.

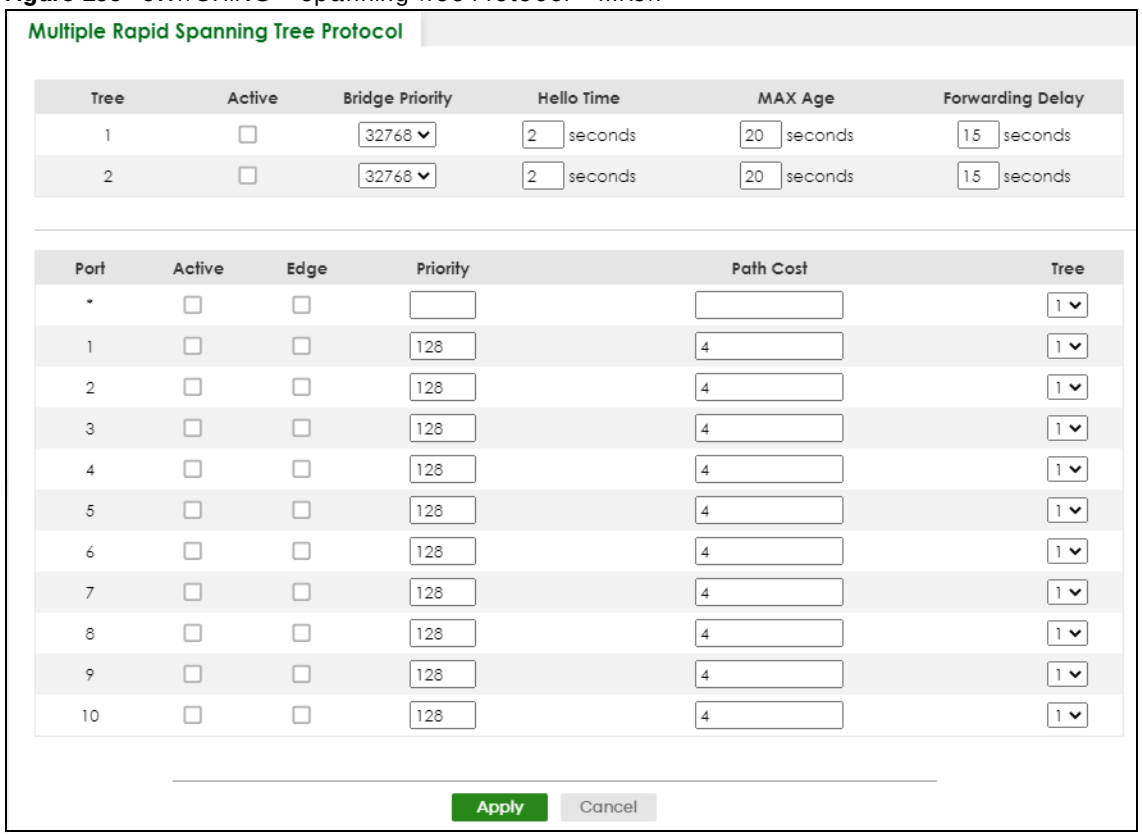
Table 145 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MRSTP (continued)

LABEL	DESCRIPTION
Port Role	This field displays the role of the port in STP. • **Root** – A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does not have a root port. • **Designated** – A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • **Alternate** – A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • **Backup** – A blocked port, which has a backup or redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • **Disabled** – Not strictly part of STP. The port can be disabled manually.
Designated Bridge ID	This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected.
Designated Port ID	This field displays the priority and number of the bridge port (on the designated bridge), through which the designated bridge transmits the stored configuration messages.
Designated Cost	This field displays the path cost to the LAN segment to which the port is connected when the port is a designated port. Otherwise, it displays the path cost to the root bridge from the designated port for the LAN segment to which this port is connected.

45.7 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **SWITCHING** > **Spanning Tree Protocol** > **MRSTP** in the navigation panel to display the screen as shown.

Figure 199 SWITCHING > Spanning Tree Protocol > MRSTP



The following table describes the labels in this screen.

Table 146 SWITCHING > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Tree	This is the index number of the STP trees.
Active	Select this checkbox to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate **Multiple Rapid Spanning Tree (MRSTP)** in the **SWITHCING** > **Spanning Tree Protocol** > **Spanning Tree Setup** screen to enable MRSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines **Hello Time**, **Max Age** and **Forwarding Delay**.
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.
Max Age	This is the maximum time (in seconds) the 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.

Table 146 SWITCHING > Spanning Tree Protocol > MRSTP (continued)

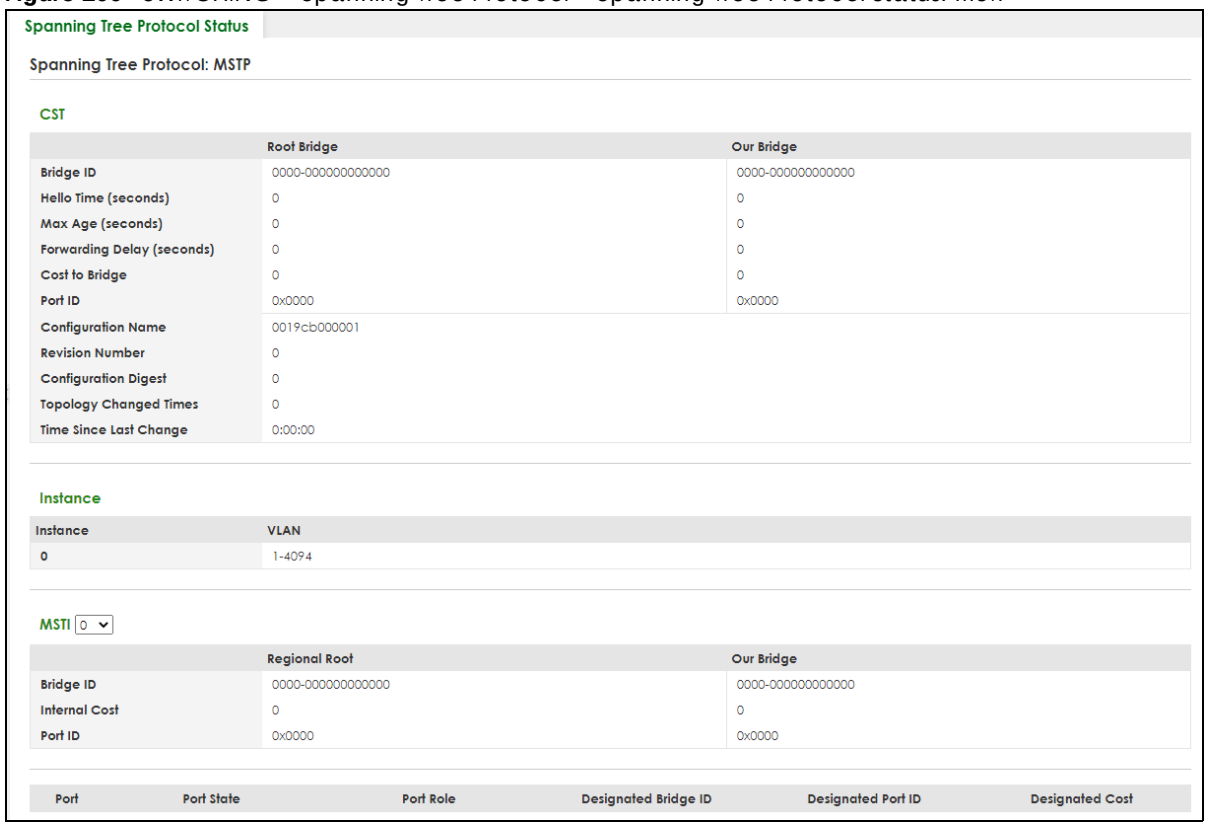
LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to activate STP on this port.
Edge	Select this checkbox to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
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.
Path Cost	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.
Tree	Select which STP tree configuration this port should participate in.
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.

45.8 Multiple Spanning Tree Protocol Status

Click **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Protocol Status** in the navigation panel to display the status screen as shown next.

Note: This screen is only available after you activate MSTP on the Switch.

Figure 200 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MSTP



The following table describes the labels in this screen.

Table 147 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MSTP

LABEL	DESCRIPTION
CST This section describes the Common Spanning Tree settings.	
Bridge	**Root Bridge** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root Bridge** and **Our Bridge** if the Switch is the root switch.
Hello Time (seconds)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time**, **Max Age** and **Forwarding Delay**.
Max Age (seconds)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (seconds)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.

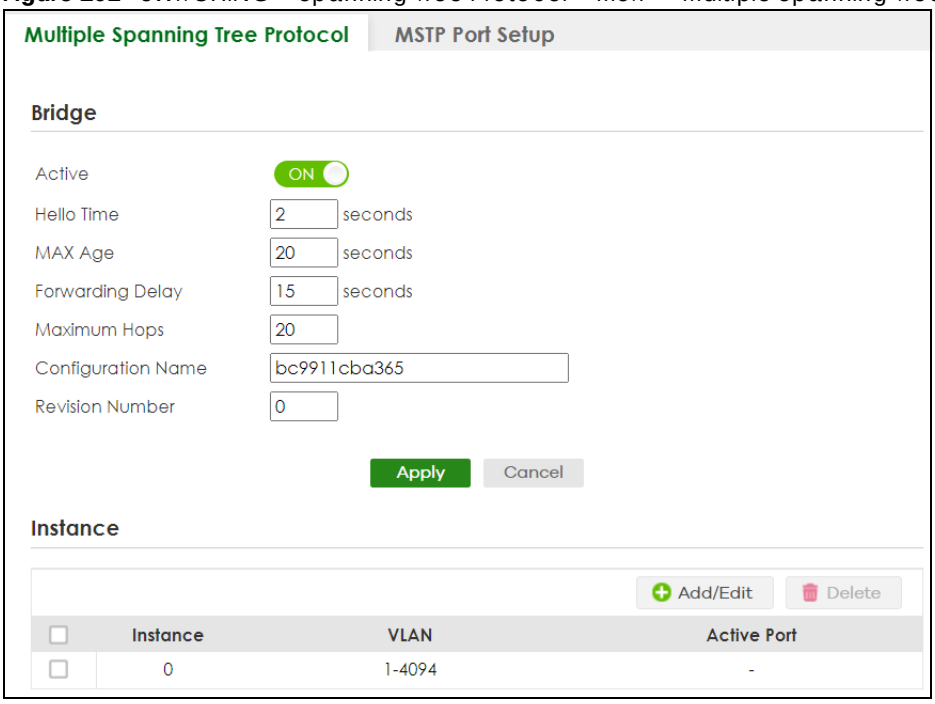
Table 147 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MSTP (continued)

LABEL	DESCRIPTION
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	
MSTI	Select the MST instance settings you want to view.
	Regional Root refers to the base of the MST instance. **Our Bridge** is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Regional Root** and **Our Bridge** if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.
Port	This field displays the number of the port on the Switch.
Port State	This field displays the port state in STP. • **DISCARDING** – The port does not forward or process received frames or learn MAC addresses, but still listens for BPDUs. • **LEARNING** – The port learns MAC addresses and processes BPDUs, but does not forward frames yet. • **FORWARDING** – The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.
Port Role	This field displays the role of the port in STP. • **Root** – A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does not have a root port. • **Designated** – A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • **Alternate** – A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • **Backup** – A blocked port, which has a backup or redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • **Disabled** – Not strictly part of STP. The port can be disabled manually.
Designated Bridge ID	This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected.
Designated Port ID	This field displays the priority and number of the bridge port (on the designated bridge), through which the designated bridge transmits the stored configuration messages.
Designated Cost	This field displays the path cost to the LAN segment to which the port is connected when the port is a designated port. Otherwise, it displays the path cost to the root bridge from the designated port for the LAN segment to which this port is connected.

45.9 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **SWITCHING** > **Spanning Tree Protocol** > **MSTP** in the navigation panel to display the screen as shown.

Figure 201 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol



The following table describes the labels in this screen.

Table 148 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol

LABEL	DESCRIPTION
Bridge	
Active	Enable the switch button to activate MSTP on the Switch. Disable the switch to disable MSTP on the Switch. Note: You must also activate **Multiple Spanning Tree (MSTP)** in the **SWITCHING** > **Spanning Tree Protocol** > **Spanning Tree Setup** screen to enable MSTP on the Switch.
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.
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.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)

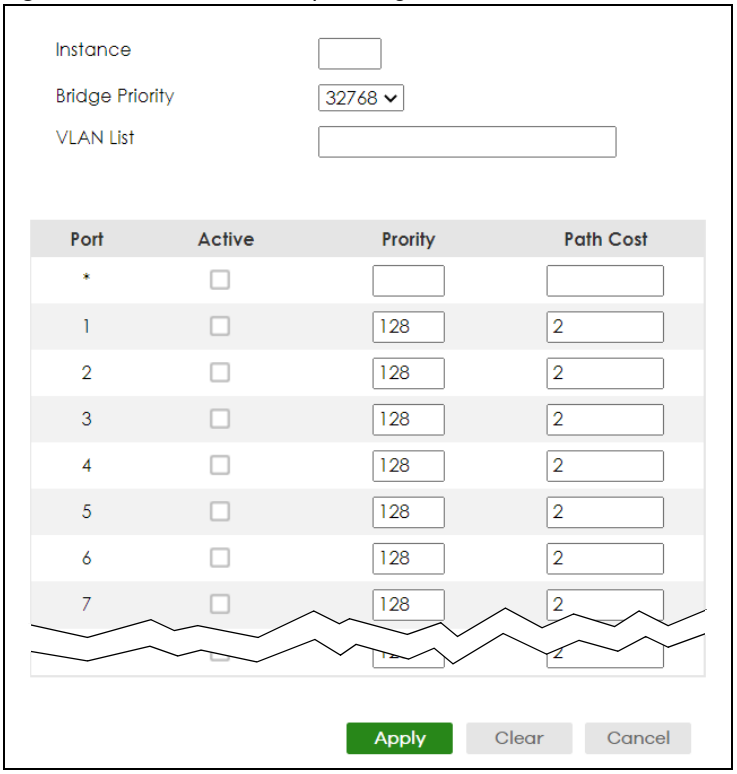
Table 148 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol (continued)

LABEL	DESCRIPTION
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [|], ['], ["], or [,]) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
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.
Instance Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.	
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new instance or edit a selected one.
Delete	Click **Delete** to remove the selected instances.

45.9.1 Add/Edit Multiple Spanning Tree

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **Spanning Tree Protocol** > **MSTP** > **Multiple Spanning Tree Protocol** screen to display this screen.

Figure 202 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol > Add/Edit



The following table describes the labels in this screen.

Table 149 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol > Add/Edit

LABEL	DESCRIPTION
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0 – 16.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).
VLAN List	Enter the VLAN ID range. You can specify multiple VLAN ID range separated by (no space) comma (,) or hyphen (“-”) for a range. For example, enter “1,3,5-7” for VLANs 1, 3, 5, 6, and 7.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the 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.

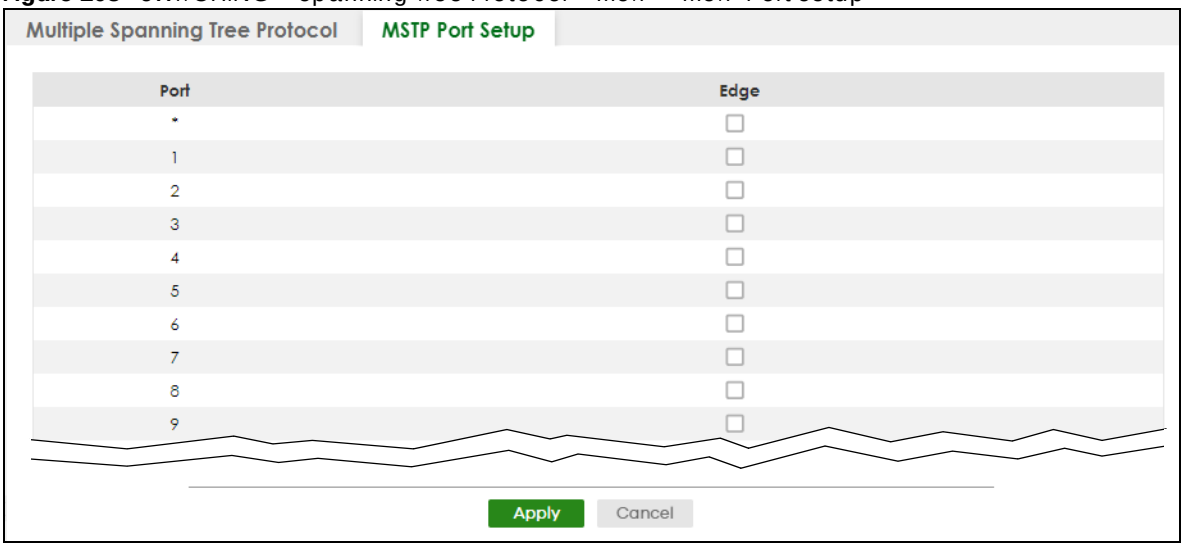
Table 149 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol > Add/Edit

LABEL	DESCRIPTION
Path Cost	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.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

45.10 Multiple Spanning Tree Protocol Port Setup

Click **SWITCHING** > **Spanning Tree Protocol** > **MSTP** > **MSTP Port Setup** to display the screen as shown next.

Figure 203 SWITCHING > Spanning Tree Protocol > MSTP > MSTP Port Setup



The following table describes the labels in this screen.

Table 150 SWITCHING > Spanning Tree Protocol > MSTP > MSTP Port Setup

LABEL	DESCRIPTION
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Edge	Select this checkbox to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).

Table 150 SWITCHING > Spanning Tree Protocol > MSTP > MSTP Port Setup (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.

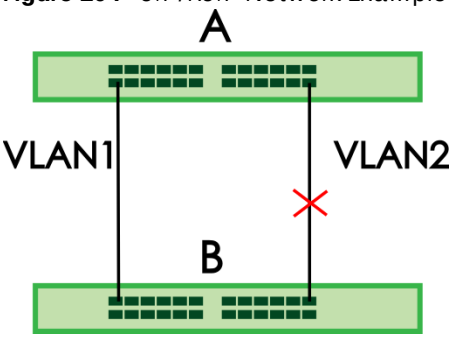
45.11 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

45.11.1 MSTP Network Example

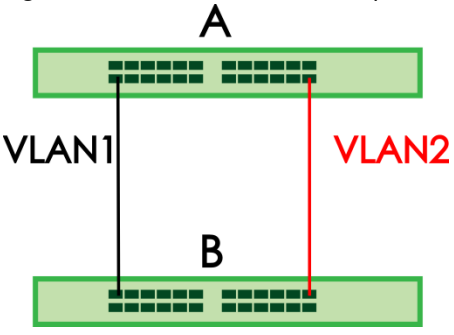
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 204 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Therefore traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 205 MSTP Network Example



45.11.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter

an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

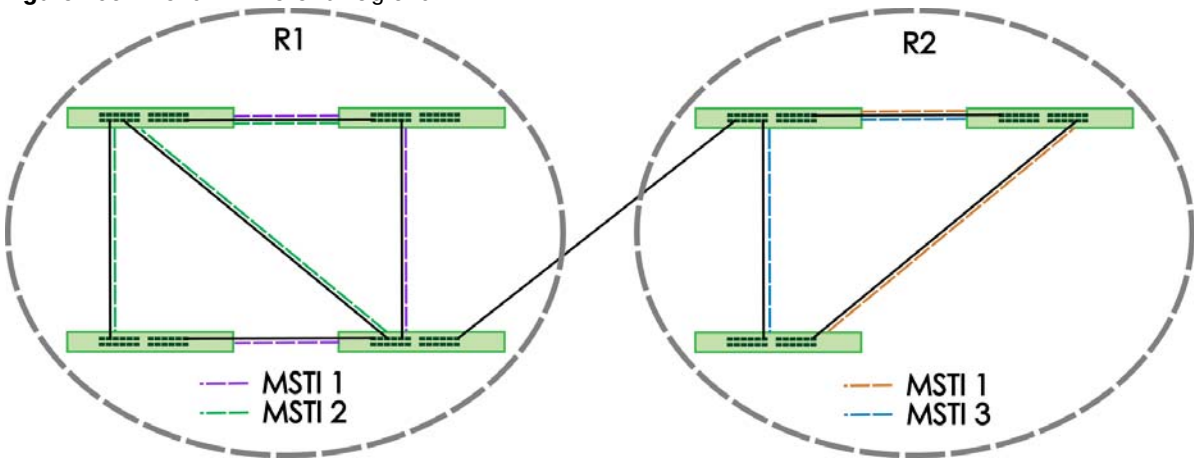
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

45.11.3 MST Instance

An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Therefore an MSTI does not span across MST regions.

The following figure shows an example where there are two MSTT regions. Regions 1 (**R1**) and 2 (**R2**) have two spanning tree instances. (**MSTI1**, **MSTI2** and **MSTI1**, **MSTI3**). The black connecting lines represent the physical connections.

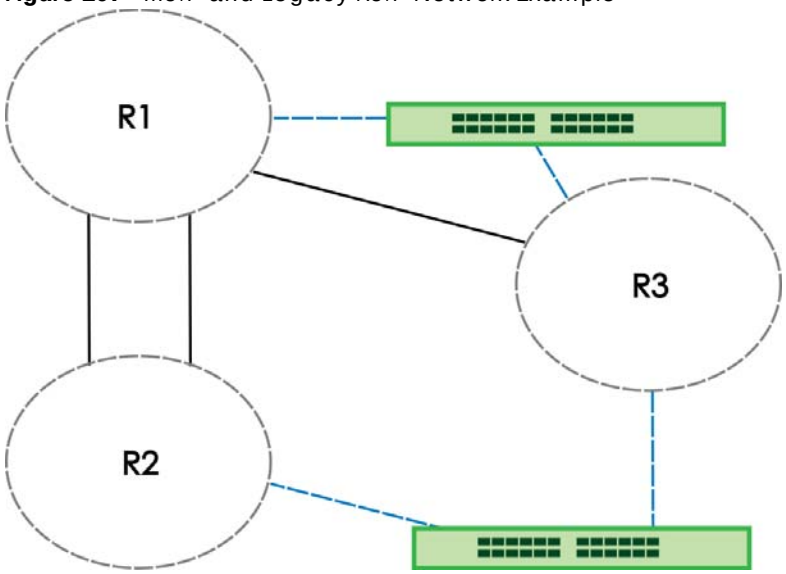
Figure 206 MSTIs in Different Regions



45.11.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions(**R1, R2, R3**) and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP. In the figure below, the black connecting lines represent the physical connections. The green connecting lines represent RSTP on the link.

Figure 207 MSTP and Legacy RSTP Network Example



CHAPTER 46
Static MAC Filtering

46.1 Static MAC Filtering Overview

This chapter discusses MAC address port filtering.

Filtering means sifting traffic going through the Switch based on the source and/or destination MAC addresses and VLAN group (ID).

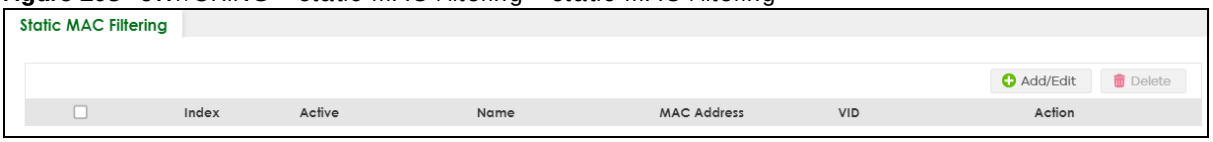
46.1.1 What You Can Do

Use the **Static MAC Filtering** screen (Section 46.2 on page 294) to create rules for traffic going through the Switch.

46.2 Configure a Static MAC Filtering Rule

Use this screen to view and configure rules for traffic going through the Switch. Click **SWITCHING** > **Static MAC Filtering** > **Static MAC Filtering** in the navigation panel to display the screen as shown next.

Figure 208 SWITCHING > Static MAC Filtering > Static MAC Filtering



The following table describes the related labels in this screen.

Table 151 SWITCHING > Static MAC Filtering > Static MAC Filtering

LABEL	DESCRIPTION
Index	This field displays the index number of the rule.
Active	This field displays whether the rule is activated or not.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source or destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Action	This field displays **Discard source**, **Discard destination**, or **Discard both** depending on what you configured above.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

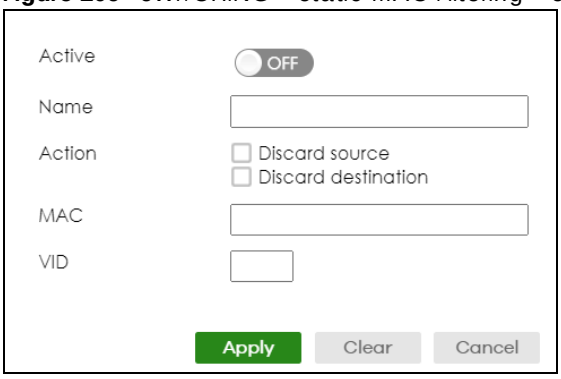
Table 151 SWITCHING > Static MAC Filtering > Static MAC Filtering (continued)

LABEL	DESCRIPTION
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

46.2.1 Add/Edit a Static MAC Filtering Rule

Use this screen to create or edit rules for traffic going through the Switch. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **Static MAC Filtering** > **Static MAC Filtering** screen to display this screen.

Figure 209 SWITCHING > Static MAC Filtering > Static MAC Filtering > Add/Edit



The following table describes the related labels in this screen.

Table 152 SWITCHING > Static MAC Filtering > Static MAC Filtering > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate your rule. You may temporarily deactivate a rule without deleting it by de-selecting this checkbox.
Name	Enter a descriptive name (up to 32 printable ASCII characters excluding [?], [|], ['], ["], or [,]) for this rule. This is for identification only.
Action	Select **Discard source** to drop the frames from the source MAC address (specified in the **MAC** field). The Switch can still send frames to the MAC address. Select **Discard destination** to drop the frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to or from the MAC address specified in the **MAC** field.
MAC	Enter a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Enter the VLAN group identification number.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 47
Static MAC Forwarding

47.1 Static MAC Forwarding Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

Use these screens to configure static MAC address forwarding.

47.1.1 What You Can Do

Use the **Static MAC Forwarding** screen (Section 47.2 on page 296) to assign static MAC addresses for a port.

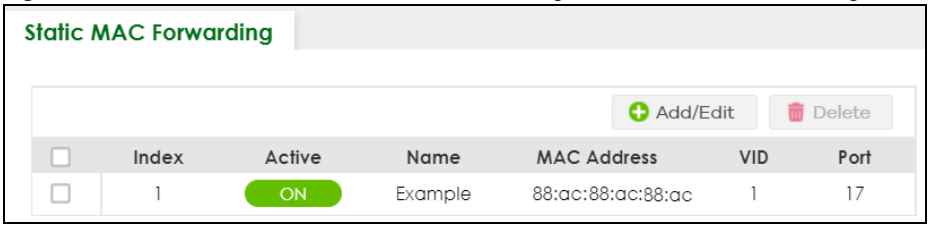
47.2 Configure Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch.

Click **SWITCHING** > **Static MAC Forwarding** > **Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 210 SWITCHING > Static MAC Forwarding > Static MAC Forwarding



The following table describes the labels in this screen.

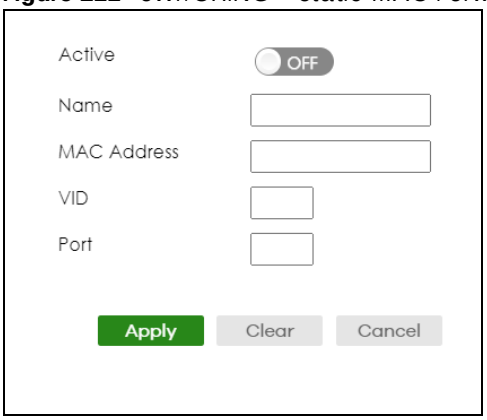
Table 153 SWITCHING > Static MAC Forwarding > Static MAC Forwarding

LABEL	DESCRIPTION
Index	This is the index number of a static MAC address rule.
Active	This field displays whether this static MAC address forwarding rule is active. You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new rule or edit a selected one.
Delete	Click **Delete** to remove the selected rules.

47.2.1 Add/Edit Static MAC Forwarding Rules

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **Static MAC Forwarding** > **Static MAC Forwarding** screen to display this screen.

Figure 211 SWITCHING > Static MAC Forwarding > Static MAC Forwarding > Add/Edit



The following table describes the labels in this screen.

Table 154 SWITCHING > Static MAC Forwarding > Static MAC Forwarding > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate your rule. You may temporarily deactivate a rule without deleting it by disabling the switch.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do NOT age out.
VID	Enter the VLAN identification number.

Table 154 SWITCHING > Static MAC Forwarding > Static MAC Forwarding > Add/Edit (continued)

LABEL	DESCRIPTION
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 48
VLAN

48.1 VLAN Overview

This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

The type of screen you see here depends on the **VLAN Type** you selected in the **SYSTEM** > **Switch Setup** screen.

48.1.1 What You Can Do

- Use the **VLAN Status** screen (Section 48.3 on page 302) to view and search all static VLAN groups.
- Use the **VLAN Status Details** screen (Section 48.3.1 on page 303) to view detailed port settings and status of the static VLAN group.
- Use the **Static VLAN Setup** screen (Section 48.4 on page 304) to configure a static VLAN for the Switch.
- Use the **VLAN Port Setup** screen (Section 48.5 on page 306) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **GVRP** screen (Section 48.6 on page 307) to enable/disable GVRP on each port.
- Use the **Subnet Based VLAN Setup** screen (Section 48.8 on page 309) to set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
- Use the **Protocol Based VLAN Setup** screen (Section 48.9 on page 311) to set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
- Use the **Voice VLAN Setup** screen (Section 48.11 on page 313) to set up VLANs that allow you to group voice traffic with defined priority and enable the Switch port to carry the voice traffic separately from data traffic to ensure the sound quality does NOT deteriorate.
- Use the **MAC Based VLAN Setup** screen (Section 48.12 on page 315) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. This eliminates the need to reconfigure the Switch when you change ports. The Switch will forward the packets based on the source MAC address you set up previously.
- Use the **Vendor ID Based VLAN Setup** screen (Section 48.13 on page 317) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. You can specify a mask for the MAC address to create a MAC address filter and enter a weight to set the VLAN rule's priority.
- Use the **Port-Based VLAN Setup** screen (Section 48.14 on page 319) to set up VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

48.1.2 What You Need to Know

Read this section to know more about VLAN and how to configure the screens.

48.2 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges – they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier, residing within the type or length field of the Ethernet frame) and 2 bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4094.

TPID	User Priority	CFI	VLAN ID
16 Bits	3 Bits	1 Bit	12 Bits

Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

48.2.0.1 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 155 IEEE 802.1Q VLAN Terminology

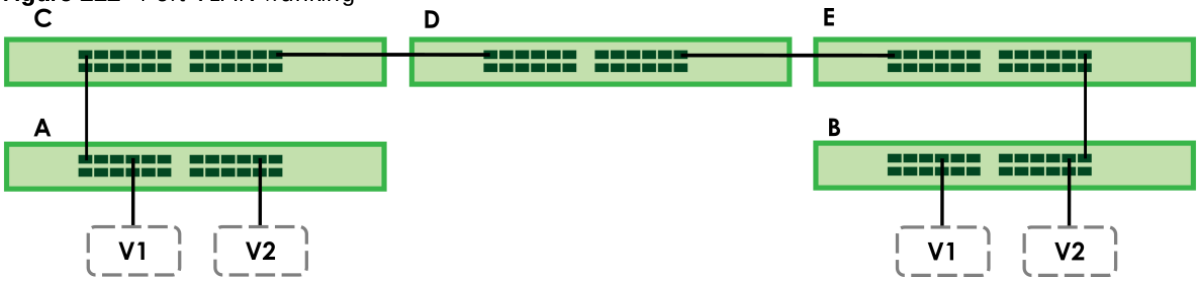
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration or de-registration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN do not tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member.

48.2.0.2 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (**V1** and **V2**) on devices **A** and **B**. Without **VLAN Trunking**, you must configure VLAN groups 1 and 2 (**V1** and **V2**) on all intermediary switches **C**, **D** and **E**; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on ports in each intermediary switch you only need to create VLAN groups in the end devices (**A** and **B**). **C**, **D** and **E** automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking ports.

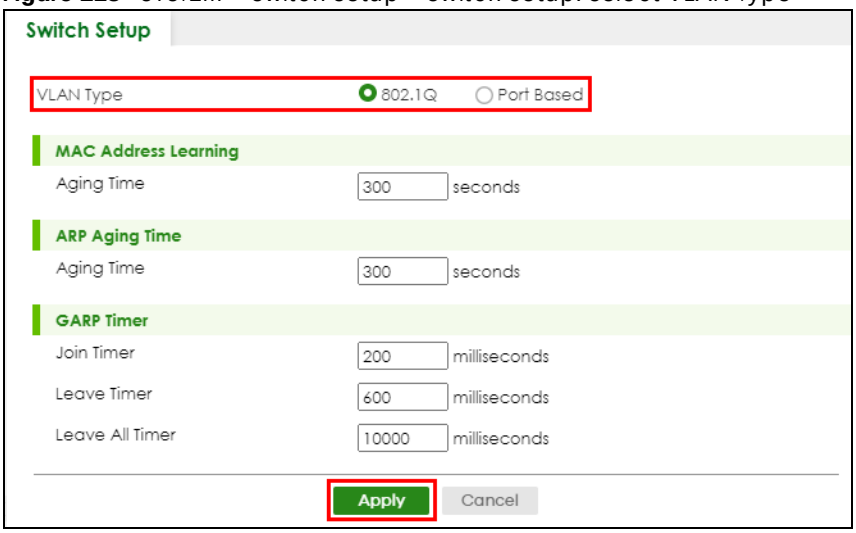
Figure 212 Port VLAN Trunking



48.2.0.3 Select the VLAN Type

Select a VLAN type in the **SYSTEM** > **Switch Setup** > **Switch Setup** screen.

Figure 213 SYSTEM > Switch Setup > Switch Setup: Select VLAN Type



802.1Q Static VLAN

Make sure **802.1Q** is selected in the **SYSTEM** > **Switch Setup** > **Switch Setup** screen.

Use a static VLAN to decide whether an incoming frame on a port should be

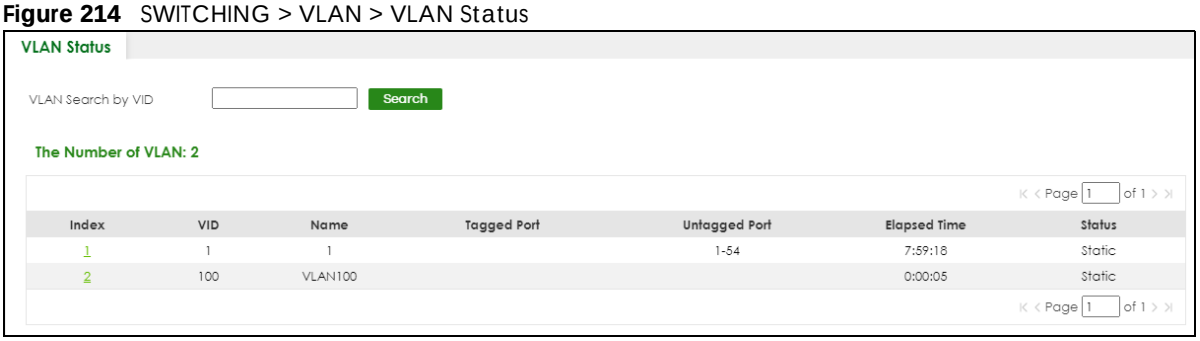
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

48.3 VLAN Status

Use this screen to view and search all VLAN groups. Click **SWITCHING** > **VLAN > VLAN Status** from the navigation panel to display the screen as shown next.

Figure 214 SWITCHING > VLAN > VLAN Status



The following table describes the labels in this screen.

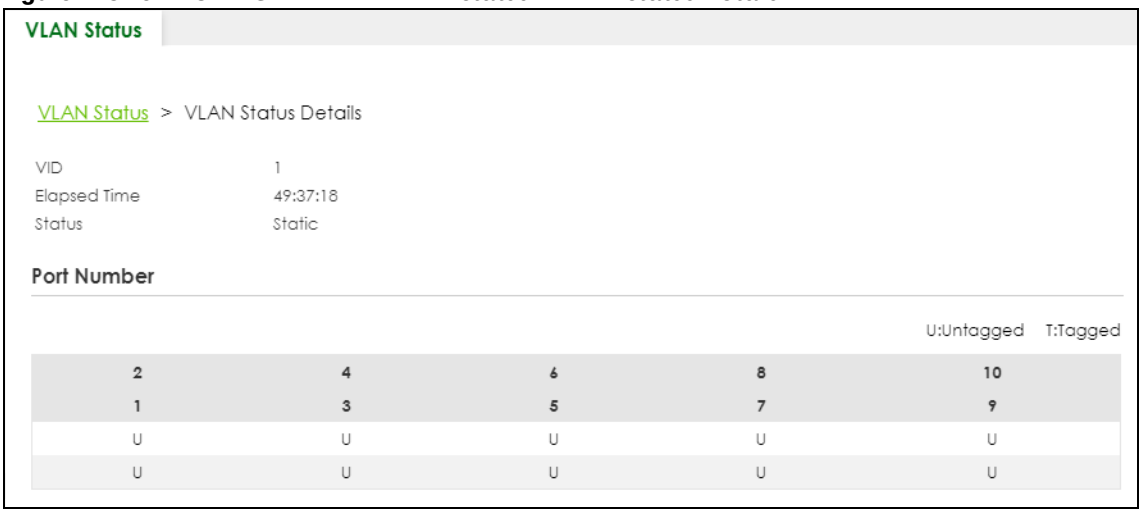
Table 156 SWITCHING > VLAN > VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter (an) existing VLAN ID numbers (use a comma (,) to separate individual VLANs or a hyphen (-) to indicate a range of VLANs. For example, “3,4” or “3-9”) and click **Search** to display only the specified VLANs in the list below. Leave this field blank and click **Search** to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the **Search** button to look for certain VLANs.
Index	This is the VLAN index number. Click an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the corresponding VLAN configuration screen.
Name	This fields shows the descriptive name of the VLAN.
Tagged Port	This field shows the tagged ports that are participating in the VLAN.
Untagged Port	This field shows the untagged ports that are participating in the VLAN.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. **Static**: added as a permanent entry.

48.3.1 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. Click an index number in the **VLAN Status** screen to display VLAN details.

Figure 215 SWITCHING > VLAN > VLAN Status > VLAN Status Details



The following table describes the labels in this screen.

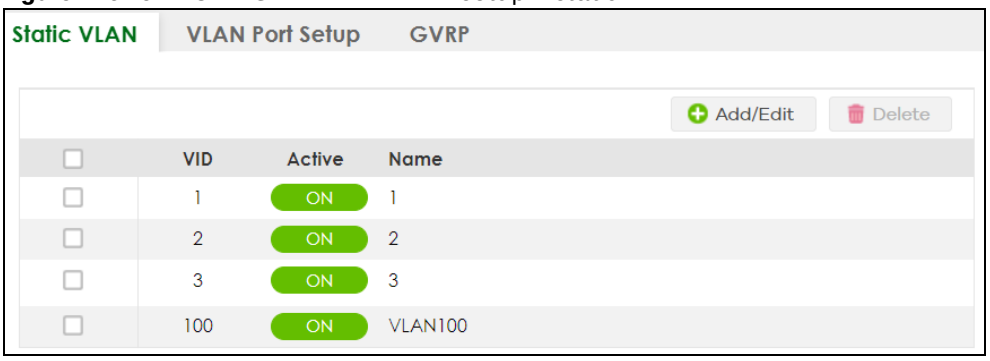
Table 157 SWITCHING > VLAN > VLAN Status > VLAN Status Details

LABEL	DESCRIPTION
VID	This is the VLAN identification number that was configured in the corresponding VLAN configuration screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. • **Dynamic**: using GVRP • **Static**: added as a permanent entry • **Voice**: manually added as a Voice VLAN • **MVR**: added through multicast VLAN registration • **MAC-based**: manually added as MAC-based VLAN
Port Number	This section displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".

48.4 Configure a Static VLAN

Use this screen to view and configure a static VLAN for the Switch. Click **SWITCHING** > **VLAN** > **VLAN Setup** > **Static VLAN** to display the screen as shown next.

Figure 216 SWITCHING > VLAN > VLAN Setup > Static VLAN



The following table describes the related labels in this screen.

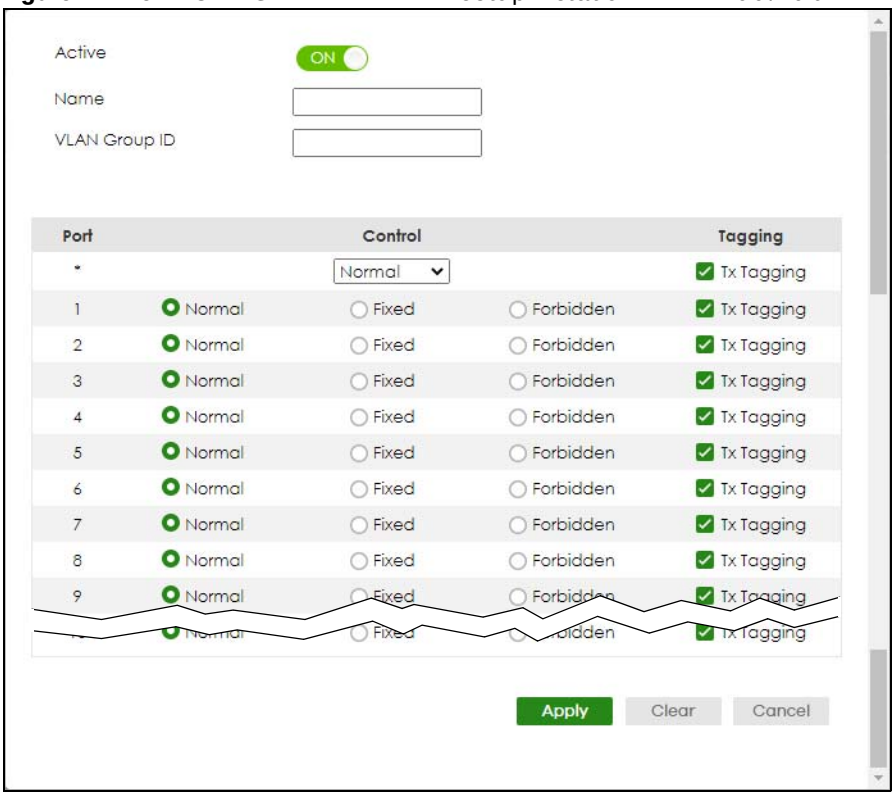
Table 158 SWITCHING > VLAN > VLAN Setup > Static VLAN

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group.
Active	This field indicates whether the VLAN settings are enabled or disabled.
Name	This field displays the descriptive name for this VLAN group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new static VLAN or edit a selected one.
Delete	Click **Delete** to remove the selected static VLAN.

48.4.1 Add/Edit a Static VLAN

Use this screen to configure a static VLAN for the Switch. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **VLAN** > **VLAN Setup** > **Static VLAN** screen to display this screen.

Figure 217 SWITCHING > VLAN > VLAN Setup > Static VLAN > Add/Edit



The following table describes the related labels in this screen.

Table 159 SWITCHING > VLAN > VLAN Setup > Static VLAN > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable ASCII characters. The string should not contain [?], [|], ['], ["], or [,].
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094. Note: Do NOT add a VLAN ID that has been used in the **SWITCHING** > **VLAN** > **Voice VLAN Setup**.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

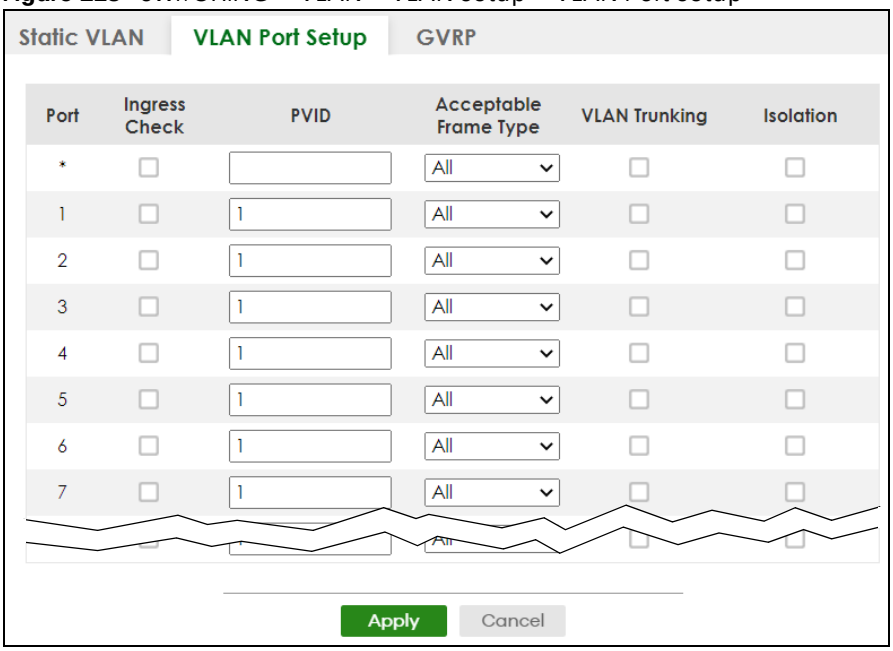
Table 159 SWITCHING > VLAN > VLAN Setup > Static VLAN > Add/Edit (continued)

LABEL	DESCRIPTION
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **Tx Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

48.5 VLAN Port Setup

Use this screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click **SWITCHING** > **VLAN** > **VLAN Setup** > **VLAN Port Setup** to display the screen as shown.

Figure 218 SWITCHING > VLAN > VLAN Setup > VLAN Port Setup



The following table describes the labels in this screen.

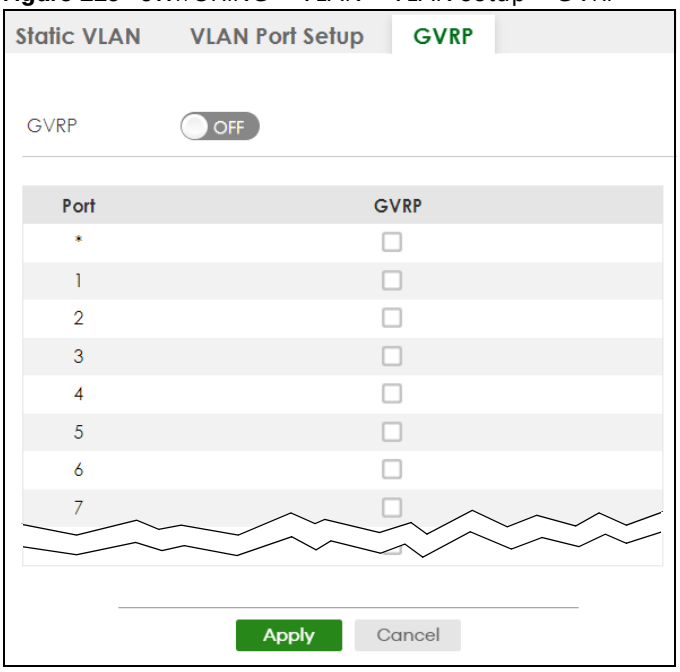
Table 160 SWITCHING > VLAN > VLAN Setup > VLAN Port Setup

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this checkbox is selected, the Switch discards incoming frames on a port for VLANs that do not include this port in its member set. Clear this checkbox to disable ingress filtering.
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. Enter a number between 1and 4094 as the port VLAN ID.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**. 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.
VLAN Trunking	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.
Isolation	Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is NOT enabled.
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.

48.6 Configure GVRP

Use this screen to configure GVRP settings on a port. Click **SWITCHING** > **VLAN** > **VLAN Setup** > **GVRP** to display the screen as shown.

Figure 219 SWITCHING > VLAN > VLAN Setup > GVRP



The following table describes the labels in this screen.

Table 161 SWITCHING > VLAN > VLAN Setup > GVRP

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable the switch button to permit VLAN groups beyond the local Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
GVRP	Select this checkbox to allow GVRP on this port.
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.

48.7 Subnet Based VLAN

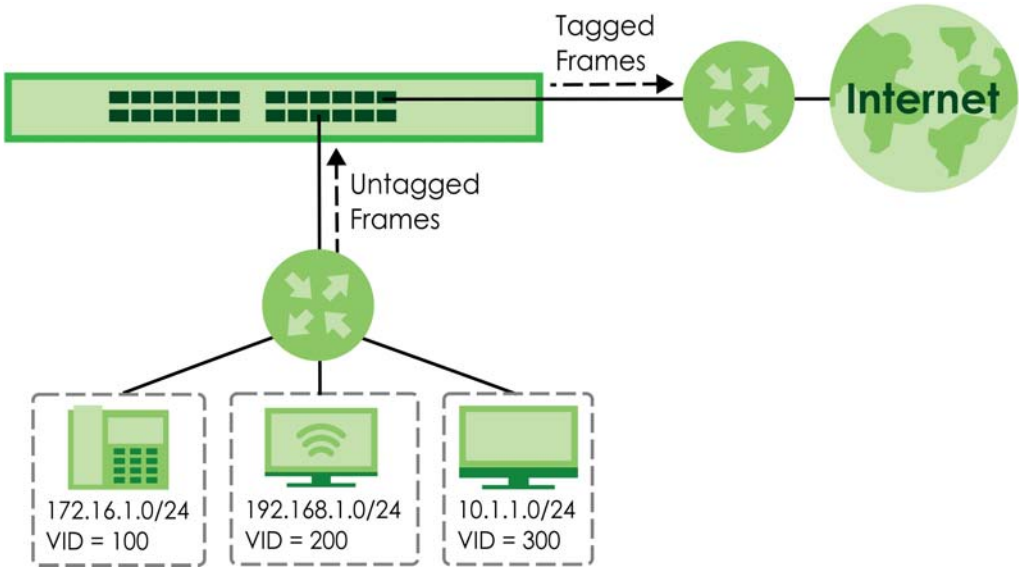
Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, an ISP (Internet Services Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data services). All **untagged** incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is video services receive the highest priority and data the lowest.

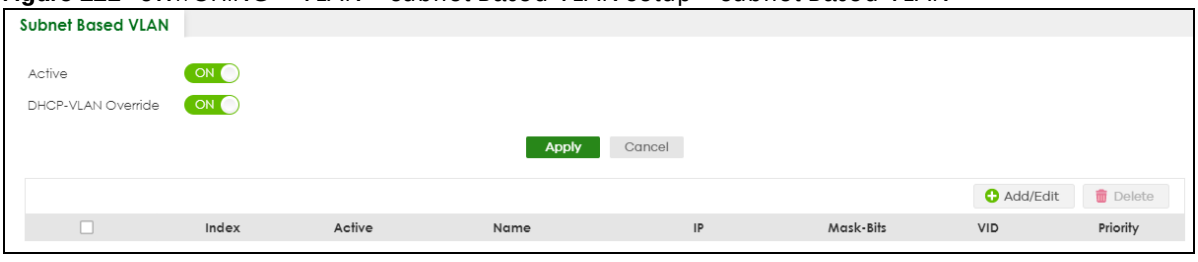
Figure 220 Subnet Based VLAN Application Example



48.8 Configuring Subnet Based VLAN

Click the **SWITCHING** > **VLAN** > **Subnet Based VLAN Setup** > **Subnet Based VLAN** link in the navigation panel to display the configuration screen as shown.

Figure 221 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN



The following table describes the labels in this screen.

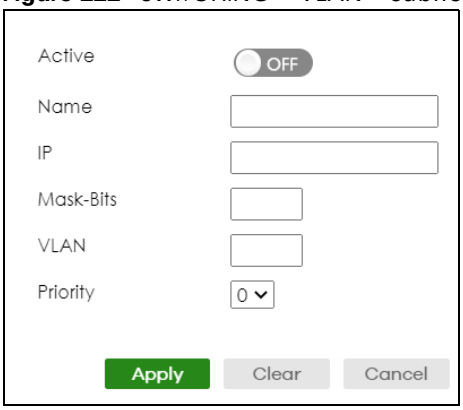
Table 162 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN

LABEL	DESCRIPTION
Active	Enable the switch button to activate this subnet based VLANs on the Switch.
DHCP-VLAN Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or through another DHCP server on the subnet based VLAN. Enable the switch button to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
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.
Index	This is the index number identifying this subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entry.

48.8.1 Add/Edit Subnet Based VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **VLAN** > **Subnet Based VLAN Setup** > **Subnet Based VLAN** screen to display this screen.

Figure 222 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN > Add/Edit



The following table describes the labels in this screen.

Table 163 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alphanumeric characters to identify this subnet based VLAN. The string should not contain [?], [|], ['], ["], or [,].
IP	Enter the IP address of the subnet for which you want to configure this subnet based VLAN.
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VLAN	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the **SWITCHING** > **VLAN** > **VLAN Setup** > **Static VLAN** screen.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

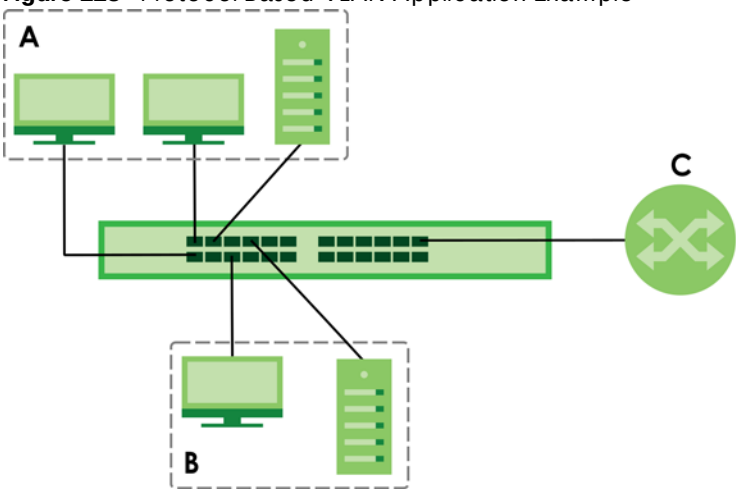
48.9 Protocol Based VLAN

Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the Switch checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

Note: Protocol-based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, port 1, 2, and 3 belong to static VLAN 100, and port 5, 6, and 7 belong to static VLAN 120. You configure a protocol based VLAN **A** with priority 3 for ARP traffic received on port 1, 2 and 3. You also have a protocol based VLAN **B** with priority 2 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic, when they go through the uplink port to a backbone switch **C**.

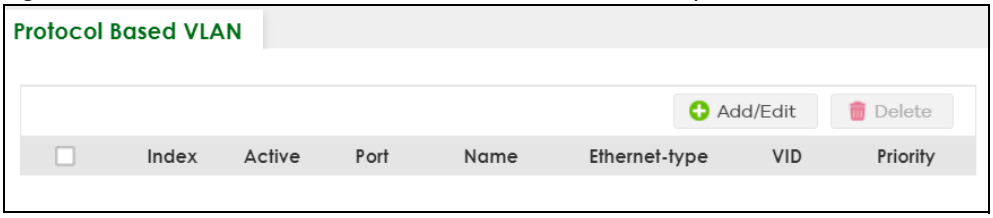
Figure 223 Protocol Based VLAN Application Example



48.10 Configuring Protocol Based VLAN

Click the **SWITCHING** > **VLAN** > **Protocol Based VLAN Setup** > **Protocol Based VLAN** link in the navigation panel to display the configuration screen as shown.

Figure 224 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN



The following table describes the labels in this screen.

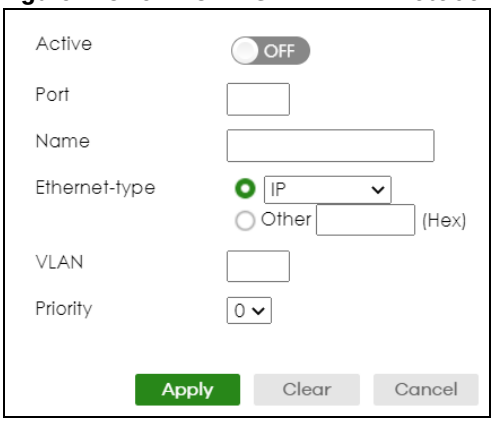
Table 164 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN

LABEL	DESCRIPTION
Index	This is the index number identifying this protocol based VLAN. Click any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name of the protocol based VLAN.
Ethernet-type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entry.

48.10.1 Add/Edit a Protocol Based VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **VLAN** > **Protocol Based VLAN Setup** > **Protocol Based VLAN** screen to display this configuration screen.

Figure 225 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN > Add/Edit



The following table describes the labels in this screen.

Table 165 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN Setup > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate this protocol based VLAN.
Port	Type a port to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN.
Name	Enter up to 32 alphanumeric characters to identify this protocol based VLAN. The string should not contain [?], [|], ['], ["], or [,].
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select **Other** and type the protocol number in hexadecimal notation. For example the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VLAN	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the **SWITCHING** > **VLAN** > **VLAN Setup** > **Static VLAN** screen.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

48.11 Voice VLAN

Voice VLAN is a VLAN that is specifically allocated for voice traffic. It ensures that the sound quality of an IP phone is preserved from deteriorating when the data traffic on the Switch ports is high. It groups the voice traffic with defined priority into an assigned VLAN which enables the separation of voice and data traffic coming onto the Switch port.

The Switch can determine whether a received packet is

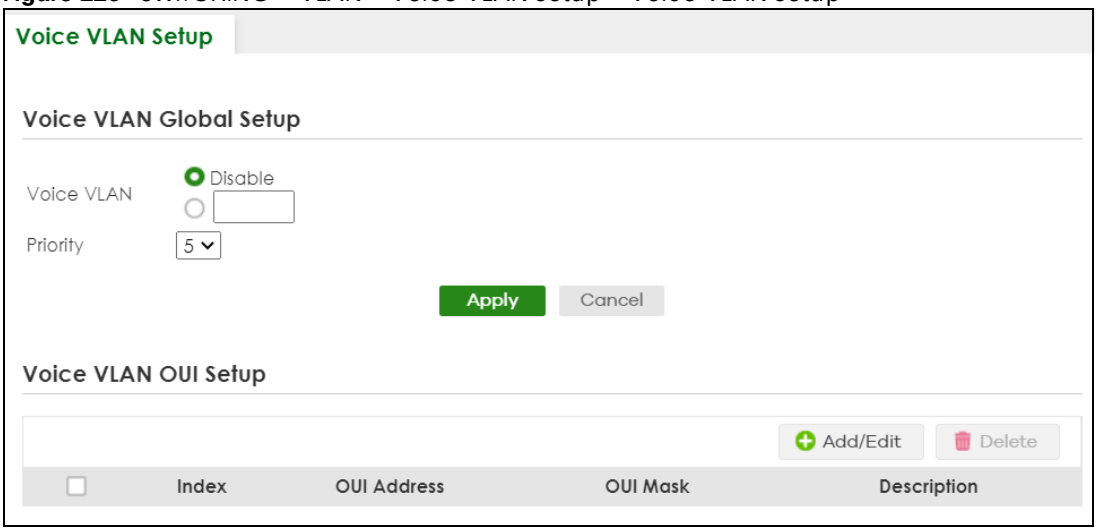
- an untagged voice packet when the incoming port is a fixed port for voice VLAN.
- a tagged voice packet when the incoming port and VLAN tag belongs to a voice VLAN.

It then checks the source packet's MAC address against an OUI list. If a match is found, the packet is considered as a voice packet.

You can set priority level to the Voice VLAN and add MAC address of IP phones from specific manufacturers by using its ID from the Organizationally Unique Identifiers (OUI).

Click **SWITCHING** > **VLAN** > **Voice VLAN Setup** > **Voice VLAN Setup** to display the configuration screen as shown.

Figure 226 SWITCHING > VLAN > Voice VLAN Setup > Voice VLAN Setup



The following table describes the fields in the above screen.

Table 166 SWITCHING > VLAN > Voice VLAN Setup > Voice VLAN Setup

LABEL	DESCRIPTION
Voice VLAN Global Setup	
Voice VLAN	Click the second radio button if you want to enable the Voice VLAN feature. Enter a VLAN ID number that is associated with the Voice VLAN. Click the **Disable** radio button if you do not want to enable the Voice VLAN feature.
Priority	Select the priority level of the voice traffic from 0 to 7. Default setting is 5. The higher the numeric value you assign, the higher the priority for this voice traffic.
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 section afresh.
Voice VLAN OUI Setup	
Index	This field displays the index number of the Voice VLAN.
OUI Address	This field displays the OUI address of the Voice VLAN.
OUI Mask	This field displays the OUI mask address of the Voice VLAN.
Description	This field displays the description of the Voice VLAN with OUI address.

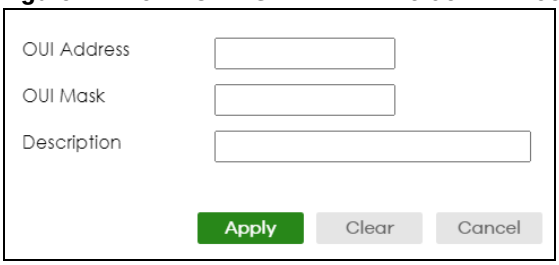
Table 166 SWITCHING > VLAN > Voice VLAN Setup > Voice VLAN Setup (continued)

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entry.

48.11.1 Add/Edit a Voice VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **VLAN** > **Voice VLAN Setup** > **Voice VLAN Setup** screen to display the configuration screen.

Figure 227 SWITCHING > VLAN > Voice VLAN Setup > Voice VLAN Setup > Add/Edit



The following table describes the fields in the above screen.

Table 167 SWITCHING > VLAN > Voice VLAN Setup > Voice VLAN Setup > Add/Edit

LABEL	DESCRIPTION
OUI Address	Enter the IP phone manufacturer's OUI MAC address. The first 3 bytes is the manufacturer identifier, the last 3 bytes is a unique station ID.
OUI Mask	Enter the mask for the specified IP phone manufacturer's OUI MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Description	Enter a description up to 32 printable ASCII characters except [?], [|], ['], or ["] for the Voice VLAN device. For example: Siemens.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

48.12 MAC Based VLAN

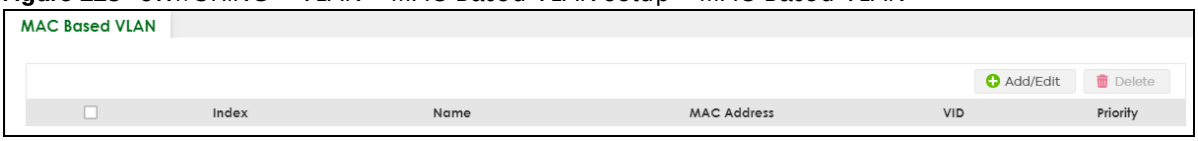
The MAC-based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. When untagged packets arrive at the Switch, the source MAC address of the packet is looked up in a MAC to VLAN mapping table. If an entry is found,

the corresponding VLAN ID is assigned to the packet. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped.

This feature allows users to change ports without having to reconfigure the VLAN. You can assign priority to the MAC-based VLAN and define a MAC to VLAN mapping table by entering a specified source MAC address in the MAC-based VLAN setup screen. You can also delete a MAC-based VLAN entry in the same screen.

Click **SWITCHING** > **VLAN** > **MAC Based VLAN Setup** > **MAC Based VLAN** to see the following screen.

Figure 228 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN



The following table describes the fields in the above screen.

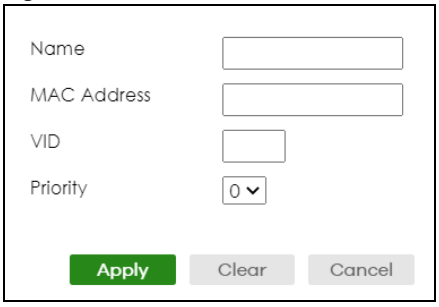
Table 168 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN

LABEL	DESCRIPTION
Index	This field displays the index number of the MAC-based VLAN entry.
Name	This field displays the name of the MAC-based VLAN entry.
MAC Address	This field displays the source MAC address that is bind to the MAC-based VLAN entry.
VID	This field displays the VLAN ID of the MAC-based VLAN entry.
Priority	This field displays the priority level which is assigned to frames belonging to this MAC-based VLAN entity.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entry.

48.12.1 Add/Edit a MAC Based VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **VLAN** > **MAC Based VLAN Setup** > **MAC Based VLAN** screen to see this screen.

Figure 229 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN > Add/Edit



The following table describes the fields in the above screen.

Table 169 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN > Add/Edit

LABEL	DESCRIPTION
Name	Enter a name up to 32 alphanumeric characters except [?], [|], ['], ["], or [,] for the MAC-based VLAN entry.
MAC Address	Enter a MAC address that is bind to the MAC-based VLAN entry. This is the source MAC address of the data packet that is looked up when untagged packets arrive at the Switch.
VID	Enter an ID (from 1 to 4094) for the VLAN that is associated with the MAC-based VLAN entry.
Priority	Enter a priority (0 to 7) that the Switch assigns to frames belonging to this VLAN. The higher the numeric value you assign, the higher the priority for this MAC-based VLAN entry.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

48.13 Vendor ID Based VLAN

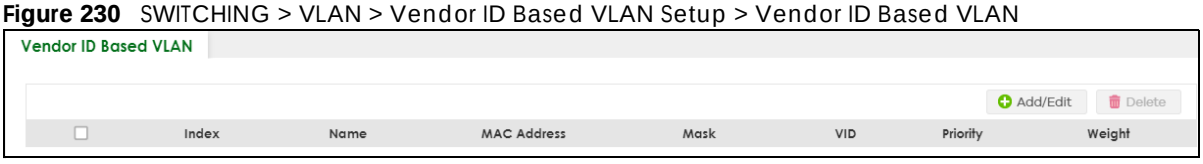
The Vendor ID based VLAN feature assigns incoming untagged packets to a VLAN and classifies the traffic based on the source MAC address of the packet. When untagged packets arrive at the switch, the source MAC address of the packet is looked up in a Vendor ID to VLAN mapping table. If an entry is found, the corresponding VLAN ID is assigned to the packet. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped.

This feature allows users to change ports without having to reconfigure the VLAN. You can assign a 802.1p priority to the vendor ID based VLAN and define a vendor ID to VLAN mapping table by entering a specified source MAC address and mask in the vendor ID based VLAN setup screen. You can also delete a vendor ID based VLAN entry in the same screen.

For every vendor ID based VLAN rule you set, you can specify a weight number to define the rule's priority level. As rules are processed one after the other, stating a priority order will let you choose which rule has to be applied first and which second.

Click the **SWITCHING** > **VLAN** > **Vendor ID Based VLAN Setup** > **Vendor ID Based VLAN** to see the following screen.

Figure 230 SWITCHING > VLAN > Vendor ID Based VLAN Setup > Vendor ID Based VLAN



The following table describes the fields in the above screen.

Table 170 SWITCHING > VLAN > Vendor ID Based VLAN Setup > Vendor ID Based VLAN

LABEL	DESCRIPTION
Index	This field displays the index number of the vendor ID based VLAN entry.
Name	This field displays the name of the vendor ID based VLAN entry.

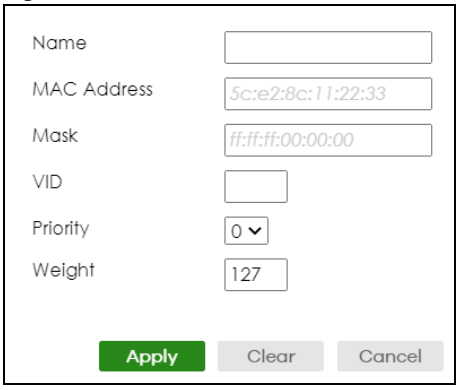
Table 170 SWITCHING > VLAN > Vendor ID Based VLAN Setup > Vendor ID Based VLAN (continued)

LABEL	DESCRIPTION
MAC Address	This field displays the source MAC address that is bind to the vendor ID based VLAN entry.
Mask	This field displays the mask for the source MAC address that is bind to the vendor ID based VLAN entry.
VID	This field displays the VLAN ID of the vendor ID based VLAN entry.
Priority	This field displays the priority level which is assigned to frames belonging to this vendor ID based VLAN.
Weight	This field displays the weight of the vendor ID based VLAN entry.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entry.

48.13.1 Add/Edit a Vendor ID Based VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **VLAN** > **Vendor ID Based VLAN** > **Vendor ID Based VLAN Setup** to see this screen.

Figure 231 SWITCHING > VLAN > Vendor ID Based VLAN Setup > Vendor ID Based VLAN > Add/Edit



The following table describes the fields in the above screen.

Table 171 SWITCHING > VLAN > Vendor ID Based VLAN Setup > Vendor ID Based VLAN > Add/Edit

LABEL	DESCRIPTION
Name	Enter a name up to 32 alphanumeric characters except [?], [|], ['], or ["] for the vendor ID based VLAN entry.
MAC Address	Enter a MAC address that is bind to the vendor ID-based VLAN entry. This is the source MAC address of the data packet that is looked up when untagged packets arrive at the Switch.
Mask	Enter the mask for the specified source MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
VID	Enter an ID (from 1 to 4094) for the VLAN that is associated with the vendor ID based VLAN entry.

Table 171 SWITCHING > VLAN > Vendor ID Based VLAN Setup > Vendor ID Based VLAN > Add/Edit

LABEL	DESCRIPTION
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN. The higher the numeric value you assign, the higher the priority for this vendor ID based VLAN entry.
Weight	Enter a number between 0 and 255 to specify the rule's weight. This is to decide the priority in which the rule is applied. The higher the number, the higher the rule's priority.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

48.14 Port-Based VLAN Setup

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.

Note: When you activate port-based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.

Note: In screens (such as **SYSTEM** > **IP Setup** > **IP Setup** and **SWITCHING** > **Static MAC Filtering** > **Static MAC Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

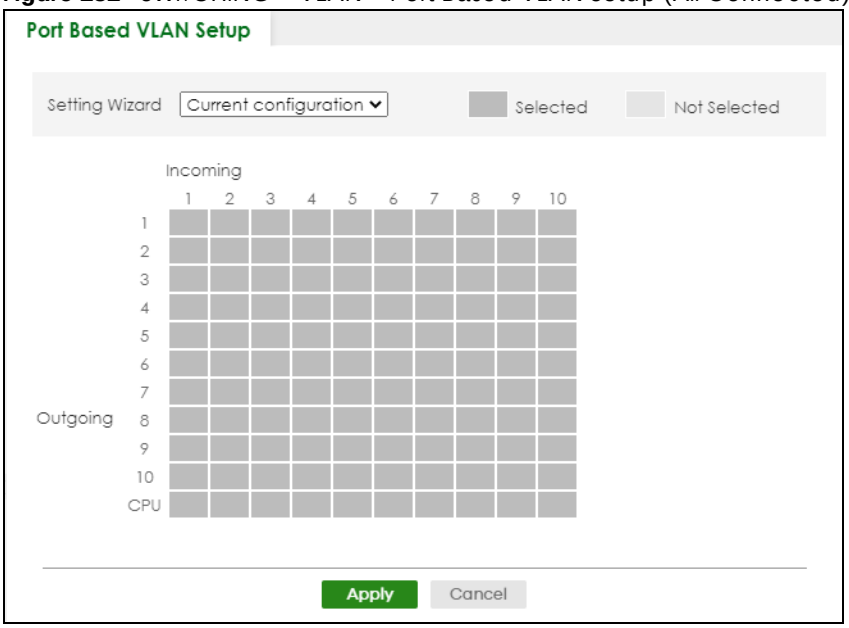
48.15 Configure a Port-Based VLAN

Select **Port Based** as the VLAN Type in the **SYSTEM** > **Switch Setup** > **Switch Setup** screen and then click **SWITCHING** > **VLAN** from the navigation panel to display the next screen.

Select either **All Connected** or **Port Isolated** from the drop-down list depending on your VLAN and VLAN security requirements. If VLAN members need to communicate directly with each other, then select **All Connected**. Select **Port Isolated** if you want to restrict users from communicating directly. Click **Apply** to save your settings.

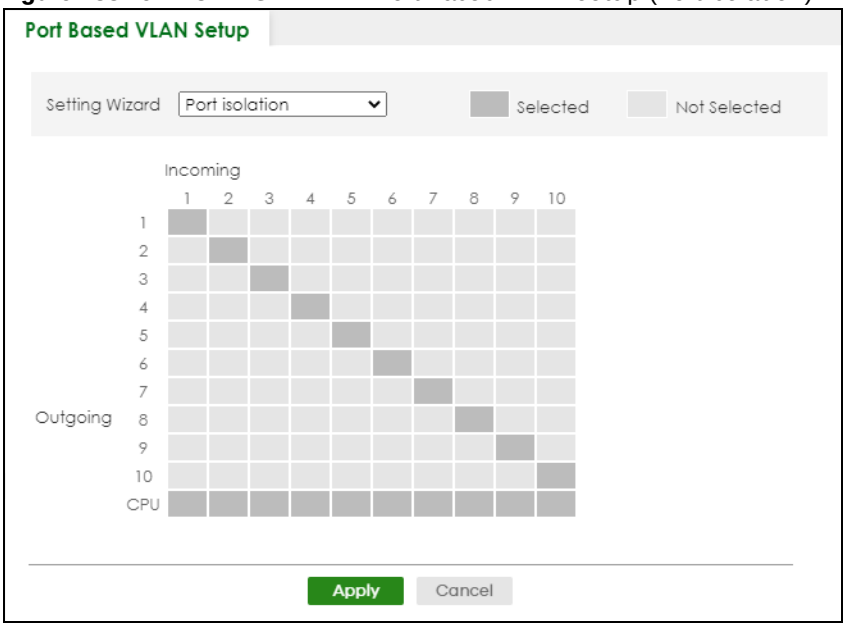
The following screen shows users on a port-based, all-connected VLAN configuration.

Figure 232 SWITCHING > VLAN > Port Based VLAN Setup (All Connected)



The following screen shows users on a port-based, port-isolated VLAN configuration.

Figure 233 SWITCHING > VLAN: Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 172 SWITCHING > VLAN > Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose **Current configuration** to display the Switch's current port-based VLAN configuration. Choose **All connected** or **Port isolation** wizard to quickly set up a port-based VLAN according to the below descriptions. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. After selecting the setting wizard, you can customize the port settings. Click on the ports to add or delete incoming or outgoing ports. The configuration will be saved only after you click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
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.

48.16 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

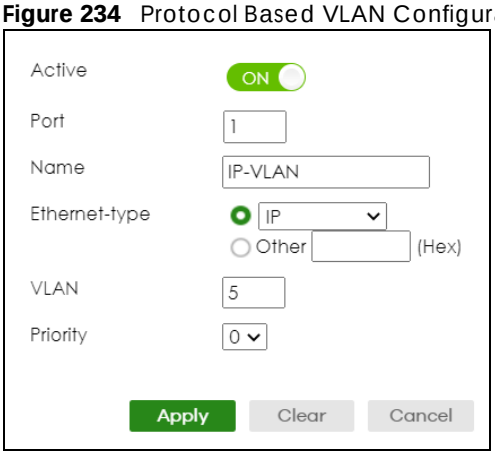
48.16.1 Create an IP-based VLAN Example

This example shows you how to create an IP VLAN which includes ports 1, 4 and 8. Follow these steps:

1. Activate this protocol based VLAN.
2. Type the port number you want to include in this protocol based VLAN. Type **1**.
3. Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.
4. Select the protocol. Leave the default value **IP**.
5. Type the VLAN ID of an existing VLAN. In our example we created a static VLAN with an ID of 5. Type **5**.

6 Leave the priority set to **0** and click **Apply**.

Figure 234 Protocol Based VLAN Configuration Example



To add more ports to this protocol based VLAN.

1 Select the protocol based VLAN entry. Click **Add/Edit**.

2 Change the value in the **Port** field to the next port you want to add.

3 Click **Apply**.

CHAPTER 49
VLAN Isolation

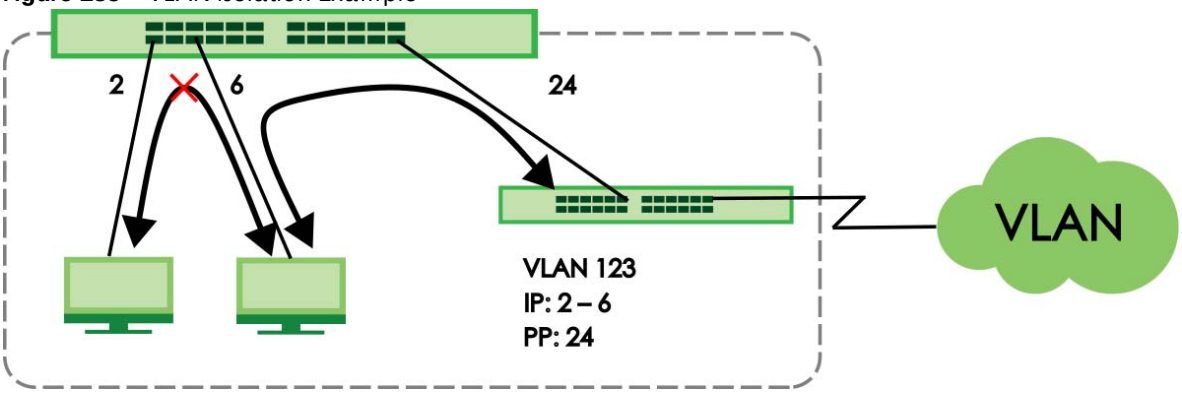
This chapter shows you how to configure the Switch to prevent communications between ports in a VLAN.

49.1 VLAN Isolation Overview

VLAN Isolation allows you to do port isolation within a VLAN in a simple way. You specify which ports in a VLAN (**VLAN 123**) is not isolated by adding it to the promiscuous port (**PP**) list. The Switch automatically adds other ports in this VLAN (**VLAN 123**) to the isolated port (**IP**) list and blocks traffic between the isolated ports (**IP**). A promiscuous port (**PP**) can communicate with any port in the same VLAN (**VLAN 123**). An isolated port (**IP**) can communicate with the promiscuous ports (**PP**) only.

Note: You can have up to one VLAN Isolation rule for each VLAN.

Figure 235 VLAN Isolation Example



Note: Make sure you keep at least one port in the promiscuous port list for a VLAN with VLAN Isolation enabled. Otherwise, this VLAN is blocked from the whole network.

49.2 Configuring VLAN Isolation

Click **SWITCHING** > **VLAN Isolation** > **VLAN Isolation** in the navigation panel to display the screen as shown.

Figure 236 SWITCHING > VLAN Isolation > VLAN Isolation

The following table describes the labels in this screen.

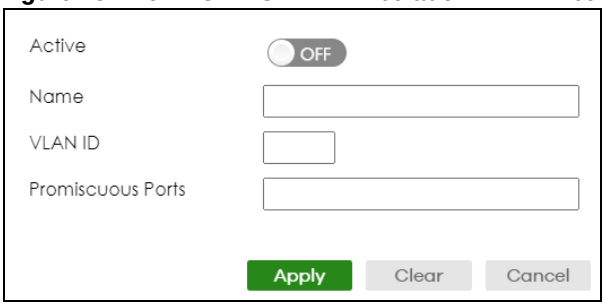
Table 173 SWITCHING > VLAN Isolation > VLAN Isolation

LABEL	DESCRIPTION
Index	This is the index number of the rule.
Active	This shows whether this rule is activated or not.
Name	This is the descriptive name for this rule.
VLAN ID	This is the VLAN to which this rule is applied.
Promiscuous Ports	This shows the ports that can communicate with any ports in the same VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

49.2.1 Add/Edit a VLAN Isolation Rule

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING** > **VLAN Isolation** > **VLAN Isolation** screen to display this screen.

Figure 237 SWITCHING > VLAN Isolation > VLAN Isolation > Add/Edit



The following table describes the labels in this screen.

Table 174 SWITCHING > VLAN Isolation > VLAN Isolation > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to enable VLAN Isolation in a VLAN.
Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [|], ['], ["], or [,]) for identification purposes.
VLAN ID	Enter a VLAN ID from 1 to 4094. This is the VLAN to which this rule applies.
Promiscuous Ports	Enter the number of the ports that can communicate with any ports in the same VLAN. Other ports belonging to this VLAN will be added to the isolation list and can only send and receive traffic from the ports you specify here.

Table 174 SWITCHING > VLAN Isolation > VLAN Isolation > Add/Edit (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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 50
NETWORKING

The following chapters introduces the configurations of the links under the **NETWORKING** navigation panel.

Quick links to chapters:

CHAPTER 51
ARP Setup

51.1 ARP Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

51.1.1 What You Can Do

Use the **ARP Learning** screen (Section 51.2 on page 329) to configure ARP learning mode on a per-port basis.

51.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

51.1.2.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

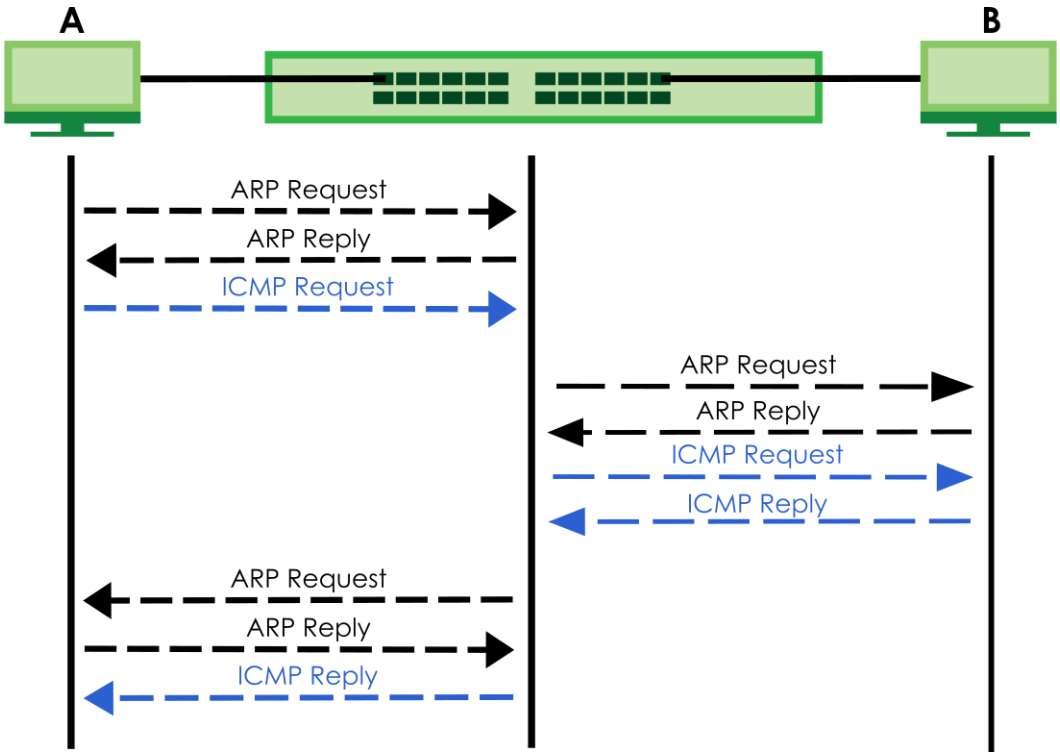
51.1.2.2 ARP Learning Mode

The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

ARP-Reply

The Switch in ARP-Reply learning mode updates the ARP table only with the ARP replies to the ARP requests sent by the Switch. This can help prevent ARP spoofing.

In the following example, the Switch does not have IP address and MAC address mapping information for hosts **A** and **B** in its ARP table, and host **A** wants to ping host **B**. Host **A** sends an ARP request to the Switch and then sends an ICMP request after getting the ARP reply from the Switch. The Switch finds no matched entry for host **B** in the ARP table and broadcasts the ARP request to all the devices on the LAN. When the Switch receives the ARP reply from host **B**, it updates its ARP table and also forwards host **A**'s ICMP request to host **B**. After the Switch gets the ICMP reply from host **B**, it sends out an ARP request to get host **A**'s MAC address and updates the ARP table with host **A**'s ARP reply. The Switch then can forward host **B**'s ICMP reply to host **A**.



Gratuitous-ARP

A gratuitous ARP is an ARP request in which both the source and destination IP address fields are set to the IP address of the device that sends this request and the destination MAC address field is set to the broadcast address. There will be no reply to a gratuitous ARP request.

A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

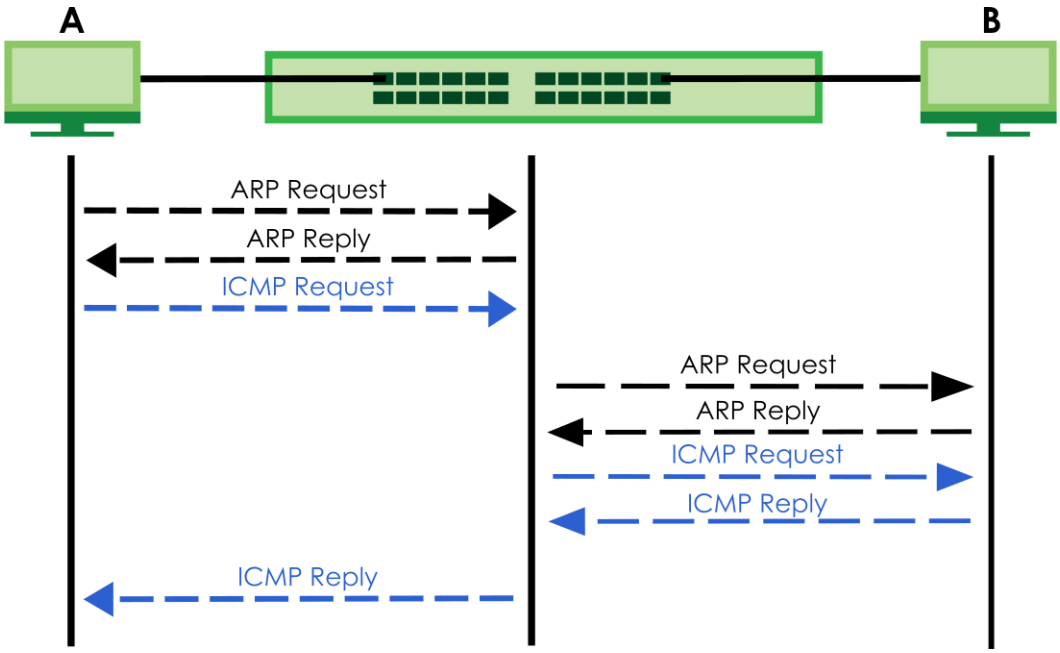
In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

ARP-Request

When the Switch is in ARP-Request learning mode, it updates the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.

Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC

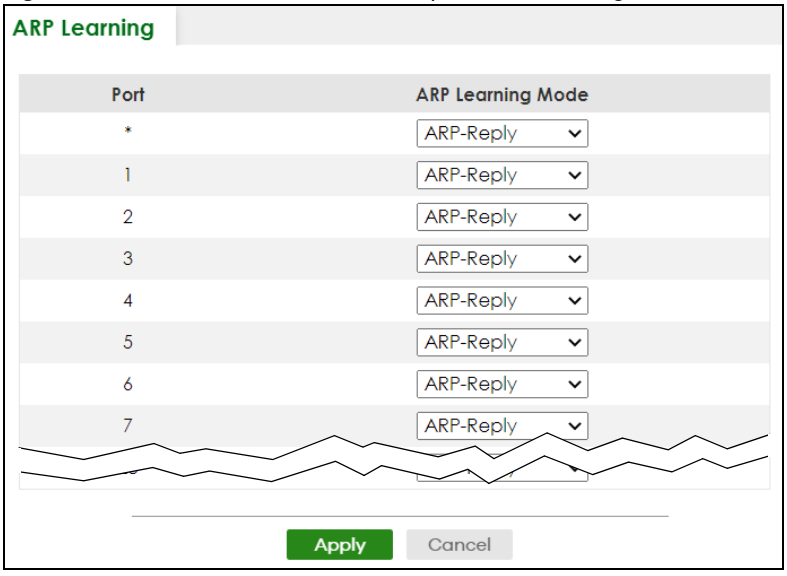
address and ICMP reply.



51.2 ARP Learning

Use this screen to configure each port's ARP learning mode. Click **NETWORKING** > **ARP Setup** > **ARP Learning** > **ARP Learning** in the navigation panel to display the screen as shown next.

Figure 238 NETWORKING > ARP Setup > ARP Learning > ARP Learning



The following table describes the labels in this screen.

Table 175 NETWORKING > ARP Setup > ARP Learning > ARP Learning

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select **ARP-Reply** to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select **Gratuitous-ARP** to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select **ARP-Request** to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.
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.

CHAPTER 52 DHCP

52.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. If you configure the Switch as a DHCP relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you do not configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

52.1.1 What You Can Do

- Use the **DHCPv4 Relay Status** screen (Section 52.2 on page 332) to display the relay mode and status.
- Use the **DHCPv4 Option 82 Profile** screen (Section 52.4 on page 333) to create DHCPv4 option 82 profiles.
- Use the **DHCPv4 Smart Relay** screen (Section 52.5 on page 335) to configure global DHCPv4 relay. You can also use this screen to apply different DHCP option 82 profile to certain ports on the Switch.
- Use the **DHCPv4 Relay VLAN Setting** screen (Section 52.6 on page 338) to configure your DHCPv4 settings based on the VLAN domain of the DHCPv4 clients. You can also use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN.
- Use the **DHCPv6 Relay** screen (Section 52.7 on page 341) to enable and configure DHCPv6 relay.

52.1.2 What You Need to Know

Read on for concepts on DHCP that can help you configure the screens in this chapter.

DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

DHCPv4 Configuration Options

The DHCPv4 configuration on the Switch is divided into **Smart Relay** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

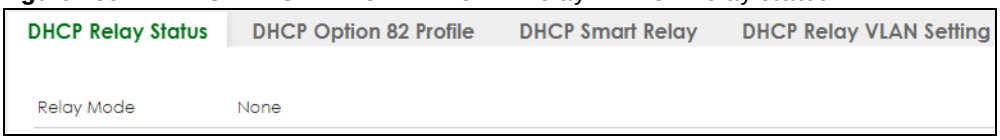
- **Smart Relay** – The Switch forwards all DHCP requests to the same DHCP server.

- **VLAN** – The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

52.2 DHCPv4 Relay Status

Click **NETWORKING** > **DHCP** > **DHCPv4 Relay** in the navigation panel. The **DHCP Relay Status** screen displays.

Figure 239 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay Status



The following table describes the labels in this screen.

Table 176 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay Status

LABEL	DESCRIPTION
Relay Mode	This field displays: **None** – if the Switch is not configured as a DHCP relay agent. **Smart**– if the Switch is configured as a DHCP relay agent only. **VLAN** – followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLANs.

52.3 DHCPv4 Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

52.3.1 DHCPv4 Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **SYSTEM** > **General Setup**.

The following describes the DHCP relay agent information that the Switch sends to the DHCP server:

Table 177 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in **SYSTEM** > **General Setup**.

52.3.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 178 DHCP Relay Agent Information Option Format

Code (82)	Length (N)	i1	i2	...	iN

i1, i2 and iN are DHCP relay agent sub-options, which contain additional information about the DHCP client. You need to define at least one sub-option.

52.3.1.2 Sub-Option Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 179 DHCP Relay Agent Circuit ID Sub-option Format

SubOpt Code	Length	Value
1 (1 byte)	N (1 byte)	Slot ID, Port ID, VLAN ID, System Name or String

Table 180 DHCP Relay Agent Remote ID Sub-option Format

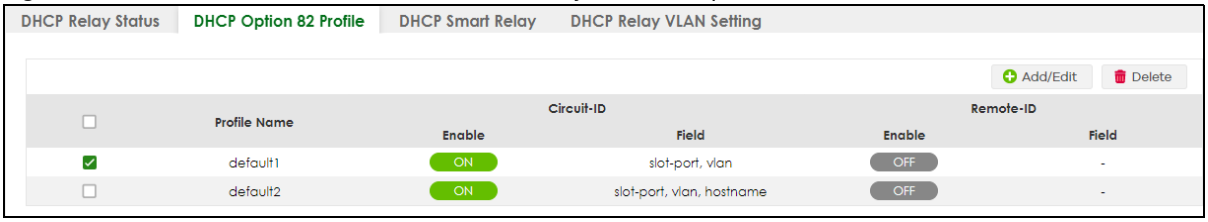
SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	MAC Address or String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and two identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

52.4 DHCPv4 Option 82 Profile

Use this screen to view and configure DHCPv4 option 82 profiles. Click **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Option 82 Profile** link to display the screen as shown.

Figure 240 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile



The following table describes the labels in this screen.

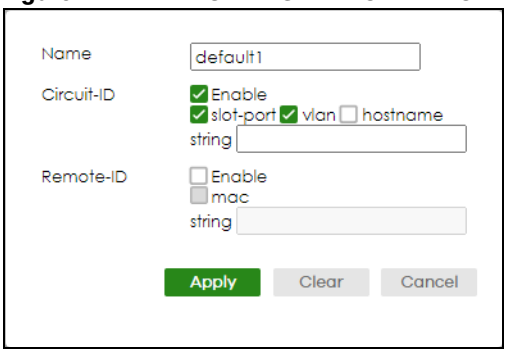
Table 181 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile

LABEL	DESCRIPTION
Profile Name	This field displays the descriptive name of the profile.
Circuit-ID	This section displays the Circuit ID sub-option including information that is specific to the relay agent (the Switch).
Enable	This field displays whether the Circuit ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Circuit ID sub-option.
Remote-ID	This section displays the Remote ID sub-option including information that identifies the relay agent (the Switch).
Enable	This field displays whether the Remote ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Remote ID sub-option.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

52.4.1 Add/Edit a DHCPv4 Option 82 Profile

Use this screen to create DHCPv4 option 82 profiles. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Option 82 Profile** link to display this screen.

Figure 241 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile > Add/Edit



Note: The string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

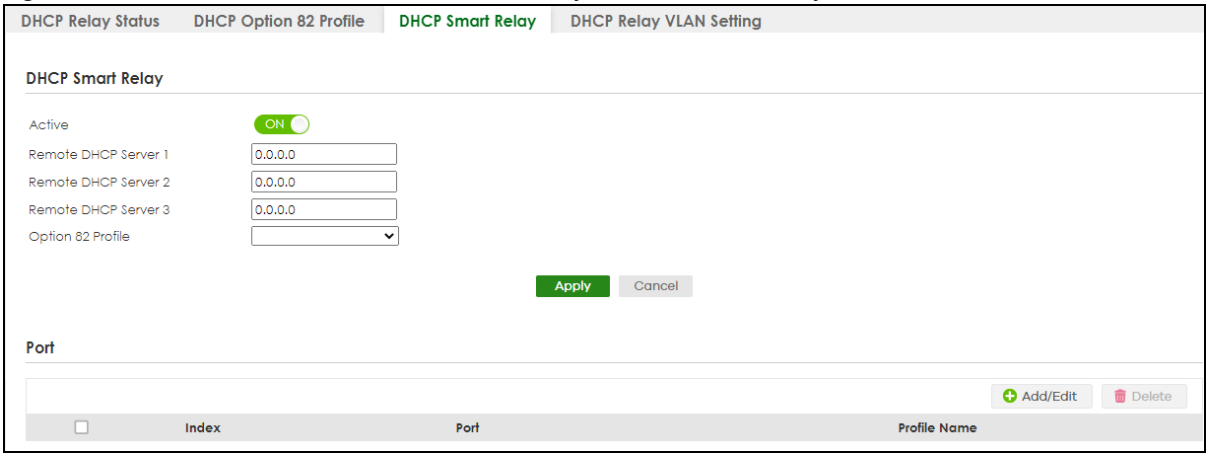
Table 182 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile > Add/Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for the profile for identification purposes. You can use up to 32 printable ASCII characters.
Circuit-ID	Use this section to configure the Circuit ID sub-option to include information that is specific to the relay agent (the Switch).
Enable	Select this option to have the Switch add the Circuit ID sub-option to client DHCP requests that it relays to a DHCP server.
slot-port	Select this option to have the Switch add the number of port that the DHCP client is connected to.
vlan	Select this option to have the Switch add the ID of VLAN which the port belongs to.
hostname	This is the system name you configure in the **SYSTEM** > **General Setup** > **General Setup** screen. Select this option for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 printable ASCII characters that the Switch adds into the client DHCP requests.
Remote-ID	Use this section to configure the Remote ID sub-option to include information that identifies the relay agent (the Switch).
Enable	Select this option to have the Switch append the Remote ID sub-option to the option 82 field of DHCP requests.
mac	Select this option to have the Switch add its MAC address to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 printable ASCII characters for the remote ID information in this field.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

52.5 Configure a DHCPv4 Smart Relay

Use this screen to configure global DHCPv4 relay. Click **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Smart Relay** to display the screen as shown.

Figure 242 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay



The following table describes the labels in this screen.

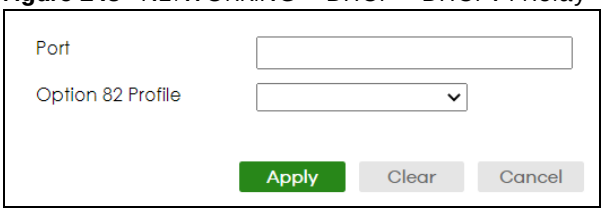
Table 183 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay

LABEL	DESCRIPTION
DHCP Smart Relay	
Active	Select this checkbox to enable DHCPv4 relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCPv4 server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
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.
Port Use this section to apply a different DHCP option 82 profile to certain ports on the Switch.	
Index	This field displays a sequential number for each entry.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

52.5.1 Add/Edit DHCPv4 Global Relay Port

Use this screen to apply a different DHCP option 82 profile to certain ports on the Switch. To open this screen, Click **Add/Edit**, or select an entry and click **Add/Edit** in the **Port** section of the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Smart Relay** screen.

Figure 243 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay > Add/Edit



The following table describes the labels in this screen.

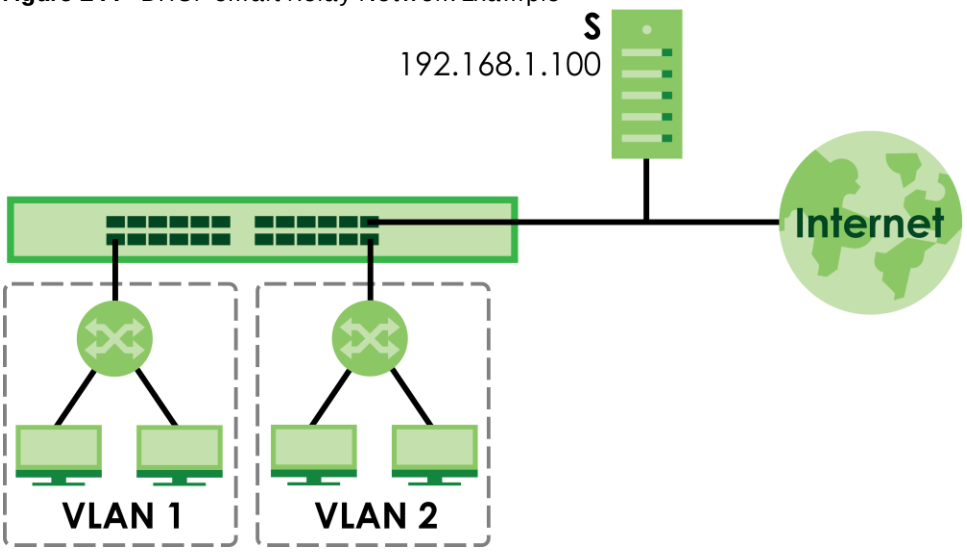
Table 184 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay > Add/Edit

LABEL	DESCRIPTION
Port	Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter “3-5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCPv4 Smart Relay** screen.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

52.5.2 DHCP Smart Relay Configuration Example

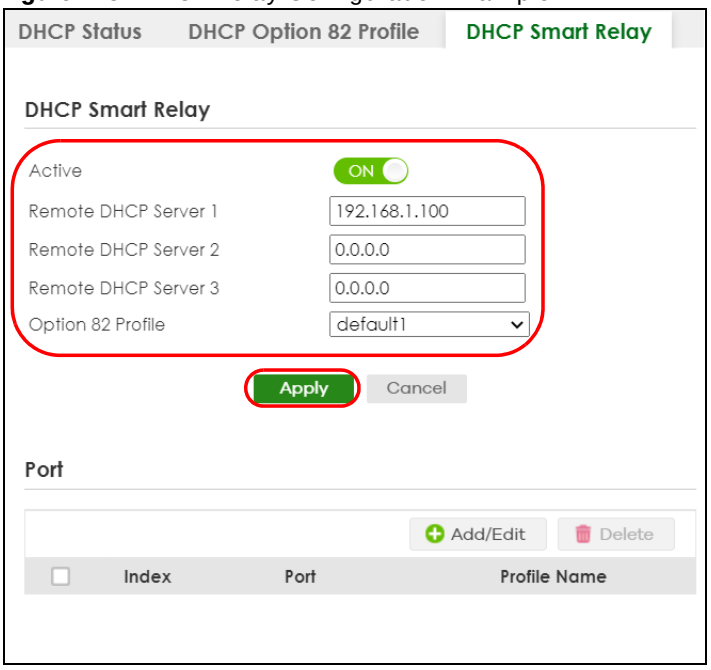
The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server (**S**) that services the DHCP clients in both domains.

Figure 244 DHCP Smart Relay Network Example



Configure the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Smart Relay** screen as shown. Make sure you select a DHCP option 82 profile (**default1** in this example) to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID. Click **Apply** after you finish the configuration.

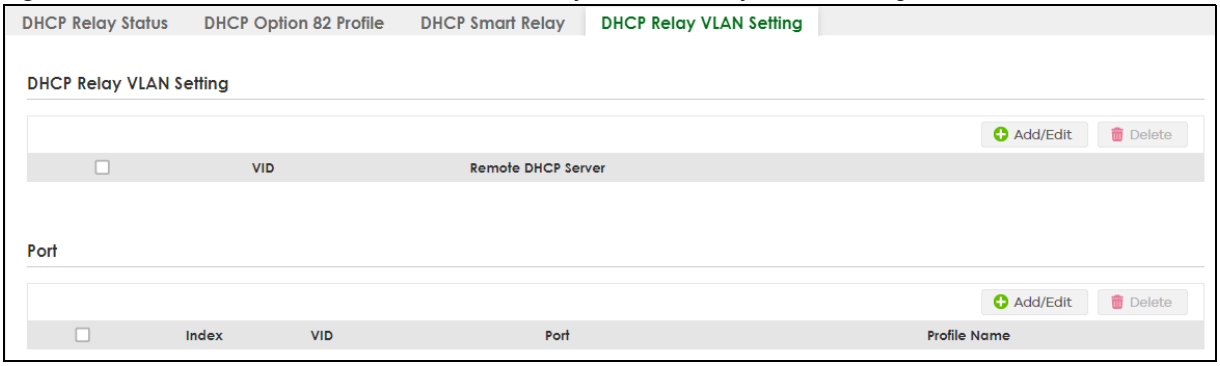
Figure 245 DHCP Relay Configuration Example



52.6 DHCPv4 VLAN Setting

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Relay VLAN Setting** to display the screen as shown.

Figure 246 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting



The following table describes the labels in this screen.

Table 185 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting

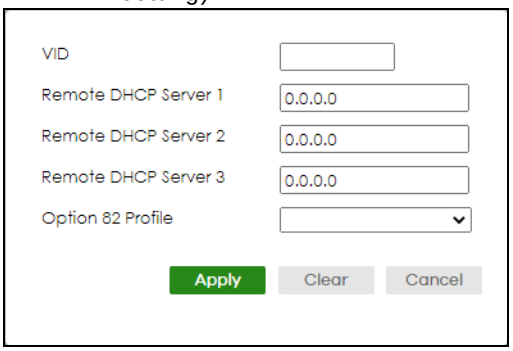
LABEL	DESCRIPTION
DHCP Relay VLAN Setting	
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Remote DHCP Server	This displays the IP address of a DHCP server in dotted decimal notation.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.
Port Use this section to apply a different DHCP option 82 profile to certain ports in a VLAN.	
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the ports belongs.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports in this VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

52.6.1 Add/Edit DHCPv4 VLAN Setting

Use this screen to add/edit your DHCP settings based on the VLAN domain of the DHCP clients. Click the **Add/Edit** button in the **DHCP Relay VLAN Setting** section of the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Relay VLAN Setting** screen to access this screen.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch.

Figure 247 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (DHCP Relay VLAN Setting)



The following table describes the labels in this screen.

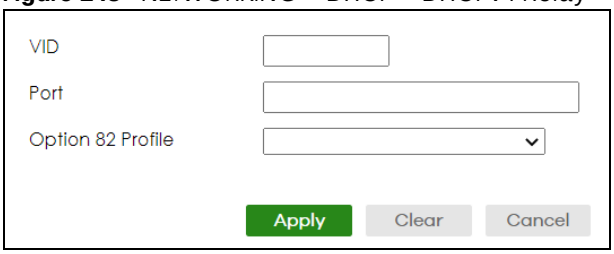
Table 186 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (DHCP Relay VLAN Setting)

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

52.6.2 Add/Edit DHCPv4 VLAN Port

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. Click the **Add/Edit** button in the **Port** section of the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Relay VLAN Setting** screen to access this screen.

Figure 248 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (Port)



The following table describes the labels in this screen.

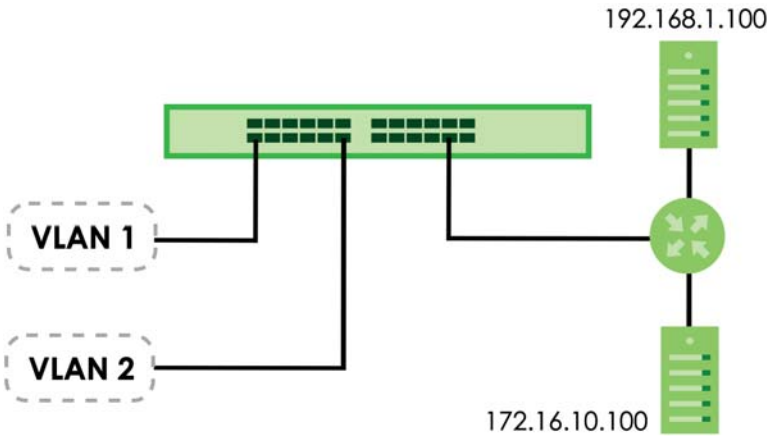
Table 187 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (Port)

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Relay VLAN Setting** (the **DHCP Relay VLAN Setting** section)> **Add/Edit** screen.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

52.6.3 Example: DHCP Relay for Two VLANs

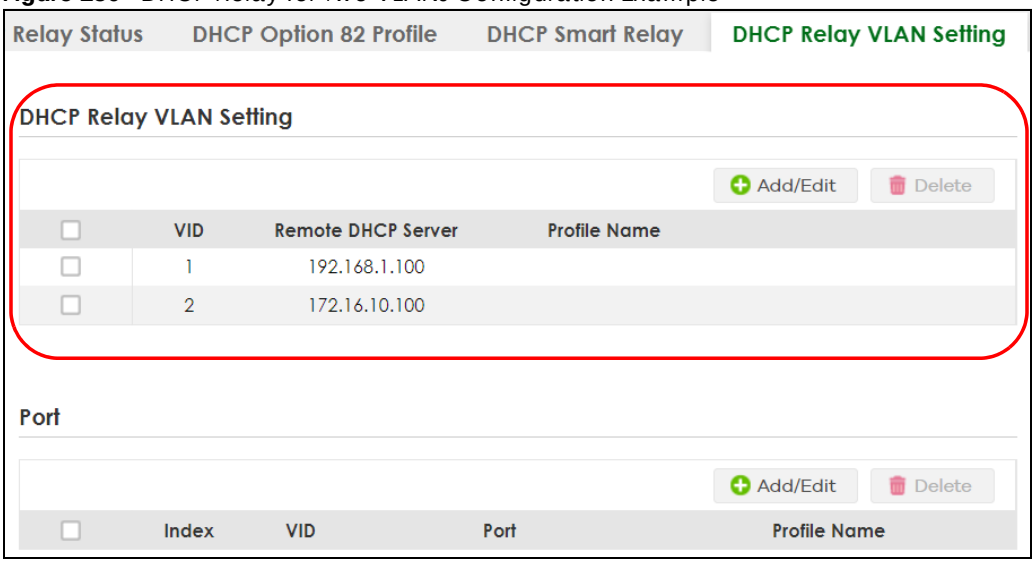
The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (**VLAN 1**) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (**VLAN 2**) are sent to the other DHCP server with an IP address of 172.16.10.100.

Figure 249 DHCP Relay for Two VLANs



For the example network, add two entries in **DHCP Relay VLAN Setting** section of the **NETWORKING** > **DHCP** > **DHCPv4 Relay** > **DHCP Relay VLAN Setting** screen as shown.

Figure 250 DHCP Relay for Two VLANs Configuration Example



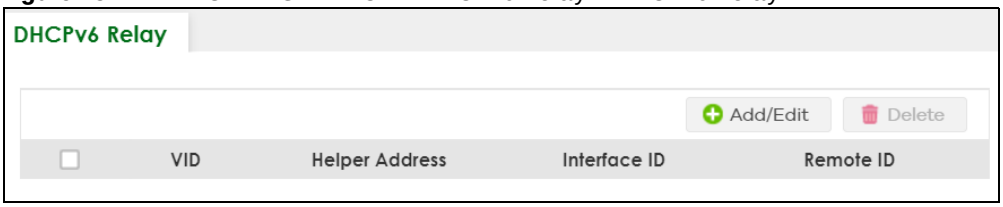
52.7 DHCPv6 Relay

A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCPv6 server on its network, it then needs a DHCPv6 relay agent to send a message to a DHCPv6 server that is not attached to the same network.

The DHCPv6 relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCPv6 server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Use this screen to view and configure DHCPv6 relay settings for a specific VLAN on the Switch. Click **NETWORKING** > **DHCP** > **DHCPv6 Relay** > **DHCPv6 Relay** in the navigation panel to display the screen as shown.

Figure 251 NETWORKING > DHCP > DHCPv6 Relay > DHCPv6 Relay



The following table describes the labels in this screen.

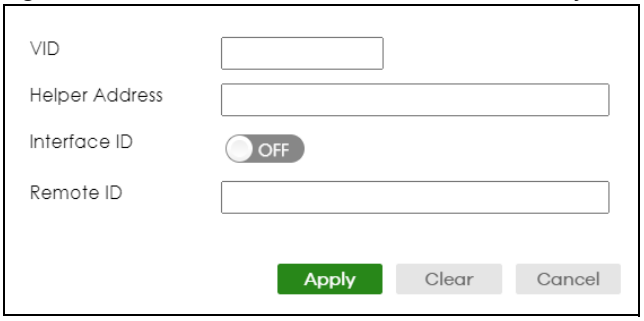
Table 188 NETWORKING > DHCP > DHCPv6 Relay > DHCPv6 Relay

LABEL	DESCRIPTION
VID	This field displays the VLAN ID number.
Helper Address	This field displays the IPv6 address of the remote DHCPv6 server for this VLAN.
Interface ID	This field displays whether the interface-ID option is added to DHCPv6 requests from clients in this VLAN.
Remote ID	This field displays whether the remote-ID option is added to DHCPv6 requests from clients in this VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

52.7.1 Add/Edit DHCPv6 Relay

Use this screen to add/edit DHCPv6 relay settings for a specific VLAN on the Switch. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **NETWORKING** > **DHCP** > **DHCPv6 Relay** > **DHCPv6 Relay** screen to display this screen.

Figure 252 NETWORKING > DHCP > DHCPv6 Relay > DHCPv6 Relay > Add/Edit



The following table describes the labels in this screen.

Table 189 NETWORKING > DHCP > DHCPv6 Relay > DHCPv6 Relay > Add/Edit

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Helper Address	Enter the remote DHCPv6 server address for the specified VLAN.
Interface ID	Enable the switch button to have the Switch add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Remote ID	Enter a string of up to 64 printable ASCII characters (except [?], [|], ['], ["], or [,]) to be carried in the remote-ID option. The Switch adds the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 53
Static Route

53.1 Static Routing Overview

This chapter shows you how to configure static routes.

IP static routes are used by layer-2 Switches to ensure they can respond to management stations not reachable through the default gateway and to proactively send traffic, for example when sending SNMP traps or conducting IP connectivity tests using ping.

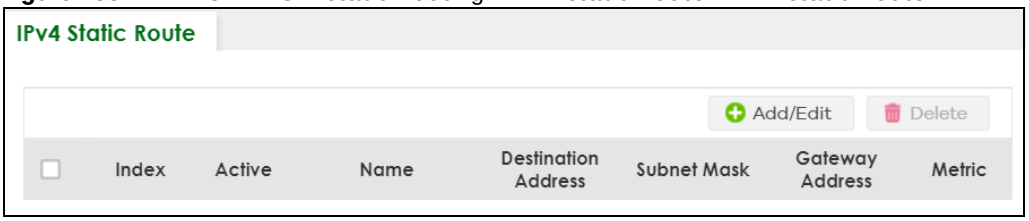
53.1.1 What You Can Do

Use the **IPv4 Static Route** screen (Section 53.2 on page 344) to configure and enable an IPv4 static route.

53.2 IPv4 Static Route

Click **NETWORKING** > **Static Routing** > **IPv4 Static Route** > **IPv4 Static Route** to display the screen as shown.

Figure 253 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route



The following table describes the related labels you use to create a static route.

Table 190 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route

LABEL	DESCRIPTION
Index	This field displays the index number of the route.
Active	This field displays whether the static route is activated or not.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.

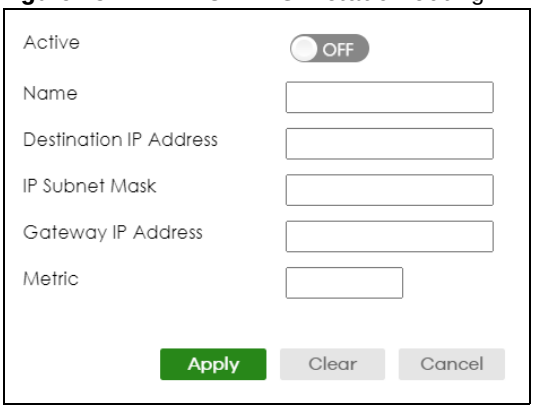
Table 190 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route (continued)

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

53.2.1 Add/Edit IPv4 Static Route

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **NETWORKING** > **Static Routing** > **IPv4 Static Route** > **IPv4 Static Route** screen to display this screen.

Figure 254 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route > Add/Edit



The following table describes the related labels you use to create a static route.

Table 191 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route > Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate or deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters except [?], [|], ['], ["], or [,]) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 54
SECURITY

The following chapters introduces the configurations of the links under the **SECURITY** navigation panel.

Quick links to chapters:

CHAPTER 55
AAA

55.1 Authentication, Authorization and Accounting (AAA)

This chapter describes how to configure authentication, authorization and accounting settings on the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers (**S**). The Switch supports RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) as the external authentication, authorization, and accounting server on clients (**C**).

Figure 255 AAA Server

55.1.1 What You Can Do

- use the **RADIUS Server Setup** screen (Section 55.2 on page 348) to configure your RADIUS server settings.
- Use the **TACACS+ Server Setup** screen (Section 55.3 on page 350) to configure your TACACS+ authentication settings.
- Use the **AAA Setup** screen (Section 55.4 on page 352) to configure authentication, authorization and accounting settings, such as the methods used to authenticate users accessing the Switch and which database the Switch should use first.

55.1.2 What You Need to Know

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.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to

track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way.

RADIUS

RADIUS is a security protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

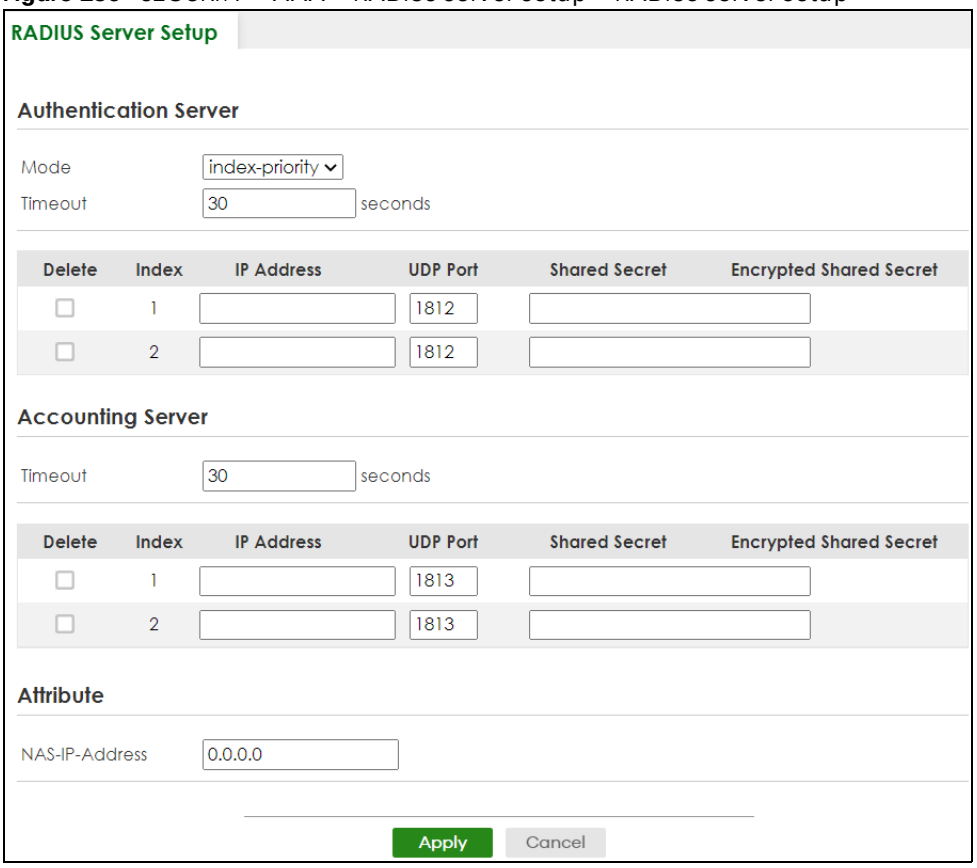
Table 192 RADIUS vs. TACACS+

	RADIUS	**TACACS+**
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

55.2 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. Click **SECURITY** > **AAA** > **RADIUS Server Setup** > **RADIUS Server Setup** to view the screen as shown.

Figure 256 SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup



The following table describes the labels in this screen.

Table 193 SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server Use this section to configure your RADIUS authentication settings.	
Mode	This field is only valid if you configure multiple RADIUS servers. Select **index-priority** and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select **round-robin** to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click **Apply**.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IPv4 address or IPv6 address of an external RADIUS server.
UDP Port	The default port of a RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.

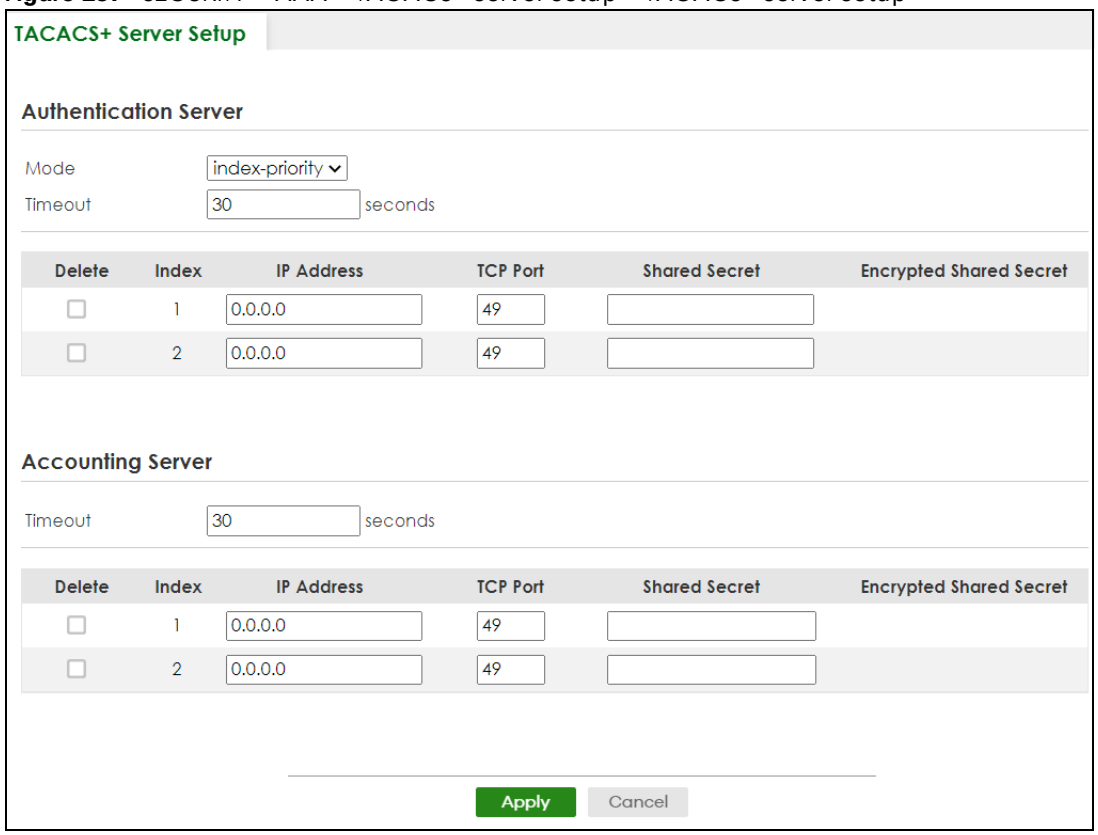
Table 193 SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,]) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Encrypted Shared Secret	This displays the encrypted shared secret in '*' format if you enabled **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: If you forget the key you set, simply reset the key in the **Shared Secret** field. If a key is encrypted, it will remain in the encrypted format even if you later disable **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
Accounting Server Use this section to configure your RADIUS accounting server settings.	
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IPv4 address or IPv6 address of an external RADIUS accounting server.
UDP Port	The default port of a RADIUS accounting server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,]) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Encrypted Shared Secret	This displays the encrypted shared secret in '*' format if you enabled **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: If you forget the key you set, simply reset the key in the **Shared Secret** field. If a key is encrypted, it will remain in the encrypted format even if you later disable **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
Attribute Use this section to define the RADIUS server attribute for its account.	
NAS-IP-Address	Enter the IP address of the NAS (Network Access Server).
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.

55.3 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. Click **SECURITY** > **AAA** > **TACACS+ Server Setup** > **TACACS+ Server Setup** to view the screen as shown.

Figure 257 SECURITY > AAA > TACACS+ Server Setup > TACACS+ Server Setup



The following table describes the labels in this screen.

Table 194 SECURITY > AAA > TACACS+ Server Setup > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server Use this section to configure your TACACS+ authentication settings.	
Mode	This field is only valid if you configure multiple TACACS+ servers. Select **index-priority** and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server. Select **round-robin** to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server. If you are using **index-priority** for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click **Apply**.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is **49**. You need not change this value unless your network administrator instructs you to do so.

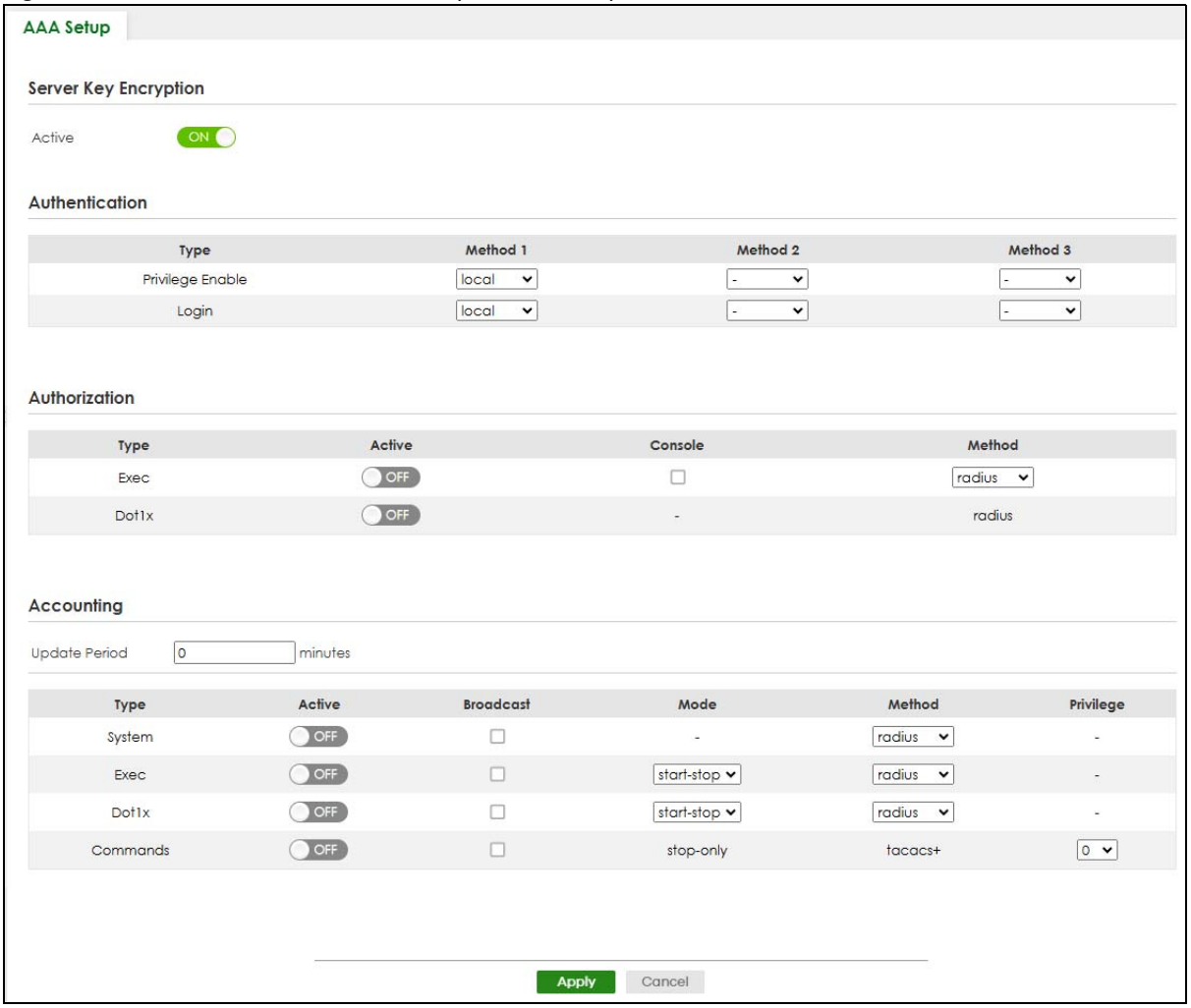
Table 194 SECURITY > AAA > TACACS+ Server Setup > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,]) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Encrypted Shared Secret	This displays the encrypted shared secret in '*' format if you enabled **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: If you forget the key you set, simply reset the key in the **Shared Secret** field. If a key is encrypted, it will remain in the encrypted format even if you later disable **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
Accounting Server Use this section to configure your TACACS+ accounting settings.	
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ accounting server is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters except [?], [|], ['], ["], [space], or [,]) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Encrypted Shared Secret	This displays the encrypted shared secret in '*' format if you enabled **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: If you forget the key you set, simply reset the key in the **Shared Secret** field. If a key is encrypted, it will remain in the encrypted format even if you later disable **Server Key Encryption** in **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup**. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
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.

55.4 AAA Setup

Use this screen to configure authentication, authorization and accounting settings on the Switch. Click **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup** to view the screen as shown.

Figure 258 SECURITY > AAA > AAA Setup > AAA Setup



The following table describes the labels in this screen.

Table 195 SECURITY > AAA > AAA Setup > AAA Setup

LABEL	DESCRIPTION
Server Key Encryption Use this section to configure server key encryption settings.	
Active	Enable the switch button to enable server key (shared secret) encryption for RADIUS server and TACACS+ server for security enhancement. The shared secret will be stored on the Switch in an encrypted format and displayed as '*' in the **SECURITY** > **AAA** > **RADIUS Server Setup** > **RADIUS Server Setup** and **SECURITY** > **AAA** > **TACACS+ Server Setup** > **TACACS+ Server Setup** screens.
Authentication Use this section to specify the methods used to authenticate users accessing the Switch.	

Table 195 SECURITY > AAA > AAA Setup > AAA Setup (continued)

LABEL	DESCRIPTION
Privilege Enable	These fields specify which database the Switch should use (first, second and third) to authenticate access privilege level for administrator accounts (users for Switch management). Configure the access privilege of accounts through commands (see the Ethernet Switch CLI Reference Guide) for **local** authentication. The **TACACS+** and **RADIUS** are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate the access privilege level of administrators. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for access privilege level specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the access privilege configured for local authentication. Select **radius** or **tacacs+** to have the Switch check the access privilege through the external servers.
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the **SYSTEM** > **Logins** > **Logins** screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for administrator accounts, specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the administrator accounts configured in the **SYSTEM** > **Logins** > **Logins** screen. Select **radius** to have the Switch check the administrator accounts configured through the RADIUS Server. Select **tacacs+** to have the Switch check the administrator accounts configured through the TACACS+ Server**.**
Authorization Use this section to configure authorization settings on the Switch.	
Type	Set whether the Switch provides the following services to a user. • **Exec**: Allow an administrator which logs into the Switch through Telnet or SSH to have a different access privilege level assigned through the external server. • **Dot1x**: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned through the external server.
Active	Enable the switch button to activate authorization for a specified event type.
Console	Select this to allow an administrator which logs in the Switch through the console port to have different access privilege level assigned through the external server.
Method	Select whether you want to use **radius** or **tacacs+** for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Accounting Use this section to configure accounting settings on the Switch.	
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the **start-stop** option for the **Exec** or **Dot1x** entries.

Table 195 SECURITY > AAA > AAA Setup > AAA Setup (continued)

LABEL	DESCRIPTION
Type	The Switch supports the following types of events to be sent to the accounting servers: • **System** – Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled. • **Exec** – Configure the Switch to send information when an administrator logs in and logs out through the console port, telnet or SSH. • **Dot1x** – Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates through the Switch), ends a session as well as interim updates of a session. • **Commands** – Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Enable the switch button to activate accounting for a specified event type.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you do not select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it does not get a response from the accounting server then it tries the second accounting server.
Mode	The Switch supports two modes of recording login events. Select: • **start-stop** – to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the **Update Period**), and when a user ends a session. • **stop-only** – to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use **radius** or **tacacs+** for accounting of specific types of events. **tacacs+** is the only method for recording **Commands** type of event.
Privilege	This field is only configurable for **Commands** type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.
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.

55.5 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

55.5.1 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID**: An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). Zyxel's vendor ID is 890.
- **Vendor-Type**: A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data**: A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating through the RADIUS server.

The following table describes the VSAs supported on the Switch.

Table 196 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **1** Vendor-data = ingress rate (Kbps in decimal format)
Egress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **2** Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = **890** Vendor-Type = **3** Vendor-Data = "**shell:priv-lvl=**N" or Vendor-ID = **9** (CISCO) Vendor-Type = **1** (CISCO-AVPAIR) Vendor-Data = "**shell:priv-lvl=**N" where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS servers and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

55.5.1.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

Table 197 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = **VLAN(13)** Tunnel-Medium-Type = **802(6)** Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch. Note: The bolded values in this table are fixed values as defined in RFC 3580.

55.5.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication elements in a user profile, which is stored on the RADIUS server. This section lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication.

This section lists the attributes used by authentication functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

55.5.3 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

55.5.3.1 Attributes Used for Authenticating Privilege Access

User-Name

– The format of the User-Name attribute is **$enab**#**$**, where # is the privilege level (1 – 14).

User-Password

NAS-Identifier

NAS-IP-Address

55.5.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

55.5.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

– This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

CHAPTER 56
Access Control

56.1 Access Control Overview

This chapter describes how to control access to the Switch.

FTP is allowed one session each, Telnet and SSH share nine sessions, up to five web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 198 Access Control Overview

SSH	Telnet	FTP	Web	SNMP
Share up to nine sessions		One session	Up to five accounts	No limit

Telnet access control session cannot coexist when multi-login is disabled.

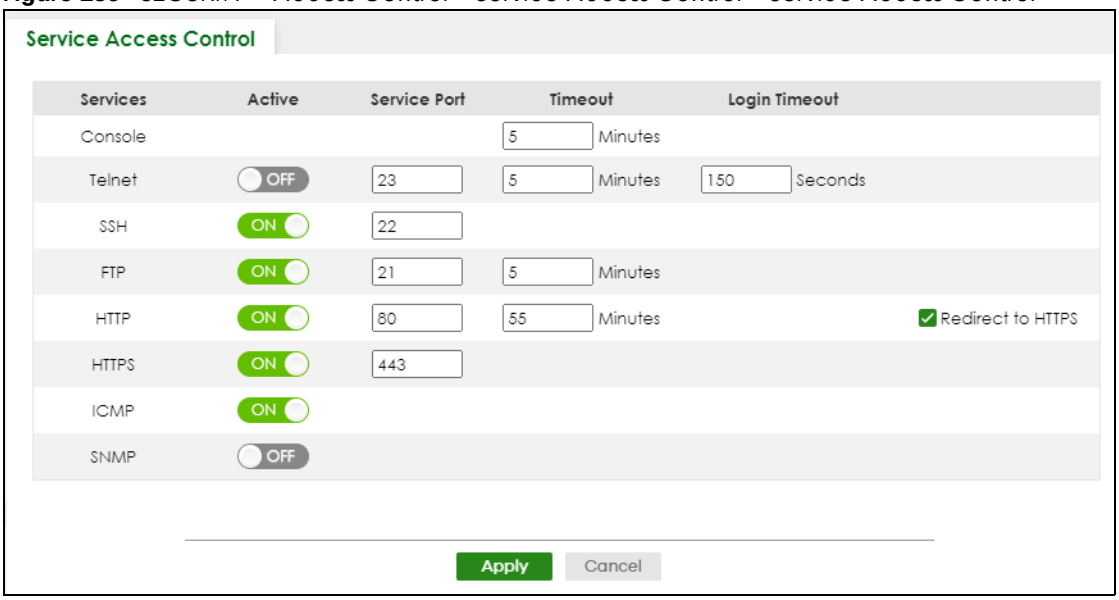
56.1.1 What You Can Do

- Use the **Service Access Control** screen (Section 56.2 on page 359) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen (Section 56.3 on page 360) to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
- Use the **Account Security** screen (Section 56.5 on page 363) to encrypt all passwords configured in the Switch. You can also display the authentication, authorization, external authentication server information (RADIUS or TACACS+), system and SNMP user account information in the configuration file saved.

56.2 Service Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure "trusted computers" for each service in the **SECURITY** > **Access Control** > **Remote Management** > **Remote Management** screen (see Section 56.3 on page 360 for more information). Click **SECURITY** > **Access Control** > **Service Access Control** > **Service Access Control** to display the following screen.

Figure 259 SECURITY > Access Control > Service Access Control > Service Access Control



The following table describes the fields in this screen.

Table 199 SECURITY > Access Control > Service Access Control > Service Access Control

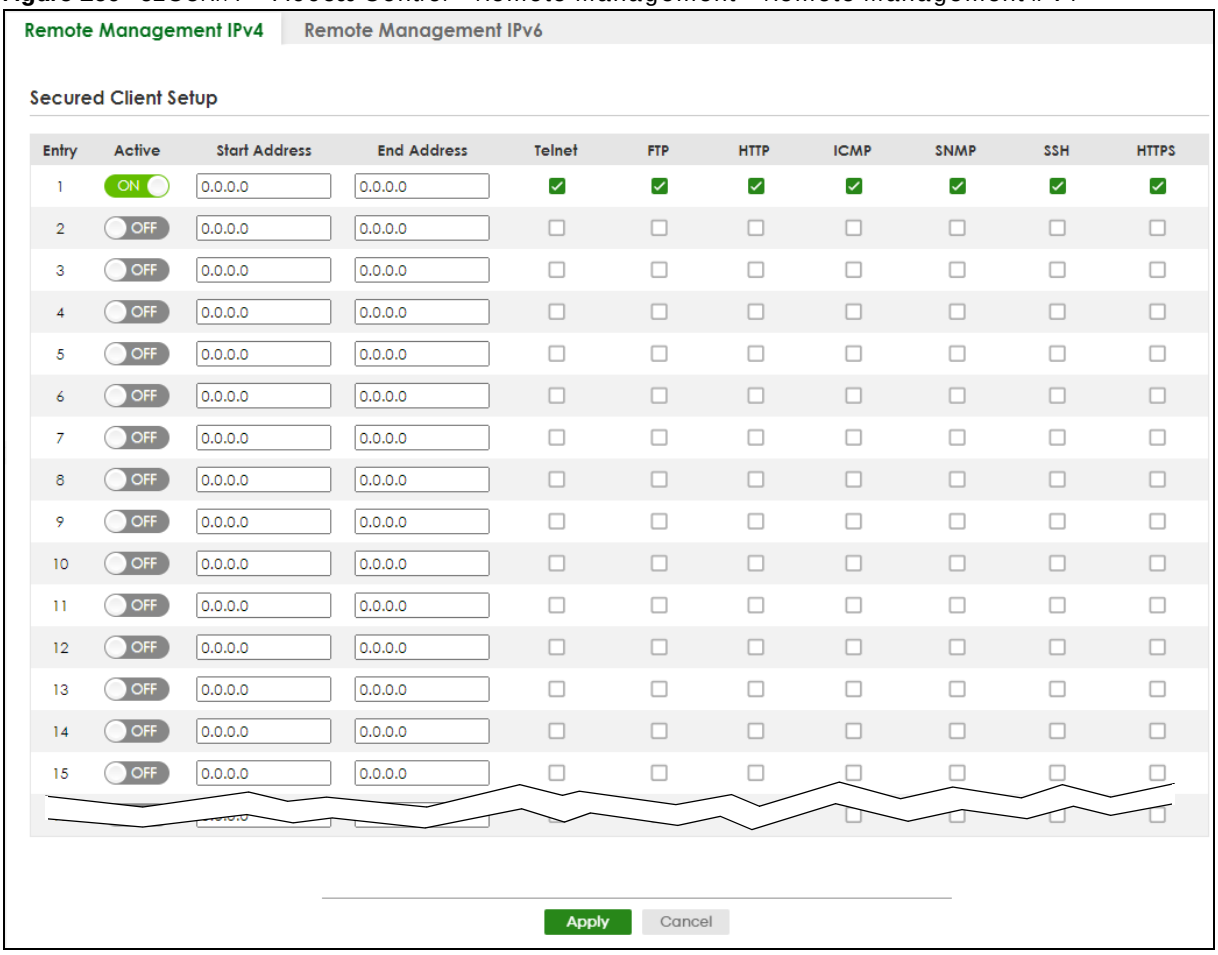
LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here. Telnet and SSH give access to a limited version of the Command Line Interface (CLI) to display information.
Active	Enable the switch button for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Service Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Enter how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Login Timeout	The Telnet or SSH server do not allow multiple user logins at the same time. Enter how many seconds (from 30 to 300 seconds) a login session times out. After it times out you have to start the login session again. Very long login session timeouts may have security risks. For example, if User A attempts to connect to the Switch (through SSH), but during the login stage, do not enter the user name and/or password, User B cannot connect to the Switch (through SSH) before the **Login Timeout** for User A expires (default 150 seconds).
Redirect to HTTPS	This option allows your web browser to automatically redirect to a secure page, from HTTP to HTTPS (secure hypertext transfer protocol). SSL (Secure Sockets Layer) in HTTPS encrypts the transferred data by changing plain text to random letters and numbers.
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.

56.3 Remote Management

Use this screen to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

Click **SECURITY** > **Access Control** > **Remote Management** > **Remote Management** to view the screen as shown next.

Figure 260 SECURITY > Access Control > Remote Management > Remote Management IPv4



The following table describes the labels in this screen.

Table 200 SECURITY > Access Control > Remote Management > Remote Management IPv4

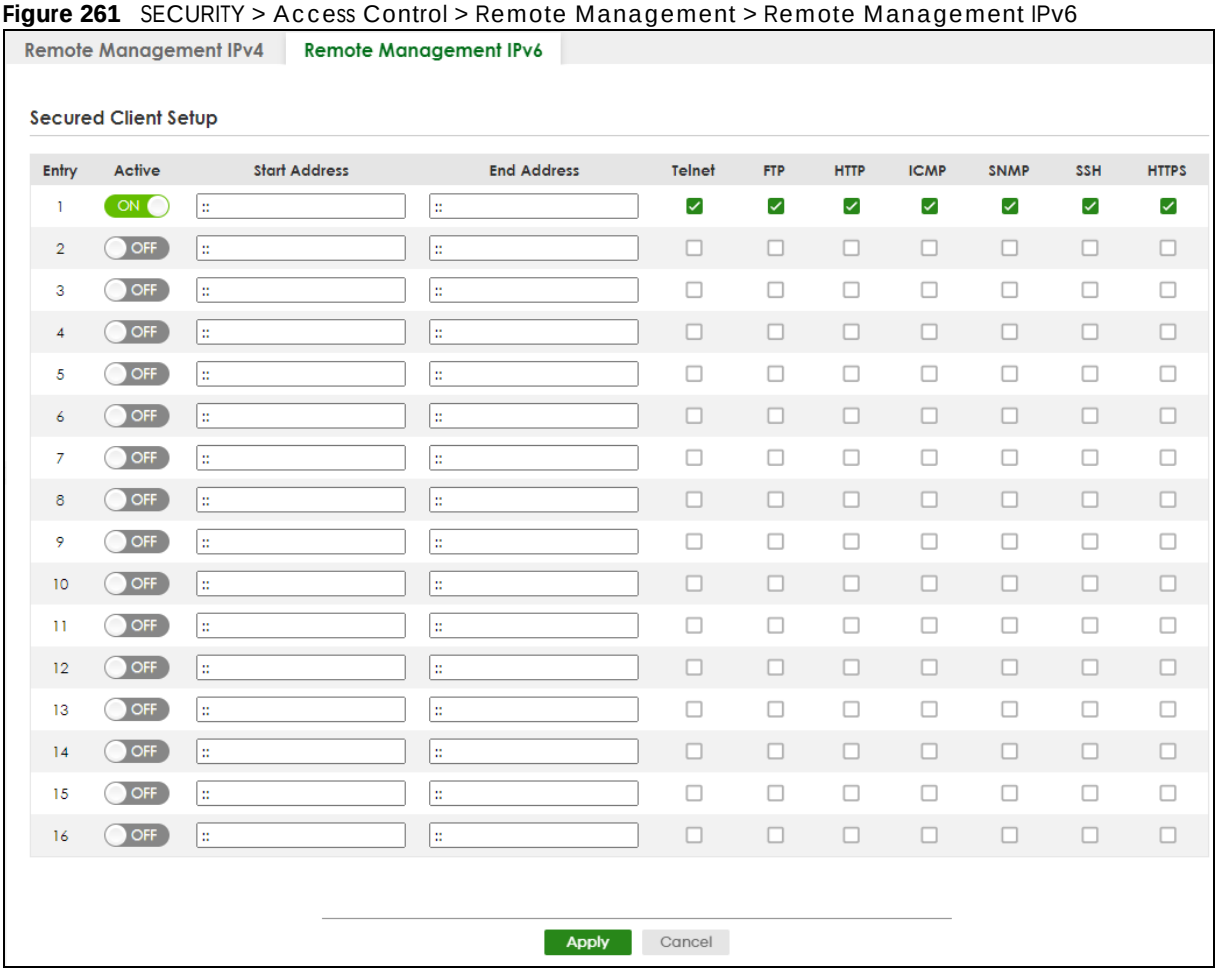
LABEL	DESCRIPTION
Entry	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
Active	Enable the switch button to activate this secured client set. Clear the checkbox if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IPv4 address range of trusted computers from which you can manage this Switch. The Switch checks if the client IPv4 address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet / FTP / HTTP / ICMP / SNMP / SSH / HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
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.

56.4 Remote Management (IPv6)

Use this screen to specify a group of one or more “trusted computers using IPv6 addresses” from which an administrator may use a service to manage the Switch.

Click **SECURITY** > **Access Control** > **Remote Management** > **Remote Management IPv6** to view the screen as shown next.

Figure 261 SECURITY > Access Control > Remote Management > Remote Management IPv6



The following table describes the labels in this screen.

Table 201 SECURITY > Access Control > Remote Management > Remote Management IPv6

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Active	Enable the switch button to activate this secured client set. Clear the checkbox if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IPv6 address range of trusted computers from which you can manage this Switch. The Switch checks if the client IPv6 address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet / FTP / HTTP / ICMP / SNMP / SSH / HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.

Table 201 SECURITY > Access Control > Remote Management > Remote Management IPv6

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.

56.5 Account Security

Use this screen to encrypt all passwords configured in the Switch. This setting will affect how the password is shown (as plain text or encrypted text) in the configuration file saved in **MAINTENANCE** > **Configuration** > **Save Configuration** > **Save Configuration**.

Note: Make sure to enable **Password Encryption** to avoid displaying passwords as plain text in the configuration file.

Note: Be careful who can access configuration files with plain text passwords!

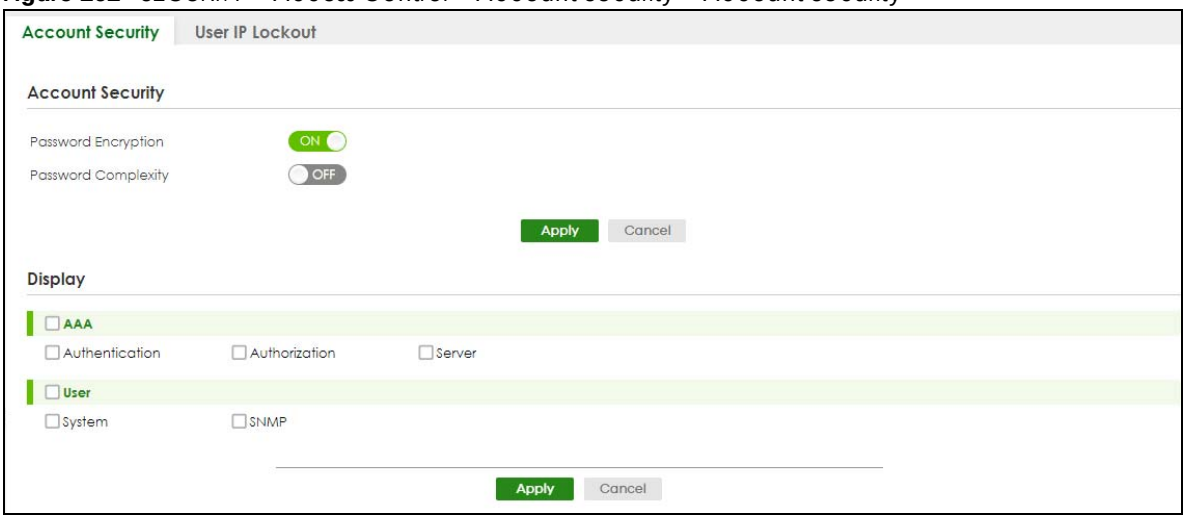
Password Encryption encrypts all passwords in the configuration file. However, if you want to show some passwords as plain text in the configuration file, select them as below:

- **Authentication** information configured for **Authentication** in the **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup** screen (**Method 1**/**2**/**3** setting in the **Privilege Enable** and **Login** fields).
- **Authorization** information configured for **Authorization** in the **SECURITY** > **AAA** > **AAA Setup** > **AAA Setup** screen (**Active**/**Console**/**Method** setting in the **Exec** and **Dot1x** fields).
- **System** account information configured in the Switch (admin, user login name, and password).
- **SNMP** user account information configured in the **SYSTEM** > **SNMP** > **SNMP User** screen (password for SNMP user authentication in the **Authentication** field, and the password for the encryption method for SNMP communication in the **Privacy** field).

Note: The passwords will appear as encrypted text when **Password Encryption** is **Active**.

Click **SECURITY** > **Access Control** > **Account Security** > **Account Security** to view the screen as shown next.

Figure 262 SECURITY > Access Control > Account Security > Account Security



The following table describes the labels in this screen.

Table 202 SECURITY > Access Control > Account Security > Account Security

LABEL	DESCRIPTION
Account Security	
Password Encryption	Click the switch to the right to encrypt all passwords configured on the Switch (default is enabled). This displays the password as encrypted text, in a saved configuration file. Otherwise, the passwords configured on the Switch are displayed in plain text.
Password Complexity	Click the switch to the right to enforce a strong login password (default is disabled). The password rules are: • 9 to 32 characters in length • Include at least three of these: numbers, uppercase letters, lowercase letters, and special characters (for example, 'Ea5yPas5W0rd') • Cannot match your login username • Cannot use the same character (case insensitive) or number three or more times in a row (for example, '777', 'AaA') • Cannot use four or more sequential keyboard characters (case insensitive) or numbers (for example, 'qWer', '1234'), and • Cannot use the present password again. Alternatively, click the switch to the left. The password rules is: • 4 to 32 characters in length Note: [?], [|], ['], ["], [,], [[ ], [ ]] and space are not allowed whether **Password Complexity** is enabled or disabled.
Apply	Click **Apply** to save your changes for **Account Security** 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 **Account Security** afresh.
Display	
AAA	Select which specific information to display in plain text, in the saved configuration file. • **Authentication** • **Authorization** • **Server**

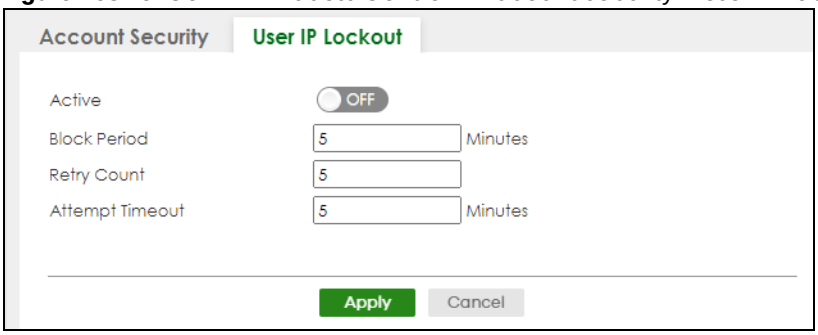
Table 202 SECURITY > Access Control > Account Security > Account Security (continued)

LABEL	DESCRIPTION
User	Select which user account information to display in plain text, in the saved configuration file. • **System** • **SNMP**
Apply	Click **Apply** to save your changes for **Display** 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 **Display** afresh.

56.6 Lock the IP Address

Use this screen to allow the Switch to block login requests after multiple failed attempts occur within a specific time frame. Click **SECURITY** > **Access Control** > **Account Security** > **User IP Lockout** to view the screen as shown next.

Figure 263 SECURITY > Access Control > Account Security > User IP Lockout



The following table describes the labels in this screen.

Table 203 SECURITY > Access Control > Account Security > User IP Lockout

LABEL	DESCRIPTION
Active	Click the switch to the right to allow the Switch to detect and block multiple failed login attempts from the same IP address (default is disable).
Block Period	Enter how many minutes (from 1 to 65535) the IP address that exceeded the **Retry Count** will be stopped from trying to log in again (default is 5 minutes).
Retry Count	Enter how many login attempts (from 1 to 99) to allow an IP address (default is 5 attempts).
Attempt Timeout	Enter how many minutes (from 1 to 65535) if the login attempts exceed the **Retry Count**, to stop the IP address from trying to log in again (default is 5 minutes). For example, the Switch will block all logins from the same IP address (IP 'A') for 5 minutes if there are 6 failed attempts within 10 minutes. IP 'A' cannot try to log in to the Switch until the **Block Period** expires.
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.

56.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

56.7.1 SSH Overview

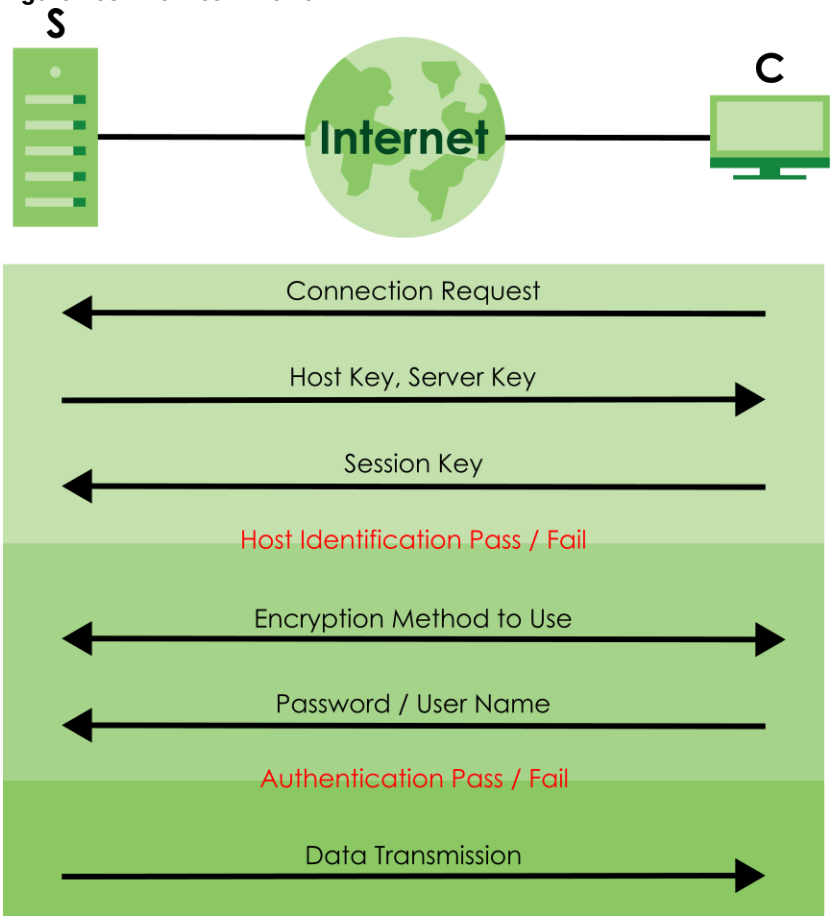
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication (**SC**) protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 264 SSH Communication Example

56.7.1.1 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts, SSH server (**S**) and SSH client (**C**).

Figure 265 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

56.7.1.2 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and the AES encryption method. The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

56.7.1.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

56.7.2 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

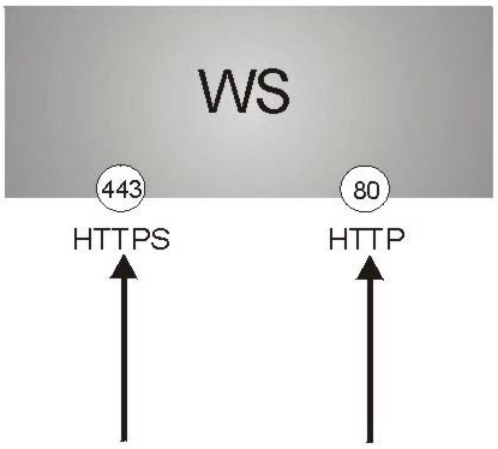
HTTPS on the Switch is used so that you may securely access the Switch using the Web Configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a Certificate Authority (CA) that is a trusted CA on the Switch.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 266 HTTPS Implementation



Note: If you disable HTTP in the Service Access Control screen, then the Switch blocks all HTTP connection attempts.

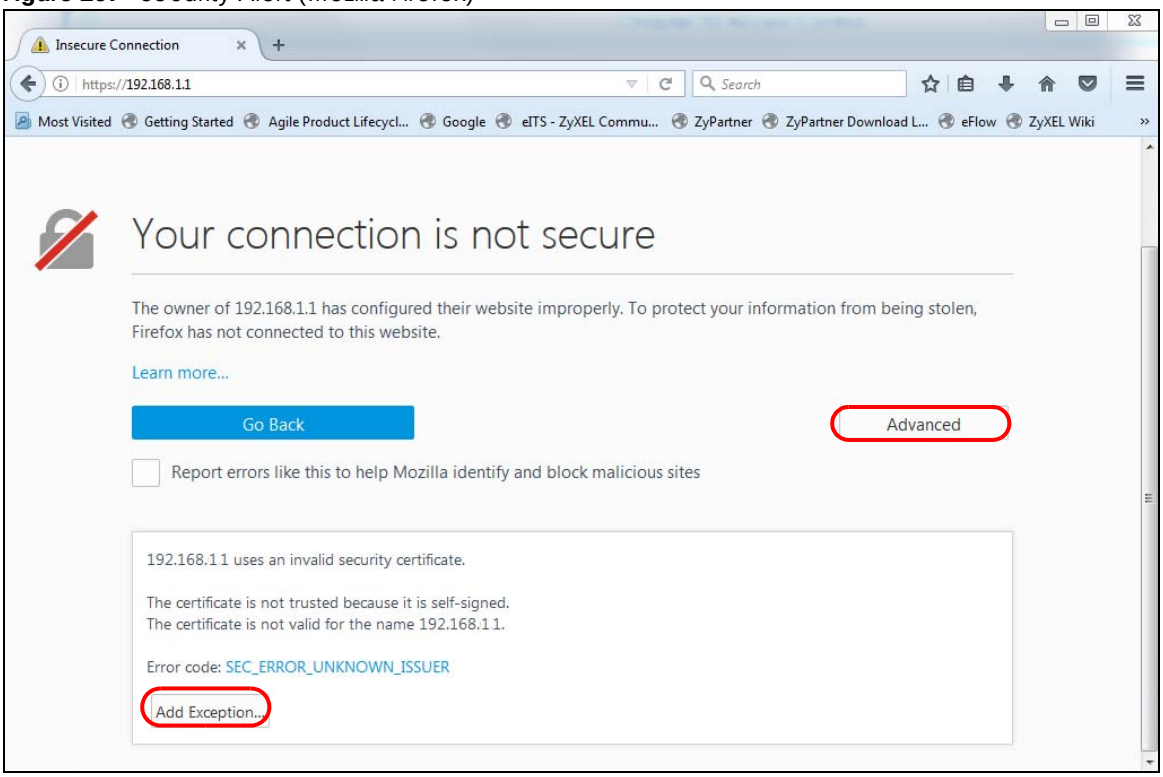
56.7.2.1 HTTPS Example

If you have not changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

Mozilla Firefox Warning Messages

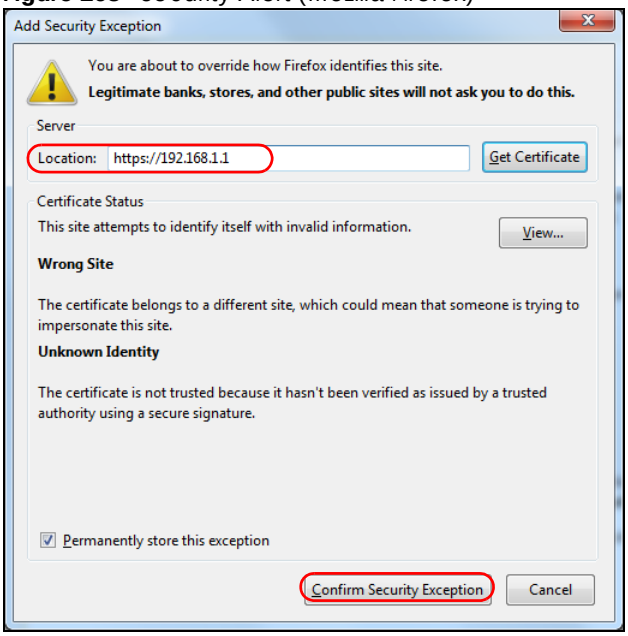
When you attempt to access the Switch HTTPS server, a **Your connection is not secure** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 267 Security Alert (Mozilla Firefox)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the Web Configurator login screen.

Figure 268 Security Alert (Mozilla Firefox)

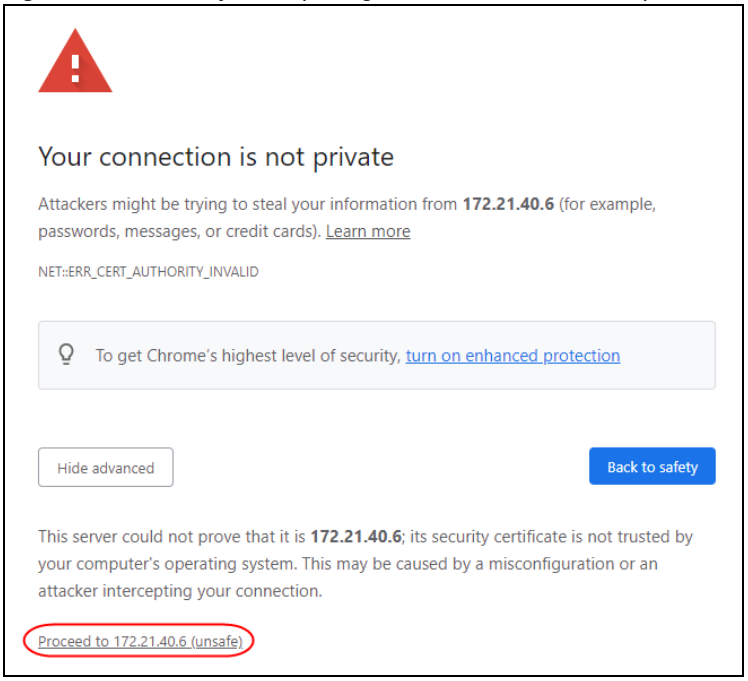


56.7.3 Google Chrome Warning Messages

When you attempt to access the Switch HTTPS server, a **Your connection is not private** screen may

display. If that is the case, click **Advanced** and then **Proceed to x.x.x.x (unsafe)** to proceed to the Web Configurator login screen.

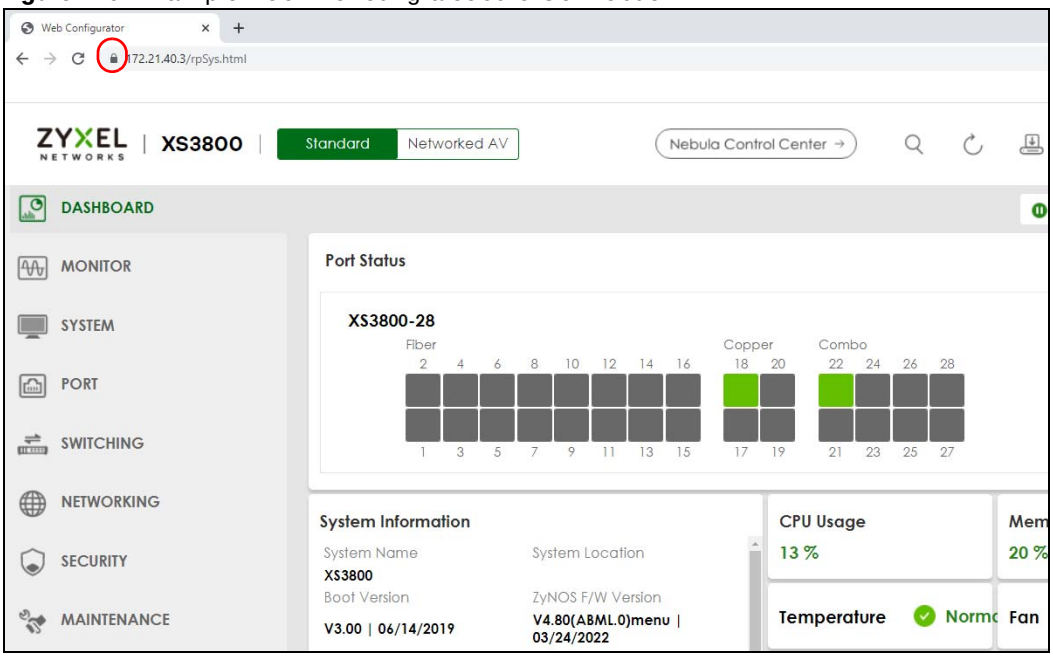
Figure 269 Security Alert (Google Chrome 99.0.4844.82)



56.7.3.1 Main Settings

After you accept the certificate and enter the login user name and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar or next to the website address denotes a secure connection.

Figure 270 Example: Lock Denoting a Secure Connection



CHAPTER 57 Classifier

57.1 Classifier Overview

This chapter introduces and shows you how to configure the packet classifier on the Switch. It also discusses Quality of Service (QoS) and classifier concepts as employed by the Switch.

57.1.1 What You Can Do

- Use the **Classifier Status** screen (Section 57.2 on page 371) to view the classifiers configured on the Switch and how many times the traffic matches the rules.
- Use the **Classifier Setup** screen (Section 57.3 on page 372) to define the classifiers and view a summary of the classifier configuration. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.
- Use the **Classifier Global Setting** screen (Section 57.4 on page 377) to configure the match order and enable logging on the Switch.

57.1.2 What You Need to Know

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.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

1. Configure classifiers to sort traffic into different flows.
2. Configure policy rules to define actions to be performed on a classified traffic flow (refer to Chapter 58 on page 380 to configure policy rules).

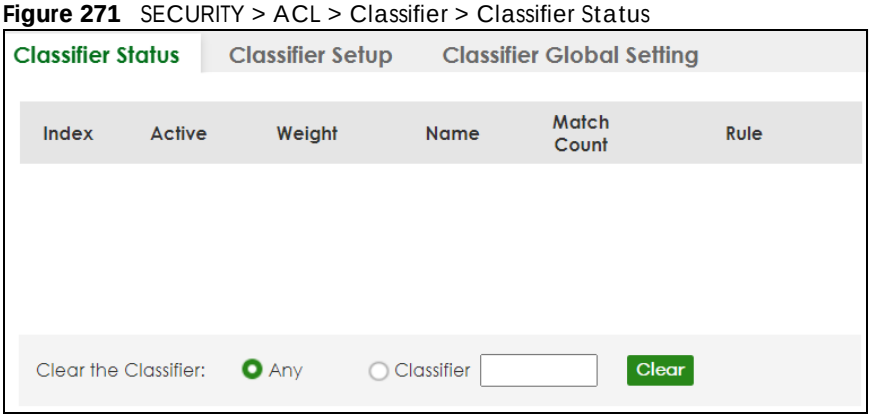
57.2 Classifier Status

Use this screen to view the classifiers configured on the Switch and how many times the traffic matches

the rules.

Click **SECURITY** > **ACL** > **Classifier** > **Classifier Status** to display the configuration screen as shown.

Figure 271 SECURITY > ACL > Classifier > Classifier Status



The following table describes the labels in this screen.

Table 204 SECURITY > ACL > Classifier > Classifier Status

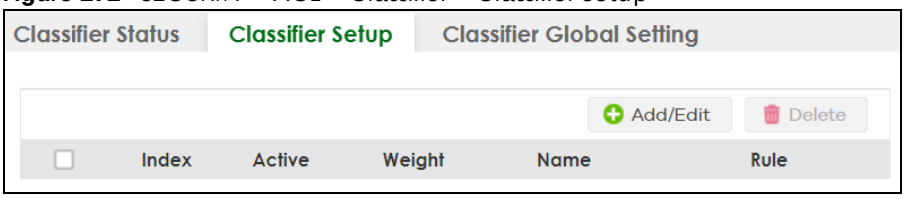
LABEL	DESCRIPTION
Index	This field displays the index number of the rule.
Active	This field displays whether the rule is activated or not.
Weight	This field displays the rule's weight. This is to indicate a rule's priority when the match order is set to **manual** in the **SECURITY** > **ACL** > **Classifier** > **Classifier Global Setting** screen. The higher the number, the higher the rule's priority.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Match Count	This field displays the number of times a rule is applied. It displays '–' if the rule does not have count enabled.
Rule	This field displays a summary of the classifier rule's settings.
Clear the Classifier	
Any	Select **Any**, then click **Clear** to clear the matched count for all classifiers.
Classifier	Select **Classifier**, enter a classifier rule name and then click **Clear** to erase the recorded statistical information for that classifier, or select **Any** to clear statistics for all classifiers.
Clear	Click **Clear** to erase the recorded statistical information for the classifier.

57.3 Classifier Setup

Use this screen to view and configure the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.

Click **SECURITY** > **ACL** > **Classifier Setup** to display the configuration screen as shown.

Figure 272 SECURITY > ACL > Classifier > Classifier Setup



The following table describes the labels in this screen.

Table 205 SECURITY > ACL > Classifier > Classifier Setup

LABEL	DESCRIPTION
Index	This field displays the index number of the rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Weight	The field displays the priority of the rule when the match order is in **manual** mode. A higher weight means a higher priority.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 206 Common Ethernet Types and Protocol Numbers

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

In the Internet Protocol there is a field, called "Protocol", to identify the next level protocol. The following table shows some common protocol types and the corresponding protocol number. Refer to *http://www.iana.org/assignments/protocol-numbers* for a complete list.

Table 207 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17

Table 207 Common IP Protocol Types and Protocol Numbers (continued)

PROTOCOL TYPE	PROTOCOL NUMBER
EGP	8
L2TP	115

Some of the most common TCP and UDP port numbers are:

Table 208 Common TCP and UDP Port Numbers

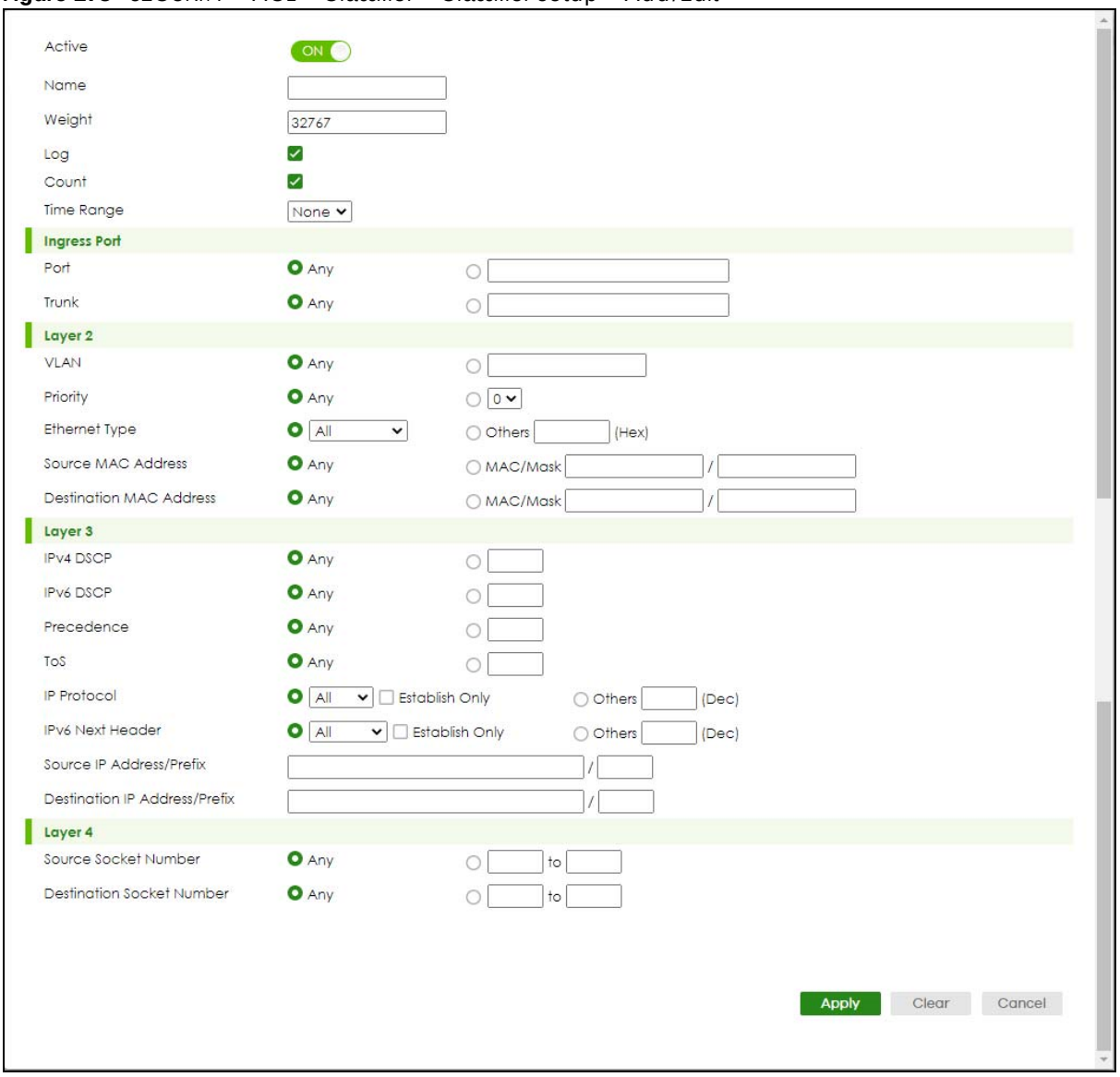
PROTOCOL NAME	TCP/UDP PORT NUMBER
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110

57.3.1 Add/Edit a Classifier

Use this screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY** > **ACL** > **Classifier** > **Classifier Setup** screen to display this screen.

Figure 273 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit



The following table describes the labels in this screen.

Table 209 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].
Weight	Enter a number between 0 and 65535 to specify the rule's weight. When the match order is in manual mode in the **Classifier Global Setting** screen, a higher weight means a higher priority.
Log	Select this option to have the Switch create a log message when the rule is applied and record the number of matched packets in a particular time interval. Note: Make sure you also enable logging in the **Classifier Global Setting** screen.
Count	Select this option to have the Switch count how many times the rule is applied.

Table 209 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit (continued)

LABEL	DESCRIPTION
Time Range	Select the name of the pre-configured schedule that you want to apply to the rule. The rule will be active only at the scheduled date and/or time. If you select **None**, the rule will be active all the time.
Ingress Port	
Port	Select **Any** to apply the rule to all ports. Alternatively, to specify the ports enter the port numbers to which the rule should be applied. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Trunk	Select **Any** to apply the rule to all trunk groups. Alternatively, to specify multiple trunks, enter the trunk group ID to apply the rule to multiple trunks. You can enter multiple trunks with (t) or (T) then the trunk group ID separated by (no space) comma (,) or hyphen (-). For example, enter "t3-t5" for trunks 3, 4, and 5. Enter "T3,T5,T7" for trunks 3, 5, and 7.
Layer 2 Specify the fields below to configure a layer 2 classifier.	
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select **Any** to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select **Other** and enter the Ethernet type number in hexadecimal value.
Source MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select **MAC/Mask** to enter the source MAC address of the packet in valid MAC address format (six hexadecimal character pairs) and type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the **Mask** field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.
Destination MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select **MAC/Mask** to enter the destination MAC address of the packet in valid MAC address format (six hexadecimal character pairs) and type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the **Mask** field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.
Layer 3 Specify the fields below to configure a layer 3 classifier.	
IPv4/IPv6 DSCP	Select **Any** to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Precedence	Select **Any** to classify traffic from any precedence or select the second option and specify an IP Precedence (the first 3 bits of the 8-bit ToS field) value between 0 and 7 in the field provided.
ToS	Select **Any** to classify traffic from any ToS or select the second option and specify Type of Service (the last 5 bits of the 8-bit ToS field) value between 0 and 255 in the field provided.

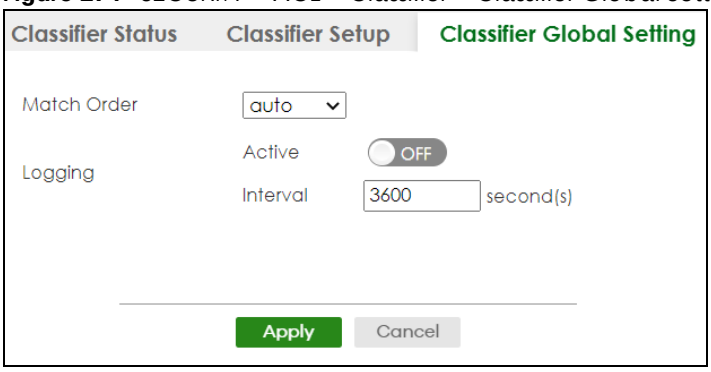
Table 209 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit (continued)

LABEL	DESCRIPTION
IP Protocol	Select an IPv4 protocol type or select **Other** and enter the protocol number in decimal value. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
IPv6 Next Header	Select an IPv6 protocol type or select **Other** and enter an 8-bit next header in the IPv6 packet. The Next Header field is similar to the IPv4 Protocol field. The IPv6 protocol number ranges from 1 to 255. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
Source IP Address/ Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask. A subnet mask can be represented in a 32-bit notation. For example, the subnet mask “255.255.255.0” can be represented as “11111111.11111111.11111111.00000000”, and counting up the number of ones in this case results in 24.
Destination IP Address/ Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Layer 4 Specify the fields below to configure a layer 4 classifier.	
Source Socket Number	Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers.
Destination Socket Number	Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

57.4 Classifier Global Setting

Use this screen to configure the match order and enable logging on the Switch. Click **SECURITY** > **ACL** > **Classifier** > **Classifier Global Setting** to display the configuration screen as shown.

Figure 274 SECURITY > ACL > Classifier > Classifier Global Setting



The following table describes the labels in this screen.

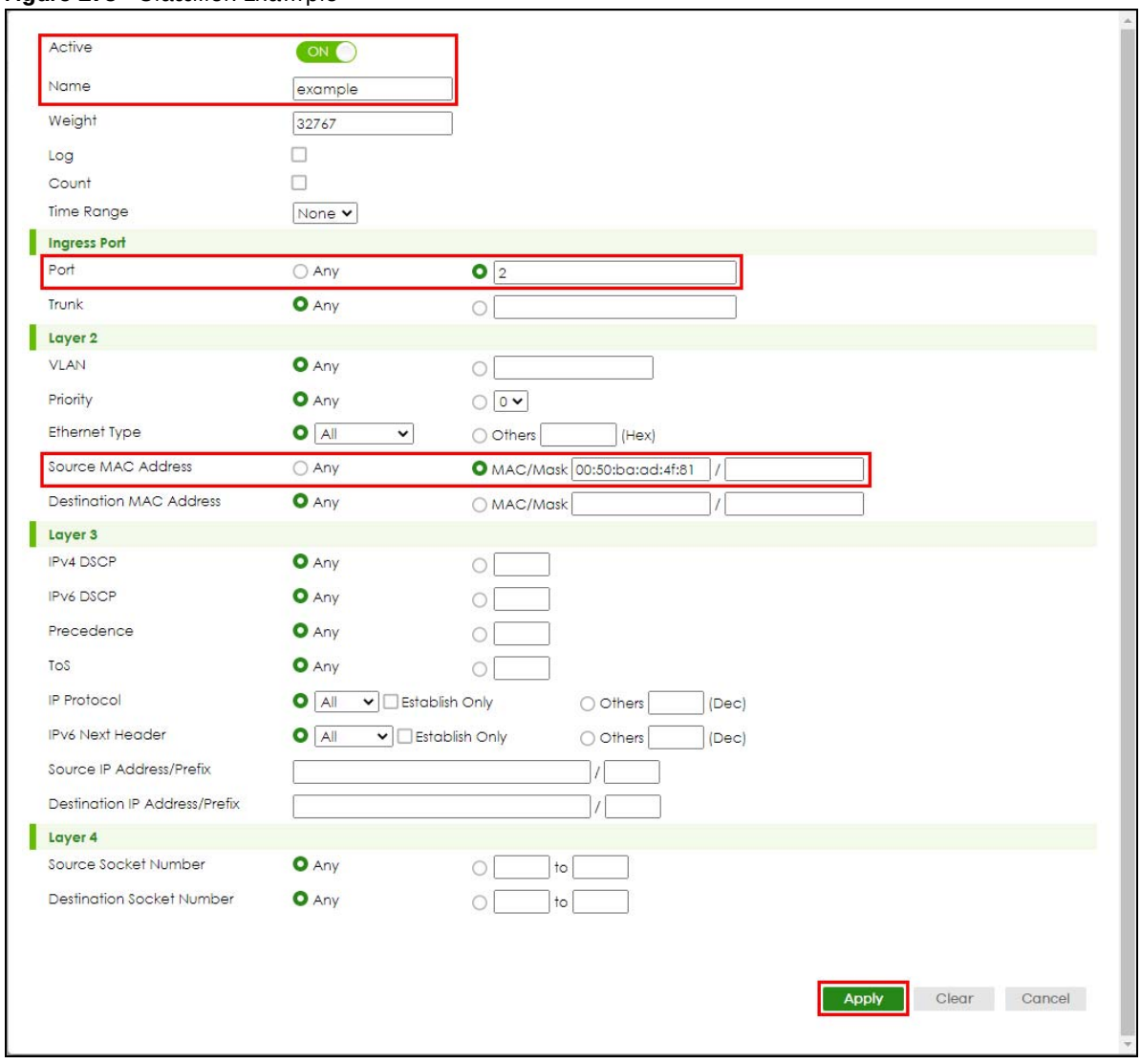
Table 210 SECURITY > ACL > Classifier > Classifier Global Setting

LABEL	DESCRIPTION
Match Order	Use this field to set the match order for the classifier rules. A traffic flow can only be classified to one classifier. When a traffic flow matches more than one classifier rule, the Switch classifies the traffic based on the **Match Order**. Select **manual** to have classifier rules applied according to the weight of each rule you configured in **SECURITY** > **ACL** > **Classifier** > **Classifier Setup**. If they have the same weight, the Switch will classify the traffic to the classifier with a higher name priority (see **Classifier Name Priority**). Alternatively, select **auto** to have classifier rules applied according to the layer of the item configured in the rule. Layer-4 items have the highest priority, and layer-2 items has the lowest priority. For example, you configure a layer-2 item (VLAN ID) in classifier A and configure a layer-3 item (source IP address) in classifier B. When an incoming packet matches both classifier rules, classifier B has priority over classifier A. If both classifiers have the same priority, the Switch will apply the classifier with a higher name priority. **Classifier Name Priority** The longer the classifier name, the higher the classifier priority. If two classifier names are the same length, the bigger the character, the higher the classifier priority. The lowercase letters (such as a and b) have higher priority than the capitals (such as A and B) in the classifier name. For example, the classifier with the name of class 2, class a or class B takes priority over the classifier with the name of class 1 or class A.
Logging	
Active	Enable the switch button to allow the Switch to create a log when packets match a classifier rule during a defined time interval.
Interval	Set the length of the time period (in seconds) to count matched packets for a classifier rule. Enter an integer from 0 – 65535. 0 means that no logging is done.
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.

57.5 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

Figure 275 Classifier: Example



After you have configured a classifier, you can configure a policy (in the **SECURITY** > **ACL** > **Policy Rule** > **Policy Rule** screen) to define actions on the classified traffic flow.

CHAPTER 58
Policy Rule

58.1 Policy Rules Overview

This chapter shows you how to configure policy rules.

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 57 on page 371 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

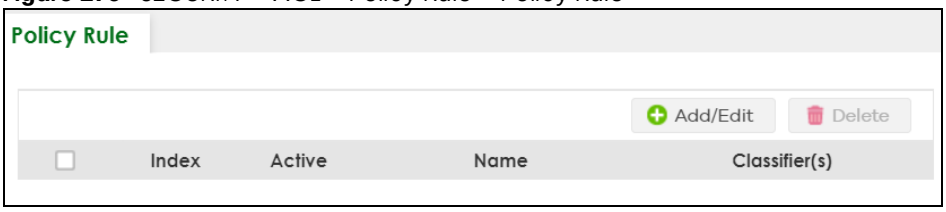
58.1.1 What You Can Do

Use the **Policy Rule** screen (Section 58.2 on page 380) to enable the policy and display the active classifiers you configure in the **Classifier** screen.

58.2 Policy Rules

Click **SECURITY** > **ACL** > **Policy Rule** in the navigation panel to display the screen as shown.

Figure 276 SECURITY > ACL > Policy Rule > Policy Rule



The following table describes the labels in this screen.

Table 211 SECURITY > ACL > Policy Rule > Policy Rule

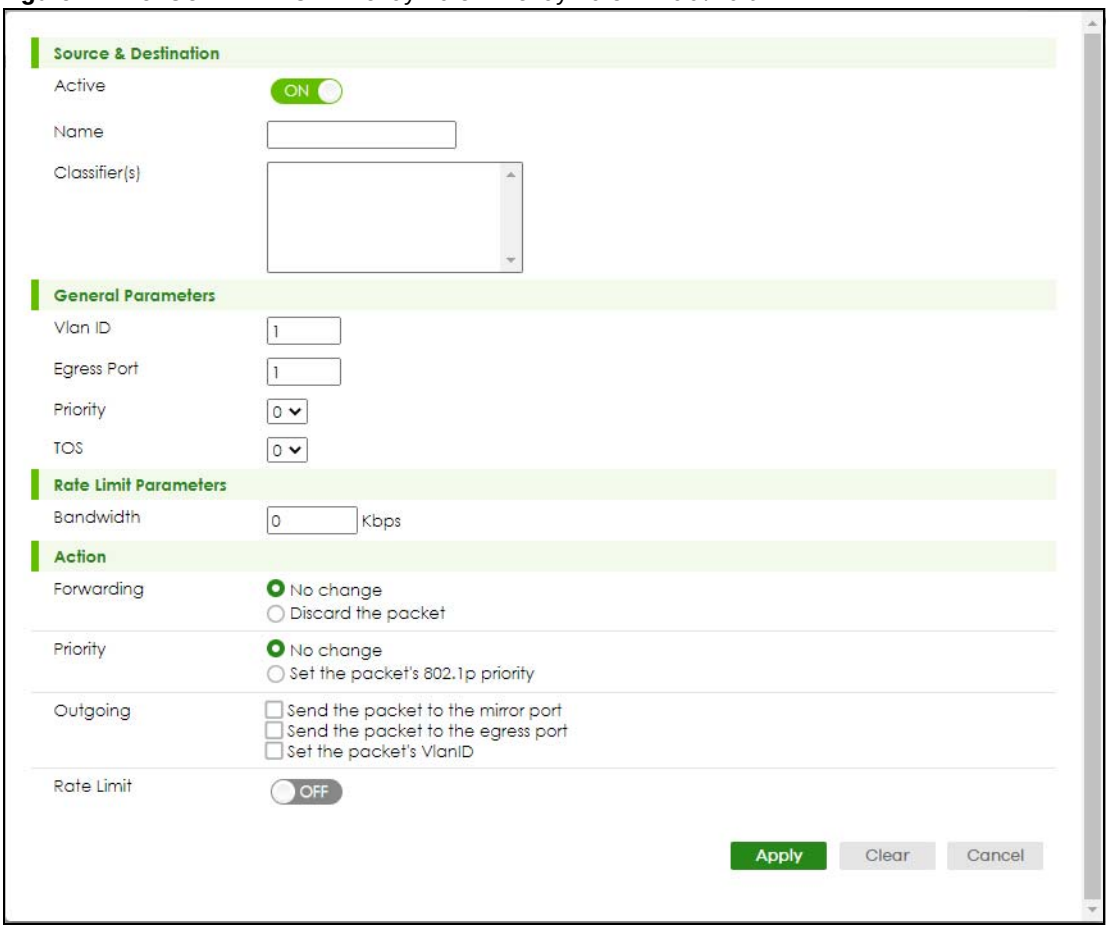
LABEL	DESCRIPTION
Index	This field displays the policy index number.
Active	This field displays whether policy is activated or not.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the names of the classifier to which this policy applies.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

58.2.1 Add/Edit a Policy Rule

You must first configure a classifier in the **SECURITY** > **ACL** > **Classifier** > **Classifier Setup** screen.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY** > **ACL** > **Policy Rule** > **Policy Rule** screen to display this screen.

Figure 277 SECURITY > ACL > Policy Rule > Policy Rule > Add/Edit



The following table describes the labels in this screen.

Table 212 SECURITY > ACL > Policy Rule > Policy Rule > Add/Edit

LABEL	DESCRIPTION
Source & Destination	
Active	Enable the switch button to enable the policy.
Name	Enter a descriptive name for identification purposes. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].
Classifier(s)	This field displays the active classifiers you configure in the **SECURITY** > **ACL** > **Classifier** > **Classifier Setup** screen. Select the classifiers to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
General Parameters Set the fields below for this policy. You only have to set the fields that is related to the actions you configure in the **Action** field.	

Table 212 SECURITY > ACL > Policy Rule > Policy Rule > Add/Edit (continued)

LABEL	DESCRIPTION
Vlan ID	Specify a VLAN ID.
Egress Port	Enter the number of an outgoing port.
Priority	Specify a priority level.
TOS	Specify the Type Of Service (TOS) priority level.
Rate Limit Parameters You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.	
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 1 and 1000000.
Action Specify the actions the Switch takes on the associated classified traffic flow. Note: You can specify only one action (option) for each category (**Forwarding**, **Priority**, **Queue**, **Outgoing**) in a policy rule. Note: The Switch only applies one policy rule for each traffic flow. Say you have a traffic flow that matches several classifiers, and you specify a different policy rule for each. The Switch only classifies the traffic flow to the classifier with the highest **Match Order**. The Switch then applies the policy rule with which the classifier is associated. You can set the classifier **Match Order** rule (**manual** or **auto**) in the **ACL** > **Classfier** > **Classifier Global settings** screen (see Section 57.4 on page 377 for more information). Let's say you set two classifiers (Class 1 and Class 2) and both identify all traffic from MAC address 11:22:33:44:55:66 on port 3. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to forward the packets to the egress port, the Switch will forward the packets. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will discard the packets immediately. If Policy 1 applies to Class 1 and the action is to forward the packets to the egress port, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will forward the packets.	
Forwarding	Select **No change** to forward the packets. Select **Discard the packet** to drop the packets.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1p priority** to replace the packet's 802.1p priority field with the value you set in the **Priority** field and put the packets in the designated queue.
Outgoing	Select **Send the packet to the mirror port** to send the packet to the mirror port. Select **Send the packet to the egress port** to send the packet to the egress port. Select **Set the packet's VLAN ID** to set the packet's VLAN ID.
Rate Limit	Select **Enable** to activate bandwidth limitation on the traffic flows then set the actions to be taken on out-of-profile packets.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 59
Storm Control

59.1 Storm Control Overview

This chapter introduces and shows you how to configure the storm control feature.

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.

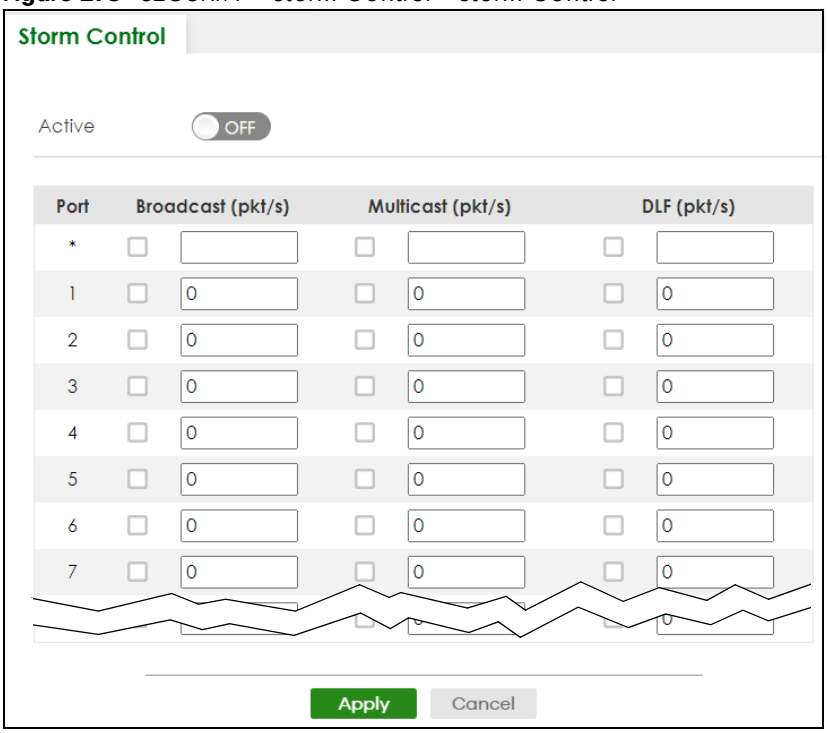
59.1.1 What You Can Do

Use the **Storm Control** screen (Section 59.2 on page 383) to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.

59.2 Storm Control Setup

Click **SECURITY** > **Storm Control** > **Storm Control** in the navigation panel to display the screen as shown next.

Figure 278 SECURITY > Storm Control > Storm Control



The following table describes the labels in this screen.

Table 213 SECURITY > Storm Control > Storm Control

LABEL	DESCRIPTION
Active	Enable the switch button to enable traffic storm control on the Switch. Disable the switch button to disable this feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
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.

CHAPTER 60
Error-Disable

60.1 Error-Disable Overview

This chapter shows you how to configure the rate limit for control packets on a port, and set the Switch to take an action (such as to shut down a port or stop sending packets) on a port when the Switch detects a pre-configured error. It also shows you how to configure the Switch to automatically undo the action after the error is gone.

60.1.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other networks. You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

60.1.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the ports loop back to the Switch, the Switch can shut down the ports automatically. After that, you need to enable the ports or allow the packets on a port manually through the Web Configurator or the commands. With error-disable recovery, you can set the disabled ports to become active or start receiving the packets again after the time interval you specify.

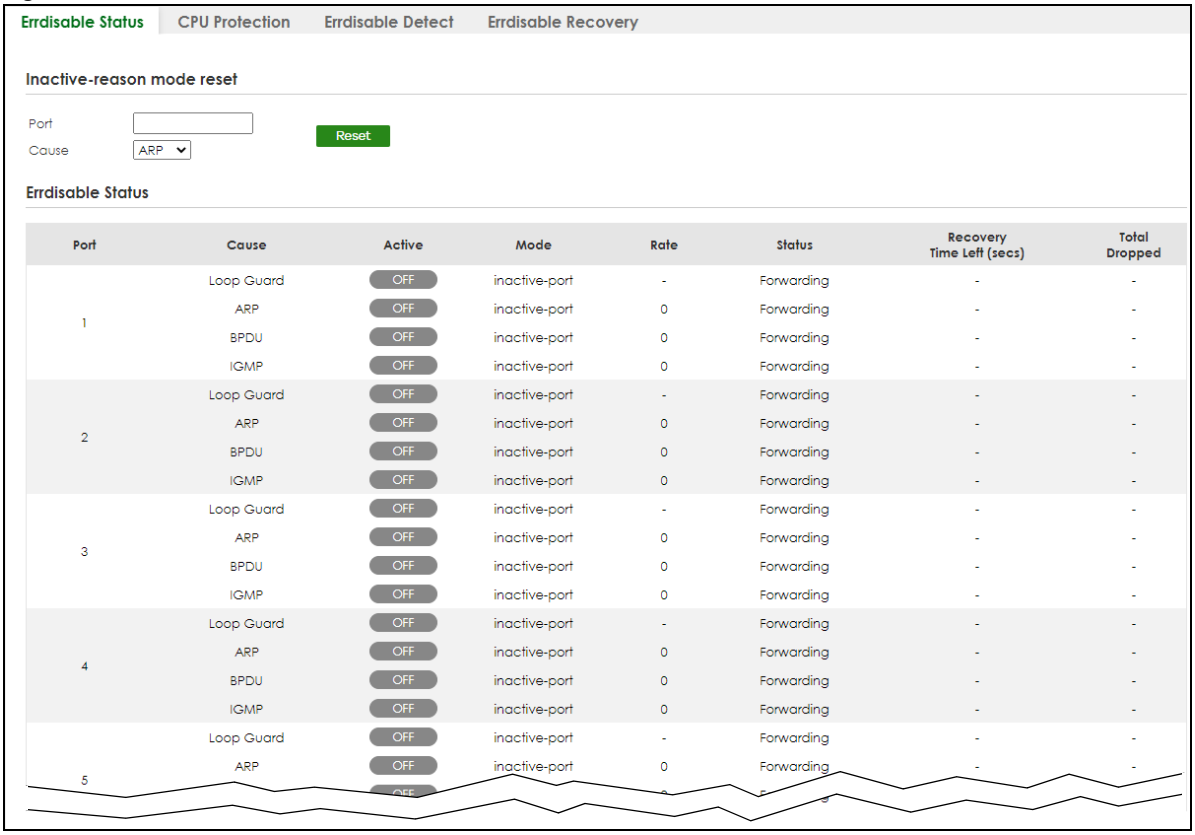
60.1.3 What You Can Do

- Use the **Errdisable Status** screen (Section 60.2 on page 386) to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information.
- Use the **CPU Protection** screen (Section 60.3 on page 387) to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
- Use the **Errdisable Detect** screen (Section 60.4 on page 388) to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
- Use the **Errdisable Recovery** screen (Section 60.5 on page 389) to set the Switch to automatically undo an action after the error is gone.

60.2 Error-Disable Status

Use this screen to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information. Click **SECURITY** > **Errdisable** > **Errdisable Status** to display the screen as shown.

Figure 279 SECURITY > Errdisable > Errdisable Status



The following table describes the labels in this screen.

Table 214 SECURITY > Errdisable > Errdisable Status

LABEL	DESCRIPTION
Inactive-reason mode reset	
Port	Enter the number of the ports (separated by a comma) on which you want to reset inactive-reason status.
Cause	Select the cause of inactive-reason mode you want to reset here.
Reset	Click to reset the specified ports to handle ARP, BPDU or IGMP packets instead of ignoring them, if the ports is in inactive-reason mode.
Errdisable Status	
Port	This is the number of the port on which you want to configure Errdisable Status.
Cause	This displays the type of the control packet received on the port or the feature enabled on the port and causing the Switch to take the specified action.
Active	This field displays whether the control packets (ARP, BPDU, and/or IGMP) on the port is being detected or not. It also shows whether loop guard is enabled on the port.

Table 214 SECURITY > Errdisable > Errdisable Status (continued)

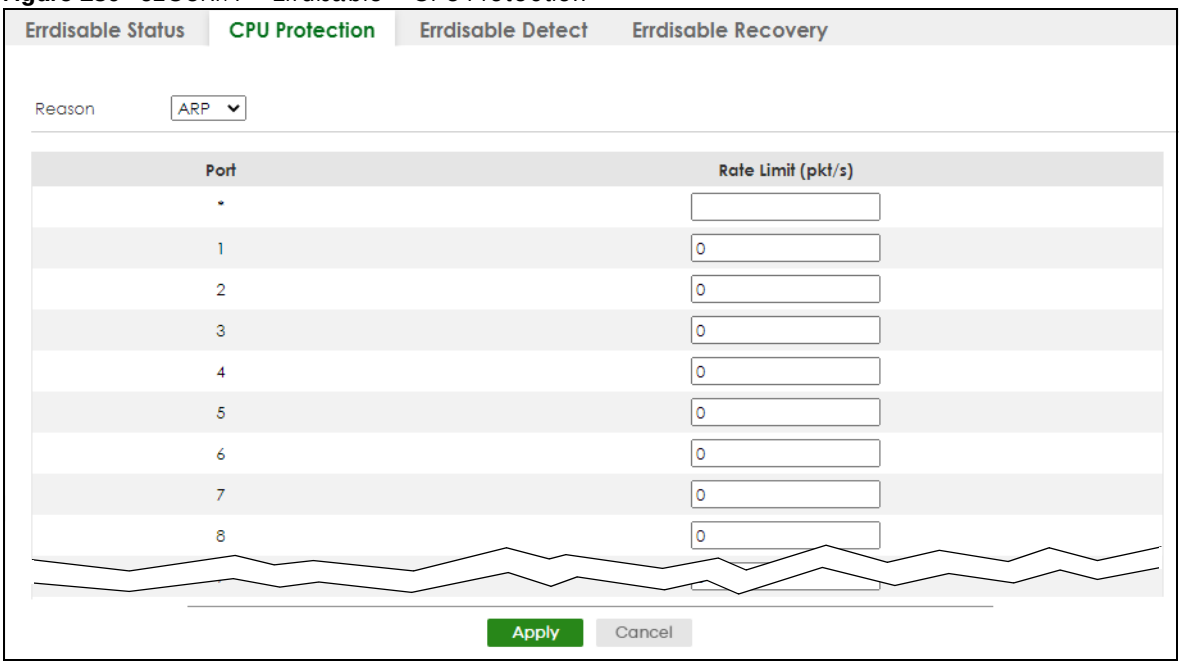
LABEL	DESCRIPTION
Mode	This field shows the action that the Switch takes for the cause. • **inactive-port** – The Switch disables the port. • **inactive-reason** – The Switch drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** – The Switch drops the additional control packets the ports has to handle in every one second.
Rate	This field displays how many control packets this port can receive or transmit per second. It can be adjusted in **CPU Protection**. **0** means no rate limit.
Status	This field displays the errdisable status. • **Forwarding**: The Switch is forwarding packets. Rate-limitation mode is always in **Forwarding** status. • **Err-disable**: The Switch disables the port on which the control packets are received (**inactive-port**) or drops specified control packets on the port (**inactive-reason**).
Recovery Time Left (secs)	This field displays the time (seconds) left before the ports becomes active of Errdisable Recovery.
Total Dropped	This field displays the total packet number dropped by this port where the packet rate exceeds the rate of mode rate-limitation.

60.3 CPU Protection Setup

Use this screen to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port. Click **SECURITY** > **Errdisable** > **CPU Protection** to display the screen as shown.

Note: After you configure this screen, make sure you also enable error detection for the specific control packets in the **SECURITY** > **Errdisable** > **Errdisable Detect** screen.

Figure 280 SECURITY > Errdisable > CPU Protection



The following table describes the labels in this screen.

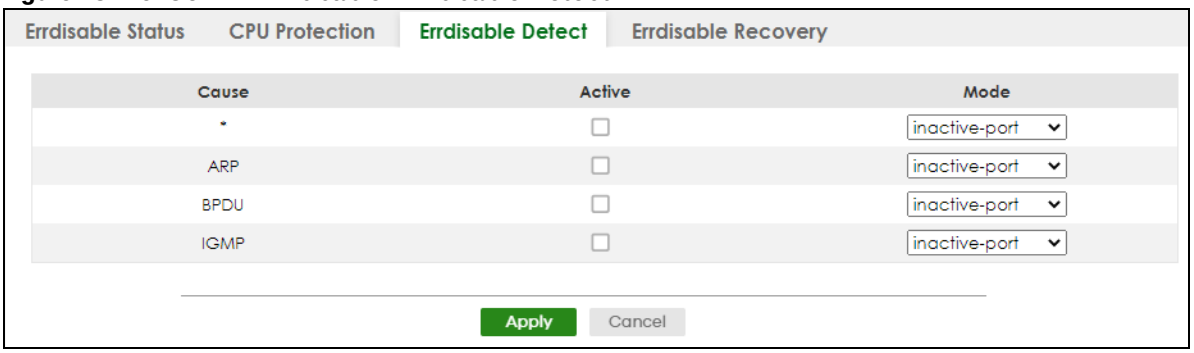
Table 215 SECURITY > Errdisable > CPU Protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. **0** means no rate limit. You can configure the action that the Switch takes when the limit is exceeded.
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.

60.4 Error-Disable Detect Setup

Use this screen to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click **SECURITY** > **Errdisable** > **Errdisable Detect** to display the screen as shown.

Figure 281 SECURITY > Errdisable > Errdisable Detect



The following table describes the labels in this screen.

Table 216 SECURITY > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.

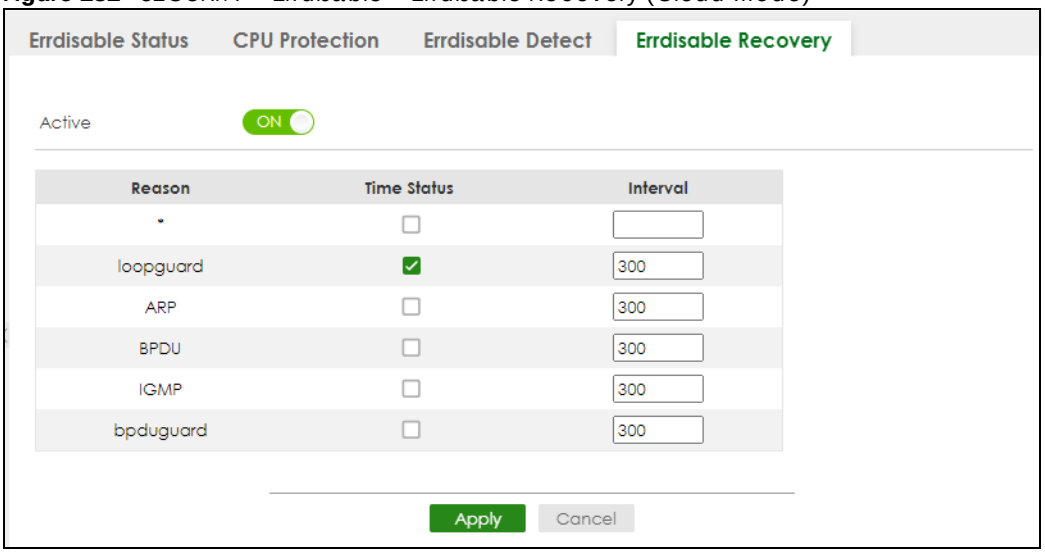
Table 216 SECURITY > Errdisable > Errdisable Detect (continued)

LABEL	DESCRIPTION
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the **SECURITY** > **Errdisable** > **CPU Protection** screen. • **inactive-port** – The Switch disables the port on which the control packets are received. • **inactive-reason** – The Switch drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** – The Switch drops the additional control packets the ports has to handle in every one second.
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.

60.5 Error-Disable Recovery Setup

Use this screen to configure the Switch to automatically undo an action after the error is gone. Click **SECURITY** > **Errdisable** > **Errdisable Recovery** to display the screen as shown.

Figure 282 SECURITY > Errdisable > Errdisable Recovery (Cloud Mode)



The following table describes the labels in this screen.

Table 217 SECURITY > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Enable the switch button to turn on the error-disable recovery function on the Switch.
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.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.

Table 217 SECURITY > Errdisable > Errdisable Recovery (continued)

LABEL	DESCRIPTION
Time Status	Select this checkbox 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. Clear the checkbox to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
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.

CHAPTER 61
IP Source Guard

61.1 IP Source Guard Overview

IP source guard consists of the following features:

- DHCP snooping. Use this to filter unauthorized DHCP server packets on the network and to build a binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.
- Static IP bindings. Use this to create static bindings in the binding table.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

Binding Table

IP source guard uses a binding table to distinguish between authorized and unauthorized ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

DHCP Snooping

The Switch only allows an authorized DHCP server on a trusted port to assign IP addresses. Unauthorized DHCP servers will not be able to assign IP addresses to network clients. When the Switch receives a DHCP server packet from an authorized DHCP server, it inspects the packet and records the DHCP information in a binding table. The binding records are used in ARP inspection to filter unauthorized ARP packets. See Section 62.1 on page 396 for more DHCP snooping information.

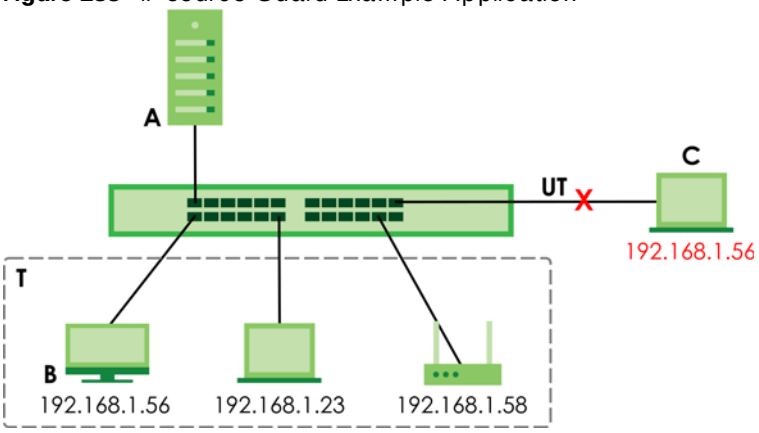
ARP Inspection

When the Switch receives an ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. Otherwise, the Switch discards the packet.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

The following figure demonstrates a scenario with DHCP snooping and ARP inspection enabled. In this scenario, we connect an authorized DHCP server (**A**) and the client devices on the ARP trusted ports (**T**). A client device (**B**) is assigned the IP address 192.168.1.56 by the authorized DHCP server (**A**). A malicious host (**C**) on an untrusted port (**UT**) puts a wrong MAC address with the IP address 192.168.1.56 in an ARP reply packet pretending to be client device (**B**) (192.168.1.56). The Switch snoops DHCP packets sent from the authorized DHCP server (**A**) and creates bindings in the binding table. When the Switch receives ARP packets from an untrusted port (**UT**), it compares the IP and MAC addresses with the existing bindings. Since the IP and MAC binding is different from the existing bindings, the Switch blocks the unauthorized ARP packets sent from the malicious host (**C**). The malicious host (**C**) therefore cannot disguise as client device (**B**) to build connections with other client devices on your network.

Figure 283 IP Source Guard Example Application



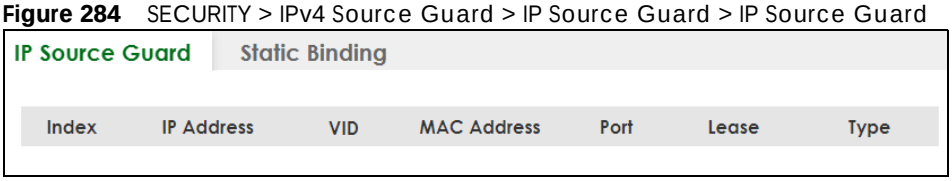
61.1.1 What You Can Do

- Use the **IP Source Guard** screen (Section 61.2 on page 392) to look at the current bindings for DHCP snooping and ARP inspection.
- Use the **Static Binding** screen (Section 61.3 on page 393) to manage static bindings for DHCP snooping and ARP inspection.

61.2 IPv4 Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by ARP inspection to distinguish between authorized and unauthorized ARP packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **SECURITY** > **IPv4 Source Guard** > **IP Source Guard** > **IP Source Guard**.

Figure 284 SECURITY > IPv4 Source Guard > IP Source Guard > IP Source Guard



The following table describes the labels in this screen.

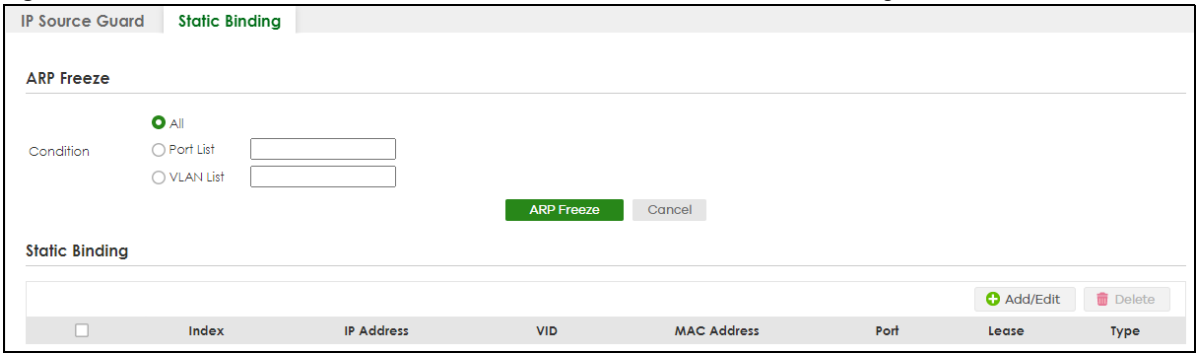
Table 218 SECURITY > IPv4 Source Guard > IP Source Guard > IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
VID	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator. **dhcp-snooping**: This binding was learned by snooping DHCP packets.

61.3 IPv4 Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **SECURITY** > **IPv4 Source Guard** > **IP Source Guard** > **Static Binding**.

Figure 285 SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding



The following table describes the labels in this screen.

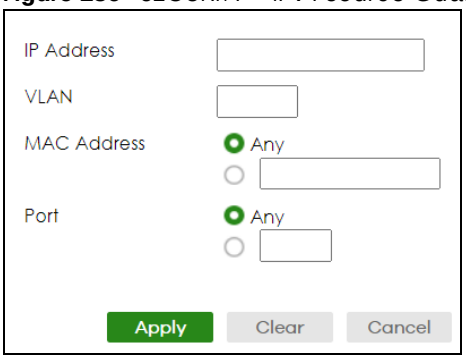
Table 219 SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding

LABEL	DESCRIPTION
ARP Freeze ARP Freeze allows you to automatically create static bindings from the current ARP entries (either dynamically learned or static ARP entries) until the Switch's binding table is full. Note: The ARP learning mode should be set to **ARP-Request** in the **NETWORKING** > **ARP Setup** > **ARP Learning** screen before you use the ARP Freeze feature.	
Condition	**All** – Select this and click **ARP Freeze** to have the Switch automatically add all the current ARP entries to the static bindings table. **Port List** – Select this and enter the number of the ports (separated by a comma). You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. ARP entries learned on the specified ports are added to the static bindings table after you click **ARP Freeze**. **VLAN List** – Select this and enter the ID number of the VLANs (separated by a comma). ARP entries for the specified VLANs are added to the static bindings table after you click **ARP Freeze**.
Static Binding	
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This field displays a sequential number for each binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
VID	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address in the binding.
Port	This field displays the port number.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. **Static**: This binding was learned from information provided manually by an administrator.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

61.3.1 Add/Edit IPv4 Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY** > **IPv4 Source Guard** > **IP Source Guard** > **Static Binding** screen to display this screen.

Figure 286 SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding > Add/Edit



The following table describes the labels in this screen.

Table 220 SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding > Add/Edit

LABEL	DESCRIPTION
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
MAC Address	Enter the source MAC address in the binding. If this binding applies to all MAC addresses, select **Any**.
Port	Specify the ports in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select **Any**.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

CHAPTER 62
DHCP Snooping

62.1 DHCP Snooping Overview

DHCP snooping filters unauthorized DHCP server packets. The Switch allows only the authorized DHCP server on a trusted port to assign IP addresses. Clients on your network will only receive DHCP packets from the authorized DHCP server.

The Switch also builds a DHCP snooping binding table dynamically by snooping DHCP packets (dynamic bindings). A DHCP snooping binding table contains the IP binding information the Switch learns from DHCP packets in your network. A binding contains these key attributes:

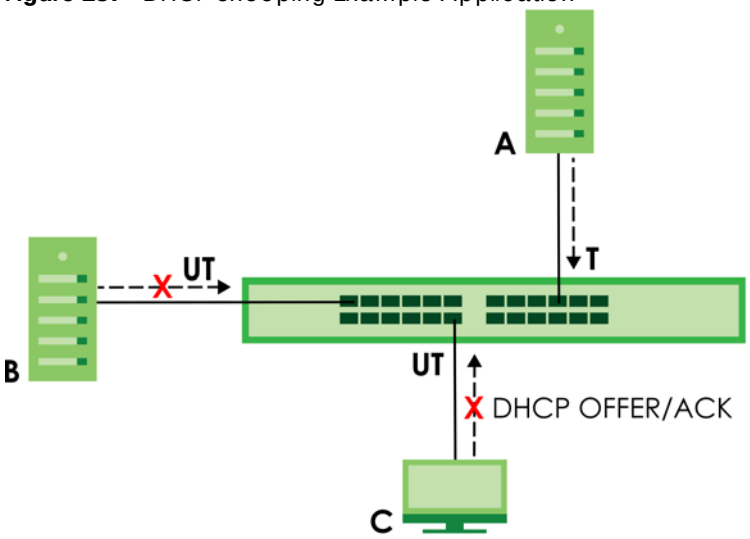
- MAC address
- VLAN ID
- IP address
- Port number

The following settings demonstrates DHCP snooping on the Switch.

- An authorized DHCP server (**A**) on a snooped VLAN from the trusted port (**T**)
- An unauthorized DHCP server (**B**) on a snooped VLAN from an untrusted port (**UT**)
- DHCP clients (**C**) on the untrusted ports (**UT**).

With DHCP snooping, the Switch blocks all DHCP server packets (**DHCP OFFER/ACK**) coming from the untrusted ports (**UT**). The Switch only forwards the DHCP server packets from the trusted port (**T**). This assures that DHCP clients on your network only receive IP addresses assigned by the authorized DHCP server (**A**).

Figure 287 DHCP Snooping Example Application



62.1.1 What You Can Do

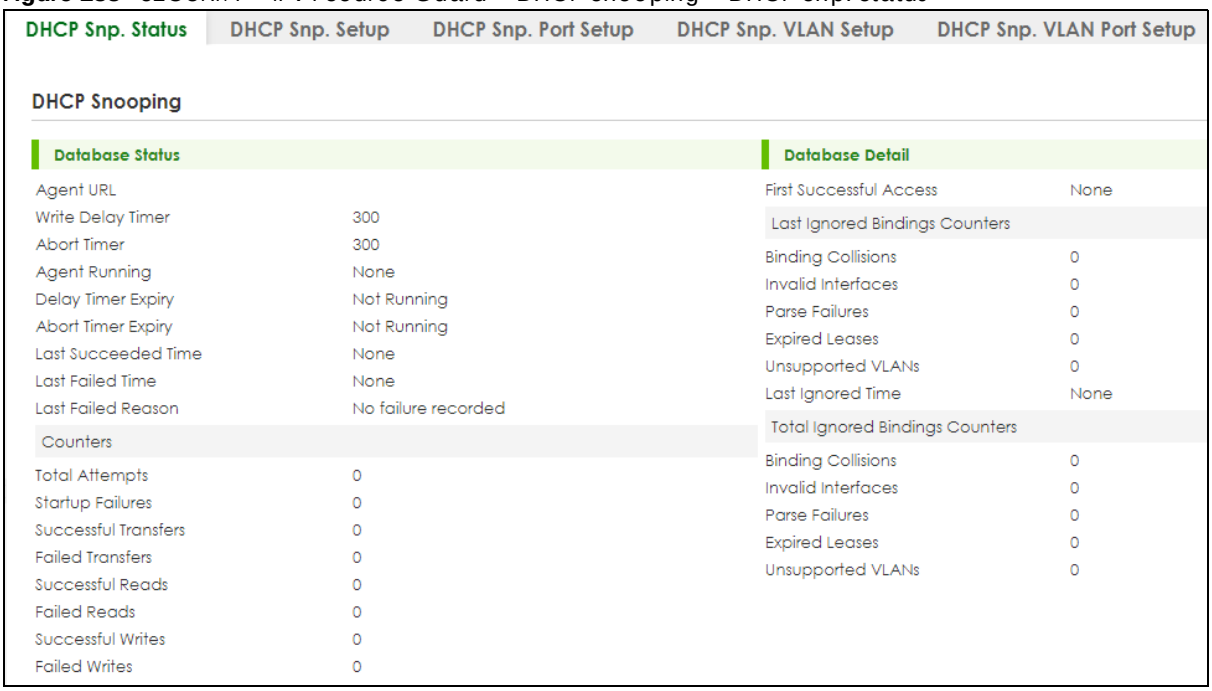
- Use the **DHCP Snooping Status** screen (Section 62.2 on page 397) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Setup** screen (Section 62.3 on page 400) to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database.
- Use the **DHCP Snooping Port Setup** screen (Section 62.4 on page 401) to specify whether ports are trusted or untrusted ports for DHCP snooping.
- Use the **DHCP Snooping VLAN Setup** screen (Section 62.5 on page 403) to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.
- Use the **DHCP Snooping VLAN Port Setup** screen (Section 62.6 on page 404) to apply a different DHCP option 82 profile to certain ports in a VLAN.

62.2 DHCP Snooping Status

Use this screen to look at various statistics about the DHCP snooping database.

To open this screen, click **SECURITY** > **IPv4 Source Guard** > **DHCP Snooping** > **DHCP Snp. Status**.

Figure 288 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status



The following table describes the labels in this screen.

Table 221 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status

LABEL	DESCRIPTION
Database Status This section displays the current settings for the DHCP snooping database. You can configure them in the **SECURITY** > **DHCP Snooping** > **DHCP Snp. Setup** screen.	
Agent URL	This field displays the location of the DHCP snooping database.
Write Delay Timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort Timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
Agent Running	This field displays the status of the current update or access of the DHCP snooping database. **None**: The Switch is not accessing the DHCP snooping database. **Read**: The Switch is loading dynamic bindings from the DHCP snooping database. **Write**: The Switch is updating the DHCP snooping database.
Delay Timer Expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays **Not Running** if the Switch is not updating the DHCP snooping database right now.
Abort Timer Expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays **Not Running** if the current bindings have not changed since the last update.
Last Succeeded Time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last Failed Time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.

Table 221 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status (continued)

LABEL	DESCRIPTION
Last Failed Reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
Counters This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.	
Total Attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup Failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful Transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed Transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful Reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed Reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.
Successful Writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.
Failed Writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database Detail	
First Successful Access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.
Last Ignored Bindings Counters This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch.	
Binding Collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid Interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.
Parse Failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired Leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported VLANs	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last Ignored Time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total Ignored Bindings Counters This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch.	
Binding Collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid Interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.

Table 221 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status (continued)

LABEL	DESCRIPTION
Parse Failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired Leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported VLANs	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

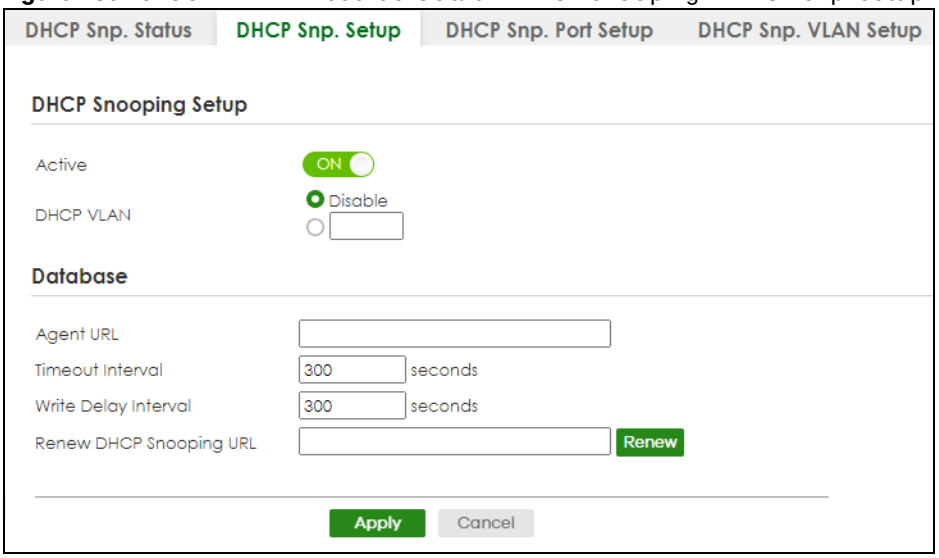
62.3 DHCP Snooping Setup

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are still available after a restart.

To open this screen, click **SECURITY** > **IPv4 Source Guard** > **DHCP Snooping** > **DHCP Snp. Setup**.

Note: The input string of any field in this screen should not contain [?], [|], ['], ["], or [,].

Figure 289 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup



The following table describes the labels in this screen.

Table 222 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup

LABEL	DESCRIPTION
DHCP Snooping Setup	
Active	Enable the switch button to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Table 222 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup (continued)

LABEL	DESCRIPTION
DHCP VLAN	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable **Option 82 Profile** in the **SECURITY** > **DHCP Snooping** > **DHCP Snp. VLAN Setup** screen to help the DHCP servers distinguish between DHCP requests from different VLAN. Select **Disable** if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database If **Timeout Interval** is greater than **Write Delay Interval**, it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.	
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: **tftp://{domain name or IP address}/directory, if applicable/file name**; for example, **tftp://192.168.10.1/database.txt**. You can enter up to 256 printable ASCII characters except [?], [|], ['], ["], or [,].
Timeout Interval	Enter how long (10 – 65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Write Delay Interval	Enter how long (10 – 65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click **Renew** if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in **Agent URL**. When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the **Binding Collisions** counter in the **DHCP Snooping Status** screen (Section 62.2 on page 397).
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 this to reset the values in this screen to their last-saved values.

62.4 DHCP Snooping Port Setup

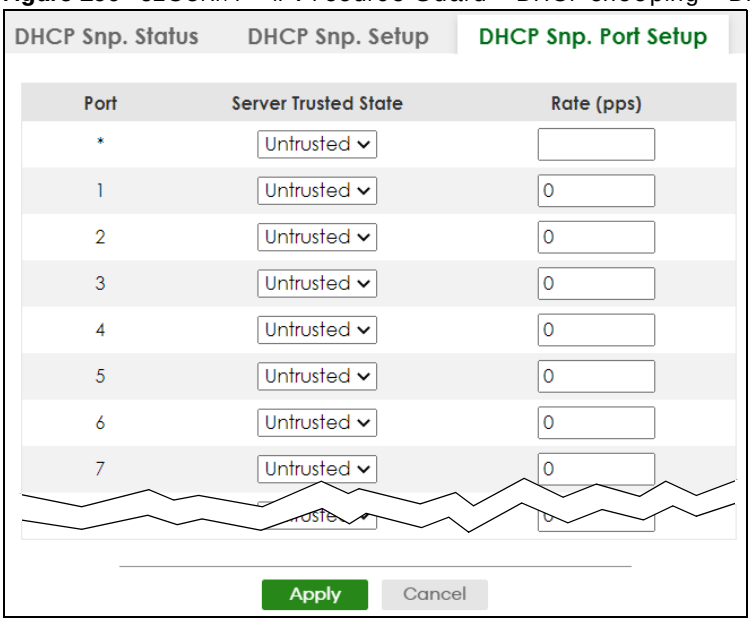
Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: If DHCP snooping is enabled but there are no trusted ports, DHCP requests cannot reach the DHCP server.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

To open this screen, click **SECURITY** > **IPv4 Source Guard** > **DHCP Snooping** > **DHCP Snp. Port Setup**.

Figure 290 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup



The following table describes the labels in this screen.

Table 223 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup

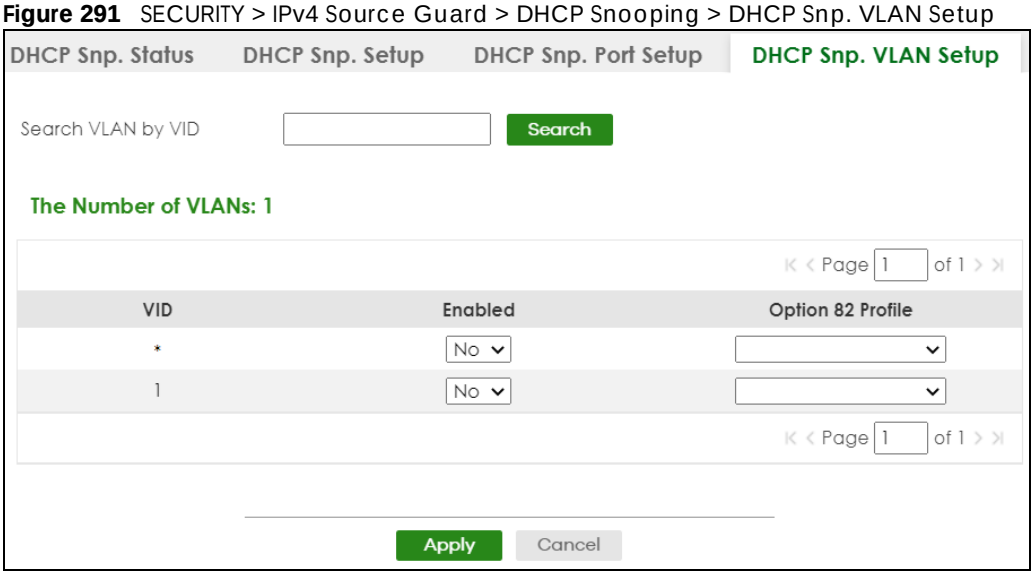
LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Server Trusted state	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations: • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1 – 2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
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 this to reset the values in this screen to their last-saved values.

62.5 DHCP Snooping VLAN Setup

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.

To open this screen, click **SECURITY** > **IPv4 Source Guard** > **DHCP Snooping** > **DHCP Snp. VLAN Setup**.

Figure 291 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Setup



The following table describes the labels in this screen.

Table 224 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Setup

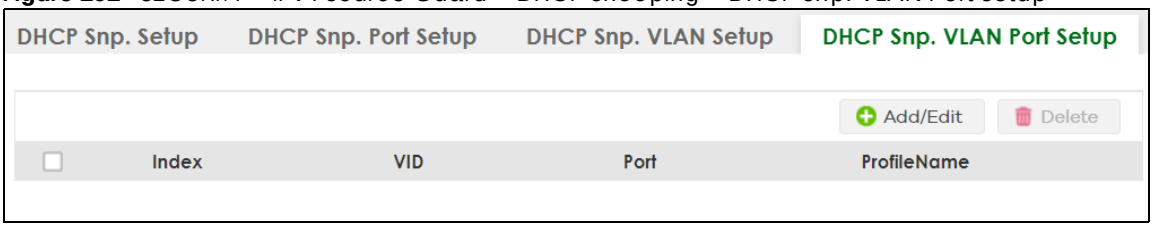
LABEL	DESCRIPTION
Search VLAN by VID	Enter the VLAN ID you want to manage. Use a comma (,) to separate individual VLANs or a hyphen (-) to indicates a range of VLANs. For example, “3,4” or “3-9”.
Search	Click this to display the specified range of VLANs in the section below.
The Number of VLANs	This displays the number of VLAN search results.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in the specified VLANs. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **SECURITY** > **DHCP Snooping** > **DHCP Snp. Setup** screen.
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 this to reset the values in this screen to their last-saved values.

62.6 DHCP Snooping VLAN Port Setup

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN.

To open this screen, click **SECURITY** > **IPv4 Source Guard** > **DHCP Snooping** > **DHCP Snp. VLAN Port Setup**.

Figure 292 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup



The following table describes the labels in this screen.

Table 225 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup

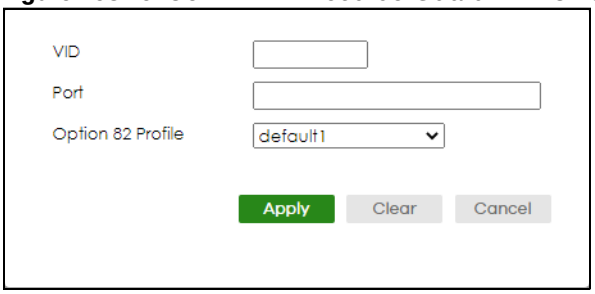
LABEL	DESCRIPTION
Index	This field displays a sequential number for each entry.
VID	This field displays the VLAN to which the ports belongs.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports.
Add/Edit	Click **Add/Edit** to add a new entry or edit a selected one.
Delete	Click **Delete** to remove the selected entries.

62.6.1 Add/EDIT DHCP Snooping VLAN Ports

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY** > **IPv4 Source Guard** > **DHCP Snooping** > **DHCP Snp. VLAN Port Setup** screen to display this screen.

Figure 293 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup > Add/Edit



The following table describes the labels in this screen.

Table 226 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup > Add/Edit

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in this VLAN. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **SECURITY** > **DHCP Snooping** > **DHCP Snp. Setup** screen. Note: The profile you select here has priority over the one you select in the **SECURITY** > **DHCP Snooping** > **DHCP Snp. VLAN Setup** screen.
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.
Clear	Click **Clear** to clear the fields to the factory defaults.
Cancel	Click **Cancel** to not save the configuration you make and return to the last screen.

62.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

62.7.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

62.7.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted or untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The rate at which DHCP packets arrive is too high.

62.7.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 294 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-..-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

62.7.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings.

62.7.1.4 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.

3 Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.

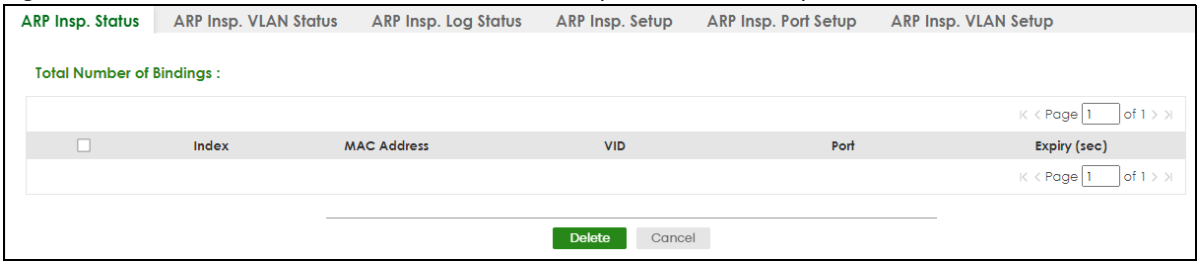
4 Configure static bindings.

CHAPTER 63
ARP Inspection

63.1 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. Status**.

Figure 295 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Status



The following table describes the labels in this screen.

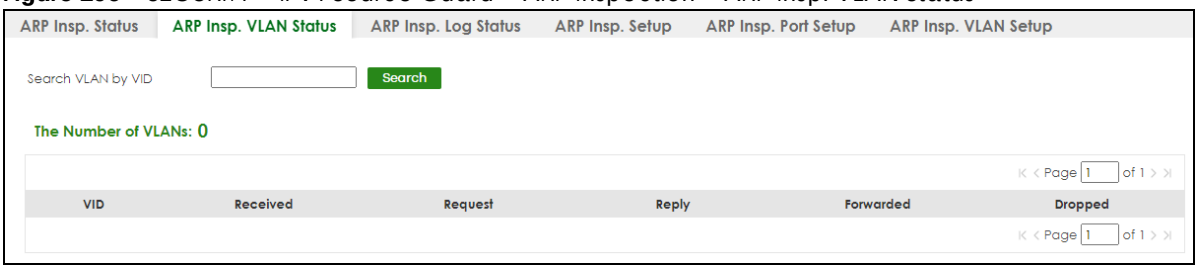
Table 227 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Status

LABEL	DESCRIPTION
Total Number of Bindings	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the **Delete** checkboxes above.

63.2 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. VLAN Status**.

Figure 296 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Status



The following table describes the labels in this screen.

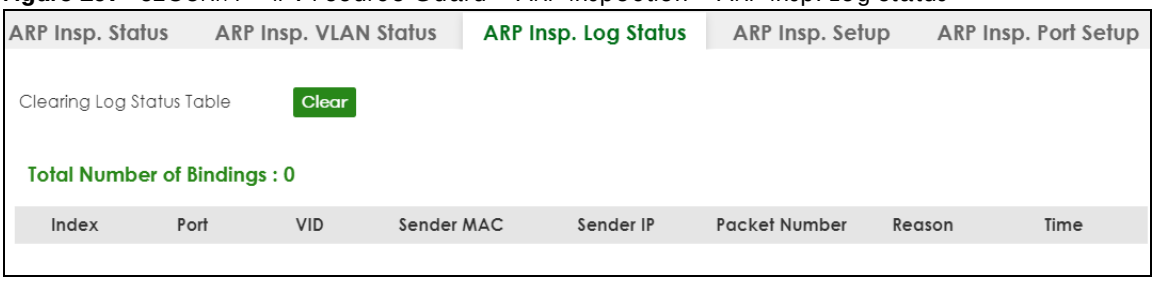
Table 228 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Status

LABEL	DESCRIPTION
Search VLAN by VID	Specify the VLANs you want to view in the section below. Use a comma (,) to separate individual VLANs or a hyphen (-) to indicates a range of VLANs. For example, “3,4” or “3-9”.
Search	Click this to display the specified range of VLANs in the section below.
The Number of VLANs	This is the number of VLANs that match the searching criteria and display in the list below. The number displays when you use the **Search** button to look for certain VLANs. The default value is 0.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

63.3 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. Log Status**.

Figure 297 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Log Status



The following table describes the labels in this screen.

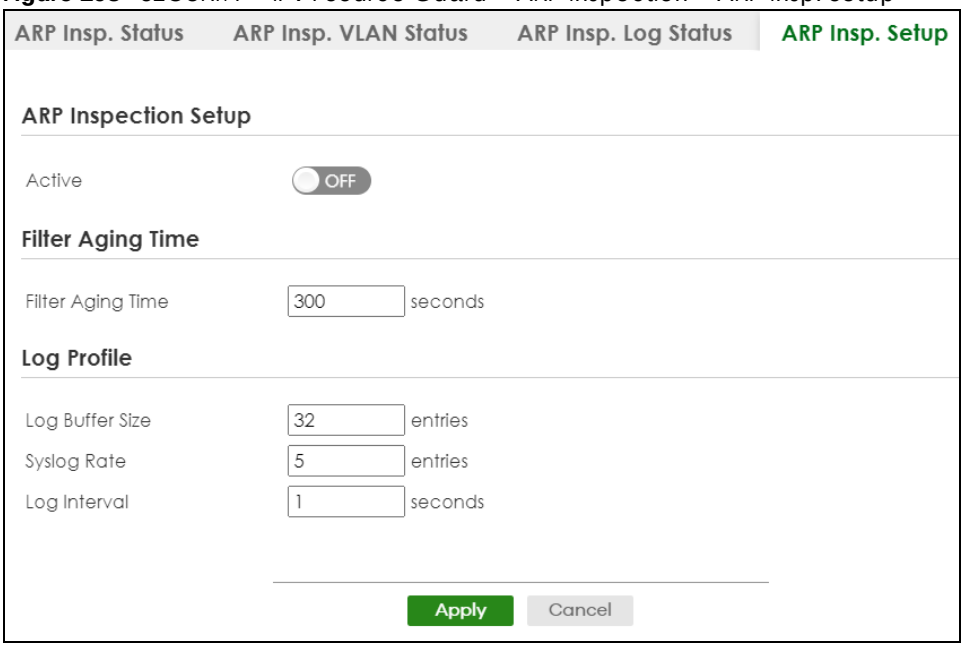
Table 229 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Log Status

LABEL	DESCRIPTION
Clearing Log Status Table	Click **Clear** to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of Bindings	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called **overflow** with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Packet Number	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. Setup** screen.
Reason	This field displays the reason the log message was generated. **dhcp deny**: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **dhcp permit**: An ARP packet was forwarded because it matched a dynamic binding. **static permit**: An ARP packet was forwarded because it matched a static binding. In the **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. VLAN Setup** screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet.
Time	This field displays when the log message was generated.

63.4 ARP Inspection Setup

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. Setup**.

Figure 298 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup



The following table describes the labels in this screen.

Table 230 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup

LABEL	DESCRIPTION
ARP Inspection Setup	
Active	Enable the switch button to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter Aging Time	This setting has no effect on existing MAC address filters. Enter how long (1 – 2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Type 0 if you want the MAC address filter to be permanent.
Log Profile	
Log Buffer Size	Enter the maximum number (1 – 1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified **Syslog Rate** and **Log Interval**. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click **Clearing Log Status Table** in the **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. Log Status** screen to clear the log and reset this counter.
Syslog Rate	Type the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the **Log Interval**. You must configure the syslog server to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between **Syslog Rate** and **Log Interval** is illustrated in the following examples: • Four invalid ARP packets per second, **Syslog Rate** is 5, **Log Interval** is 1: the Switch sends 4 syslog messages every second. • Six invalid ARP packets per second, **Syslog Rate** is 5, **Log Interval** is 2: the Switch sends 5 syslog messages every 2 seconds.

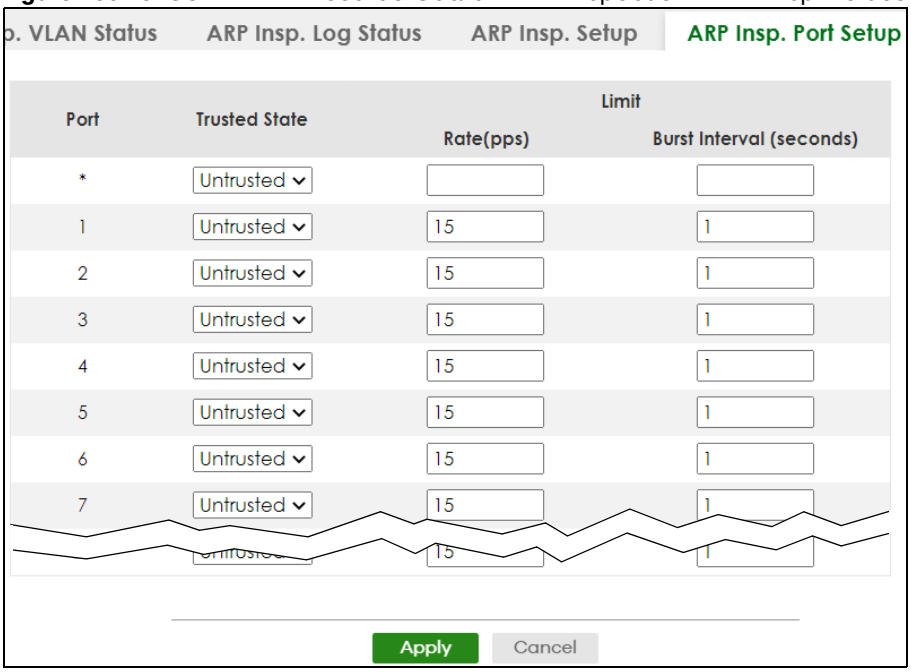
Table 230 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup (continued)

LABEL	DESCRIPTION
Log interval	Type how often (1 – 86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See **Syslog Rate** for an example of the relationship between **Syslog Rate** and **Log Interval**.
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 this to reset the values in this screen to their last-saved values.

63.5 ARP Inspection Port Setup

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To open this screen, click **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. Port Setup**.

Figure 299 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup



The following table describes the labels in this screen.

Table 231 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

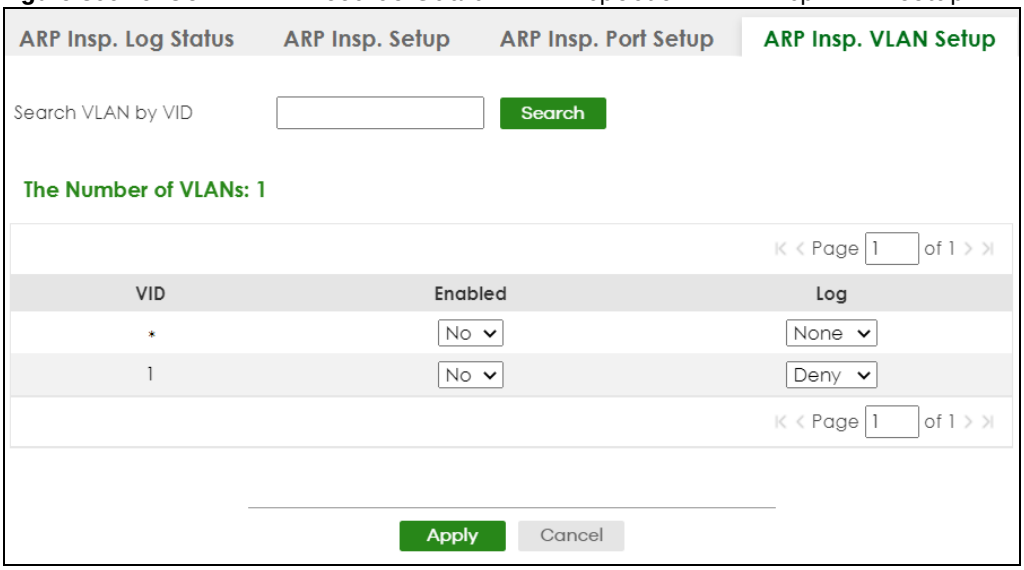
Table 231 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup (continued)

LABEL	DESCRIPTION
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	Rate and Burst Interval settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1 – 2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.
Burst Interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1 – 15 seconds) of the burst interval.
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 this to reset the values in this screen to their last-saved values.

63.6 ARP Inspection VLAN Setup

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **SECURITY** > **IPv4 Source Guard** > **ARP Inspection** > **ARP Insp. VLAN Setup**.

Figure 300 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Setup



The following table describes the labels in this screen.

Table 232 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Setup

LABEL	DESCRIPTION
Search VLAN by VID	Specify the VLANs you want to manage in the section below. Use a comma (,) to separate individual VLANs or a hyphen (-) to indicates a range of VLANs. For example, “3,4” or “3-9”.
Search	Click this to display the specified range of VLANs in the section below.
The Number of VLANs	This display the number of ARP inspection VLAN search results.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable ARP inspection on the VLAN. Select **No** to disable ARP inspection on the VLAN.
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. **None**: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. **Deny**: The Switch generates log messages when it discards an ARP packet from the VLAN. **Permit**: The Switch generates log messages when it forwards an ARP packet from the VLAN. **All**: The Switch generates log messages every time it receives an ARP packet from the VLAN.
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 this to reset the values in this screen to their last-saved values.

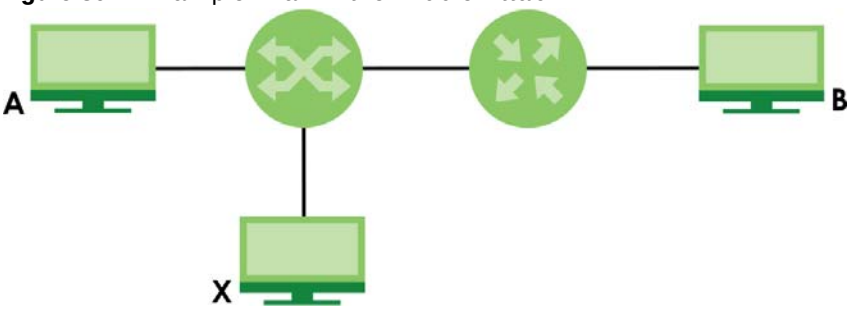
63.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

63.7.1 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 301 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

63.7.1.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters.

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

63.7.1.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted or untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

63.7.1.3 Syslog

The Switch can send syslog messages to the specified syslog server when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

63.7.1.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1. Configure DHCP snooping.

   Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

2. Enable ARP inspection on each VLAN.

3. Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

CHAPTER 64
Port Authentication

64.1 Port Authentication Overview

This chapter describes the IEEE 802.1x, MAC, and Guest VLAN authentication methods.

Port authentication is a way to validate access to ports on the Switch to clients based on an external authentication server. The Switch supports the following methods for port authentication:

- **IEEE 802.1x**[2] – An authentication server validates access to a port based on a user name and password provided by the user. A user that fails an authentication server can still access the port, but traffic from the user is forwarded to the guest VLAN port.
- **MAC Authentication** – An authentication server validates access to a port based on the MAC address and password of the client.
- **Guest VLAN** – In either mode, if authentication fails the Switch can still allow the client to access the network on a **Guest VLAN**.

Note: All types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. You must configure a RADIUS server before enabling port authentication.

Note: If you enable IEEE 802.1x authentication and MAC authentication on the same port, the Switch performs IEEE 802.1x authentication and MAC authentication. If a user fails to authenticate either through the IEEE 802.1x or MAC authentication method, then access to the port is denied.

Note: IEEE 802.1x is not supported by all user operating systems. For details on compatibility, see your operating system documentation. If your operating system does not support 802.1x, you must install 802.1x client software.

64.1.1 What You Can Do

- Use the **802.1x** screen (Section 64.2 on page 418) to activate IEEE 802.1x security.
- Use the **MAC Authentication** screen (Section 64.3 on page 419) to activate MAC authentication.
- Use the **Guest VLAN** screen (Section 64.4 on page 421) to enable and assign a guest VLAN to a port.

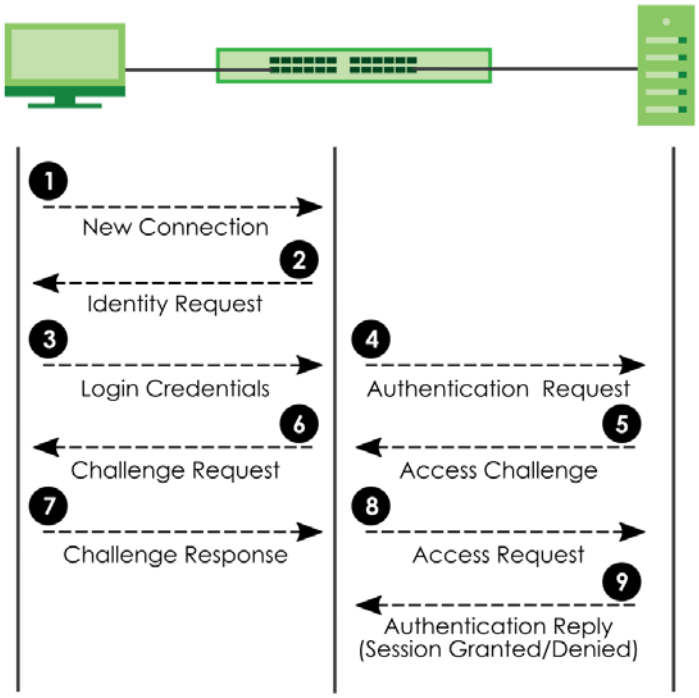
2. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

64.1.2 What You Need to Know

IEEE 802.1x Authentication

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password after the client responds to its identity request. When the client provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

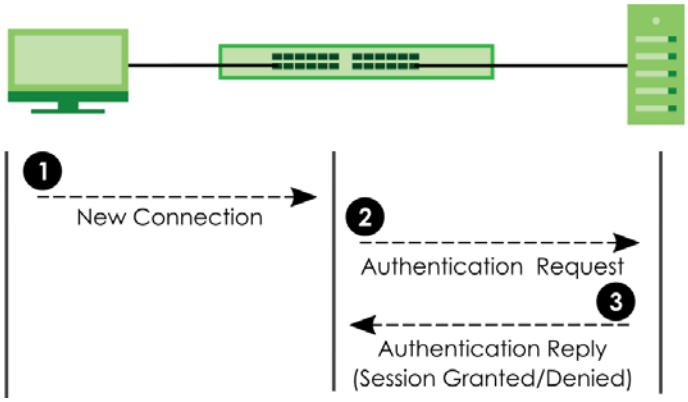
Figure 302 IEEE 802.1x Authentication Process



64.1.3 MAC Authentication

MAC authentication works in a very similar way to IEEE 802.1x authentication. The main difference is that the Switch does not prompt the client for login credentials. The login credentials are based on the source MAC address of the client connecting to a port on the Switch along with a password configured specifically for MAC authentication on the Switch.

Figure 303 MAC Authentication Process

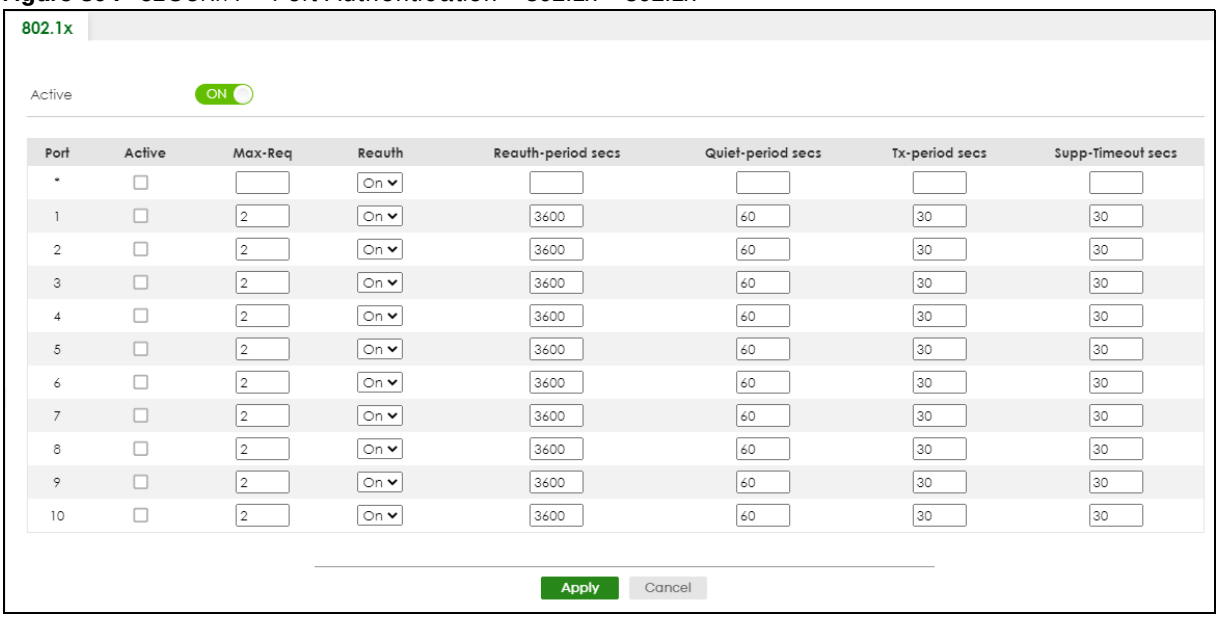


Note: To enable port authentication, first activate the port authentication methods (both on the Switch and the ports), then configure the RADIUS server settings in the **SECURITY**> **AAA** > **RADIUS Server Setup** > **RADIUS Server Setup** screen.

64.2 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. Click **SECURITY** > **Port Authentication** > **802.1x** > **802.1x** to display the configuration screen as shown.

Figure 304 SECURITY > Port Authentication > 802.1x > 802.1x



The following table describes the labels in this screen.

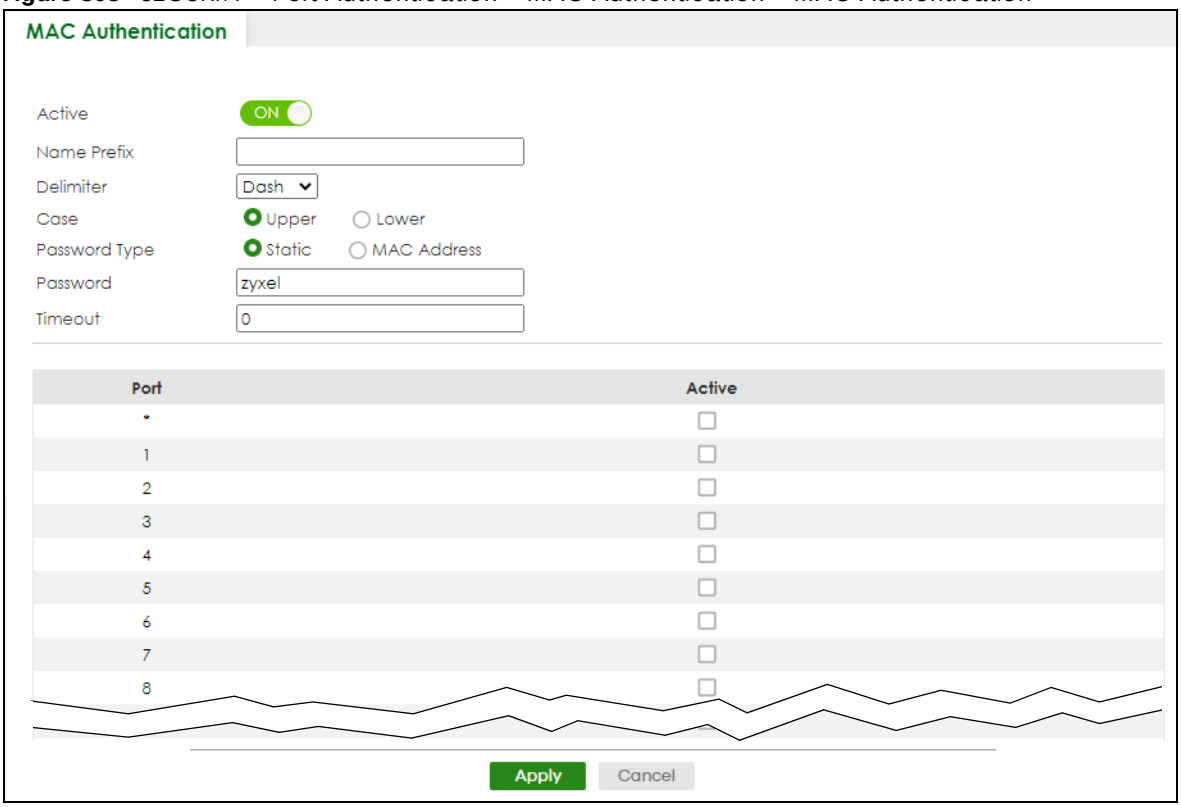
Table 233 SECURITY > Port Authentication > 802.1x > 802.1x

LABEL	DESCRIPTION
Active	Enable the switch button to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Max-Req	Specify the number of times the Switch tries to authenticate clients before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.
Reauth	Specify if a subscriber has to periodically re-enter his or her user name and password to stay connected to the port.
Reauth-period secs	Specify the length of time required to pass before a client has to re-enter his or her user name and password to stay connected to the port.
Quiet-period secs	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period secs	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout secs	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
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.

64.3 Activate MAC Authentication

Use this screen to activate MAC authentication. Click **SECURITY** > **Port Authentication** > **MAC Authentication** > **MAC Authentication** to display the configuration screen as shown.

Figure 305 SECURITY > Port Authentication > MAC Authentication > MAC Authentication



The following table describes the labels in this screen.

Table 234 SECURITY > Port Authentication > MAC Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	Enable the switch button to permit MAC authentication on the Switch. Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], [,]. If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Delimiter	Select the delimiter the RADIUS server uses to separate the pairs in MAC addresses used as the account user name (and password). You can select **Dash** (–), **Colon** (:), or **None** to use no delimiters at all in the MAC address.
Case	Select the case (**Upper** or **Lower**) the RADIUS server requires for letters in MAC addresses used as the account user name (and password).
Password Type	Select **Static** to have the Switch send the password you specify below or **MAC-Address** to use the client MAC address as the password.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].

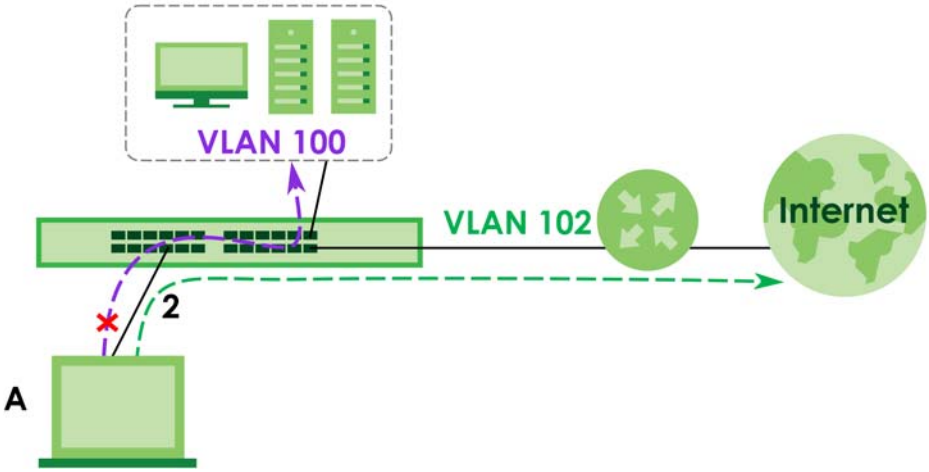
Table 234 SECURITY > Port Authentication > MAC Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
Timeout	Specify the amount of time (in seconds) before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds. When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, the Switch uses the **Aging Time** configured in the **SYSTEM** > **Switch Setup** > **Switch Setup** screen. Note: If the **Aging Time** in the **SYSTEM** > **Switch Setup** > **Switch Setup** screen is set to a lower value, then it supersedes this setting.
Port	This field displays a port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
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.

64.4 Guest VLAN

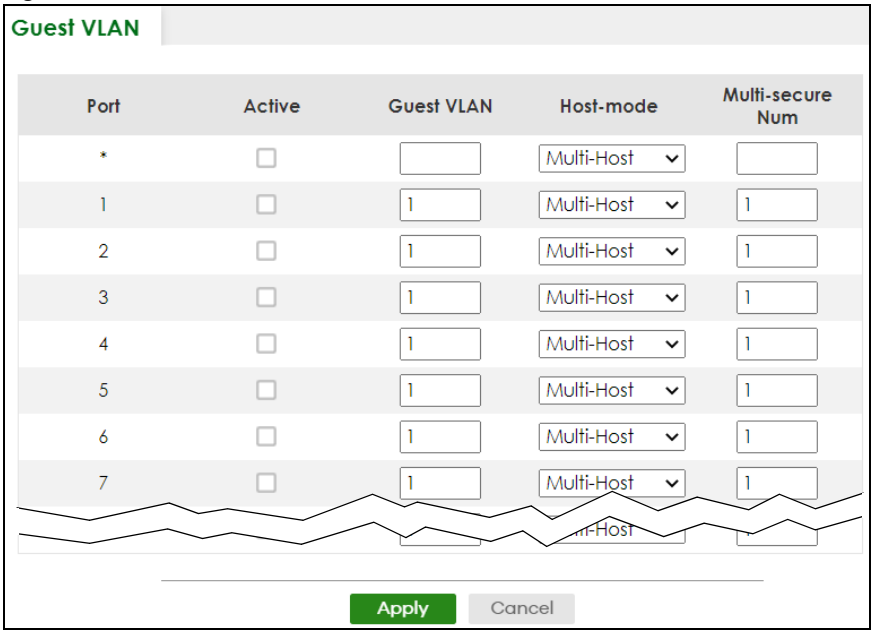
When 802.1x or MAC Authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the ports. You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in the example), the user (**A** in the example) that is not IEEE 802.1x capable or fails to enter the correct user name 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 access granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 306 Guest VLAN Example



Use this screen to enable and assign a guest VLAN to a port. Click **SECURITY** > **Port Authentication** > **Guest VLAN** > **Guest VLAN** to display the configuration screen as shown.

Figure 307 SECURITY > Port Authentication > Guest VLAN > Guest VLAN



The following table describes the labels in this screen.

Table 235 SECURITY > Port Authentication > Guest VLAN > Guest VLAN

LABEL	DESCRIPTION
Port	This field displays a port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.
Guest VLAN	A guest VLAN is a pre-configured VLAN on the Switch that allows non-authenticated users to access limited network resources through the Switch. You must also enable IEEE 802.1x authentication on the Switch and the associated ports. Enter the number that identifies the guest VLAN. Make sure this is a VLAN recognized in your network.
Host-mode	Specify how the Switch authenticates users when more than one user connect to the port (using a hub). Select **Multi-Host** to authenticate only the first user that connects to this port. If the first user enters the correct credential, any other users are allowed to access the port without authentication. If the first user fails to enter the correct credential, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, the rest of the users are blocked until a user does the authentication process again. Select **Multi-Secure** to authenticate each user that connects to this port.
Multi-secure Num	If you set **Host-mode** to **Multi-Secure**, specify the maximum number of users (between 1 and 5) that the Switch will authenticate on this port.

Table 235 SECURITY > Port Authentication > Guest VLAN > Guest VLAN (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.

64.5 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

64.5.1 IEEE 802.1x

The IEEE 802.1x is a standard for authentication as well as providing additional accounting and control features. It can be implemented both on wired and wireless networks. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the switch or the wired clients.

64.5.2 RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The RADIUS server handles the following tasks:

- Authentication

Determines the identity of the users.

- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting

Keeps track of the actions that are perform on the switch, such as login events.

RADIUS is a simple package exchange in which your switch acts as a message relay between the wired client and the network RADIUS server.

64.5.2.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the switch and the RADIUS server for user authentication:

- Access-Request

Sent by a switch requesting authentication.

- Access-Reject

Sent by a RADIUS server rejecting access.

- Access-Accept

Sent by a RADIUS server allowing access.

- Access-Challenge

Sent by a RADIUS server requesting more information in order to allow access. The switch sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the switch and the RADIUS server for user accounting:

- Accounting-Request

Sent by the switch requesting accounting.

- Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

The switch and the RADIUS server use a shared secret key, which is a password, they both know to authenticate the communications between them, and ensure network security. A shared key is not sent over the network.

The switch forwards the RADIUS requests of a client to the RADIUS server. The login password information exchanged is sent over the network and encrypted to protect the network from unauthorized access.

64.5.3 EAP (Extensible Authentication Protocol) Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wired LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, a switch helps a wired station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary switch that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificates from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

- EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wired client. The wired client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plain text passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

- EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wired clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAPTLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

- EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending user name and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

- PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple user name and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

- LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

CHAPTER 65
Port Security

65.1 Port Security Overview

This chapter shows you how to set up port security.

65.2 About Port Security

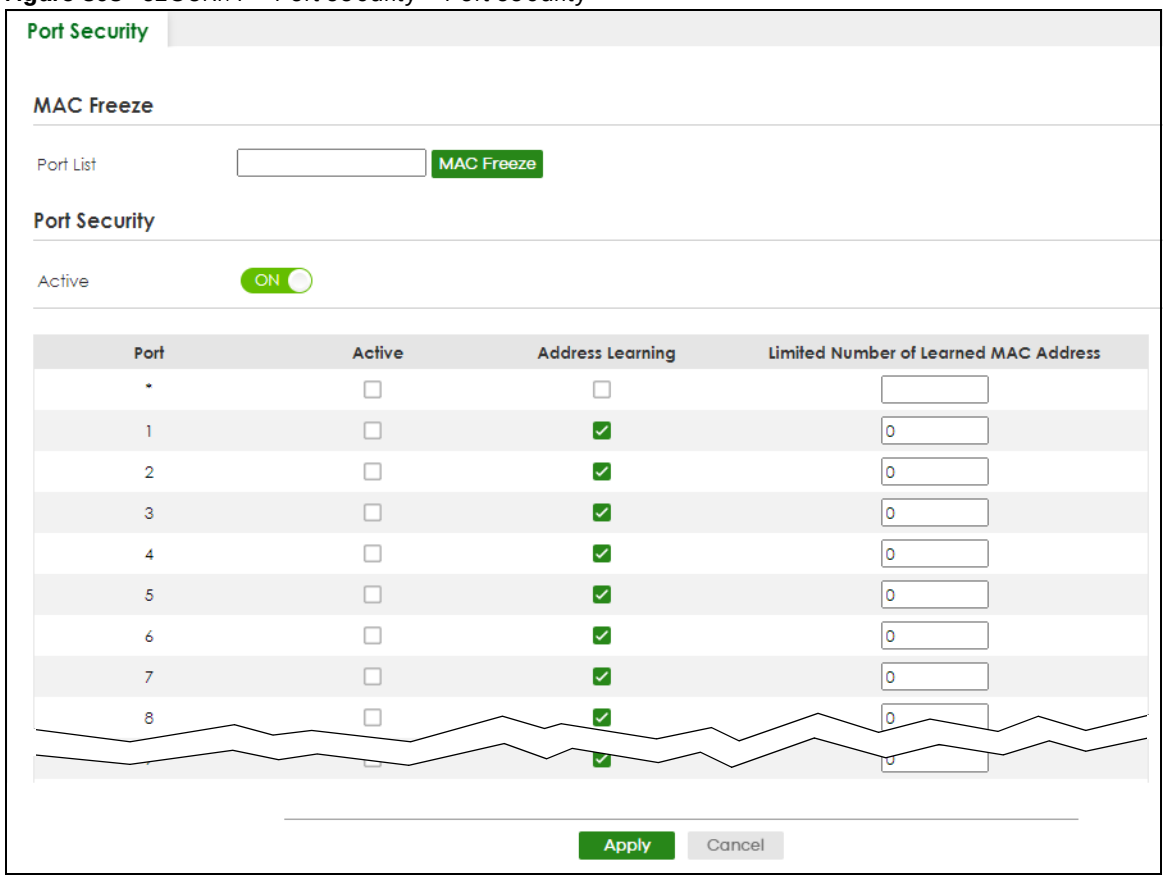
Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC addresses for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

65.3 Port Security Setup

Click **SECURITY** > **Port Security** > **Port Security** in the navigation panel to display the screen as shown.

Figure 308 SECURITY > Port Security > Port Security



The following table describes the labels in this screen.

Table 236 SECURITY > Port Security > Port Security

LABEL	DESCRIPTION
MAC Freeze	
Port List	Enter the number of the ports (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click **MAC Freeze**, all previously learned MAC addresses on the specified ports will become static MAC addresses and display in the **SWITCHING** > **Static MAC Forwarding** > **Static MAC Forwarding** screen.
MAC Freeze	Click **MAC Freeze** to have the Switch automatically select the **Active** checkboxes and clear the **Address Learning** checkboxes only for the ports specified in the **Port List**.
Port Security	
Active	Enable the switch button to enable port security on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 236 SECURITY > Port Security > Port Security (continued)

LABEL	DESCRIPTION
Active	Select this checkbox to enable the port security feature on this port. The Switch forwards packets whose MAC addresses is in the MAC address table on this port. Packets with no matching MAC addresses are dropped. Clear this checkbox to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the **SYSTEM** > **Switch Setup** screen. The valid range is from “0” to “32K”. “0” means this feature is disabled.
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.

CHAPTER 66
MAINTENANCE

66.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

66.1.1 What You Can Do

- Use the **Certificates** screen (Section 66.2 on page 429) to see the **Certificates** screen and import the Switch's CA-signed certificates.
- Use the **Cluster Management** screens (Section 66.5 on page 434) to manage the switches within a cluster and view cluster status.
- Use the **Restore Configuration** screen (Section 66.8 on page 439) to upload a stored device configuration file.
- Use the **Backup Configuration** screen (Section 66.9 on page 439) to save your configurations for later use.
- Use the **Erase Running-Configuration** screen (Section 66.10 on page 440) to reset the configuration to the Zyxel default configuration settings.
- Use the **Save Configuration** screen (Section 66.11 on page 441) to save the current configuration settings to a specific configuration file on the Switch.
- Use the **Configure Clone** screen (Section 66.12 on page 442) to copy the basic and advanced settings from a source port to a destination port or ports.
- Use the **Diagnostic** screen (Section 66.13 on page 443) to ping IP addresses, run a traceroute, perform port tests or show the Switch's location between devices.
- Use the **Firmware Upgrade** screen (Section 66.14 on page 446) to upload the latest firmware.
- Use the **Reboot System** screen (Section 66.15 on page 447) to restart the Switch without physically turning the power off and load a specific configuration file.
- Use the **SSH Authorized Keys** screen (Section 66.16 on page 449) to authenticate secure SSH connections between a client computer and the Switch (also called the server) without needing a password to connect to the Switch.
- Use the **SSH Host Keys** screen (Section 66.17 on page 455) to regenerate the Switch's SSH host key. You may want to do this to change the factory default SSH host key.
- Use the **Tech-Support** screen (Section 66.18 on page 456) to create reports for customer support if there are problems with the Switch.

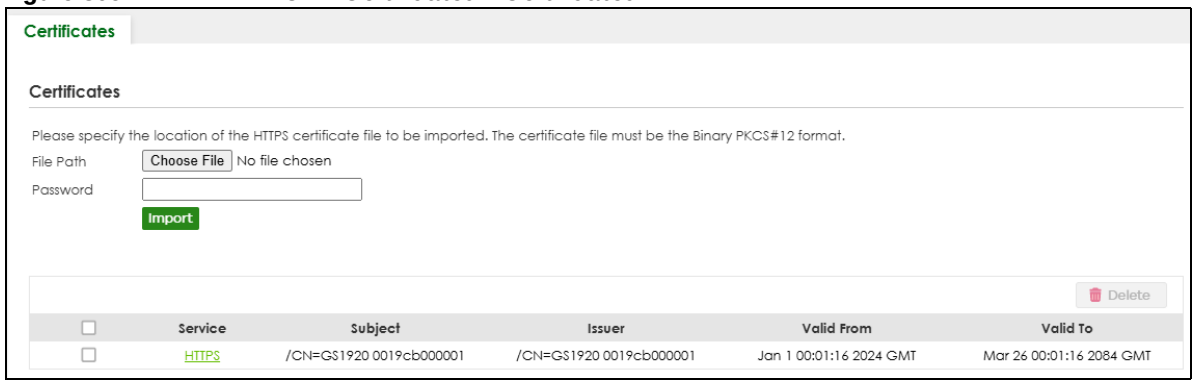
66.2 Certificates

The Switch can use HTTPS certificates that are verified by a third party to create secure HTTPS connections between your computer and the Switch. This way, you may securely access the Switch using the Web Configurator. See Section 56.7.2 on page 367 for more information about HTTPS.

Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Click **MAINTENANCE** > **Certificates** > **Certificates** to open the following screen. Use this screen to import the Switch's CA-signed certificates.

Figure 309 MAINTENANCE > Certificates > Certificates



The following table describes the labels in this screen.

Table 237 MAINTENANCE > Certificates > Certificates

LABEL	DESCRIPTION
File Path	Click **Choose File** or **Browse** to find the certificate file you want to upload.
Password	Enter the certificate file's password that was created when the PKCS #12 file was exported. The password consists of up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].
Import	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Switch.
Service	This field displays the service type that this certificate is for.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires.
	Select an entry's checkbox to select a specific entry.
Delete	Click this button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

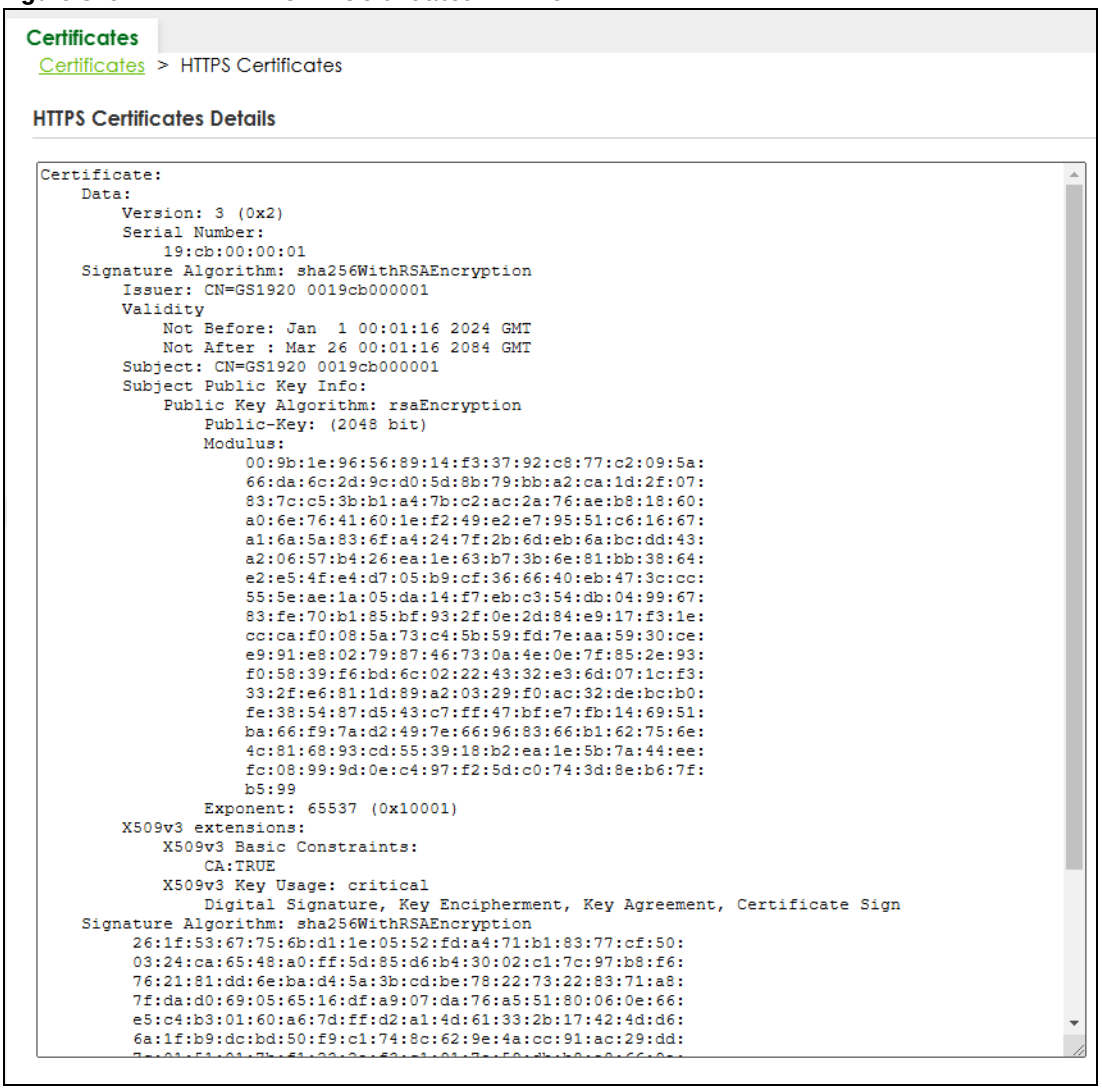
66.2.1 Install Certificates

After buying the certificates from a trusted third-party Certificate Authorities (CA), (for example, DigiCert), install the certificates. See Importing a Certificate for more information.

66.2.2 HTTPS Certificates

Use this screen to view the HTTPS certificate details. Click a hyperlink in the **Service** column in the **MAINTENANCE** > **Certificates** > **Certificates** screen to open the following screen.

Figure 310 MAINTENANCE > Certificates > HTTPS



66.3 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

66.3.1 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

66.3.2 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the Zyxel factory default configuration settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (Zyxel Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 238 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config1 config2	*.cfg	This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

You can store up to two images, or firmware files of the same device model, on the Switch. Only one image is used at a time.

- Run the `boot image <1|2>` command to specify which image is updated when firmware is loaded using the Web Configurator and to specify which image is loaded when the Switch starts up.
- You can also use FTP commands to upload firmware to any image.

The Switch supports dual firmware images, `ras-0` and `ras-1`. You can switch from one to the other by using the `boot image <index>` command, where `<index>` is 1 (ras-0) or 2 (ras-1). See the CLI Reference Guide for more information about using commands. The system does not reboot after it switches from one image to the other.

66.3.2.1 Example FTP Commands

```
ftp> put firmware.bin ras-0
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch's **Firmware 1**.

```
ftp> get config1 config1.cfg
```

This is a sample FTP session saving the Switch's configuration file 1 (**Config1**) to a file called "config1.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

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

66.3.3 FTP Command Line Procedure

1. Launch the FTP client on your computer.
2. Enter open, followed by a space and the IP address of your Switch.
3. Press [ENTER] when prompted for a user name.
4. Enter your password as requested (the default is "1234").
5. Enter bin to set transfer mode to binary.
6. Use put to transfer files from the computer to the Switch, for example, put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the Switch and renames it to "ras". Similarly, put config.cfg config1 transfers the configuration file on your computer (config.cfg) to the Switch and renames it to "config1". Likewise get config1 config.cfg transfers the configuration file on the Switch to your computer and renames it to "config.cfg".
7. Enter quit to exit the ftp prompt.

66.3.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 239 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either single-byte printable characters (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

66.3.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **SECURITY** > **Access Control** > **Service Access Control** > **Service Access Control** screen.
- The IP addresses in the **SECURITY** > **Access Control** > **Remote Management** > **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

66.4 Cluster Management Overview

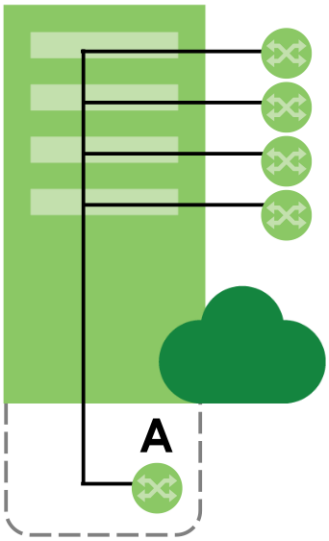
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 240 Zyxel Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with Zyxel cluster management implementation.
Cluster Manager	The Switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager Switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 311 Clustering Application Example



66.4.1 What You Can Do

- Use the **Cluster Management Status** screen (Section 66.5 on page 434) to view the role of the Switch within the cluster and to access a cluster member Switch's Web Configurator.
- Use the **Cluster Management Setup** screen (Section 66.6 on page 435) to configure clustering management.

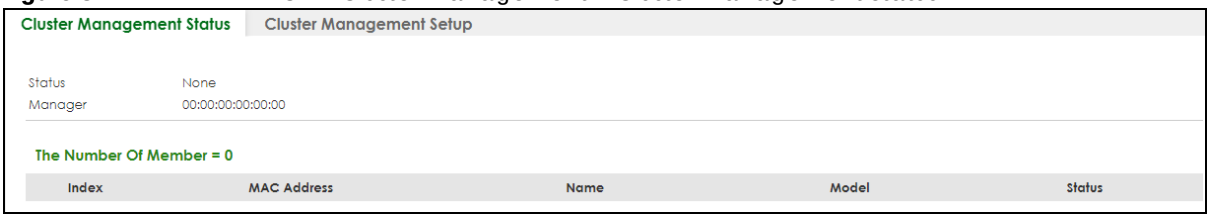
66.5 Cluster Management Status

Use this screen to view the role of the Switch within the cluster and to access a cluster member Switch's Web Configurator.

Click **MAINTENANCE** > **Cluster Management** > **Cluster Management Status** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 312 MAINTENANCE > Cluster Management > Cluster Management Status



The following table describes the labels in this screen.

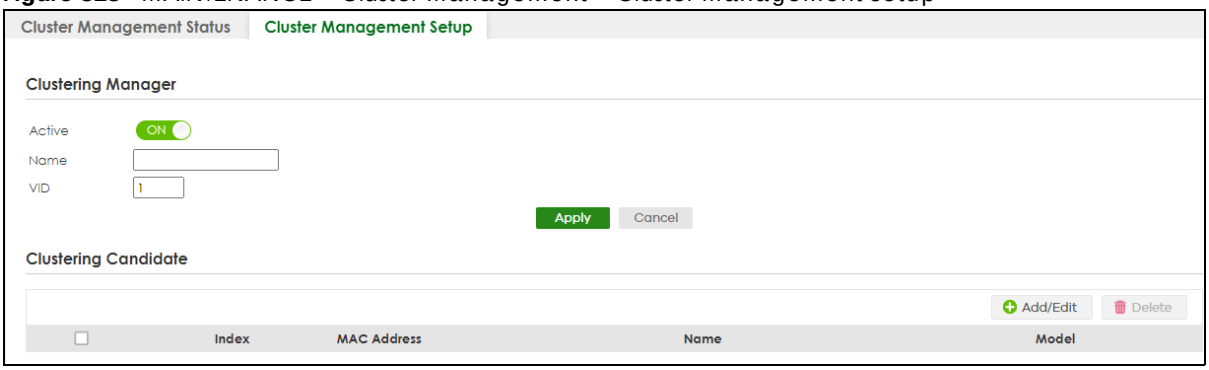
Table 241 MAINTENANCE > Cluster Management > Cluster Management Status

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member Switch directly and not through the cluster manager) **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager Switch's hardware MAC address.
The Number Of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches through the cluster manager Switch. Each number in the **Index** column is a hyperlink leading to the cluster member Switch's Web Configurator.
MAC Address	This is the cluster member Switch's hardware MAC address.
Name	This is the cluster member Switch's **System Name**.
Model	This field displays the model name.
Status	This field displays: **Online** (the cluster member Switch is accessible) **Error** (for example the cluster member Switch password was changed or the Switch was set as the manager and so left the member list, and so on) **Offline** (the Switch is disconnected – **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

66.6 Clustering Management Setup

Use this screen to configure clustering management. Click **MAINTENANCE** > **Cluster Management** > **Cluster Management Setup** to display the next screen.

Figure 313 MAINTENANCE > Cluster Management > Cluster Management Setup



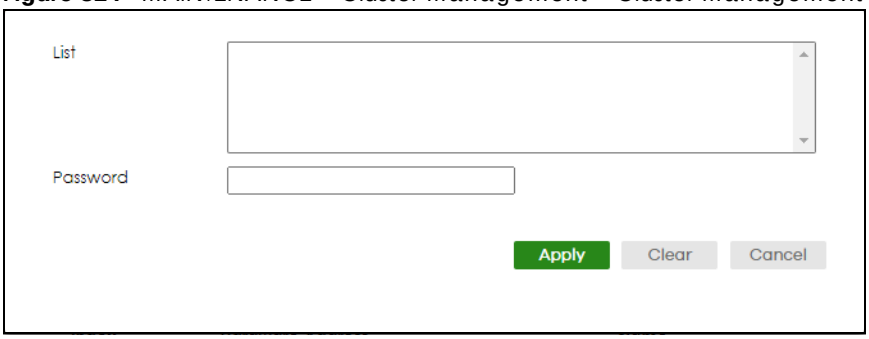
The following table describes the labels in this screen.

Table 242 MAINTENANCE > Cluster Management > Cluster Management Setup

LABEL	DESCRIPTION
Clustering Manager	The following fields relate to configuring the cluster manager.
Active	Enable the switch button to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a Switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 32 printable ASCII characters except [?], [|], ['], ["], or [,]. (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
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.
Clustering Candidate	The next summary table shows the information for the clustering members configured.
Add/Edit	Click this button to create or configure a clustering candidate.
Delete	Click this button to remove the clustering candidate.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This is the index number of a cluster member switch.
MAC Address	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.

Click the **Add/Edit** button to open the **Add/Edit** screen. Use this screen to configure a clustering candidate for the Switch.

Figure 314 MAINTENANCE > Cluster Management > Cluster Management Setup > Add/Edit



The following table describes the labels in this screen.

Table 243 MAINTENANCE > Cluster Management > Cluster Management Setup > Add/Edit

LABEL	DESCRIPTION
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its Web Configurator password. Select a member in the **Clustering Candidate** list and then enter its Web Configurator password. If that switch administrator changes the Web Configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common Web Configurator password. You can enter 4 up to 32 printable ASCII characters except [?], [|], ['], ["], or [,].
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.
Clear	Click **Clear** to reset the fields to the factory defaults.
Cancel	Click **Cancel** to begin configuring this screen afresh.

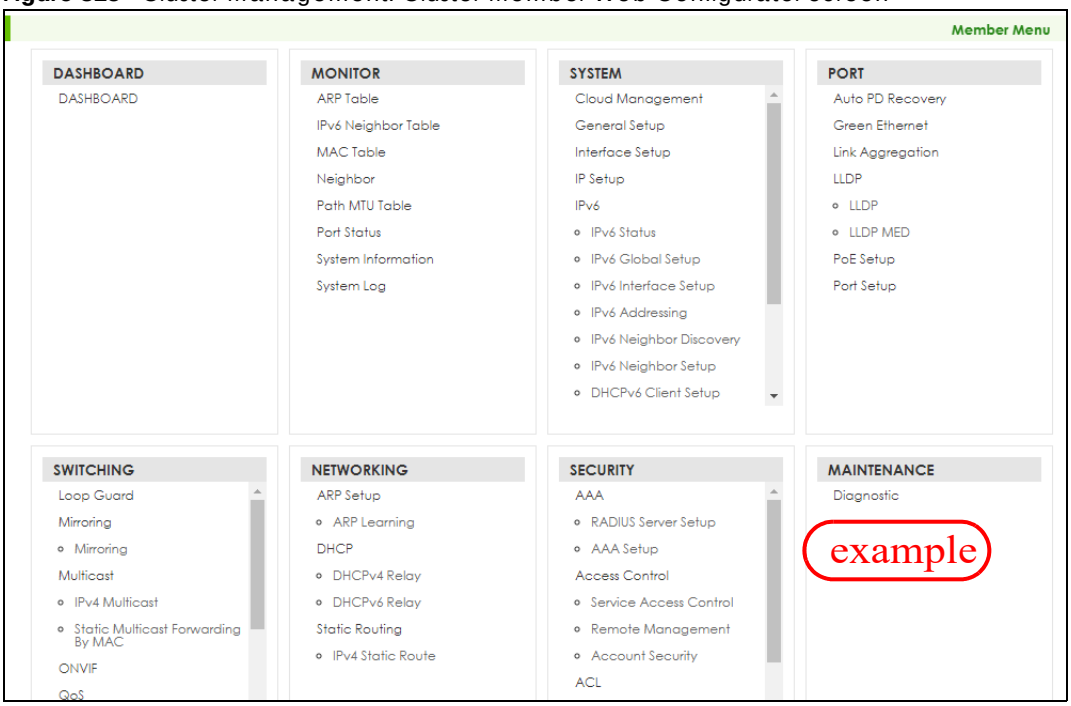
66.7 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

66.7.1 Cluster Member Switch Management

Go to the **MAINTENANCE** > **Cluster Management** > **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's Web Configurator home page. This cluster member Web Configurator home page and the home page that you would see if you accessed it directly are different.

Figure 315 Cluster Management: Cluster Member Web Configurator Screen



66.7.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 316 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 470ACAQ0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

Table 244 FTP Upload to Cluster Member Example

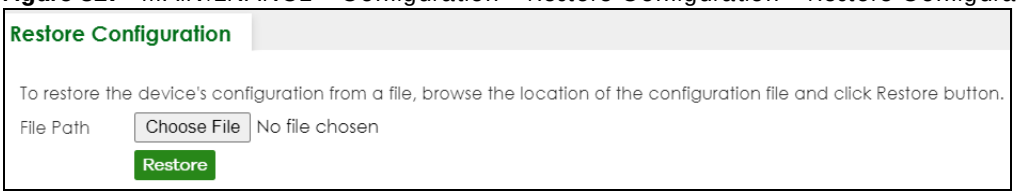
FTP PARAMETER	DESCRIPTION
User	Enter "admin".
Password	The Web Configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
470ACAQ0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-01-23-46	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

66.8 Restore Configuration

Use this screen to restore a previously saved configuration file (See Section 66.9 on page 439 for more information on how to back up a configuration file) from your computer to the Switch.

Click **MAINTENANCE** > **Configuration** > **Restore Configuration** > **Restore Configuration** to access this screen.

Figure 317 MAINTENANCE > Configuration > Restore Configuration > Restore Configuration

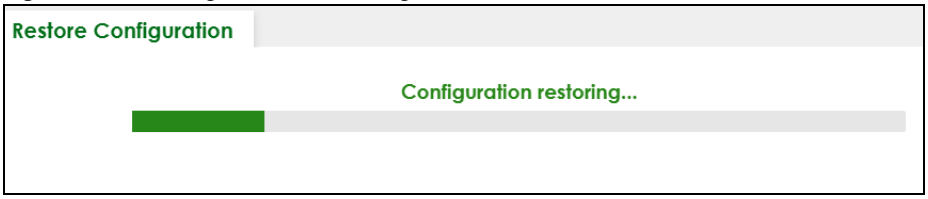


1 Click **Choose File** or **Browse** to locate the configuration file you wish to restore.

2 After you have specified the file, click **Restore**.

The Switch will run on the restored configuration after the restore process.

Figure 318 Configuration Restoring

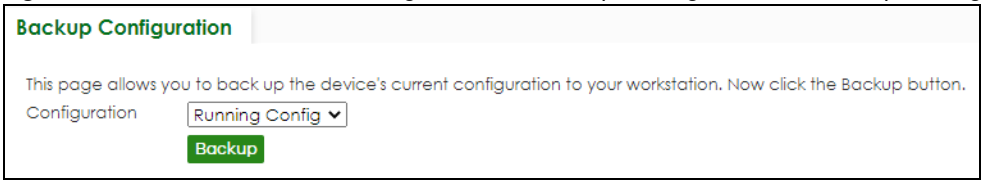


66.9 Backup Configuration

Backing up your Switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date. Use this screen to back up your current Switch configuration to a computer.

To access this screen, click **MAINTENANCE** > **Configuration** > **Backup Configuration** > **Backup Configuration** in the navigation panel.

Figure 319 MAINTENANCE > Configuration > Backup Configuration > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Select which Switch configuration file you want to download to your computer.

2 Click **Backup**.

3 If the current configuration file is open and/or downloaded to your computer automatically, you can click **File** > **Save As** on your computer to save the file to a specific place.

If a dialog box pops up asking whether you want to open or save the file, click **Save** or **Save File** to download it to the default downloads folder on your computer. If a **Save As** screen displays after you click **Save** or **Save File**, choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

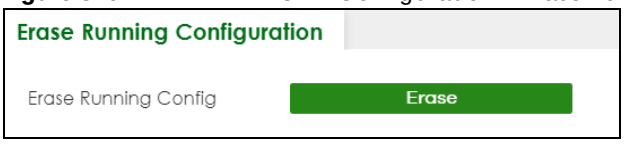
66.10 Erase Running-Configuration

Follow the steps below to reset the Switch back to the Zyxel default configuration settings.

To access this screen, click **MAINTENANCE** > **Configuration** > **Erase Running Configuration** > **Erase Running Configuration** in the navigation panel.

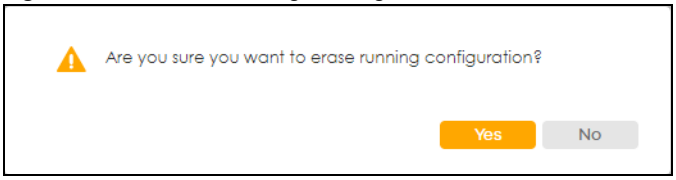
1 In the **Erase Running Configuration** screen, click the **Erase** button to clear all Switch configuration information you configured and return to the Zyxel default configuration settings.

Figure 320 MAINTENANCE > Configuration > Erase Running Configuration > Erase Running Configuration



2 Click **YES** to remove the running configuration on the Switch.

Figure 321 Erase Running Configuration: Confirmation



3 In the Web Configurator, click the **Save** button in the top of the screen to make the changes take effect. 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 or DHCP-assigned IP).

66.11 Save Configuration

To access this screen, click **MAINTENANCE** > **Configuration** > **Save Configuration** > **Save Configuration** in the navigation panel.

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch. These configurations are set up according to your network environment.

Click **Config 2** to save the current configuration settings permanently to **Configuration 2** on the Switch. These configurations are set up according to your network environment.

Click **Custom Default** to save the current configuration settings permanently to a customized default file on the Switch. If configuration changes cause the Switch to behave abnormally, click **Custom Default** (in the **MAINTENANCE** > **Reboot System** > **Reboot System** screen) to have the Switch automatically reboot and restore the saved **Custom Default** configuration file.

Note: **Custom Default** is only available in Standalone mode.

Figure 322 MAINTENANCE > Configuration > Save Configuration > Save Configuration (Standalone Mode)

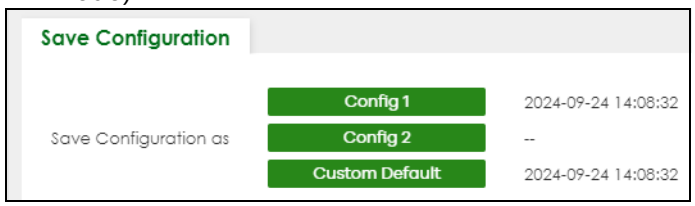
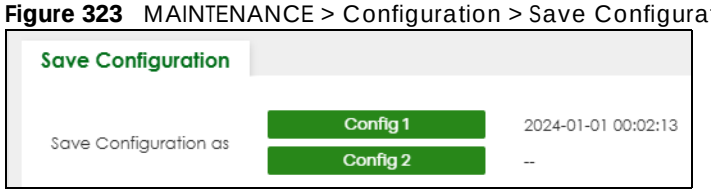


Figure 323 MAINTENANCE > Configuration > Save Configuration > Save Configuration (Cloud Mode)



Note: If a customized default file was not saved, clicking **Custom Default** in the **MAINTENANCE** > **Reboot System** > **Reboot System** screen loads the factory default configuration on the Switch.

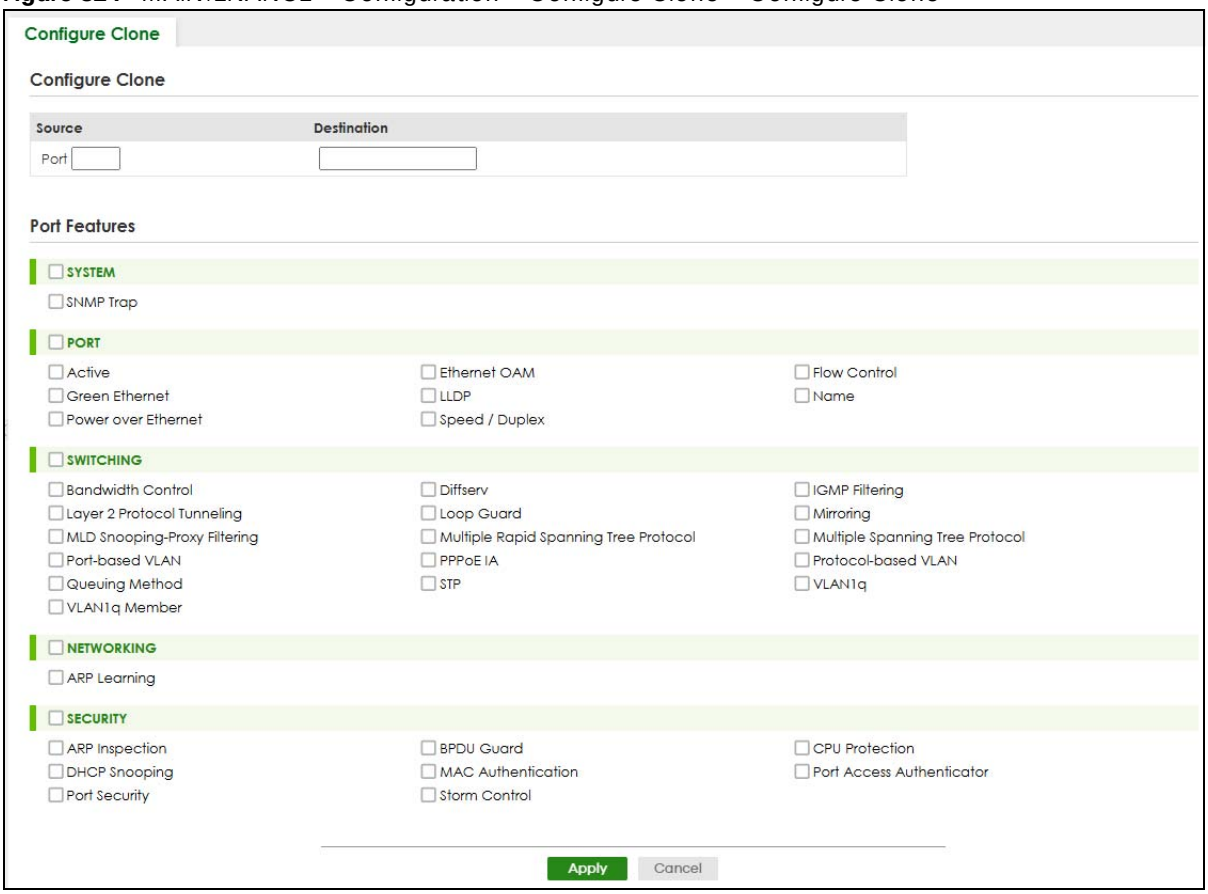
Alternatively, click **Save** on the top right in any screen to save the configuration changes to the current configuration.

Note: Clicking the **Apply** button after making configuration does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

66.12 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **MAINTENANCE** > **Configuration** > **Configure Clone** > **Configure Clone** to open the following screen.

Figure 324 MAINTENANCE > Configuration > Configure Clone > Configure Clone



The following table describes the labels in this screen.

Table 245 MAINTENANCE > Configuration > Configure Clone > Configure Clone

LABEL	DESCRIPTION
Configure Clone	
Source/ Destination Port	Enter the source port under the **Source** label. This port's attributes are copied. Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: **2, 4, 6** indicates that ports 2, 4 and 6 are the destination ports. **2-6** indicates that ports 2 through 6 are the destination ports.
Port Features	
	Select a feature's checkbox to select a specific feature. Otherwise, select the checkbox in the table heading row to select all features for a category.

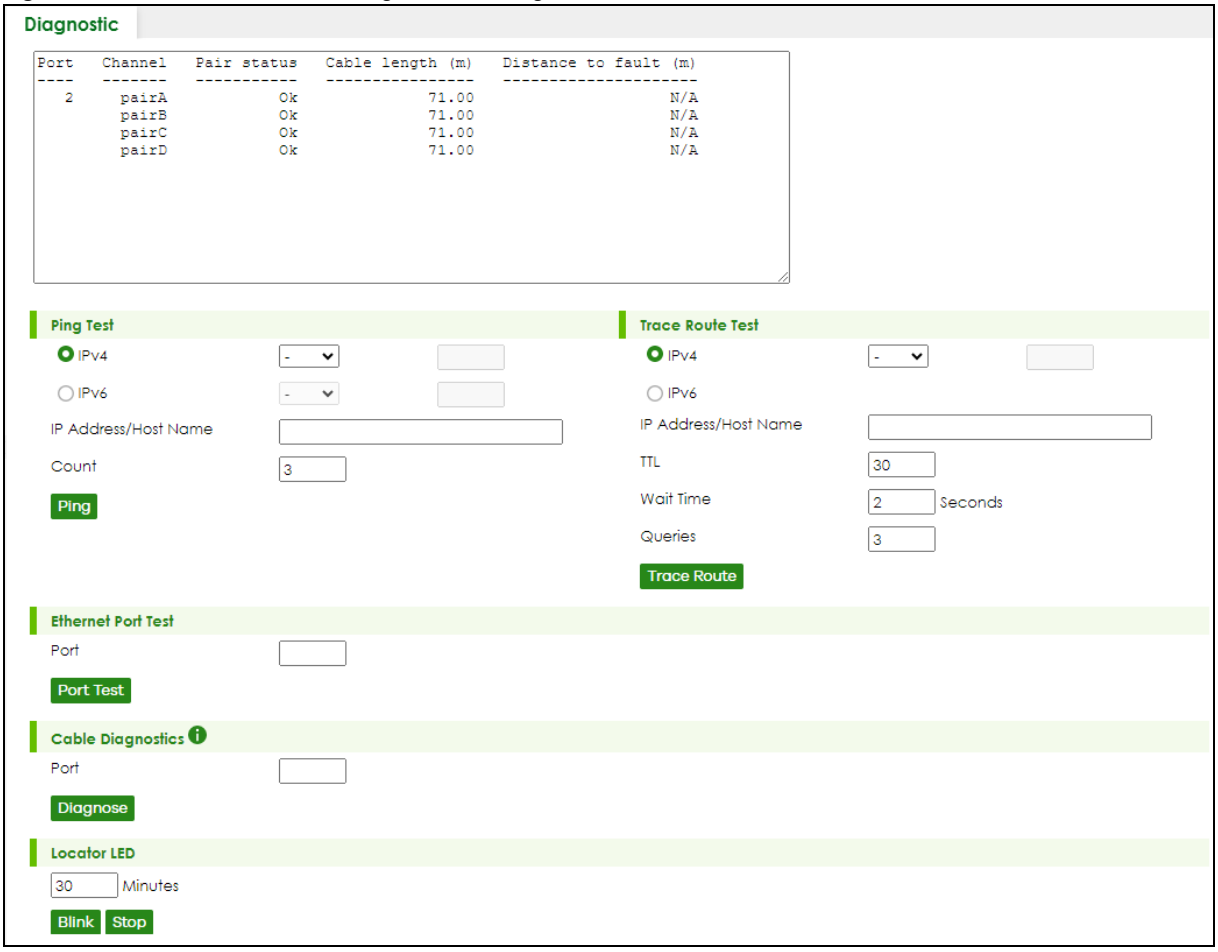
Table 245 MAINTENANCE > Configuration > Configure Clone > Configure Clone (continued)

LABEL	DESCRIPTION
SYSTEM	Select the system feature (you configured in the **SYSTEM** menus) to be copied to the destination ports. Otherwise, select the **SYSTEM** checkbox in the table heading row to select all features for a category.
PORT	Select which port features (you configured in the **PORT** menus) should be copied to the destination ports. Otherwise, select the **PORT** checkbox in the table heading row to select all features for a category.
SWITCHING	Select which switching features (you configured in the **SWITCHING** menus) should be copied to the destination ports. Otherwise, select the **SWITCHING** checkbox in the table heading row to select all features for a category.
NETWORKING	Select the networking feature (you configured in the **NETWORKING** menus) to be copied to the destination ports. Otherwise, select the **NETWORKING** checkbox in the table heading row to select all features for a category.
SECURITY	Select which security features (you configured in the **SECURITY** menus) should be copied to the destination ports. Otherwise, select the **SECURITY** checkbox in the table heading row to select all features for a category.
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.

66.13 Diagnostic

Click **MAINTENANCE** > **Diagnostic** > **Diagnostic** in the navigation panel to open this screen. Use this screen to ping IP addresses, run a traceroute, perform port tests or show the Switch's location between devices.

Figure 325 MAINTENANCE > Diagnostic > Diagnostic



The following table describes the labels in this screen.

Table 246 MAINTENANCE > Diagnostic > Diagnostic

LABEL	DESCRIPTION
Ping Test	
IPv4	Select this option if you want to ping an IPv4 address. Otherwise, select **–** to send ping requests to all VLANs on the Switch.
IPv6	Select this option if you want to ping an IPv6 address. You can also select **vlan** and specify the ID number of the VLAN to which the Switch is to send ping requests. Otherwise, select **–** to send ping requests to all VLANs on the Switch.
IP Address/Host Name	Type the IP address or host name of a device that you want to ping in order to test a connection. Click **Ping** to have the Switch ping the IP address.
Count	Enter the number of ICMP Echo Request (ping) messages the Switch continuously sends.
Trace Route Test	
IPv4	Select this option if you want to trace the route packets taken to a device with an IPv4 address. Otherwise, select **–** to trace the path on any VLAN. Note: The device to which you want to run a traceroute must belong to the VLAN you specify here.

Table 246 MAINTENANCE > Diagnostic > Diagnostic (continued)

LABEL	DESCRIPTION
IPv6	Select this option if you want to trace the route packets taken to a device with an IPv6 address.
IP Address/Host Name	Enter the IP address or host name of a device to which you want to perform a traceroute. Click **Trace Route** to have the Switch perform the traceroute function. This determines the path a packet takes to the specified device.
TTL	Enter the Time To Live (TTL) value for the ICMP Echo Request packets. This is to set the maximum number of the hops (routers) a packet can travel through. Each router along the path will decrement the TTL value by one and forward the packets. When the TTL value becomes zero and the destination is not found, the router drops the packets and informs the sender.
Wait Time	Specify how many seconds the Switch waits for a response to a probe before running another traceroute.
Queries	Specify how many times the Switch performs the traceroute function.
Ethernet Port Test	
Port	Enter a port number and click **Port Test** to perform an internal loopback test.
Port	This is the number of the physical Ethernet port on the Switch.
Cable Diagnostics	
Port	This is the number of the physical Ethernet port on the Switch.
Channel	An Ethernet cable usually has four pairs of wires. A 10BASE-T or 100BASE-TX port only use and test two pairs, while a 1000BASE-T port requires all four pairs. This displays the descriptive name of the wire-pair in the cable.
Pair status	**Ok**: The physical connection between the wire-pair is okay. **Open**: There is no physical connection (an open circuit detected) between the wire-pair. **Short**: There is an short circuit detected between the wire-pair. **Unknown**: The Switch failed to run cable diagnostics on the cable connected this port. **Unsupported**: The port is a fiber port or it is not active.
Cable length	This displays the total length of the Ethernet cable that is connected to the port when the **Pair status** is **Ok** and the Switch chipset supports this feature. This shows **N/A** if the **Pair status** is **Open** or **Short**. Check the **Distance to fault**. This shows **Unsupported** if the Switch chipset does not support to show the cable length.
Distance to fault	This displays the distance between the port and the location where the cable is open or shorted. This shows **N/A** if the **Pair status** is **Ok**. This shows **Unsupported** if the Switch chipset does not support to show the distance.
Locator LED	
	Enter a time interval (in minutes) and click **Blink** to show the actual location of the Switch between several devices in a rack. The default time interval is 30 minutes. Click **Stop** to have the Switch terminate the blinking locater LED.

66.14 Firmware Upgrade

You can upgrade the Switch's firmware through Web Configurator or NCC.

Firmware Upgrade Through NCC

In cloud management mode, NCC will first check if the firmware on the Switch needs to be upgraded. If it does, the Switch will upgrade the firmware immediately. If the firmware does not need to be upgraded, but there is newer firmware available for the Switch, then it will be upgraded according to the firmware upgrade schedule for the Switch on the NCC.

On the NCC web portal, go to **Site-wide** > **Configure** > **Firmware management** > **Firmware management** to schedule the firmware upgrade time.

Note: While the Switch is rebooting, do NOT turn off the power.

Firmware Upgrade Through the Web Configurator

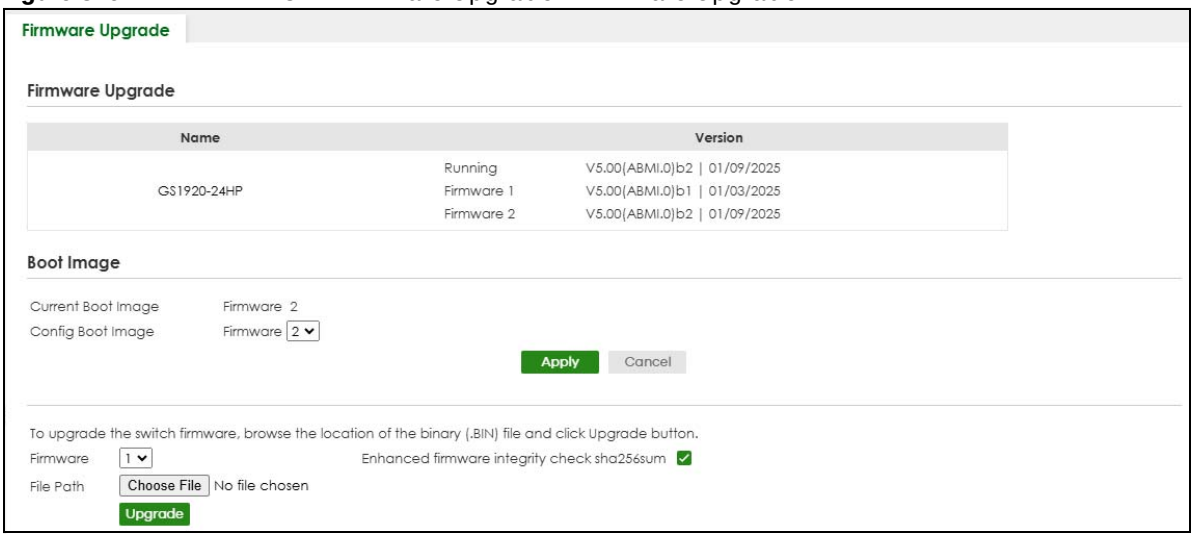
Use the following screen to upgrade your Switch to the latest firmware. The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the Web Configurator and to specify which image is loaded when the Switch starts up.

You can check the **Hardware Version** of your Switch in the **DASHBOARD** screen to determine which model firmware to upgrade to the Switch. You should see **V2.x** in the **Hardware Version** field. The integer, 2, identifies the GS1920v2 Series. Go to the Zyxel website to download the correct model firmware.

Note: Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Click **MAINTENANCE** > **Firmware Upgrade** > **Firmware Upgrade** to view the screen as shown next.

Figure 326 MAINTENANCE > Firmware Upgrade > Firmware Upgrade



The top of the screen shows which firmware version is currently **Running** on the Switch. Click **Choose File** or **Browse** to locate the firmware file you wish to upload to the Switch in the **File Path** field. Click **Upgrade** to load the new firmware. The Switch does not apply the uploaded firmware immediately. Firmware upgrades are only applied after you reboot the Switch using the uploaded firmware.

Click the **Config Boot Image** drop-down list box to select the boot image (**Firmware1** or **Firmware2**) you want the Switch to use when rebooting, click **Apply**. Restart the Switch (manually or using the **MAINTENANCE** > **Reboot System** > **Reboot System** screen) to apply the firmware image you selected.

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

Table 247 MAINTENANCE > Firmware Upgrade > Firmware Upgrade

LABEL	DESCRIPTION
Name	This is the name of the Switch that you are configuring.
Version	The Switch has 2 firmware sets, **Firmware 1** and **Firmware 2**, residing in flash. • **Running** shows the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch (**Firmware 1** or **Firmware 2)**. The firmware information is also displayed at System Information in Basic Setting. • **Firmware 1** shows its version number (and model code) and MM/DD/YYYY creation date. • **Firmware 2** shows its version number (and model code) and MM/DD/YYYY creation date.
Boot Image	
Current Boot Image	This displays which firmware is currently in use on the Switch (**Firmware 1** or **Firmware 2)**.
Config Boot Image	Select which firmware (**Firmware 1** or **Firmware 2)** should load, click **Apply** and reboot the Switch to see changes, you will also see changes in the **Current Boot Image** field above as well.
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.
Firmware	Choose to upload the new firmware to (Firmware) **1** or (Firmware) **2**.
File Path	Click **Choose File** or **Browse** to locate the firmware file you wish to upload to the Switch.
Upgrade	Click **Upgrade** to load the new firmware. Firmwares are only applied after a reboot. To reboot, go to **MAINTENANCE** > **Reboot System** > **Reboot System** and click **Config 1**, **Config 2** or **Factory Default** (**Config 1**, **Config 2, Factory Default,** and **Custom Default** are the configuration files you want the Switch to use when it restarts).
Enhanced firmware integrity check sha256sum	Select this to allow the Switch to verify the SHA-256 checksum of the firmware file. A SHA-256 checksum is a calculated 256 bits value made of numbers and letters used to verify the integrity of a file. The Switch compares the SHA-256 checksum value to confirm whether a firmware file is corrupted or has been tampered with since it was originally created. Note: When the firmware file fails the SHA-256 checksum comparison, a warning will appear and the upgrade stopped. You cannot continue the firmware upgrade.

66.15 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**), configuration two (**Config 2**), a **Custom Default** or the **Factory Default** configuration when you reboot. Follow the steps below to reboot the Switch.

Note: **Custom Default** is only available in Standalone mode.

Click **MAINTENANCE** > **Reboot System** > **Reboot System** to view the screen as shown next.

Figure 327 MAINTENANCE > Reboot System > Reboot System (Standalone Mode)

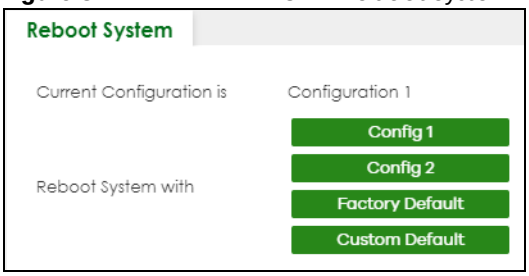
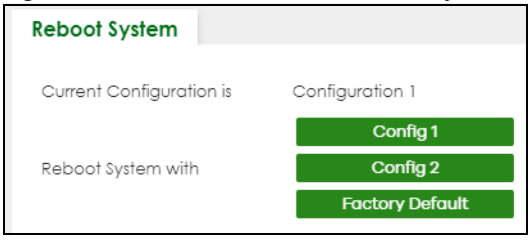
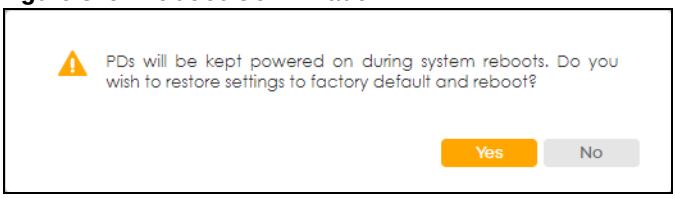


Figure 328 MAINTENANCE > Reboot System > Reboot System (Cloud Mode)



1 Click the **Config 1**, **Config 2**, **Factory Default**, or **Custom Default** button to reboot and load that configuration file. The confirmation screen displays.

Figure 329 Reboot Confirmation



2 Click **YES** and then wait for the Switch to restart. This takes up to 2 minutes.

Click **Config 1** and follow steps 1 to 2 to reboot and load configuration one on the Switch.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

Click **Factory Default** and follow steps 1 to 2 to reboot and load Zyxel factory default configuration settings on the Switch.

Click **Custom Default** and follow steps 1 to 2 to reboot and load a customized default file on the Switch. This will save the custom default configuration settings to both **Configuration 1** and **Configuration 2**.

Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration on the Switch.

66.16 SSH Authorized Keys

The Switch can use SSH-authorized keys to authenticate secure SSH connections between a client computer and the Switch (also called the server) without needing a password to connect to the Switch. You can use a third-party utility to generate a private and public key for SSH, for example:

- In Windows, use the PuTTY terminal emulator
- In Linux Ubuntu, use the "ssh-keygen" command.

The Switch and the client computer should have a unique set of private and public keys for encryption/decryption. See Section 56.7.1 on page 366 for more information about SSH.

Click **MAINTENANCE** > **SSH Authorized Keys** > **SSH Authorized Keys** to open the following screen. Use this screen to import the client computer's public key into the Switch.

Figure 330 MAINTENANCE > SSH Authorized Keys > SSH Authorized Keys

The following table describes the labels in this screen.

Table 248 MAINTENANCE > SSH Authorized Keys > SSH Authorized Keys

LABEL	DESCRIPTION
File Path	Click **Choose File** or **Browse** to find the authorized key file you want to upload.
Import	Click this button to save the authorized key file you want to import from your computer to the Switch.
	Select an entry's checkbox to select a specific key.
User	This field displays the user name of the authorized key file (up to 32 characters).
Hostname	This field displays the hostname of the authorized key file (up to 32 characters only).
Content	This field displays the actual encryption key's text string (up to 64 characters).
Delete	After selecting an entry's checkbox, click this button to delete the authorized key file.

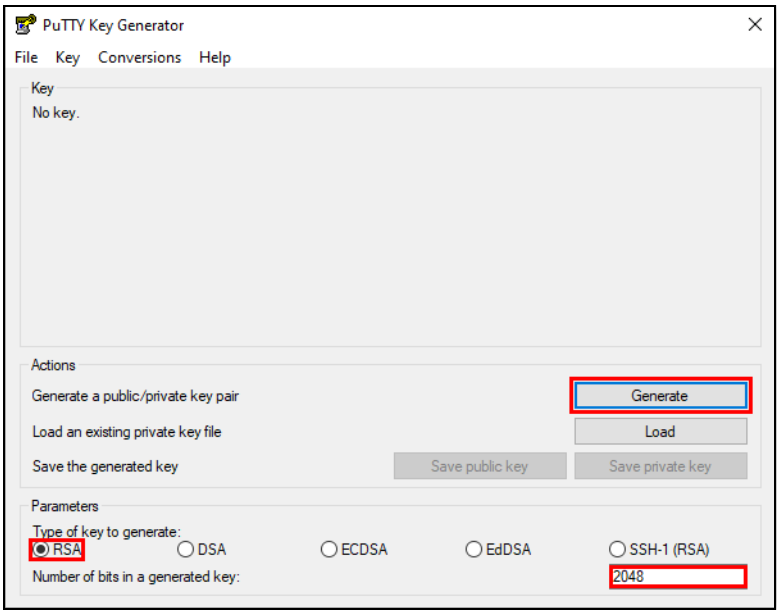
66.16.1 Generate the SSH Authorized Keys

You must install an SSH client program on a client computer (Windows or Linux operating system) to connect to the Switch over SSH.

Example – Generate the SSH Authorized Keys on Windows

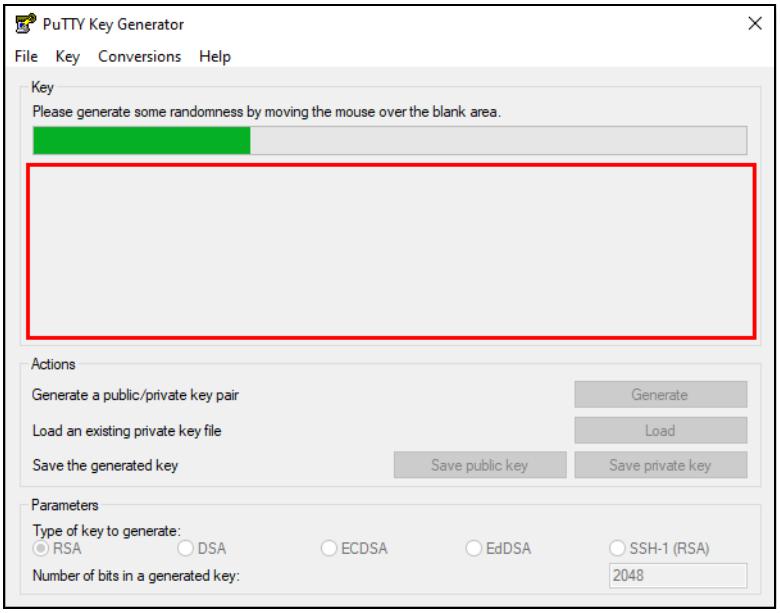
PuTTY is a free and open-source terminal emulator. It supports the SSH network protocol. To generate the SSH-authorized keys in PuTTY, the following are the steps at the time of writing:

1 Run PuTTYgen.

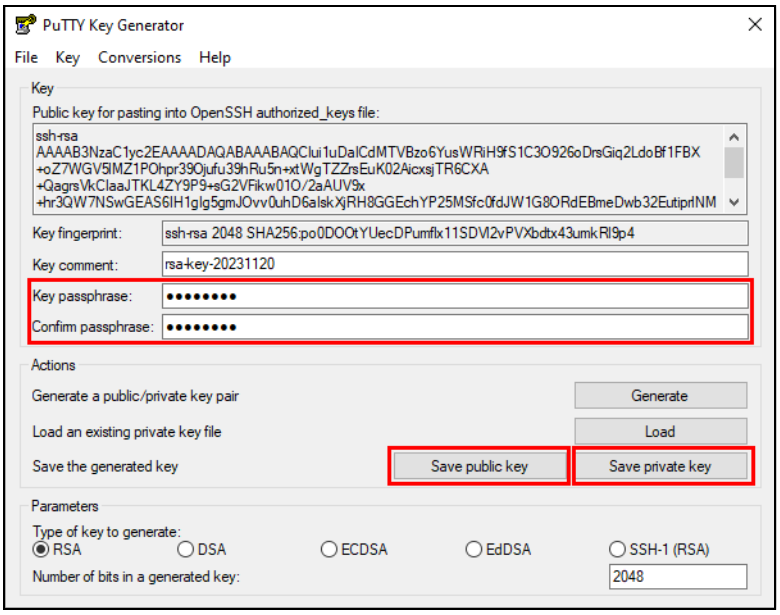


2 Select **RSA** in the **Type of key to generate**. RSA (Rivest-Shamir-Adleman) is an asymmetric encryption scheme that generates its keys by multiplying two pseudo-random prime numbers. Enter **2048** in the **Number of bits in a generated key**. SSH keys with encryption lower than 2048 are considered insecure. Then click **Generate**.

3 Move the mouse back and forth over the blank area to complete the key generation.

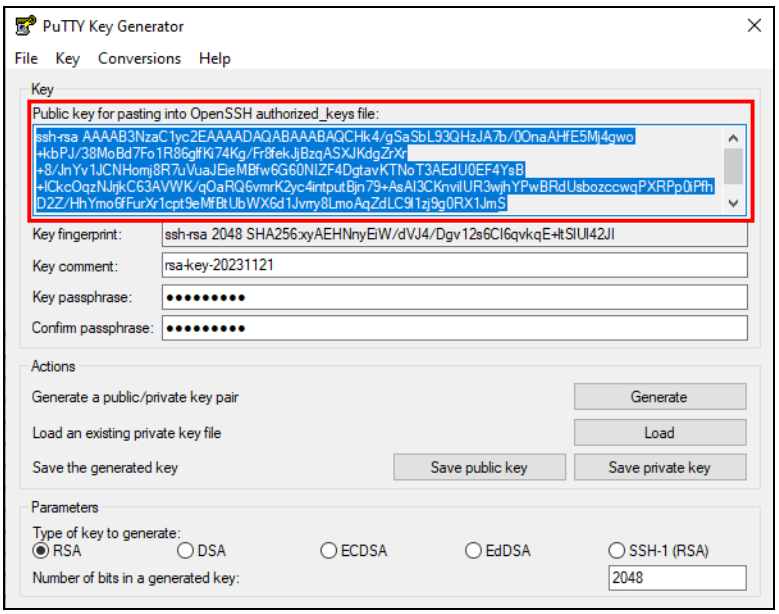


4 (Optional) The **Key passphrase** and **Confirm passphrase** fields allow you to set a passphrase for your key. Use the passphrase to encrypt the key on your computer. When set, you need to enter the passphrase to use the key. See step 5 on Run PuTTY for SSH Connections on Windows for more information.

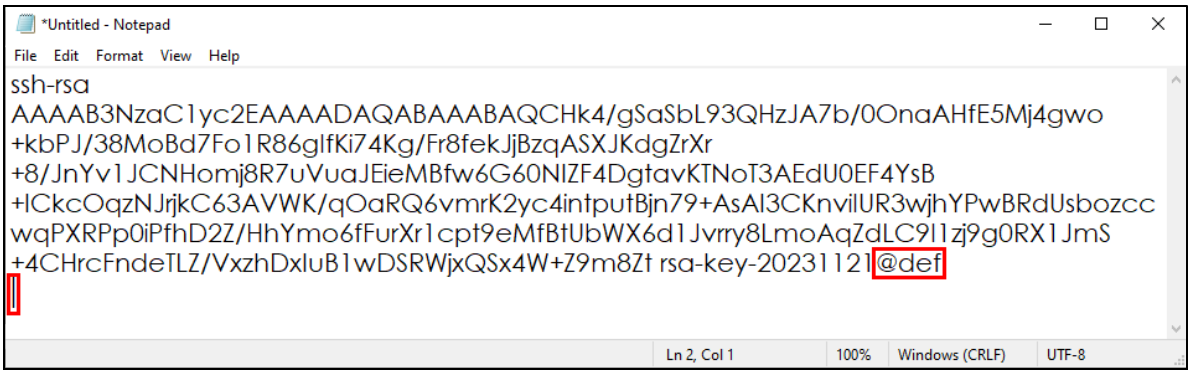


5 Click **Save public key** and **Save private key** to save the generated keys in your computer.

6 Copy the text on the generated public key into a text editor app like Notepad.



7 At the end of the text string, enter “@(Hostname)”. This will appear in the **Hostname** field in the **MAINTENANCE** > **SSH Authorized Keys** > **SSH Authorized Keys** screen. Press **Enter** to add a line break, then save the text file. Import the text file into the Switch using the **SSH Authorized Keys** screen.

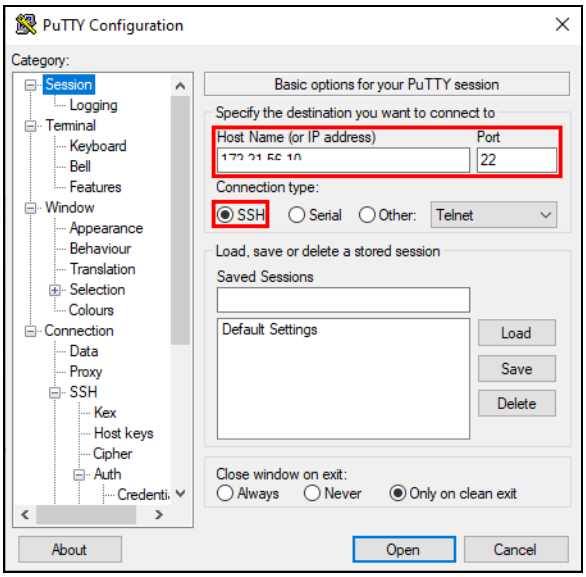


Note: The Switch only supports one SSH-authorized key at a time. Only one client computer can authenticate without entering a password using an SSH connection.

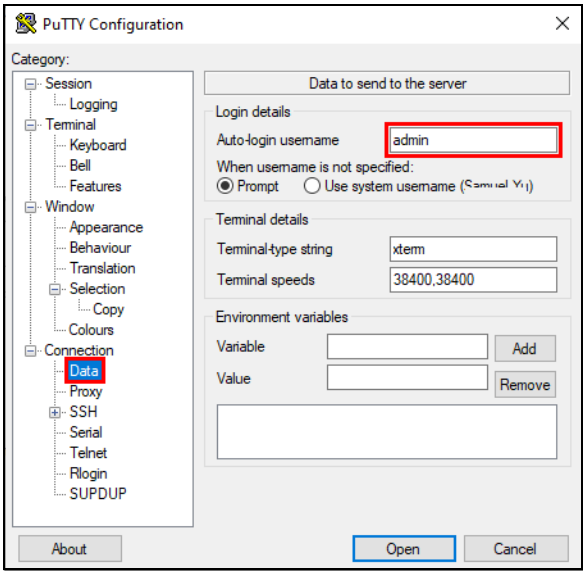
Run PuTTY for SSH Connections on Windows

To use PuTTY to connect to the Switch through SSH, the following are the steps at the time of writing:

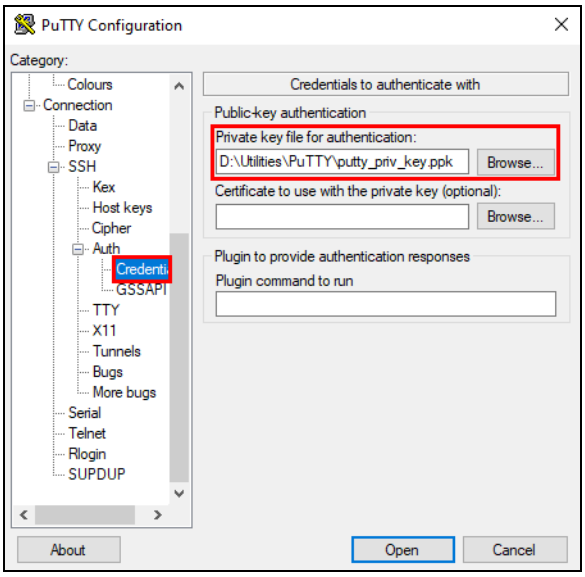
1 Run PuTTY. In the **Session** screen, enter the IP address of the Switch and "22" for the **Port**. Select **SSH** for the **Connection type**.



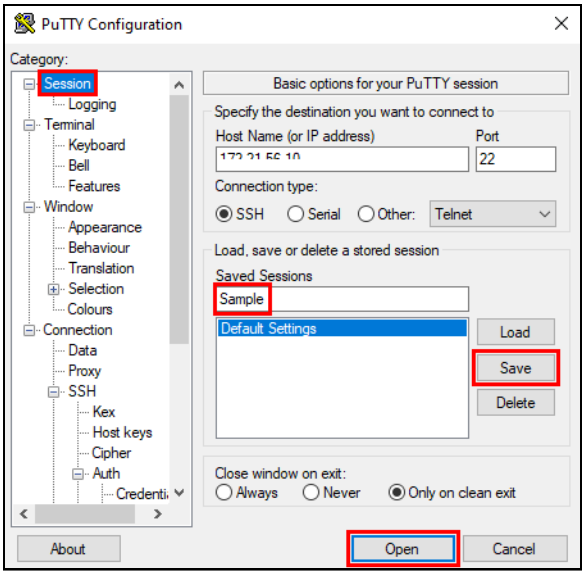
2 In the **Data** screen, enter **admin** for **Auto-login username**. The Switch only supports the **admin** login for the SSH-authorized key.



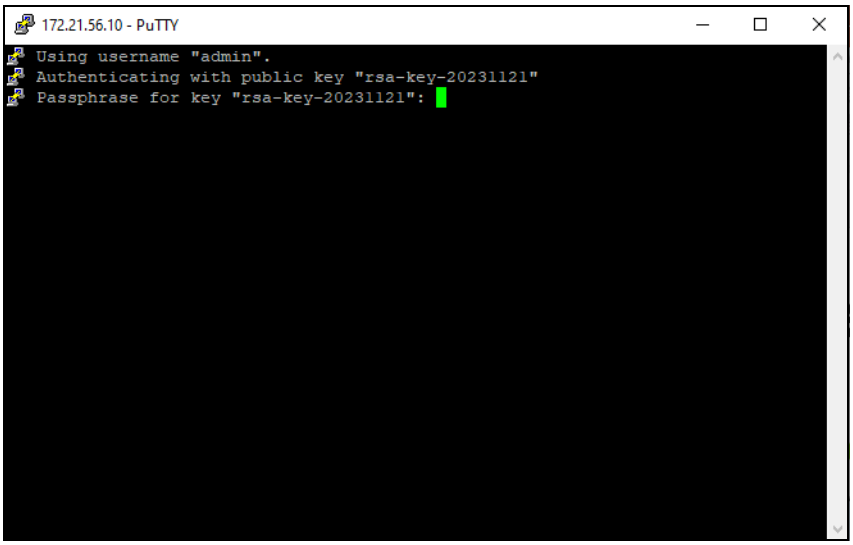
3 In the **Credentials** screen, click **Browse** to locate the generated private key.



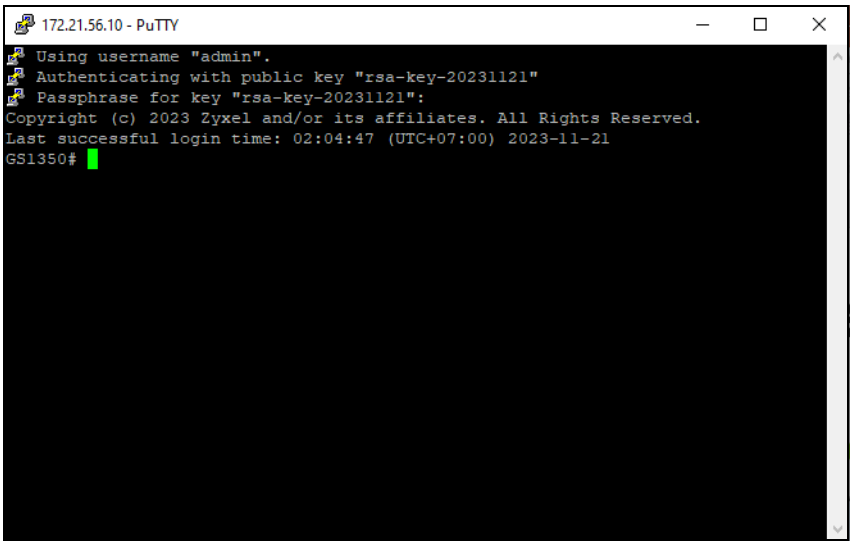
4 In the **Session** screen, you can save the PuTTY configuration by entering a name (for example, “Sample”) in the **Saved Sessions**, then click **Save**. Click **Open** to start the SSH connection.



5 Enter the **Passphrase for key** if you configured the **Key passphrase** in step 4 of using the PuTTY Key Generator.



You have now logged in to the Switch.



Example – Generate the SSH Authorized Keys on Linux

To generate the SSH-authorized keys in Ubuntu, enter the following commands at the time of writing:

```
UserA@UbuntuClient:~$ ssh-keygen –t rsa –b 2048
.........(enter..)
UserA@UbuntuClient:~$ ls –all .ssh/
.........
-rw-------  1 UserA UserA  1831 Mar 25  09:46 id_rsa
-rw-r--r--  1 UserA UserA   408 Mar 25  09:46 id_rsa.pub
.........
```

“id_rsa” is the private key and “id_rsa.pub” is the public key generated in Ubuntu.

66.17 SSH Host Keys

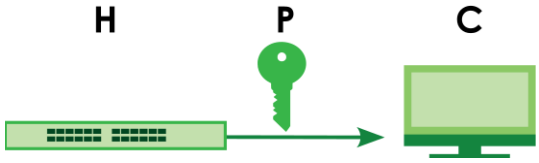
The Switch uses its SSH host public key (P) to authenticate secure SSH connections from an SSH client (C).

When the Switch receives a connection request from an SSH client, the Switch sends its public key to the SSH client. If it's the first time the SSH client accesses the Switch, the SSH client may receive a warning message prompting it to accept or reject the public key.

After the SSH client accepts the Switch's public key, the SSH client encrypts the SSH client's username and password with the Switch's public key and sends the encrypted credentials to the Switch.

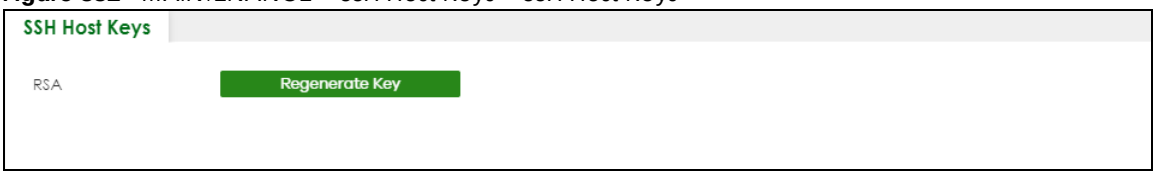
When the Switch gets the encrypted credentials from the SSH client, the Switch uses its private key to decrypt the encrypted credentials from the SSH client. If the credentials are correct, the Switch authenticates the SSH client and the SSH client can log into the Switch using SSH.

Figure 331 SSH Host Keys



Click **MAINTENANCE** > **SSH Host Keys** > **SSH Host Keys** to open the following screen. Use this screen to regenerate the Switch's SSH host key. You may want to do this to change the factory default SSH host key.

Figure 332 MAINTENANCE > SSH Host Keys > SSH Host Keys



The following table describes the labels in this screen.

Table 249 MAINTENANCE > SSH Host Keys > SSH Host Keys

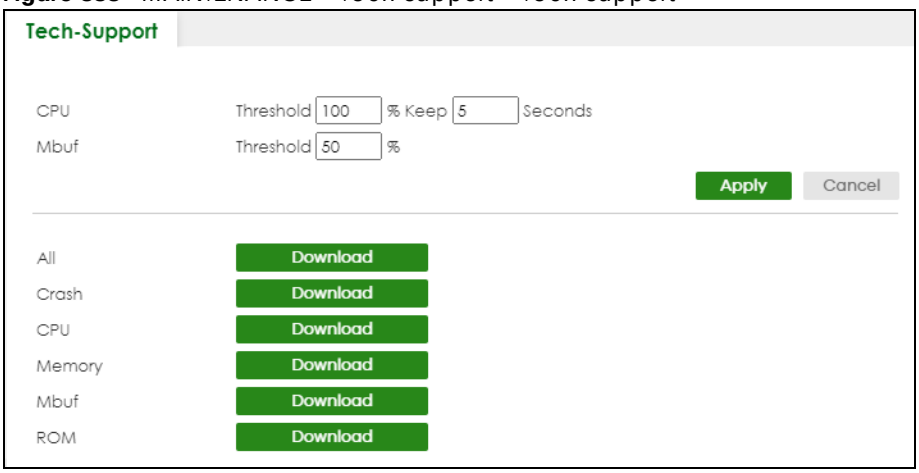
LABEL	DESCRIPTION
RSA	At the time of writing, the Switch supports RSA encryption for the SSH host key. See Section 66.16.1 on page 449 for information about the RSA.
Regenerate Key	Click this button to regenerate the Switch's default host key. Note: After the Switch regenerates the host key, the previous authenticated SSH clients may receive a message to replace the old host key with the new one the next time they connect to the Switch.

66.18 Tech-Support

The Tech-Support feature is a log enhancement tool that logs 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. The Tech Support menu eases your effort in obtaining reports and it is also available in CLI command by entering the “Show tech-support” command.

Click **MAINTENANCE** > **Tech-Support** > **Tech-Support** to see the following screen.

Figure 333 MAINTENANCE > Tech-Support > Tech-Support



You may need WordPad or similar software to see the log report correctly. The table below describes the fields in the above screen.

Table 250 MAINTENANCE > Tech-Support > Tech-Support

LABEL	DESCRIPTION
CPU	Type a number ranging from 50 to 100 in the CPU threshold box, and type another number ranging from 5 to 60 in the seconds box then click **Apply**. For example, 80 for CPU threshold and 5 for seconds means a log will be created when CPU utilization reaches over 80% and lasts for 5 seconds. The log report holds 7 days of CPU log data and is stored in volatile memory (RAM). The data is lost if the Switch is turned off or in event of power outage. After 7 days, the logs wrap around and new ones and replace the earliest ones. The higher the CPU threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Mbuf	Type a number ranging from 50 to 100 in the Mbuf (Memory Buffer) threshold box. The Mbuf log report is stored in flash (permanent) memory. For example, Mbuf 50 means a log will be created when the Mbuf utilization is over 50%. The higher the Mbuf threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
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.
All	Click **Download** to see all the log report and system status. This log report is stored in flash memory. If the **All** log report is too large, you can download the log reports separately below.
Crash	Click **Download** to see the crash log report. The log will include information of the last crash and is stored in flash memory.
CPU	Click **Download** to see the CPU history log report. The 7-days log is stored in RAM and you will need to save it, otherwise it will be lost when the Switch is shutdown or during power outage.
Memory	Click **Download** to see the memory section log report. This log report is stored in flash memory.

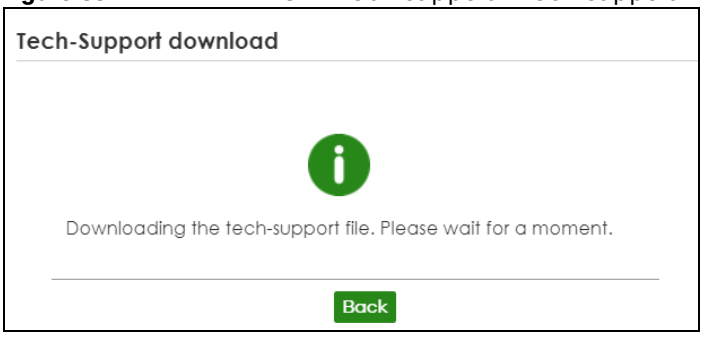
Table 250 MAINTENANCE > Tech-Support > Tech-Support (continued)

LABEL	DESCRIPTION
Mbuf	Click **Download** to see the Mbuf (Memory Buffer) log report. This log report is stored in flash memory.
ROM	Click **Download** to see the Read Only Memory (ROM) log report. This report is stored in flash memory.

66.18.1 Tech-Support Download

When you click **Download** to save your current Switch configuration to a computer, the following screen appears. When the log report has downloaded successfully, click **Back** to return to the previous screen.

Figure 334 MAINTENANCE > Tech-Support > Tech-Support: Download



PART III
Troubleshooting and Appendices

CHAPTER 67
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
- PoE Supply
- Nebula Registration

67.1 Power, Hardware Connections, and LEDs

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

1. Make sure you are using the power adapter or cord included with the Switch.
2. 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.
3. Disconnect and re-connect the power adapter or cord to the Switch.
4. 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 3.4 on page 46.
2. Check the hardware connections. See Section 3.2 on page 39.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adapter or cord to the Switch.
5. If the problem continues, contact the vendor.

67.2 Switch Access and Login

I can see the **Login** screen, but I cannot log in to the Switch. (I forgot the user name and/or password.)

1. Check the Switch's management mode by using the **CLOUD** LED. See Section 3.4 on page 46 for more information on the LED descriptions.
   - If you are in Cloud management mode, use the **Local credentials Password** to log in to the cloud mode – local GUI. The **Local credentials Password** can be found in **Site-wide** > **Configure** > **Site settings** > **Device configuration**: **Local credentials**: **Password** in the NCC portal.
   - If you are in standalone management mode, use the default user name **admin** and the default password **1234**.
2. Depending on your Switch's management mode, make sure you have entered the correct user name and password. These fields are case-sensitive, please make sure [Caps Lock] is not on.

   Note: Steps 1 and 2 are applicable if you get an invalid administrator password when using some functions in the ZON utility. See Section 1.4.2 on page 30 for more information.
3. You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet sessions or try connecting again later.

   Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
4. If this does not work, or you are not sure what the Switch's management mode is, you have to reset the device to its factory defaults (Standalone management mode) first. See Section 4.7 on page 66 for more information on resetting the Switch. (Temporarily disconnect the Internet connection to the Switch after the reset process, to prevent the Switch from being managed by NCC again.)

   Note: After performing step 4 and you want to use the Cloud management mode, make sure the Switch is registered in your organization and site in the NCC portal. To register the Switch again, scan the QR code using the Zyxel Nebula Mobile app. See the Section 1.4.1 on page 27 for more information on using the app to register the Switch.

I forgot the IP address for the Switch.

1. You can use the default IP address **https://DHCP-assigned IP** (when connecting to a DHCP server) or **192.168.1.1**. When in Cloud mode, the DHCP-assigned IP address could be found in the NCC portal, in **Site-wide** > **Devices** > **Switches** (The Switch must be registered and added to a site in Nebula in order for it to be managed by Nebula).

   Note: When your computer is directly connected to the Switch, you can always use the domain name **setup.zyxel** to access the Web Configurator. This requires your computer to be able to connect to a DNS server.

2 If the Switch is removed from a site in Nebula, all the settings in the configuration file are reset to the Nebula factory defaults except for the IP address. If you changed the default dynamic IP address to a static IP address while the Switch was in a site in Nebula, the Switch will retain that static IP address after you remove it from the site in Nebula.

3 Use the ZON utility to find the IP address.

4 If you are using the console/USB port, use the command line **show ip** to find the IP address.

5 If the Switch is removed from a site in Nebula, all the settings in the configuration file are reset to the Nebula factory defaults except for the IP address. If you changed the default dynamic IP address to a static IP address while the Switch was in a site in Nebula, the Switch will retain that static IP address after you remove it from the site in Nebula.

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

7 If this does not work, you have to reset the device to its factory defaults. See Section 4.7 on page 66.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is https://DHCP-assigned IP (when connecting to a DHCP server) or 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Switch.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 3.4 on page 46.

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 Switch to its factory defaults, and try to access the Switch with the default IP address. See Section 4.6 on page 65.

6 If the problem continues, contact Zyxel technical support, or try the advanced suggestion.

Advanced Suggestion

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

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).

There is unauthorized access to my Switch through telnet, HTTP and SSH.

Go to the **MONITOR** > **System Log** screen to check for logs of unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **SECURITY** > **Access Control** > **Remote Management** screen for telnet, HTTP and SSH (see Section 55.5 on page 355). Computers not belonging to the secured client set cannot get permission to access the Switch.

The Switch is already registered with NCC, but it is still in Standalone mode; it cannot connect to the NCC.

1. Make sure that NCC Discovery is enabled. Check the three NCC connection status circles on the **DASHBOARD** screen. All status circles display green (normal) when the Switch is connected and managed by NCC. If a circle displays orange (fails), hover a mouse over the circle to see diagnostic messages for troubleshooting. You can also go to the **SYSTEM** > **Cloud Management** screen to check the diagnostic messages.
2. Check your network's firewall or security settings. Make sure the following TCP ports are allowed: 443, 4335, and 6667.
3. Make sure your Switch can access the Internet.
4. Make sure your Switch does not have to go through network authentication such as a captive portal, If your network uses a captive portal, the network administrator may have to create a new VLAN without this requirement. Change your Switch's management VLAN settings as necessary.

67.3 Switch Configuration

I lost my configuration settings after I restarted the Switch.

Make sure you save your configuration into the Switch's non-volatile memory each time you make changes. Click **Save** at the top right of the Web Configurator to save the configuration permanently. See also Section 66.11 on page 441 for more information about how to save your configuration.

I accidentally unplugged the Switch. I am not sure which configuration file will be loaded.

If you plug the power cable back to the Switch, it will reboot and load the configuration file that was used the last time. For example, if **Config 1** was used on the Switch before you accidentally unplugged the Switch, **Config 1** will be loaded when rebooting.

I want to use a different configuration file on the Switch, what should I do?

1. Go to **MAINTENANCE** > **Configuration** > **Restore Configuration**.
2. Click **Choose File** or **Browse** to locate the configuration file you wish to restore.
3. After you have specified the file, click **Restore**. The Switch will run on the restored configuration after the restore process.

I cannot access the NCC portal.

- Check that you are using the correct URL:
  - NCC: *https://nebula.zyxel.com/*
- Make sure your computer's Ethernet card is installed and functioning properly.
- Check that you have Internet access. In your computer, click **Start**, **(All) Programs**, **Accessories** and then **Command Prompt**. In the **Command Prompt** window, enter 'ping' followed by a website such as 'zyxel.com'. If you get a reply, try to ping 'nebula.zyxel.com'.
- Make sure you are using the correct web browser that supports HTML5. View the browser in full screen mode to display the NCC portal properly. Browsers supported are:
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

I cannot log into the NCC portal.

- Open your web browser and go to *https://nebula.zyxel.com.* If you do not have a Nebula Zyxel Account, click **Create account** and create an account.
- If you already have an account but cannot login, click **Forgot Password** to reset the password.

Some features I set using the NCC do not work as expected.

1. Make sure your Switch can access the Internet.
2. Make sure the Switch's **Status** displays "**Online**" in **Site-wide** > **Devices** > **Switches** on the NCC portal.

3 If the Switch is offline when the settings were changed, wait for ten minutes after the Switch goes back online.

4 After changing your Switch settings using the NCC, wait 1 – 2 minutes for the changes to take effect.

5 Check the Switch **Configuration status** in **Site-wide** > **Devices** > **Switches** on the NCC portal. The status should display "**up to date**".

67.4 PoE Supply

My Powered Devices (PDs) are not receiving power.

1 Check the PoE usage of the Switch.

- Check the **PoE Usage** on the **Dashboard**. This field displays the amount of power the Switch is currently supplies to the connected PDs and the total power the Switch can provide to the connected PDs. It also shows the percentage of PoE power usage. Or, see the **PoE** LED on the front panel of your Switch.
- If the PoE usage exceeds the Switch's PoE power budget, follow the step below to configure the PoE power or add another PoE-capable Switch for additional PDs.

2 Check the PoE configuration of the Switch.

- Make sure the **Active** checkbox for the port supplying PoE power to PDs is enabled.
- Check the **Priority** on the ports. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD **Priority** which you configured in **PORT** > **PoE Setup** > **PoE Setup**.
- Check if you have set a pre-defined schedule to control when the Switch enables PoE to provide power on the port in **PORT** > **PoE Setup** > **PoE Time Range Setup**.

3 Make sure the PDs are functional.

- Check whether the PDs are malfunctioning. See your PDs user's guide for more information.
- Make sure the connected PDs support PoE.

4 Make sure the Ethernet cables connected to the PDs are functional.

- Use the correct type of Ethernet cable for the corresponding PoE standard you are using. See Section 1.4.3 on page 30 for the Switch's supported PoE standards and supported Ethernet cables.
- Check whether the Ethernet cables are malfunctioning. Use functional Ethernet cables to reconnect the Switch to the PDs.

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 Zyxel technical support.

67.5 Nebula Registration

I cannot register the Switch in Nebula because the previous owner has registered/locked it.

- To register a pre-owned Switch in Nebula, use the Nebula Mobile app to scan the Nebula QR code on the back label of the Switch.
- To register a pre-owned Switch in Nebula locked by the previous owner, inform the previous owner to remove the Switch from the Nebula organization or contact Zyxel technical support.

I no longer want to use Nebula to manage the Switch, what should I do?

- Remove the Switch from the Nebula organization first. See From Nebula-managed to Standalone Mode on page 30 for details. The Switch will reboot and restore its factory-default settings.
- Make sure the **CLOUD** LED is off or blinking green. See LEDs on page 46 for more information on LED behavior. This means the Switch is operating in standalone mode. Nebula Control Center Discovery is disabled in **SYSTEM** > **Cloud Management** > **Nebula Control Center Discovery** in the Web Configurator.

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.

For Zyxel Communications offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Networks offices, see *https://www.zyxel.com/index.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 (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Kazakhstan
- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *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 Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria

- *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*

Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

France

- Zyxel France
- *https://www.zyxel.com/fr/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 S.r.l.
- *https://www.zyxel.com/it/it*

Norway

- Zyxel Communications A/S
- *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*

Russian Federation

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Slovakia

- Zyxel Slovakia
- *https://www.zyxel.com/sk/sk*

Spain

- Zyxel Iberia
- *https://www.zyxel.com/es/es*

Sweden

- Zyxel Communications A/S
- *https://www.zyxel.com/se/sv*

Switzerland

- Studerus AG
- *https://www.zyxel.com/ch/de-ch*
- *https://www.zyxel.com/fr/fr*

Turkey

- Zyxel Turkey A.S.
- *https://www.zyxel.com/tr/tr*

UK

- Zyxel Communications UK Ltd.
- *https://www.zyxel.com/uk/en-gb*

Ukraine

- Zyxel Ukraine
- *https://www.zyxel.com/ua/uk-ua*

South America

Argentina

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Brazil

- Zyxel Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX B
Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type or code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 251 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example *www.zyxel.com*) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by email.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client or server protocol for the world wide web.

Table 251 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System – NFS is a client or server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 251 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

APPENDIX C
IPv6

Overview

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.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 252 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 253 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and cannot be assigned to a multicast group.

Table 254 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses 4 bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by 4 hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 255

MAC	00	:	13	:	49	:	12	:	34	:	56

Table 256

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

DHCPv6

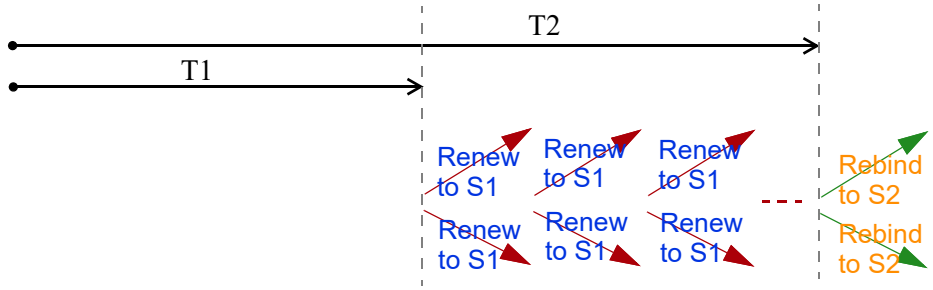
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the

client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Switch uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Switch passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and

forward packets.

- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Switch maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Switch configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Switch also sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Switch uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Switch creates an entry in the default router list cache if the router can be used as a default router.

When the Switch needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Switch uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Switch determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Switch looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 7

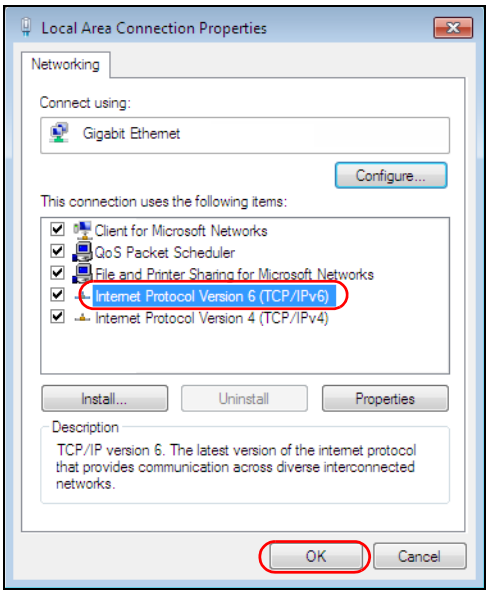
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** check box to enable it.

3 Click **OK** to save the change.



4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is enabled when you enable IPv6 on a Windows 10 PC.

To enable IPv6 in Windows 10:

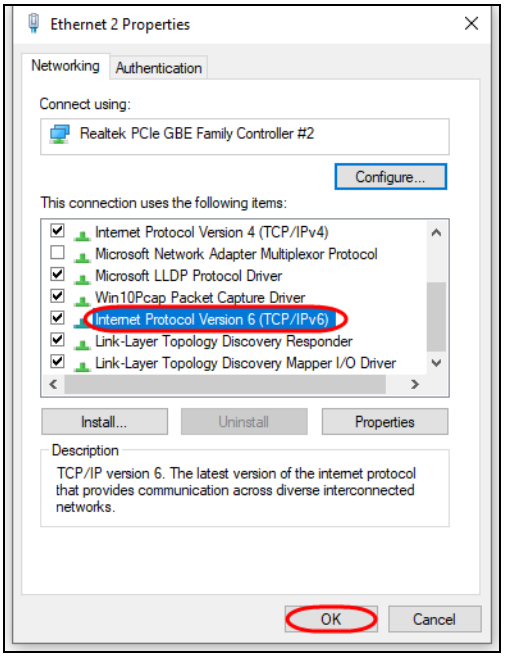
1 Select **Control Panel** > **Network and Sharing Center**.

2 On the left side of the **Network and Sharing Center**, select **Change adapter settings**.

3 Right-click your network connection and select **Properties**.

4 Select the **Internet Protocol Version 6 (TCP/IPv6)** check box to enable it.

5 Click **OK** to save the changes for the selected network adapter.



6 Click **OK** to exit the selected network adapter **Properties** screen.

Example – Enabling DHCPv6 on Windows 10

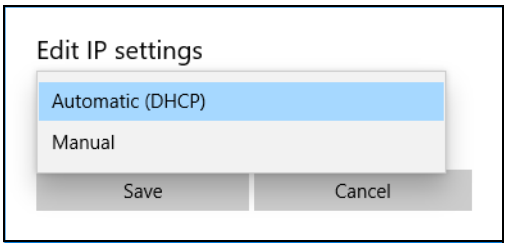
Windows 10 supports DHCPv6 by default. To enable DHCPv6 client on your computer:

1 Select **Start** > **Settings** > **Network & Internet**.

2 On the left side of the **Network & Internet**, select **Ethernet**. Then select the Ethernet network you are connected to.

3 Under **IP assignment**, select **Edit**.

4 Under **Edit IP settings**, select **Automatic (DHCP)** or **Manual**. Then click **Save**.



- When you select **Automatic (DHCP)**, the IP address settings and DNS server address setting are set automatically by your router.
- When you select **Manual**, you can manually set your IP address settings and DNS server address.

Now your computer can obtain an IPv6 address from a DHCPv6 server.

APPENDIX D
Importing a Certificate

When you connect to the Switch Web Configurator using HTTPS, a warning screen "Your connection is not private" may show up. If you see this warning screen, it indicates that your web browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to the website.

This appendix shows you how to import a public key certificate into your web browser to avoid the "Your connection is not private" screen. The web browsers are:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the website to be issued to all visiting web browsers to let them know that the website is legitimate.

Many Zyxel products, such as the Switch, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the Zyxel-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL on your web browser's address bar begins with `https://` or there is a sealed padlock icon () somewhere in the web browser window (not all web browsers show the padlock in the same location).

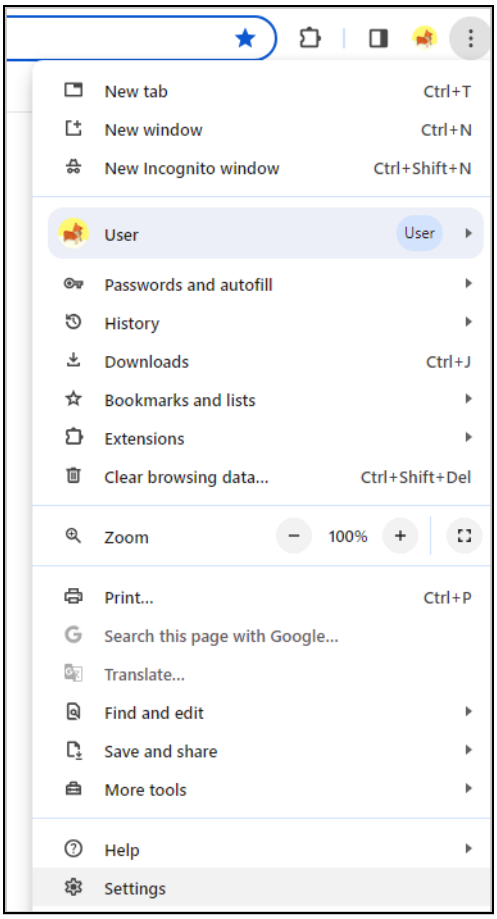
Note: You need a certificate from a trusted Certification Authority (CA) for this Switch.

Importing a Certificate to Google Chrome and Microsoft Edge

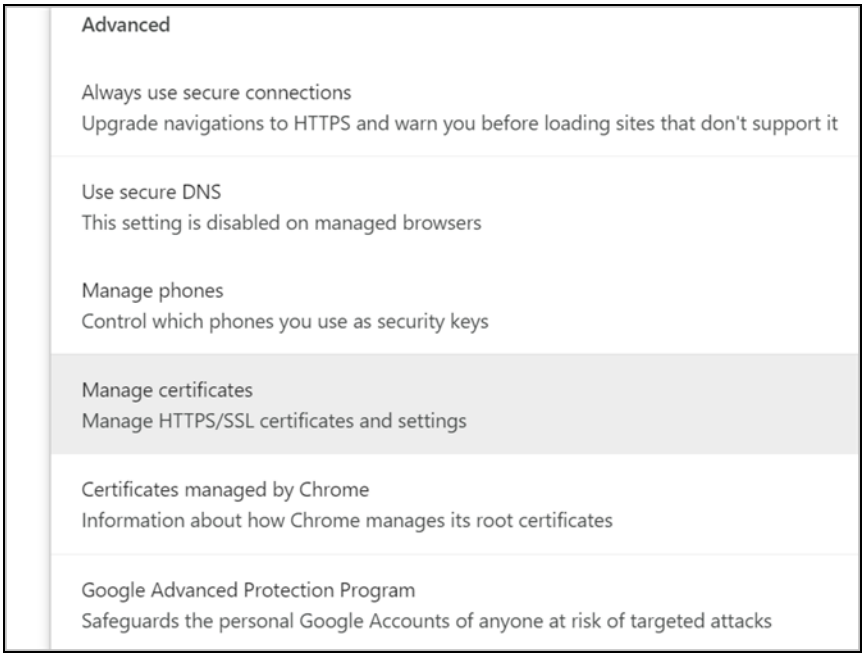
The following example uses Google Chrome on Windows 10. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorial.

The Importing process is quite similar between Google Chrome and Microsoft Edge. The following procedures in Google Chrome can apply the same way in Microsoft Edge.

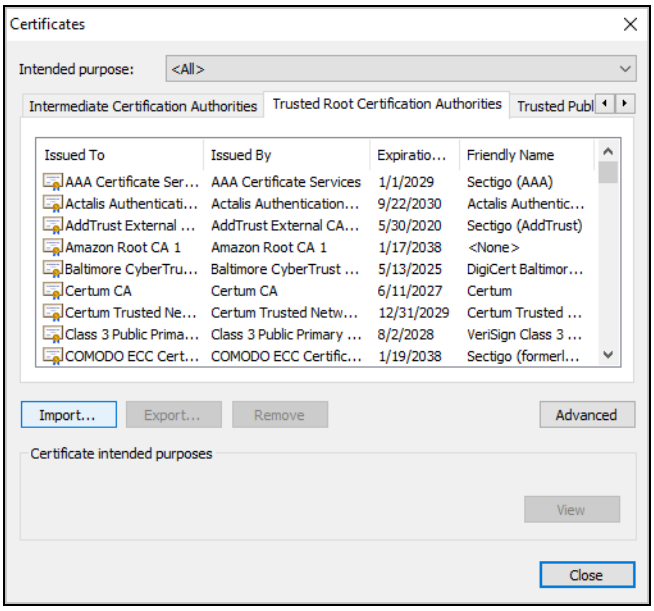
1 Open the Google Chrome browser. Click the three dots on the upper right. Then choose **Settings**.



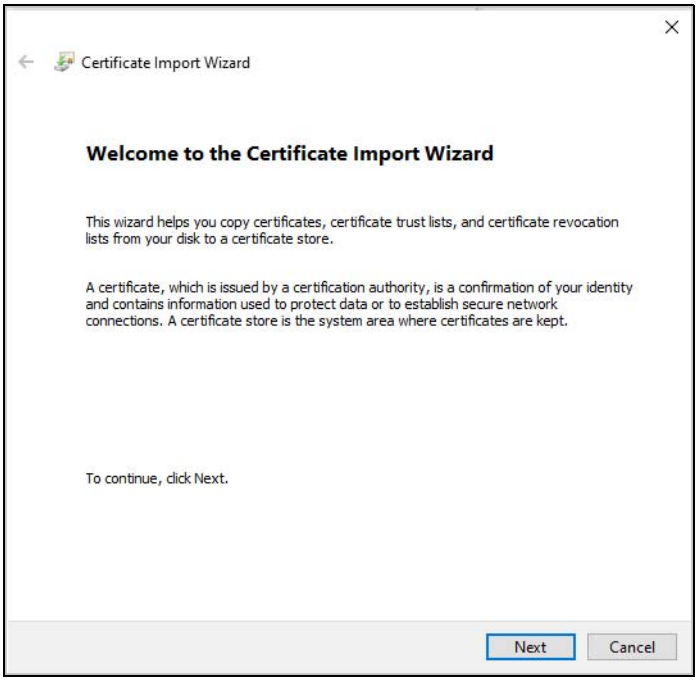
2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates**.
In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates**.



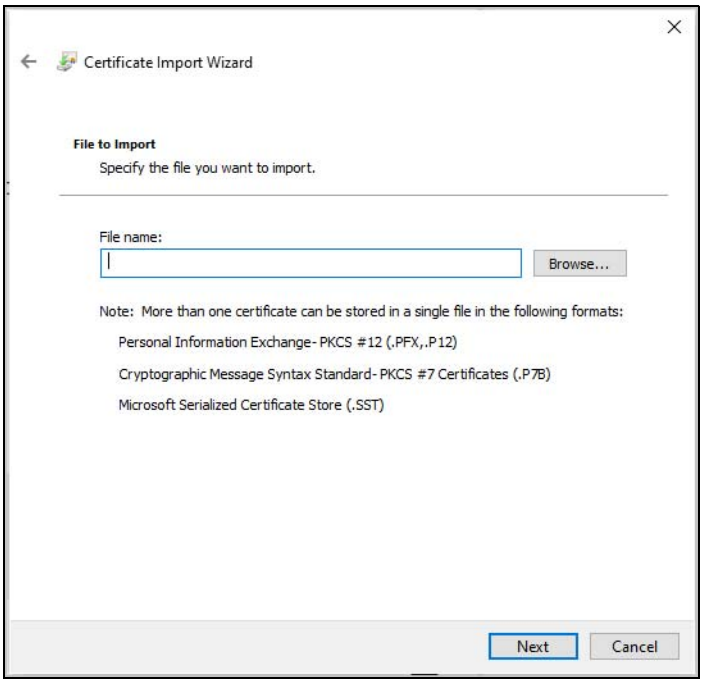
3 Select the **Trusted Root Certification Authorities** tab and click **Import**.



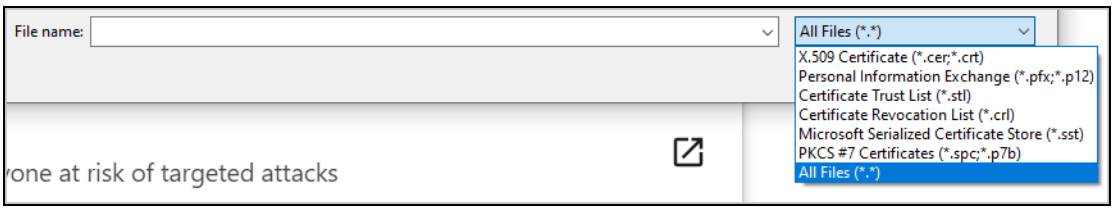
4 The **Certificate Import Wizard** screen appears. Click **Next** to continue.



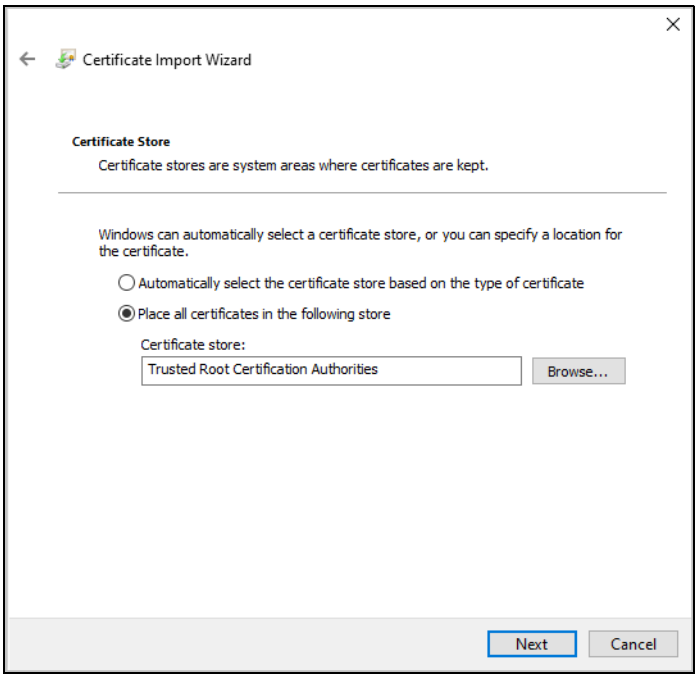
5 Click **Browse** to select a certificate already saved in your computer and click **Next** to continue.



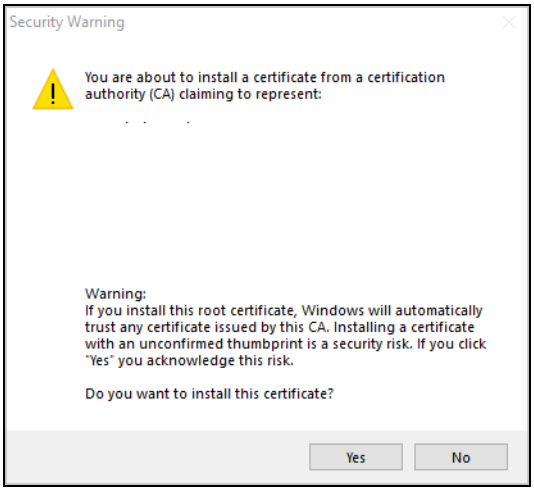
6 Select **All Files** to locate the certificate in your computer.



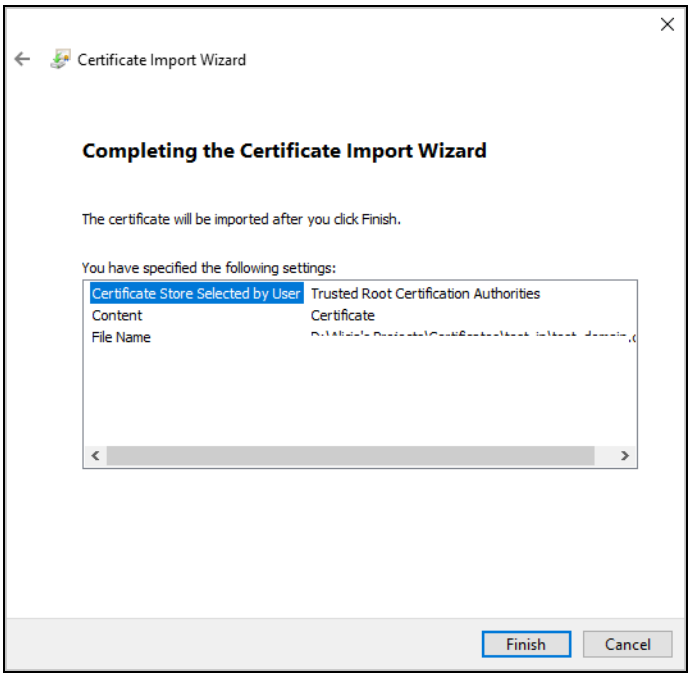
7 Two options are available for certificate stores. One is **Automatically select the certificate store based on the type of certificate**. This means the certificate import wizard can identify from the certificate whether it is a CA certificate or a personal certificate, and install it into the appropriate certificate store. The other option is **Place all certificates in the following store**. With this option, you can choose the desired folder for the certificate store. After selection, click **Next**.



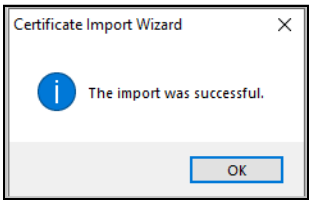
8 A security warning message appears, click **Yes** to continue.



9 Click **Finish** to exit the wizard.



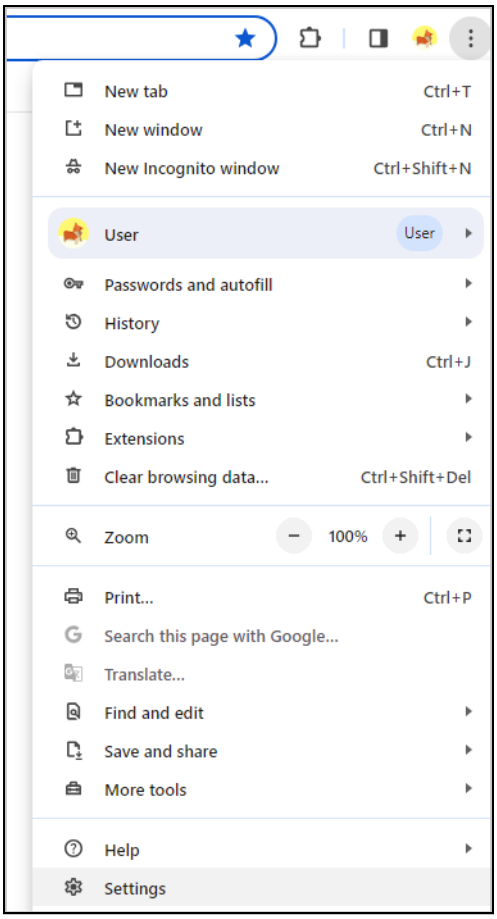
A pop-up screen informs you that the import was successful.



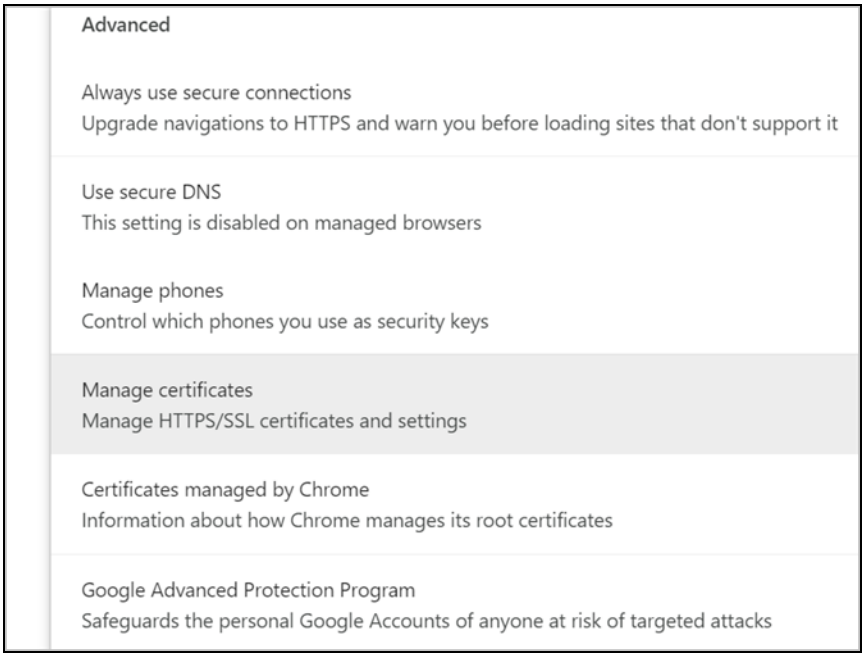
Remove a Certificate in Google Chrome and Microsoft Edge

This section shows you how to remove a public key certificate in Google Chrome and Microsoft Edge on Windows 10.

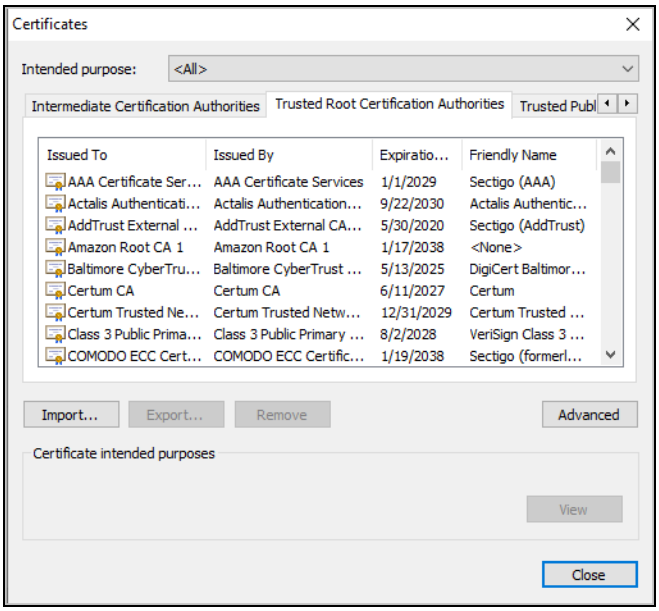
1 Open your web browser, click the three dots on the upper right, and click **Settings**.



2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates**.
In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates**.

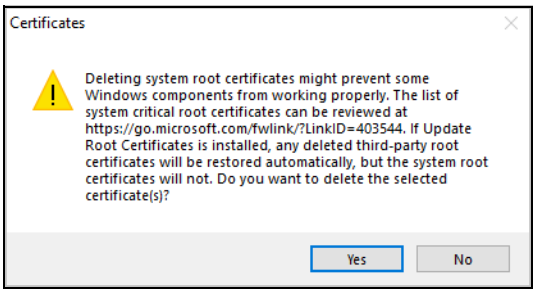


3 On the **Certificates** screen, select the **Trusted Root Certification Authorities** tab.



4 Select the certificate you want to remove and click **Remove**.

5 Click **Yes** when you see the following warning message.

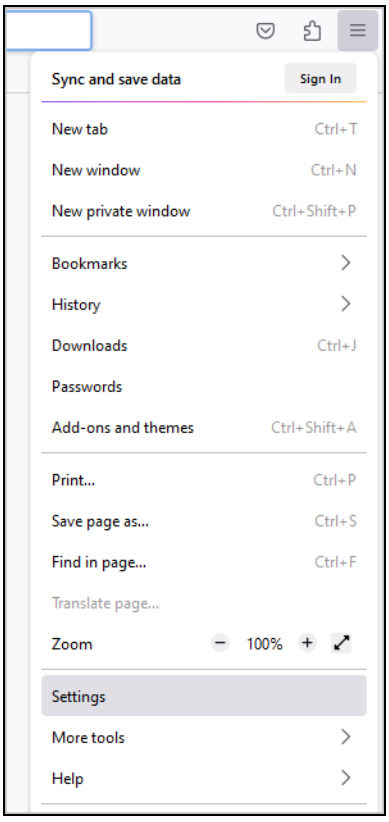


6 Confirm the details displayed in the warning message and click **Yes**.

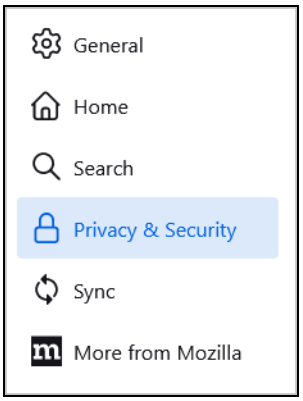
Import a Certificate to Mozilla Firefox

The following example uses Mozilla Firefox on Windows 10. You first have to store the certificate in your computer and then install it as a Trusted Root CA. To import a certificate to the Firefox browser, do the following:

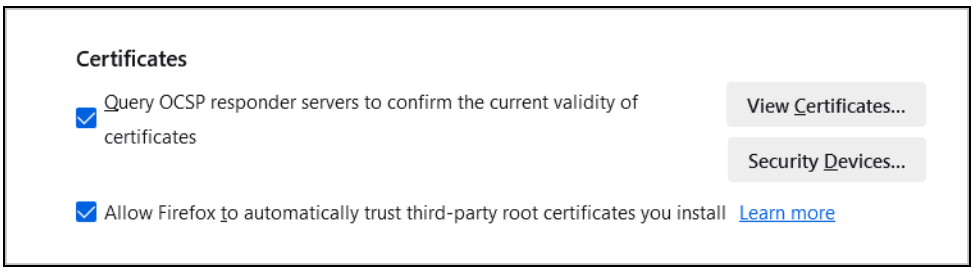
1 Open the Firefox browser and click the **Open application menu** icon on the upper right. Then click **Settings**.



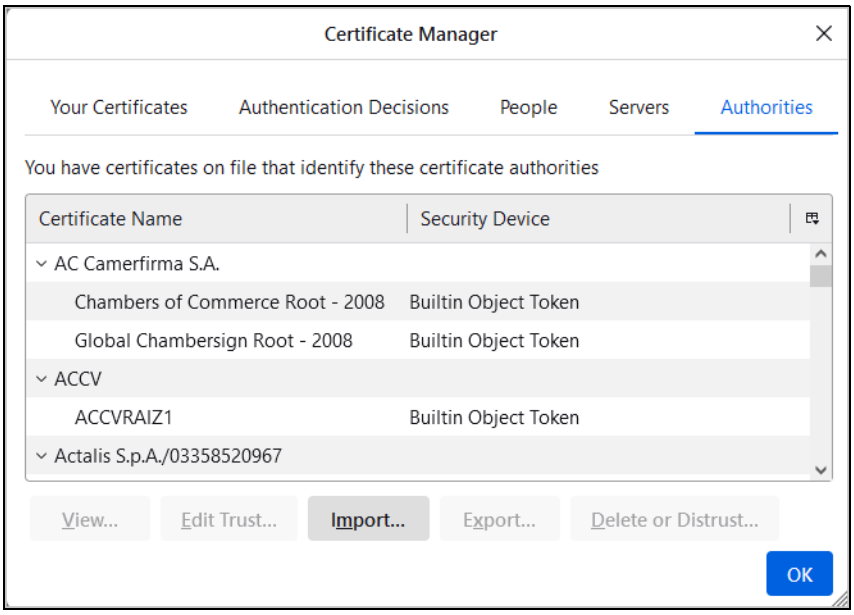
2 Click **Privacy & Security**.



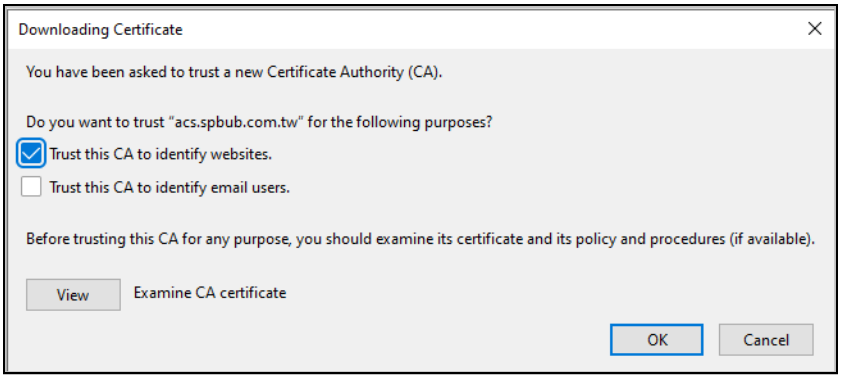
3 On the **Privacy & Security** screen, scroll down to locate **Certificates** and click **View Certificates**.



4 On the **Certificate Manager** screen, select the **Authorities** tab and click **Import**.



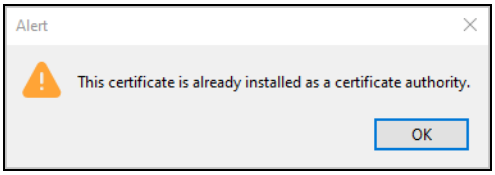
5 Open the certificate file in your computer and the **Downloading Certificate** screen appears. Click **Trust this CA to identify websites**. Click **View** to examine the imported CA certificate.



6 When the certificate details appear, view the content to confirm the correct organization name. Confirm that the validity period has the correct start and end dates. The **Common Name** can be either an IP address or domain name. Confirm that the client's IP address or domain name aligns with the **Common Name** on the certificate. If all the information on the certificate is correct, close the certificate screen and click **OK**.

The certificate file is now installed in the Firefox browser.

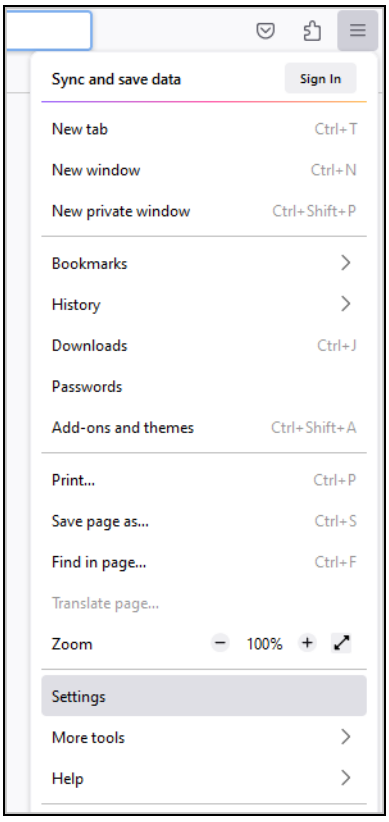
To check if the import is successful, click **Import** to select the same certificate again to see if the alert **This certificate is already installed as a certificate authority** pops up.



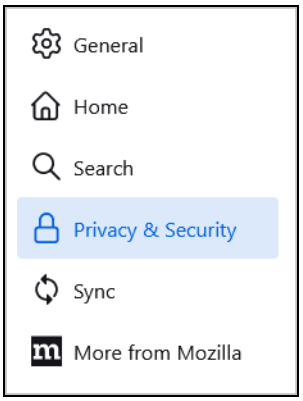
Removing a Certificate in Mozilla Firefox

This section shows you how to remove a public key certificate in Mozilla Firefox.

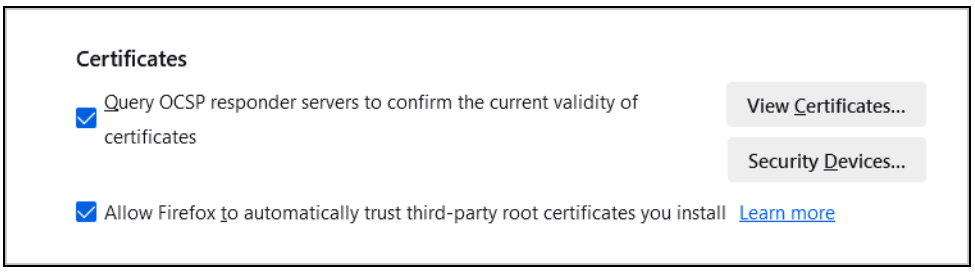
1 Open the Firefox browser and click the **Open application menu** icon on the upper right. Then click **Settings**.



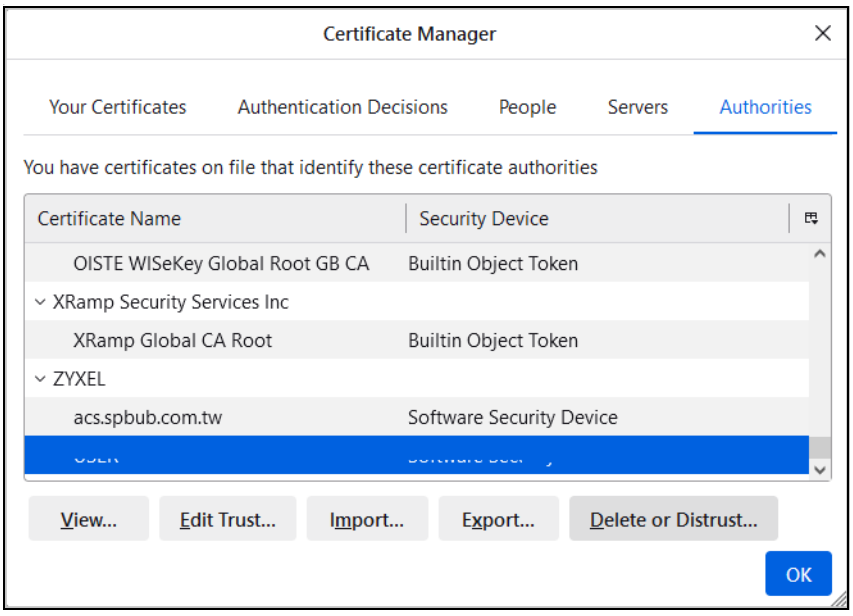
2 Click **Privacy & Security**.



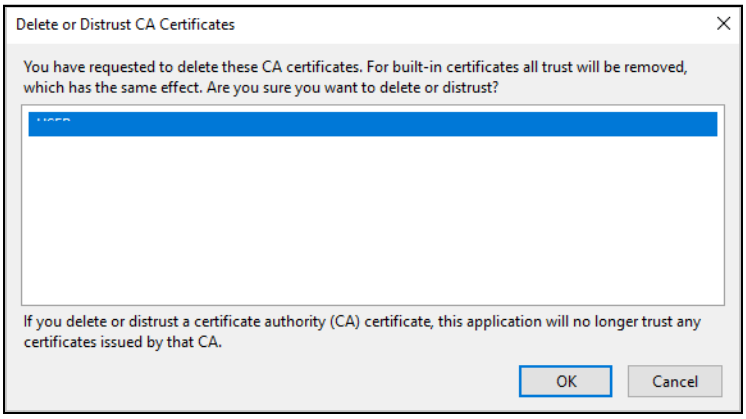
3 On the **Privacy & Security** screen, locate **Certificates** and click **View Certificates**.



4 In the **Certificate Manager** screen, click the **Authorities** tab and select the certificate you want to remove. Then, click **Delete or Distrust**.



5 On the next screen, click **OK**.



The next time you visit the web site with the public key certificate removed, a certification error will appear.

APPENDIX E
Legal Information

Copyright

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America

The following information applies if you use the product within USA area.

US Importer: Zyxel Communications, Inc, 1130 North Miller Street Anaheim, CA92806-2001, *https://www.zyxel.com/us/en/*

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.

Innovation, Science and Economic Development Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

Europe and the United Kingdom

The following information applies if you use the product within the European Union and United Kingdom.

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

- To avoid possible eye injury, do NOT look into an operating fiber-optic module's connector.
- Do NOT use this device 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 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 device 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, 120V 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 device, please contact your local city office, your household waste disposal service or the store where you purchased the device.
- 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 by qualified service personnel. 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.
- If your device has an earthing screw (frame ground), connect the screw to a ground terminal using an appropriate AWG ground wire. Do this before you make other connections.
- If your device has no earthing screw, but has a 3-prong power plug, make sure to connect the plug to a 3-hole earthed socket.
- 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.
- Do not put the device in a place that is humid, dusty or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.

- CLASS 1 LASER PRODUCT & “IEC 60825-1:2014”
- Caution – Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Important Safety Instructions

1 Warning! Energy Hazard. Remove all metal jewelry, watches, and so on from your hands and wrists before serving the Switch.

2 Caution! The RJ-45 jacks are not used for telephone line connection.

3  Hazardous Moving Parts. Keep body parts away from fan blades.

4  Hot Surface. Do not touch.

1 Avertissement: Risque de choc électrique. Retirer tout bijoux en métal et votre montre de vos mains et poignets avant de manipuler cet appareil.

2 Attention: Les câbles RJ-45 ne doivent pas être utilisés pour les connections téléphoniques.

3  Mobilité des pièces détachées. S'assurer que les pièces détachées ne sont pas en contact avec les pales du ventilateur.

4  Surface brûlante. Ne pas toucher.

Environment Statement

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.

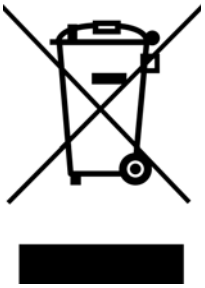
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung 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

以下訊息僅適用於產品銷售至台灣地區

- 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。
- 為避免電磁干擾，本產品不應安裝或使用於住宅環境。

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。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 (如 : 台灣供應電壓 110 伏特)。
- 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。

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): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: 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 *https://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 *https://www.zyxel.com/global/en/support/warranty-information*.

Registration

Register your product online at *www.zyxel.com* to receive email notices of firmware upgrades and related information.

Trademarks

The trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Index

Numbers

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z