ZYXEL NETWORKS

User's Guide

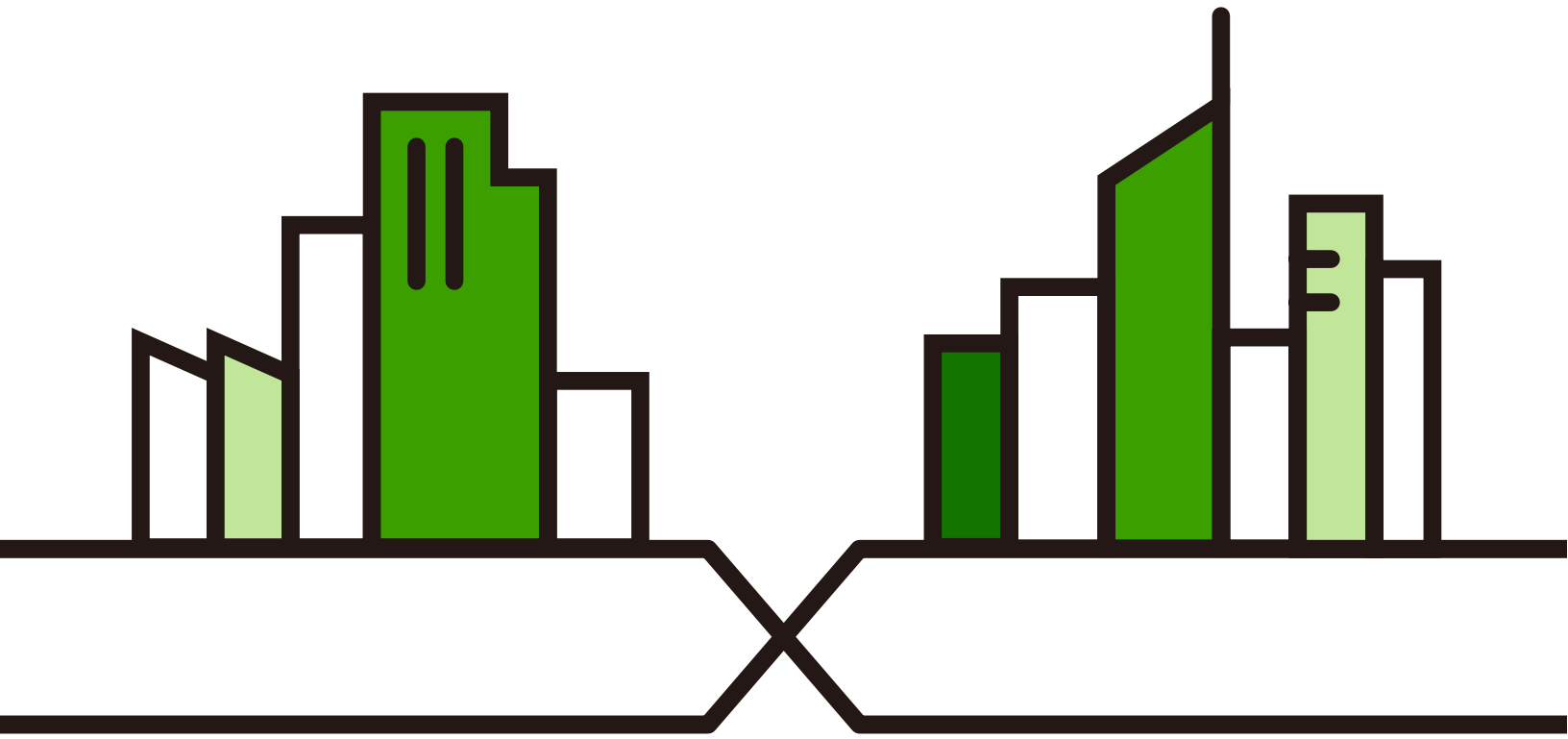
GS1200v3 Series

GS1200-5v3 / GS1200-5HPv3 / GS1200-8v3 / GS1200-8HPv3 / GS1200-10v3

5-Port / 8-Port / 10-Port Web Managed (PoE) Gigabit Switch

Default Login Details	
LAN IP Address	https://DHCP-assigned IP or 192.168.1.3
Password	On the back label on the Switch

Version 1.00 Edition 3, 03/2026



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. 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.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Switch and access the Web Configurator.

- 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

- The GS1200-5v3, GS1200-5HPv3, GS1200-8v3, GS1200-8HPv3, and GS1200-10v3 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, **QoS** > **Port-Based QoS** means you first click **QoS** in the navigation panel, then the **Port-Based QoS** sub menu to get to that screen.

Icons Used in Figures

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

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

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Getting to Know Your Switch

1.1 Introduction

This chapter introduces the main features and applications of the Switch. The GS1200 Series consists of the following models:

- GS1200-5v3
- GS1200-5HPv3
- GS1200-8v3
- GS1200-8HPv3
- GS1200-10v3

You can easily connect different devices, such as computers, network storage devices, IP cameras, print servers to your home network.

The PoE ports on the GS1200-5HPv3 and GS1200-8HPv3 support Power over Ethernet, including IEEE 802.3at High Power (PoE+) and IEEE 802.3af (PoE) standards. They can provide power to IP cameras, wall-mounted access points, and other devices that may be installed far from a power outlet. These devices receive power from the Switch through an Ethernet port. 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.

The Switch also provides a utility like Web Configurator to give you an easy configuration for VLAN, QoS, basic system management, and firmware upgrade. The Switch is compliant with IEEE 802.3az (Energy Efficient Ethernet Standard), and provides power-saving benefits without compromising performance.

VLANs allow you to limit access to a specified group of users by dividing workstations into different isolated LAN segments.

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.

Bandwidth control allows you to set the maximum bandwidth allowed in kilobits per second (kbps) for incoming and out-going traffic flow on a port.

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

Table 1 GS1200 Series Comparison Table

MODEL	GS1200-5V3	GS1200-5HPV3	GS1200-8V3	GS1200-8HPV3	GS1200-10V3
Total Port Number	5	5	8	8	10
10/100/1000 Mbps PoE Ports	–	Ports 1 to 4	–	Ports 1 to 4	–
10/100/1000 Mbps Ethernet Ports	Ports 1 to 5	Port 5	Ports 1 to 8	Ports 5 to 8	Ports 1 to 8

Table 1 GS1200 Series Comparison Table (continued)

MODEL	GS1200-5V3	GS1200-5HPV3	GS1200-8V3	GS1200-8HPV3	GS1200-10V3
100 Mbps/1Gbps SFP Interface	–	–	–	–	Ports 9, 10
Link Aggregation	LAG 1: Port 3 and 4	LAG 1: Port 3 and 4	LAG 1: Port 3 and 4 LAG 2: Port 7 and 8	LAG 1: Port 3 and 4 LAG 2: Port 7 and 8	LAG 1: Port 7 and 8 LAG 2: Port 9 and 10
802.1p QoS and Port-Based QoS	v	v	v	v	v
IGMP Snooping v1/v2 and v3 Compatible	v	v	v	v	v
Broadcast Storm Control	v	v	v	v	v
Port Isolation	v	v	v	v	v
Bandwidth Control	v	v	v	v	v
Management VLAN	v	v	v	v	v
Firmware Upgrade	v	v	v	v	v
Configuration Restore and Backup	v	v	v	v	v

Bandwidth control allows you to set the maximum bandwidth allowed on a port.

1.1.1 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.

Table 2 GS1200v3 Series Models and PoE Features

POE FEATURES	GS1200-5HPV3	GS1200-8HPV3
IEEE 802.3at PoE+	Ports 1 – 4	Ports 1 – 4
Power Management Mode	Classification (default)	Classification (default)
PoE Power Budget	68 W	68 W

Table 3 PoE Standards

POE FEATURES	POE				POE+
IEEE Standard	IEEE 802.3af				IEEE 802.3at
PoE Type	Type 1				Type 2
Switch Port Power					
IEEE Power Classification	Class 0	Class 1	Class 2	Class 3	Class 4
Maximum Power Per Port	15.4 W	4 W	7 W	15.4 W	30 W

Table 3 PoE Standards

POE FEATURES	POE	POE+
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

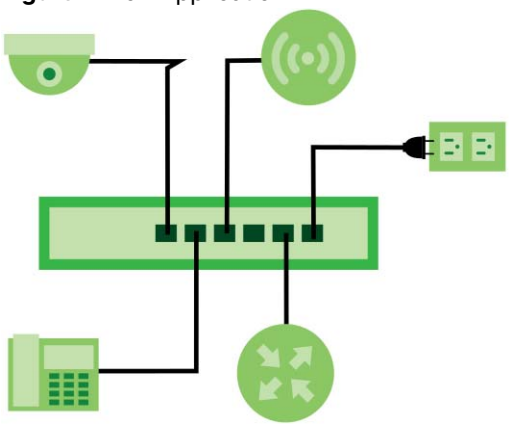
1.2 Applications

This section shows a few examples of using the Switch in various network environments.

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 Application

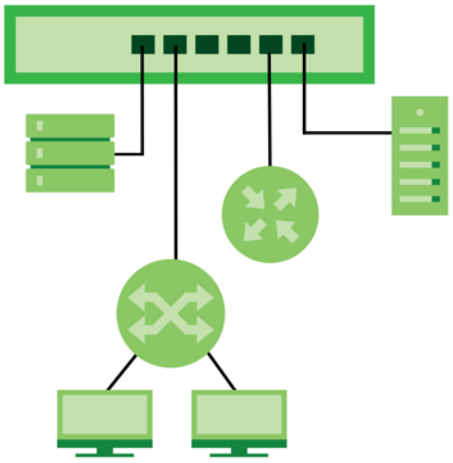


1.2.2 Backbone Example Application

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.

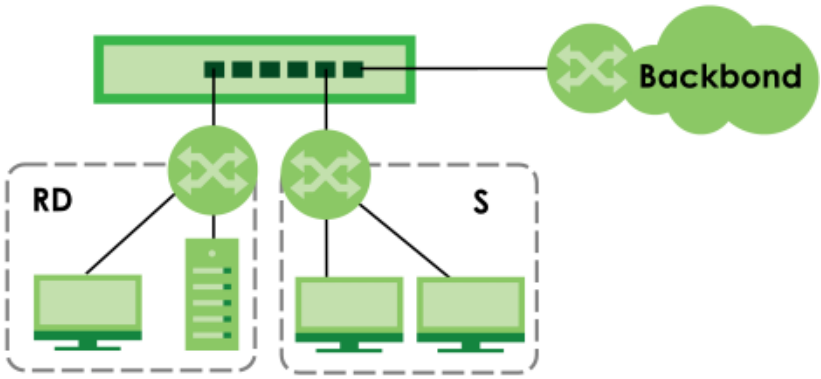
Figure 2 Backbone Application



1.2.3 Bridging 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.

Figure 3 Bridging Application



1.2.4 VLAN Application Example

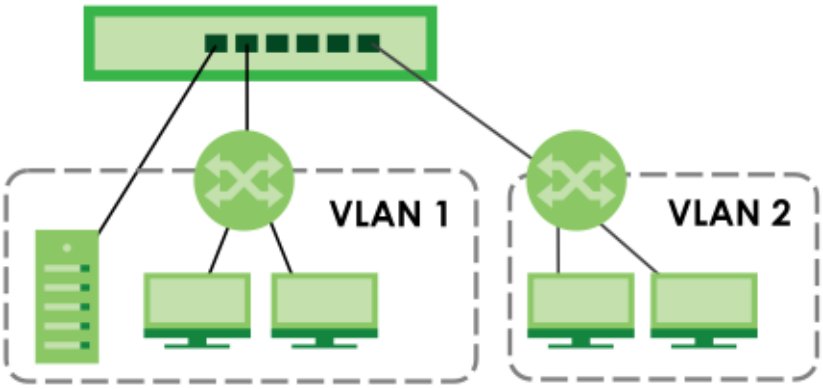
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes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

1.2.4.1 Tag-based VLAN Example

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

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of **VLAN1**. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



1.3 Ways to Manage the Switch

- Web Configurator. This allows easy Switch setup and management using a (supported) web browser. See Chapter 4 on page 25.
- SNMP. The Switch can be monitored by an SNMP manager. See SNMP on page 70.
- ZON Utility. ZON Utility is a program designed to help you deploy and perform initial setup on a network more efficiently. See Section 4.4 on page 27.

1.4 Good Habits for Managing the Switch

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

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

CHAPTER 2
Hardware Installation

2.1 Installation Scenarios

This chapter shows you how to install and connect the Switch. The Switch can be:

- Freestanding Installation Procedure
- Wall Mounting

2.2 Safety Precautions

Please observe the following before using the Switch:

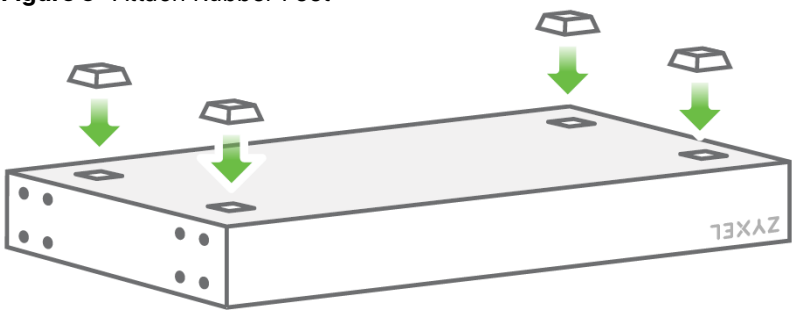
- It is recommended to ask an authorized technician to attach the Switch on a desk or to the rack or wall. Use the proper screws to prevent damage to the Switch. See the **Screw Specifications** figure in this chapter to know the type of screw and screw driver for this model.
- Make sure there is at 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 cable.

2.2.1 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 5 Attach 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 Switch 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.

2.2.2 Wall Mounting

The distance between mounting holes for each Switch is as follows.

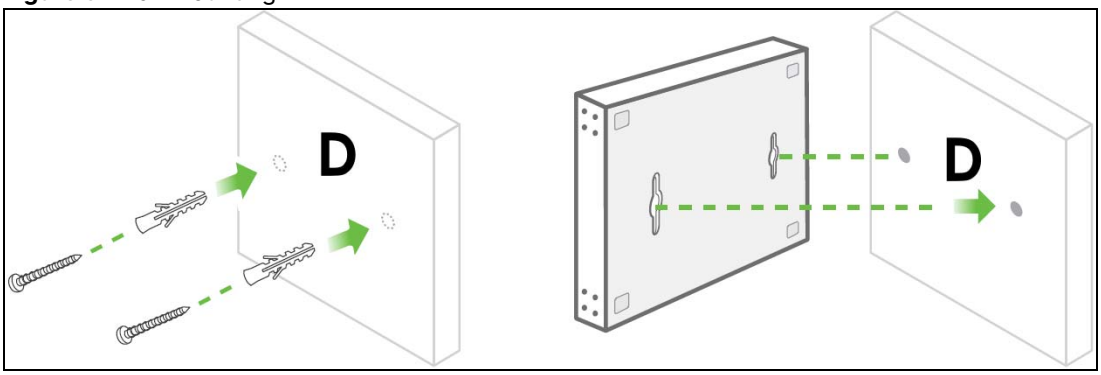
Table 4 Wall Mounting Distances

MODEL	DISTANCE 'D' BETWEEN MOUNTING HOLES
GS1200-5v3	60 mm / 2.36 in
GS1200-8v3	100 mm / 3.94 in
GS1200-5HPv3	100 mm / 3.94 in
GS1200-8HPv3	100 mm / 3.94 in
GS1200-10v3	94 mm / 3.70 in

Do the following to mount your Switch on a wall.

1 Drill two holes a distance 'D' apart into a wall.

Figure 6 Wall Mounting



2 Place two screw anchors in the holes. Screw two screws into the screw anchors. Do not screw the screws all the way in to the wall; leave a small gap between the head of the screw and the wall.

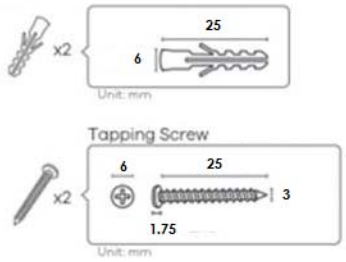
3 The gap must be big enough for the screw heads to slide into the screw slots and the power cord to run down the back of the Switch.

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

4 Use the mounting holes on the Switch to hang the Switch on the screws.

Wall mount the Switch with the Ethernet ports facing down and the ventilation holes on the side.

Figure 7 Screw Specifications



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 Front Panel

The following figures show the front panels of the Switch.

Figure 8 Front Panel: GS1200-5v3

Figure 9 Front Panel: GS1200-5HPv3

Figure 10 Front Panel: GS1200-8v3

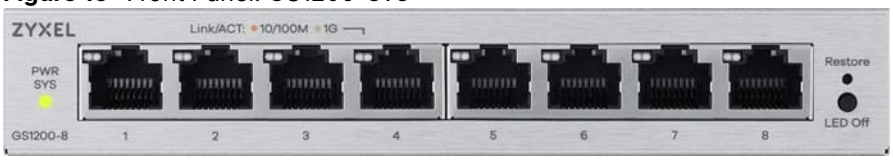


Figure 11 Front Panel: GS1200-8HPv3

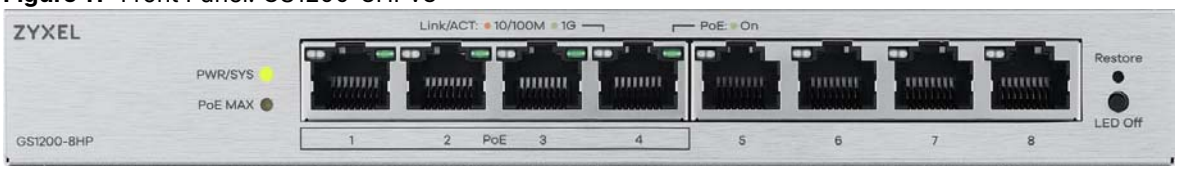
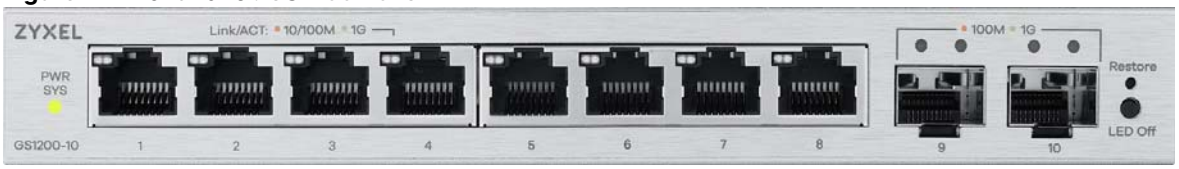


Figure 12 Front Panel: GS1200-10v3



3.1.1 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 5 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The system power is on.
		Blinking	The system is starting up.
		Off	The system power is off.
LINK/ACT	Amber (10/100 Mbps) Green (1000 Mbps)	On	The port has a successful 10/100 Mbps or 1000 Mbps connection.
		Blinking	The system is transmitting data through the port.
		Off	The port is disconnected or disabled. If you enable **Loop Prevention** in the **Port** screen, and a loop happens on two ports, the higher-numbered port will be off.
PoE (GS1200-5HPv3 & GS1200-8HPv3)	Green	On	PoE is enabled and power is supplied to the connected PoE-enabled device.
		Off	PoE is disabled or power is not being supplied.
PoE MAX (GS1200-5HPv3 & GS1200-8HPv3)	Amber	On	More than 60 W has been supplied to the PoE-enabled devices, and the PoE power output is approaching the power budget.
		Off	Less than 60 W has been supplied to the PoE-enabled devices.

3.1.2 LED Off Button

Press the **LED Off** button to toggle all LEDs on or off. Note that the **PWR/SYS** LEDs are not affected by this button.

3.1.3 Restore Button

Press and hold the **Restore** button for more than 3 seconds until the **PWR/SYS** LED blinks green to restore the Switch to the factory default settings. See Section 3.1.1 on page 19 for more information about the LED behavior.

3.1.4 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 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.

3.1.4.1 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 ?ber optic cables and the transceiver. Insert the ?ber optic cable into the transceiver.

Figure 13 Latch in the Lock Position

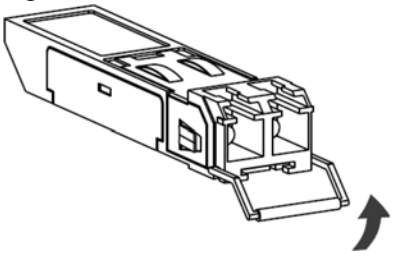


Figure 14 Transceiver Installation Example

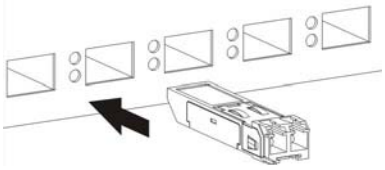
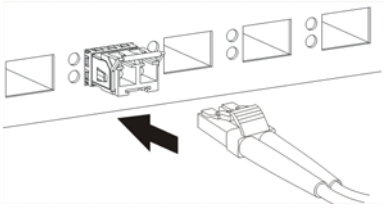


Figure 15 Connecting the Fiber Optic Cables



3.1.4.2 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 ?nger 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 16 Removing the Fiber Optic Cables

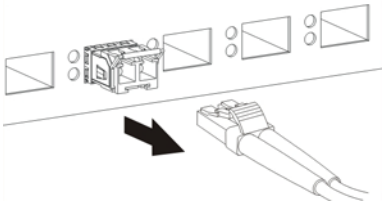


Figure 17 Opening the Transceiver's Latch Example

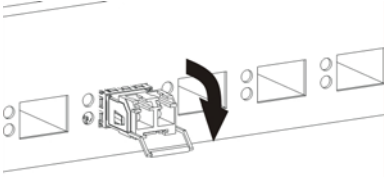
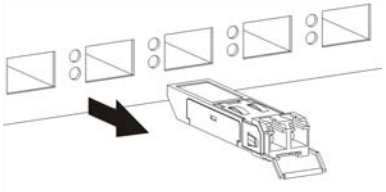


Figure 18 Transceiver Removal Example



3.2 Rear Panel

The following figures show the rear panels of the Switch.

Figure 19 Rear Panel: GS1200-5v3

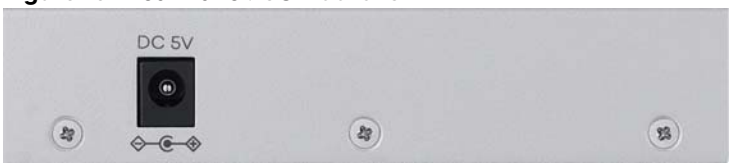


Figure 20 Rear Panel: GS1200-5HPv3

Figure 21 Rear Panel: GS1200-8v3

Figure 22 Rear Panel: GS1200-8HPv3

Figure 23 Rear Panel: GS1200-10v3

3.2.1 Power Connector

Note: Make sure you are using the correct power source as shown on the panel.

To connect power to the Switch, insert the female end of the power cord to the DC power receptacle on the rear panel. Connect the other end of the supplied power cord to a power outlet. Make sure that no objects obstruct the airflow.

3.2.2 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 power supply to ground the Switch.

The grounding terminal and 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 separated from 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.

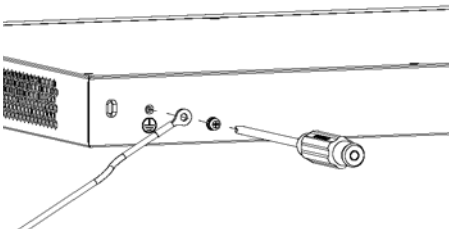
Any device that is located outdoors and connected to this product must be properly grounded and surge protected. To the extent permissible by your country's applicable law, failure to follow these guidelines could result in damage to your Switch which may not be covered by its warranty.

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

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

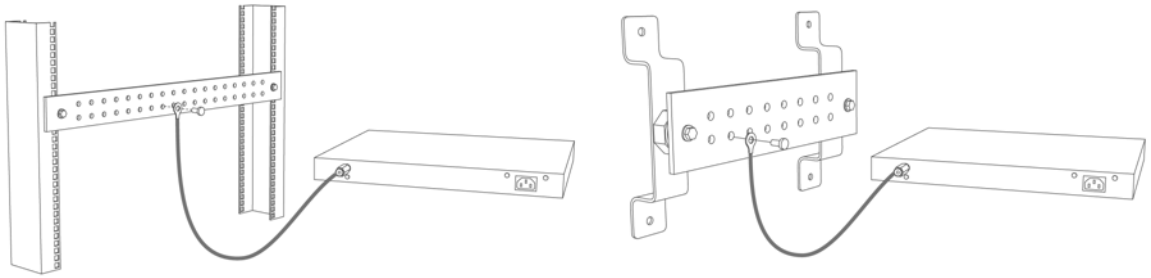
2 Secure a green and yellow ground cable (16 AWG or smaller) to the Switch's rear panel using the ground screw.

Figure 24 Grounding



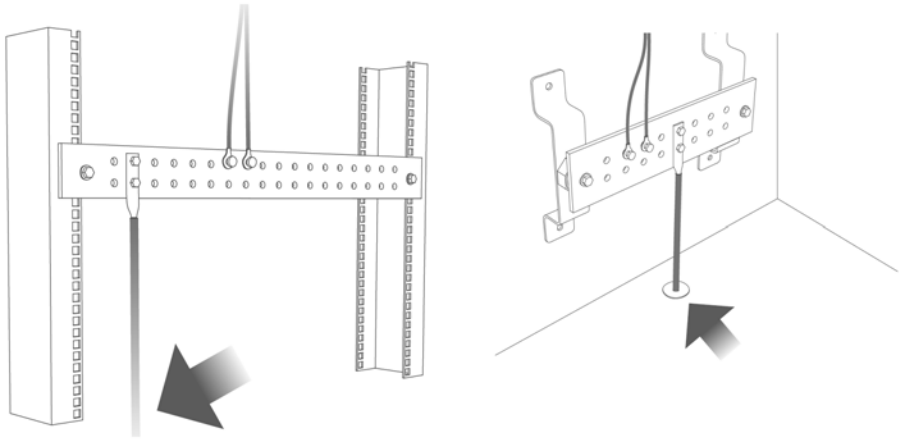
3 Attach the other end of the ground cable to a grounding bar located on the rack where you install the Switch or to an on-site grounding terminal.

Figure 25 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 26 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.

CHAPTER 4
Web Configurator

4.1 Overview

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

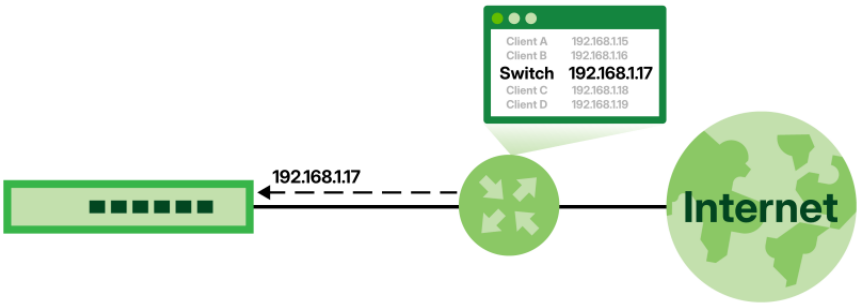
The Web Configurator is an HTML-based management interface that allows easy system setup and management through a web browser. Use a web browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

4.2 Access the Switch

The Switch may have a dynamic (default) or static IP address.

Dynamic IP Address

By default, the Switch operates as a DHCP client and automatically obtains an IP address when connected to a network with an active DHCP server. The graphic below shows an example.



1 Use one of these methods to find the dynamic IP address of the Switch

1a Use the ZON Utility to check the Switch's IP address (See Section 4.4 on page 27 for details).

1b Log in to the router and check its DHCP clients list to find the IP address assigned to the Switch.

2 Open your web browser and enter the IP address of the Switch in the address bar to access the Web Configurator.

Static IP Address

If the Switch does not receive a dynamic IP address, the Switch will assign itself a management IP address of 192.168.1.3/24. In this case, you can access the Switch and change the management IP address to a static IP address that is in the network where the Switch will be deployed.

1 Make sure your Switch is not connected to a network.

2 Set your computer's IP address manually to one that is in the same subnet as the Switch's static IP address. The Switch's default IP is 192.168.1.3, you can assign your computer any IP address from 192.168.1.4 to 192.168.1.254.

3 Open your web browser and enter the 192.168.1.3 in the address bar to access the Web Configurator.

4 Go to the **Management** screen and set the Switch's IP address to an available static IP address that is in the network where the Switch will be deployed. See Chapter 14 on page 70.

Note: Make sure you can use the static IP address. Do not randomly assign one.

5 Your computer will be disconnected from the Switch once the static IP address is applied. Change your computer's network settings to use a DHCP-assigned IP address and connect it to the network where you will deploy the Switch.

6 On your computer, open a web browser and enter the IP address of the Switch that you configured above.

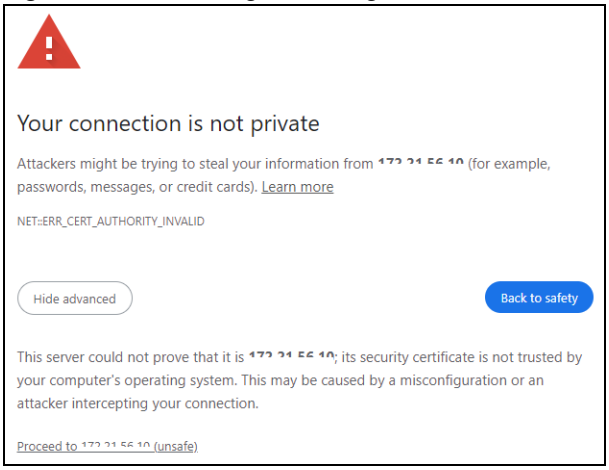
4.3 Log in to the Web Configurator

Log in to the Web Configurator after accessing the Switch.

1 If a "Your connection is not private" screen appears, click **Advanced** and **Proceed to DHCP-assigned IP (unsafe)** to go to the **Log in** screen. This screen appears as the Switch uses a certificate for the HTTPS connection.

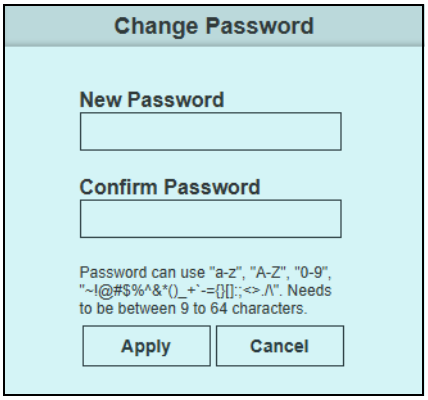
Note: If you see this warning page, it indicates that your browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to the login IP address.

Figure 27 Unsafe Login Warning



2 The **Log in** screen appears. Enter the default password located on the back label of the Switch.

3 The following screen displays if you log into the Switch for the first time. Enter a new password. Password length has to be between 9 and 64 characters. Allowed characters include lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and special characters such as ~ ! @ # $ % ^ & * ( ) _ + ` - = { } [ ] : ; < > . / \. Spaces are not allowed. Retype it to confirm and click **Apply** to view the first Web Configurator screen.



4.4 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).

4.4.1 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.

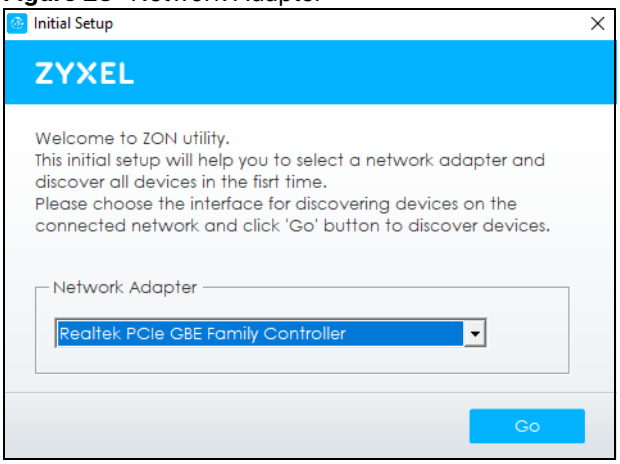
- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280 by 800)

4.4.2 Run the ZON Utility

1 Double-click the ZON Utility to run it.

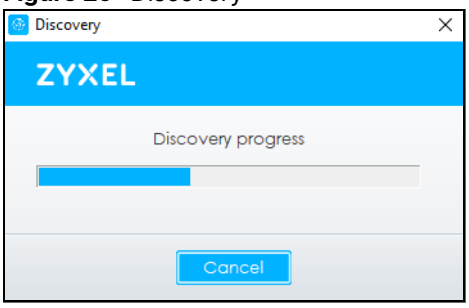
2 Select a network adapter to which your supported devices are connected.

Figure 28 Network Adapter



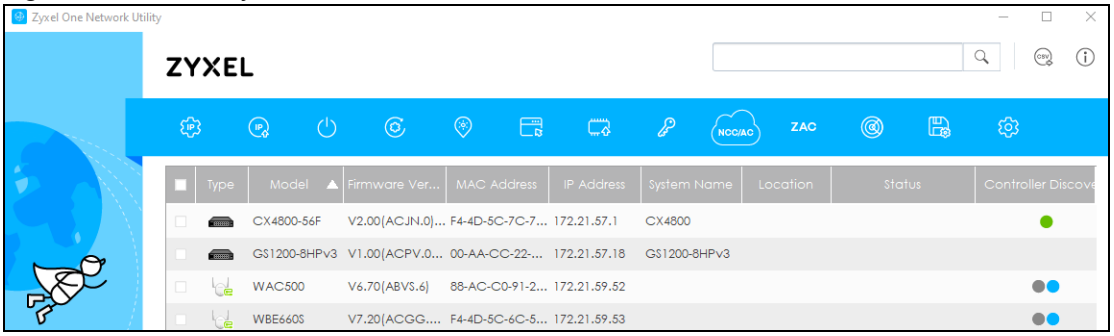
3 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 29 Discovery



4 The ZON Utility screen shows the devices discovered.

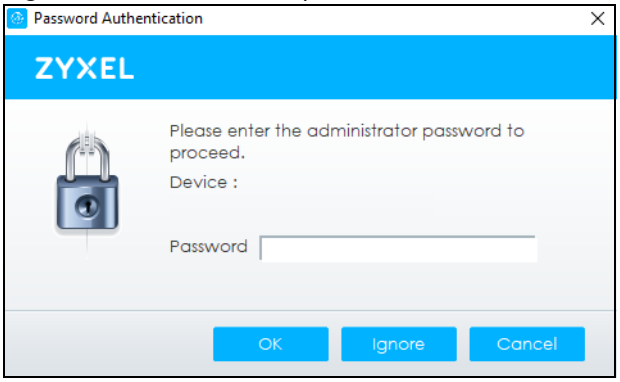
Figure 30 ZON Utility Screen



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 31 Password Prompt



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

Table 6 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.

Table 6 ZON Utility Icons (continued)

ICON	DESCRIPTION
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.

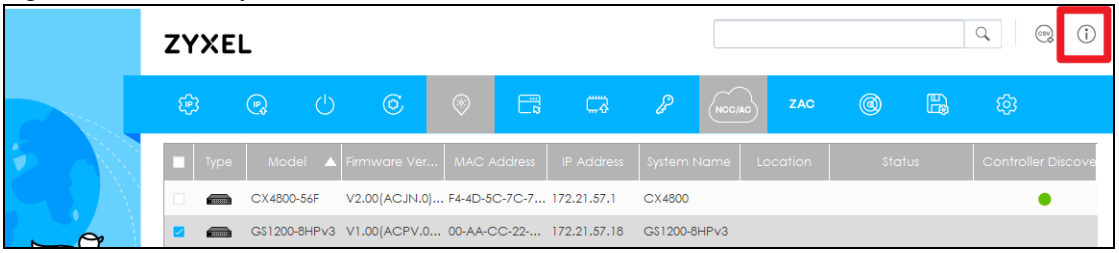
The following table describes the fields in the ZON Utility main screen.

Table 7 ZON Utility Fields

LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.
IP Address	This field displays the IP address of an internal interface on the discovered device that first received 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 32 ZON Utility Screen

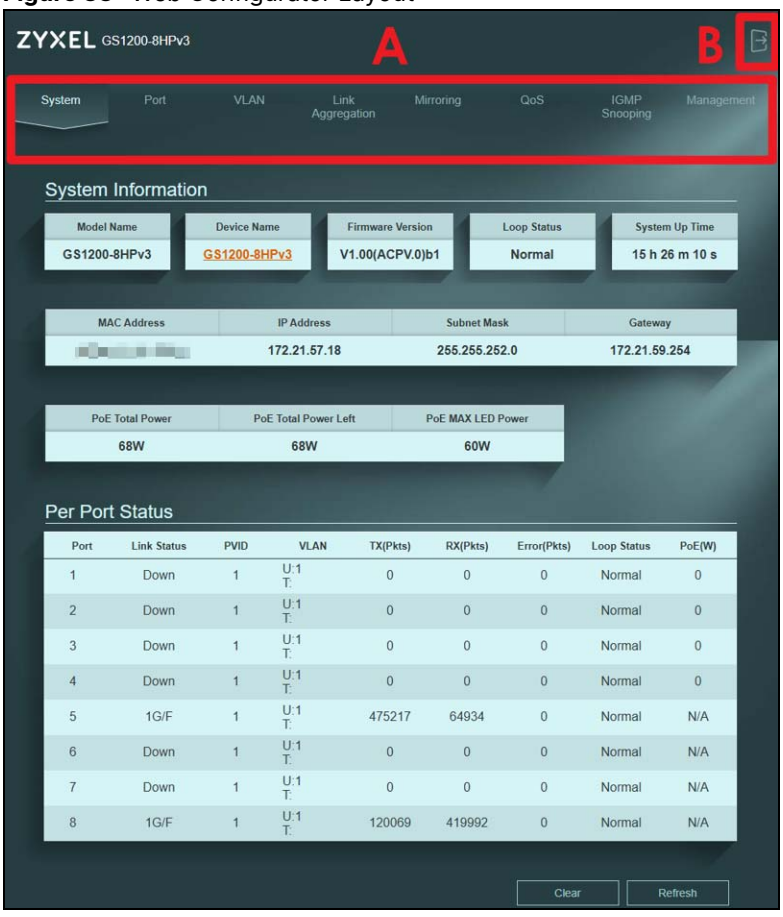


4.5 Web Configurator Layout

The **System** screen is the first screen that displays when you access the Web Configurator. The screens may vary slightly for different models.

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

Figure 33 Web Configurator Layout



A – Click the menu items to open the screen in the main window.

B – Click this link to log out of the Web Configurator.

The following table describes the links in the navigation panel.

Table 8 Navigation Panel Links

LINK	DESCRIPTION
System	This link takes you to a screen that displays general system information, PoE status, and individual port statistics.
Port	This link takes you to a screen to enable **Broadcast Storm Control** and **Loop Prevention**. You can also configure the transmission speed, flow control, port isolation, bandwidth control, and PoE on a port.
VLAN	This link takes you to a screen where you can set the PVID (Port VLAN ID) on a port and create/modify/delete IEEE 802.1Q VLAN for the Switch.
Link Aggregation	This link takes you to screens where you can logically aggregate physical links to form one logical and higher-bandwidth link.
Mirroring	This link takes you to a screen where you can copy traffic from one port or ports to another port so that you can examine the traffic from the first port without interference.
QoS	This link takes you to a screen where you can configure port-based or IEEE 802.1p QoS. The Switch can put packets into the queues according to the port on which the packet is received or the priority tag in the packet.
IGMP Snooping	This link takes you to a screen where you can configure IGMP snooping. You must enable IGMP snooping to use the IPTV service. It checks the IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. Traditionally, 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 packets to just a group of hosts on the network.
Management	This link takes you to screens where you can change the system login password, perform firmware upgrade and configuration file maintenance as well as reset/reboot the system. You can also configure the IP address and subnet mask, set management VID, configure SNMP, and enable IEEE 802.3az EEE.

4.6 Switch Lockout / Reseting the Switch

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

- Remove all ports from VLAN1 and you do not configure other VLAN groups.
- Forget the password and/or IP address.
- 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.

If you forget the administrator password or cannot access the Web Configurator, you will need to use the **Restore** button at the front panel of the Switch to reset it back to the factory defaults.

This means that you will lose all configurations that you had previously and the password will be reset to the default unique password located on the Switch's back label. The IP address will also be reset to 192.168.1.3.

1 Make sure the **PWR/SYS** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **Restore** button for more than 3 seconds until the **PWR/SYS** LED begins to blink and then release it. When the **PWR/SYS** LED begins to blink, the defaults have been restored and the device restarts.

4.7 Logging Out of the Web Configurator

Click the logout icon  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.

Note: By default, you are automatically logged out of the Web Configurator after 5 minutes of inactivity. You can change this setting in **Management** > **HTTP Timeout**.

CHAPTER 5
Initial Setup Example

5.1 Overview

This chapter shows how to set up the Switch for use.

The following lists the configuration steps for the initial setup:

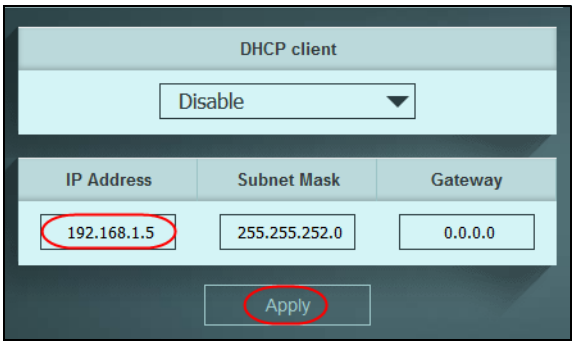
- Change the IP Address
- Change the Password

5.1.1 Change the IP Address

If you do not wish to set your Switch as a DHCP client (**DHCP client** field is **Disable**), assign an IP address for the Switch. The IP address makes it accessible from an outside network. It is used by the Switch to communicate with other devices in other networks.

In this example, you want to change the IP address to 192.168.1.5.

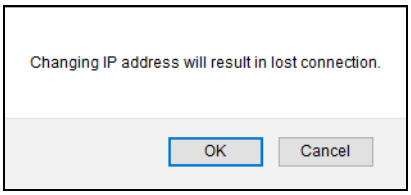
1 Click **Management** in the navigation panel to open the following screen.



2 Enter the new IP address **192.168.1.5** in the **IP Address** field.

3 Click **Apply**.

4 The following screen appears. Click **OK** to save the setting. Connection to the Web Configurator will be lost.



5 On your web browser, go to https://192.168.1.5.

6 A **Log in** screen appears. Enter the existing password and click **SIGN IN** to log in using the new IP address.

5.1.2 Change the Password

The first time you log in to the Web Configurator, you will be asked to change the default password. If you wish to change the password again, perform the following steps:

1 Click **Management** in the navigation panel.

2 Under **Change Password**, enter your current password in the **Old Password** field.

3 Enter the new system password in the **New Password** field. The password must be 8 to 15 characters long. assword length has to be between 9 and 64 characters. Allowed characters include lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and special characters such as ~ ! @ # $ % ^ & * ( ) _ + ` - = { } [ ] : ; < > . /\. Spaces are not allowed.

4 Enter the new password again to in the **Confirm Password** field for confirmation.

5 Click **Apply**. You will automatically be logged out of the Web Configurator.

6 A **Log in** screen appears. Enter the new password and click **SIGN IN** to log in using the new password.

CHAPTER 6 Tutorials

6.1 Overview

This chapter shows you how to set up the Switch's various features.

- Creating a VLAN and Setting Port VID
- Setting Up Bandwidth Control
- Setting Up QoS (Quality of Service)
- Upgrade Firmware on the Switch
- Back up a Configuration File
- Restore Configuration
- Power over Ethernet (PoE) Configuration

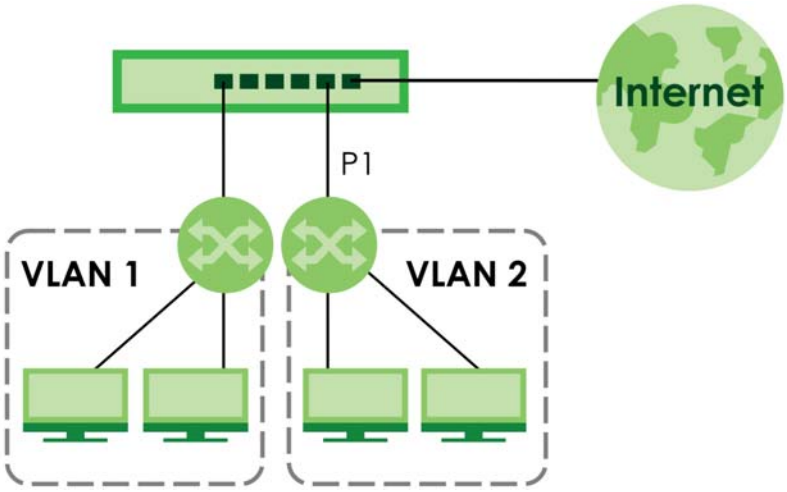
6.2 Creating a VLAN and Setting Port VID

By default, all ports on the Switch are in VLAN 1.

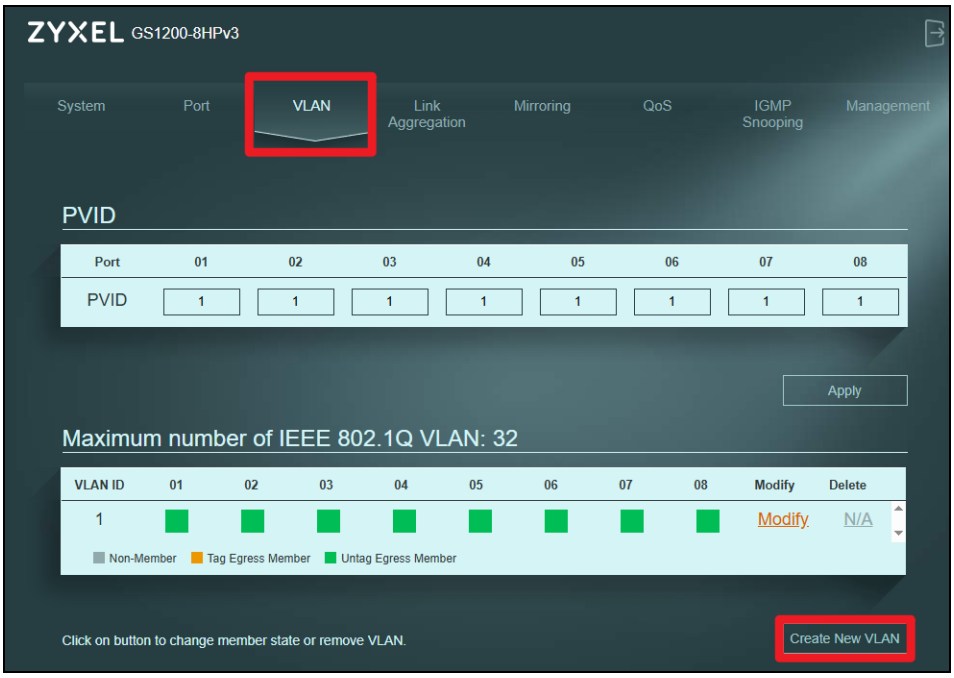
VLANs confine broadcast frames to the VLAN group in which the ports belongs. You can create a VLAN group with fixed port members to do this.

If you want to have a port (for example port 1 (**P1**)) belong to another VLAN as well, say **VLAN 2**, you need to create a VLAN first, and then add the port to the VLAN.

Figure 34 Initial Setup Network Example: VLAN



1 Click **VLAN** in the navigation panel and click the **Create New VLAN** button.



2 Enter 2 in the **VLAN ID** field for the VLAN2 network.

3 Since the VLAN2 network is connected to port 1 on the Switch, configure port 1 to be a permanent member of the VLAN. To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, click the port's box color to green to set the Switch to remove VLAN tags before sending. Clicking the port's check box loops between untagging, non-member, and tagging.

4 Change the box color of other ports not a member of the VLAN group to gray.

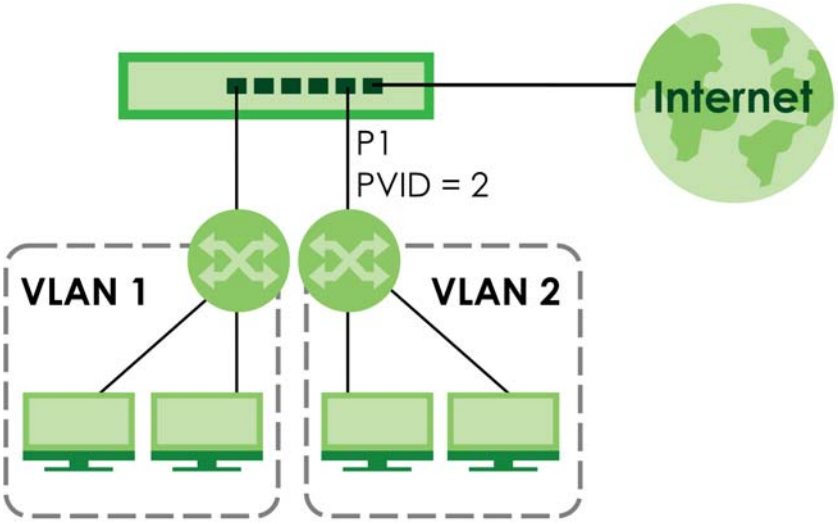
5 Click **Apply** to save the settings.

6.2.1 Setting 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 2**.

Figure 35 Initial Setup Network Example: Port VID



1 Click **VLAN** in the navigation panel.

2 Enter 2 in the **PVID** field for port 2 and click **Apply** to save your changes back to the Switch.

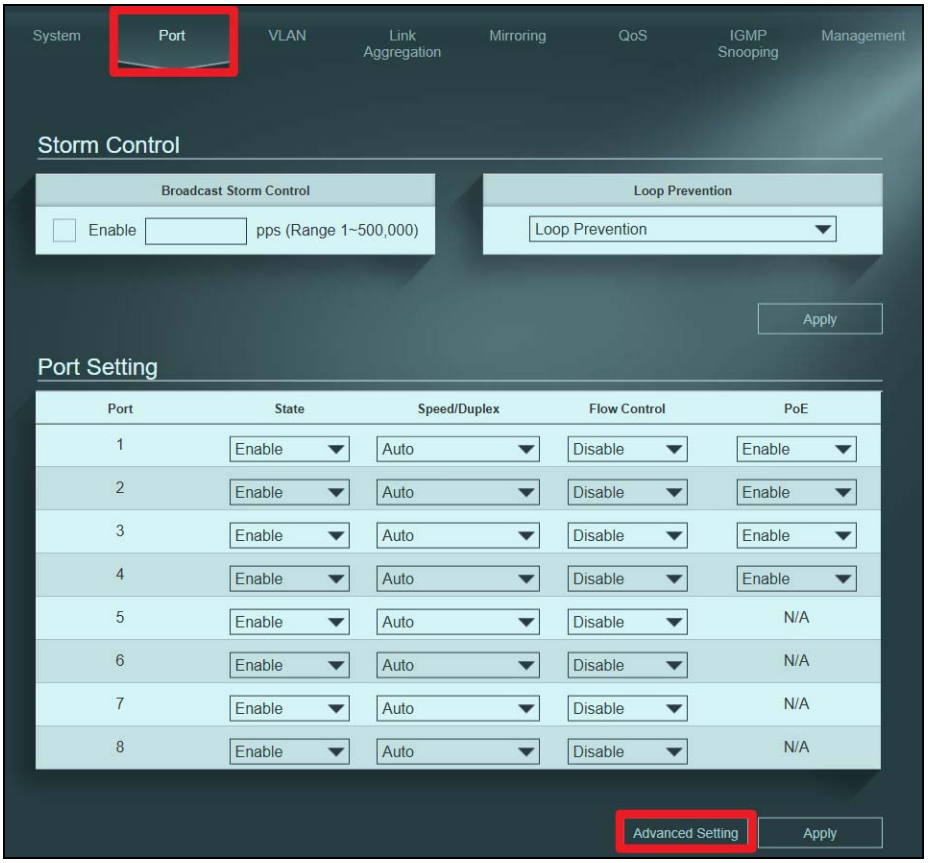
6.3 Setting Up Bandwidth Control

In a home network, the bandwidth is shared by all computers. This means any computer using high-bandwidth applications, for example torrent programs or other P2P software, will affect the other computers. This may also include negative influence on the performance of the entire network.

Bandwidth control minimizes the impact caused when the connection is under heavy load. By configuring bandwidth control, you can assign a maximum bandwidth for each port.

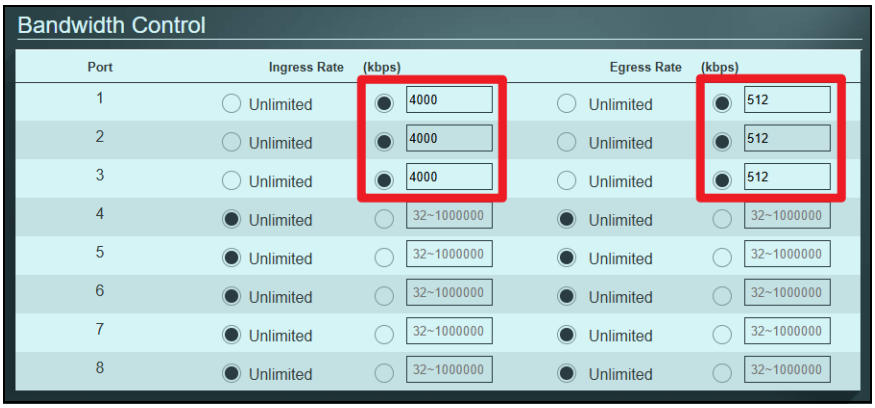
In the example network, configure three computers (connect to ports 1, 2, and 3) to share 512 Kbps egress bandwidth and 4 Mbps ingress bandwidth.

1 Click **Port** in the navigation panel and click the **Advanced Settings** button.



2 Enter 4000 in the **Ingress Rate** field and 512 in the **Egress Rate** field for **Port 1**. Click the radio button for both.

3 Do the same for **Port**s **2** and **3**.



4 Click **Apply** to save the settings.

6.4 Setting Up QoS (Quality of Service)

The QoS (Quality of Service) feature allows you to prioritize the flow of data passing through the Switch.

Use the Port-Based QoS feature to assign priority to data transmitted through a particular port. Or, use the IEEE 802.1p QoS feature to assign the priority value (from 0 to 7) and define up to eight traffic types.

The Switch allows eight priority levels, shown in the table below.

Table 9 Priority Queuing Levels in QoS

QUEUE NAME	PRIORITY LEVEL
Queue 0	Low Priority
Queue 1	
Queue 2	
Queue 3	
Queue 4	
Queue 5	
Queue 6	
Queue 7	High Priority

To apply Port-Based QoS to the Switch, follow these steps:

1 Click the **Port-Based QoS** radio button.

2 Choose which ports will carry the sensitive data, using the priority queuing levels given. Click on each port's radio button to assign a priority queue.

3 Assign the weight (the number you select in the queue **Weight** field) to each priority. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.

4 Click **Apply** after you are finished assigning priorities to the ports to save the settings.

To apply IEEE 802.1p QoS to the Switch, follow these steps:

1 Click the **IEEE 802.1p QoS** radio button.

2 Choose which priority tags will carry the sensitive data, using the priority queuing levels given. Click on each priority tag's radio button to assign a priority queue.

3 Assign the weight (the number you select in the queue **Weight** field) to each priority. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.

4 Click **Apply** after you are finished assigning priorities to the priority tags to save the settings.

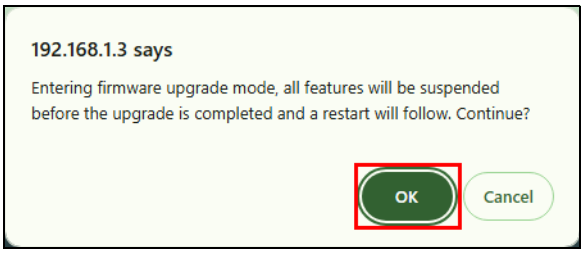
6.5 Upgrade Firmware on the Switch

Upload the firmware to the Switch for feature enhancements.

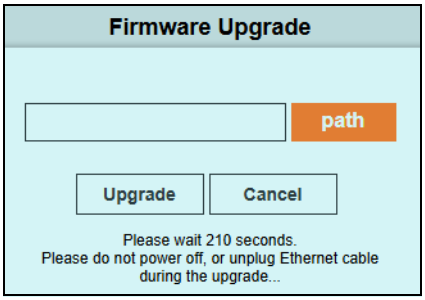
1 Download the firmware file at *www.zyxel.com* in a compressed file. Decompress the file.

2 Click **Management** in the navigation panel and click the **Firmware Upgrade** button.

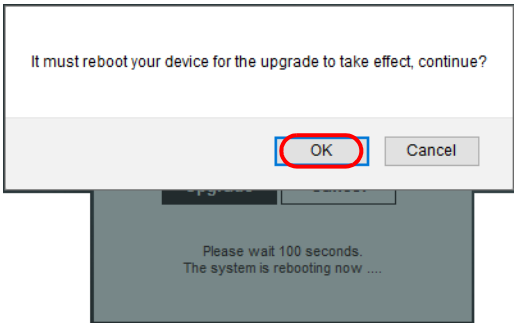
3 You will not be able to configure other settings during the firmware upgrade process to avoid system crashes on the Switch. Click **OK**.



4 Type the path and file name of the firmware file you wish to upload to the Switch in the text box or click **path** to locate it. After you select the firmware file, click the **Upgrade** button to load the new firmware.



5 After a successful upload, the system will reboot, and you will need to log into the Switch again. Click **OK**.



If you click the **Cancel** button in the **Firmware Upgrade** page, the Switch will reboot, and you will be directed to the login screen.

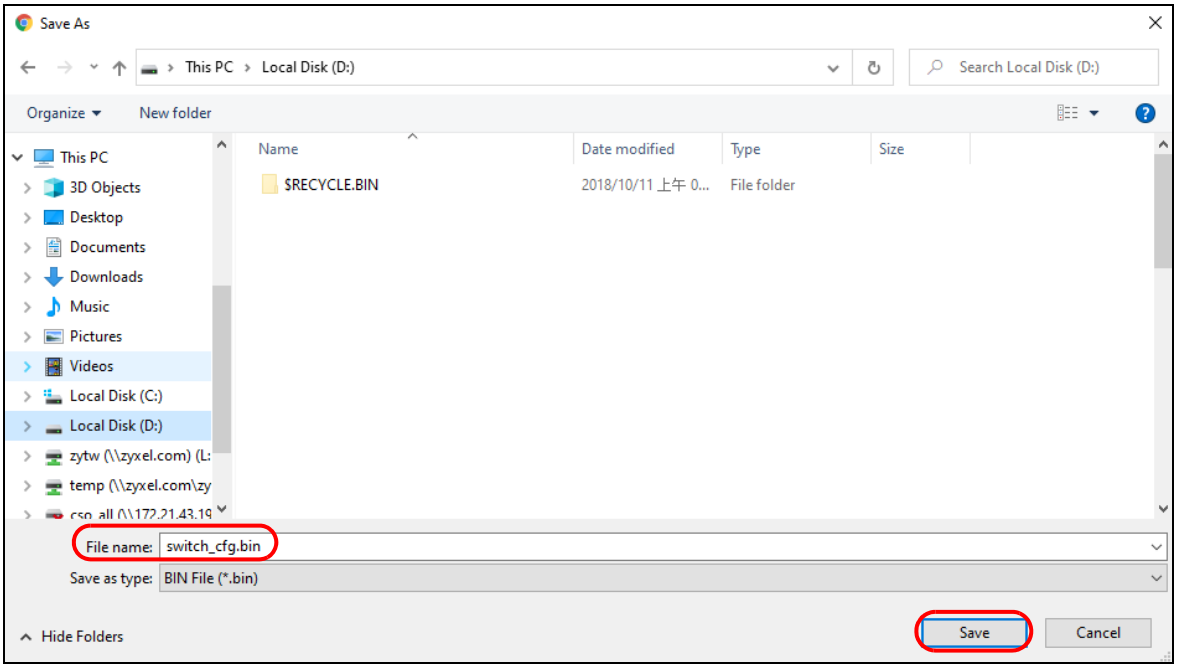
6.6 Back up a Configuration File

Back up a configuration file in case you want to return to your previous settings.

1 Click **Management** in the navigation panel and click the **Backup** button.

2 Specify the location where you want to save the backup file. The default filename is **switch_cfg.bin**.

3 Click the **Save** button to save and store your current Switch settings.

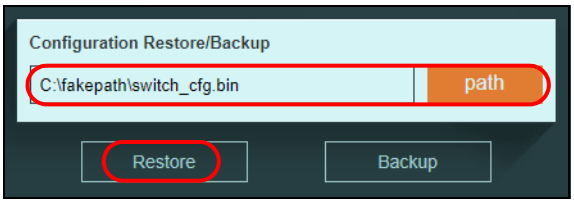


6.7 Restore Configuration

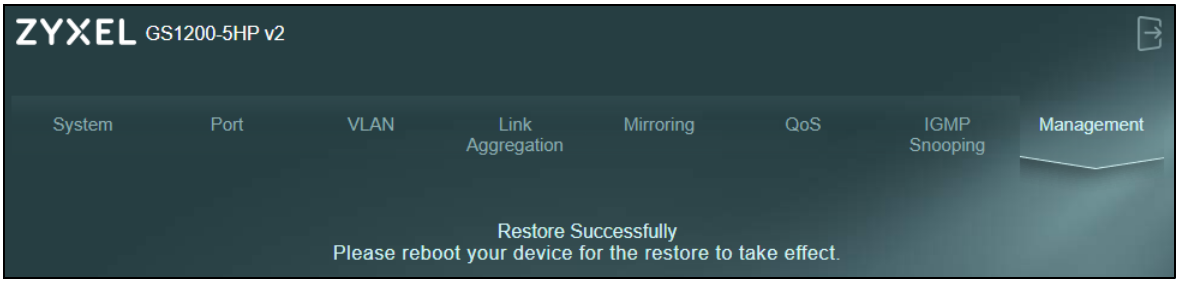
You can upload a previously saved configuration file from your computer to your Switch to restore that previous configuration.

1 Click **Management** in the navigation panel.

2 Click **path** and select a .bin file to restore.



3 Click **Restore**. The following message appears after a successful restore.



4 Reboot the Switch.

6.8 Power over Ethernet (PoE) Configuration

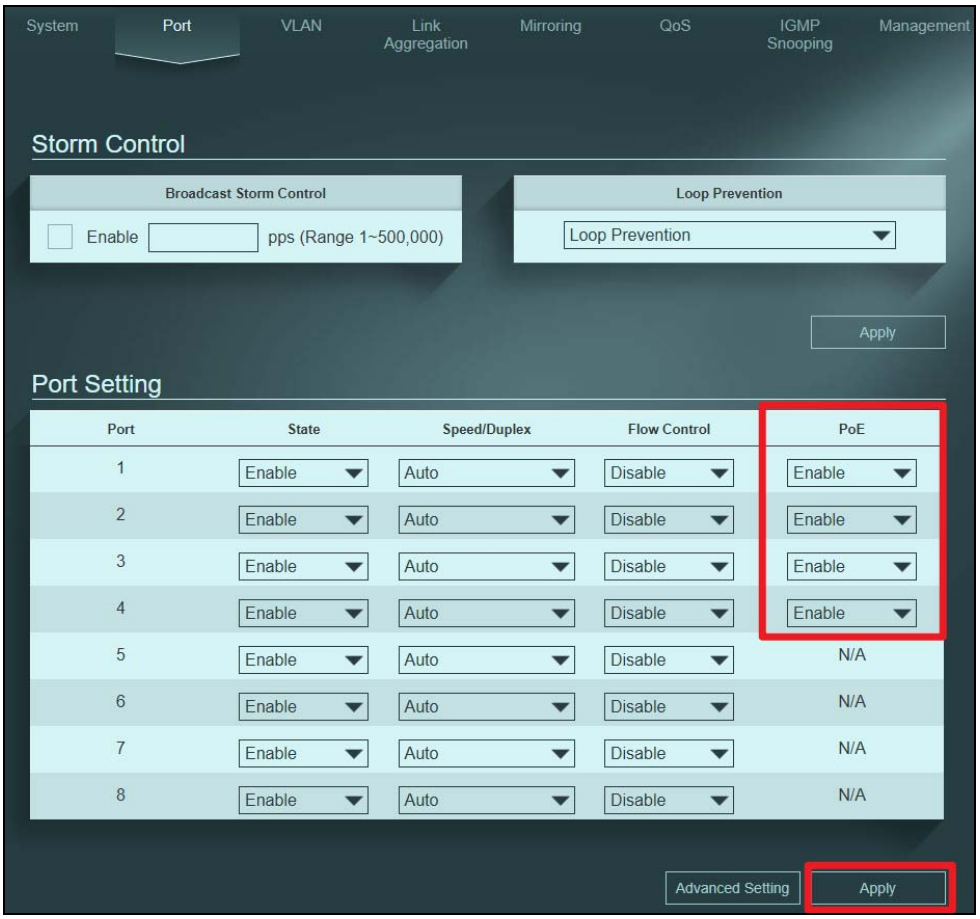
This example is for GS1200-5HPv3 and GS1200-8HPv3.

See Figure 1 on page 12 for an example of using PoE to power devices.

Before connecting devices that require PoE to the PoE ports, PD (Powered Devices), you must enable PoE on those ports.

1 Click **Port** in the navigation panel.

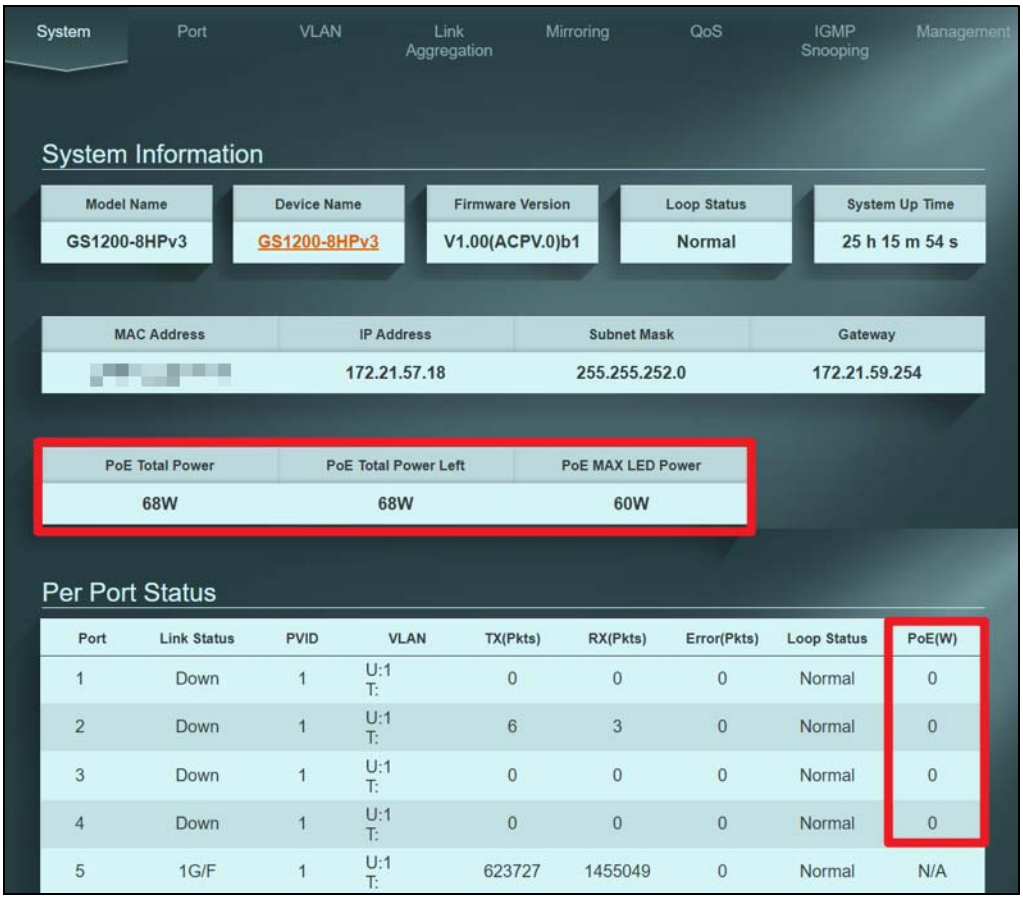
2 Go to **Port Setting**, select **Enable** or **Disable** for ports that will supply power to PDs in the **PoE** field, and click **Apply** to save your changes back to the Switch.



3 After connecting the PDs to the **PoE** ports, you can go to the **System** screen to check the amount of power the PDs are consuming (**PoE Status**), the maximum power the Switch can provide (**PoE Total Power**), and so on. See Section 7.2 on page 47 for more information about **PoE**.

Note: The total power the Switch can supply is shown in the **PoE Total Power** field. You can refer to Section 1.1.1 on page 11 for the maximum power a PoE port can supply.

Note: The Switch allocates power to PDs in the order that they were connected. When the total power requested by the PDs exceeds the total PoE power budget on the Switch, the last PD connected to the Switch will not be powered up.


System
Port
VLAN
Link Aggregation
Mirroring
QoS
IGMP Snooping
Management
System Information
Model Name
GS1200-8HPv3
Device Name
GS1200-8HPv3
Firmware Version
V1.00(ACPV.0)b1
Loop Status
Normal
System Up Time
25 h 15 m 54 s
MAC Address
IP Address
Subnet Mask
Gateway
172.21.57.18
255.255.252.0
172.21.59.254
PoE Total Power
PoE Total Power Left
PoE MAX LED Power
68W
68W
60W
Per Port Status
Port
Link Status
PVID
VLAN
TX(Pkts)
RX(Pkts)
Error(Pkts)
Loop Status
PoE(W)
1 Down 1 U:1 T: 0 0 0 Normal 0
2 Down 1 U:1 T: 6 3 0 Normal 0
3 Down 1 U:1 T: 0 0 0 Normal 0
4 Down 1 U:1 T: 0 0 0 Normal 0
5 1G/F 1 U:1 T: 623727 1455049 0 Normal N/A

PART II
Technical Reference

CHAPTER 7
System

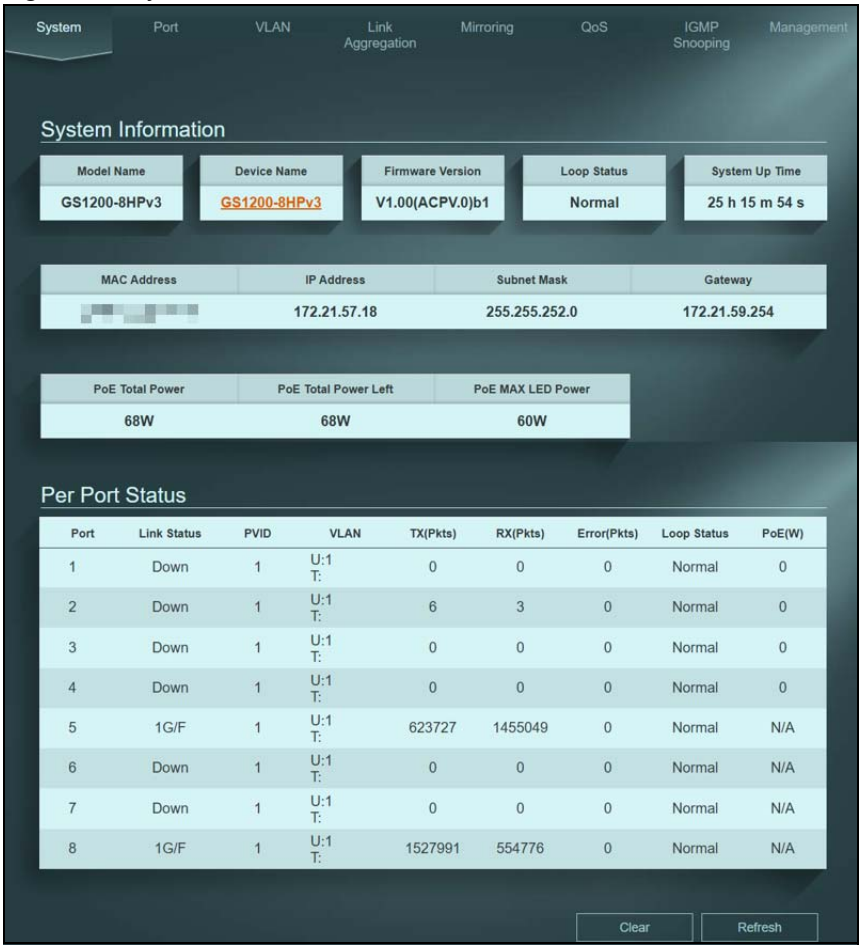
7.1 Overview

This chapter describes the screens for system status, and port details.

7.2 System Screen

The **System** screen displays when you log into the Switch or click **System** at the top of the Web Configurator. The **System** screen displays the Switch's general device information, PoE status, and the port statistics.

Figure 36 System (PoE Model)



The following table describes the labels in this screen.

Table 10 System

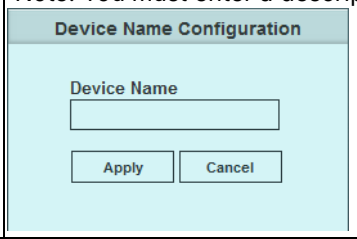
LABEL	DESCRIPTION
System Information	
Model Name	This field displays the model name of this Switch.
Device Name	This field displays the name used to identify the Switch on any network. The device name is a link that you can click to open a screen where you can change the name. Enter a descriptive name of up to 14 characters. Also, spaces and the following special characters listed in the brackets ["`<>^$|&;\/:*?'] are not allowed. Note: You must enter a descriptive name to identify the Switch. 
Firmware Version	This field displays the version number and date of the firmware the Switch is currently running. The firmware on each Switch is identified by the firmware trunk version, followed by a unique code which identifies the model, and then the release number after the period. For example, V1.00 (ACPV.0) is a firmware for the 1.00 version trunk, the ACPV code identifies the GS1200-8HPv3 model, and '.0' is the first firmware release for the model.
Loop Status	It displays **Loop** when the Switch detects a loop on the port. Otherwise, it displays **Normal**.
System Up Time	This field displays how long the Switch has been running since it last restarted or was turned on.
MAC Address	This field displays the MAC addresses of the Switch.
IP Address	The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.3. This field displays the Switch's current IPv4 address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0. This field displays the Switch's subnet mask.
Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
PoE Total Power (GS1200-5HPv3 / GS1200-8HPv3)	This field displays the total power the Switch can provide to the connected PoE-enabled devices on the **PoE** ports.
PoE Total Power Left (GS1200-5HPv3 / GS1200-8HPv3)	This field displays the amount of power the Switch can still provide for PoE.

Table 10 System (continued)

LABEL	DESCRIPTION
PoE MAX LED Power (GS1200-5HPv3 / GS1200-8HPv3)	This field displays the point when the **PoE MAX** LED turns on, indicating the Switch is reaching its maximum power. When the total power requested by the PoE-enabled devices exceeds the total PoE power budget on the Switch, the last PoE-enabled device connected to the Switch will not be powered up. For example, the first PoE-enabled device connected to port 1 requires 20 W, the second one connected to port 2 requires 20 W, and the third one connected to port 3 requires 25 W. In this case, the total power consumption is 65 W which exceeds the maximum power the Switch can supply. Therefore, the third PoE-enabled device will not be powered up as it was connected last.
Per Port Status	
Port	This identifies the Ethernet port on the Switch.
Link status	This field displays the current status or speed/duplex of each port. **F** stands for full-duplex mode, while **H** stands for half-duplex mode. • **1G/F** • **100M/F** • **100M/H** • **10M/F** • **10M/H** • **Down**
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.
VLAN Status	This field shows the untagged and tagged VLAN members configured on the port. "**U**" stands for untagged VLANs, where the traffic sent and received without a VLAN tag. "**T**" stands for tagged VLANs, where the traffic includes an VLAN tag.
TX(Pkts)	This field shows the number of transmitted frames on this port.
RX(Pkts)	This field shows the number of received frames on this port.
Error (Pkts)	This field shows the number of frames received with CRC (Cyclic Redundancy Check) errors.
Loop Status	This field displays whether the port is in a loop state. **Normal**: The Switch does not detect any loops on this port. **Loop**: The Switch has detected a loop on this port. This port continues to receive and forward packets. **Blocked**: The Switch has detected a loop on this port. This port is blocked to prevent loops. If two ports on the Switch are involved in a loop, the port with the higher number is blocked first. For example, if both port 1 and port 2 are part of a loop, port 2 will be marked as **Blocked** and stop receiving packets, while port 1 will be marked as **Loop** and continue to receive and forward packets. Note: To allow the Switch to detect loops and block ports accordingly, enable **Loop Prevention** on the **Port** screen.
PoE (W) (GS1200-5HPv3 / GS1200-8HPv3)	This field displays the amount of power the Switch is currently supplying to the PoE-enabled device connected to the port.
Clear	Click this button to clear the statistics in the TX(Pkts) and RX(Pkts) fields.
Refresh	Click this button to update the information in this screen.

CHAPTER 8
Port

8.1 Overview

This chapter introduces and shows you how to configure the broadcast storm control feature and use loop prevention to prevent loops in your network. In addition, you can configure transmission speed, flow control, port isolation, bandwidth control, and PoE on a port.

8.1.1 What You Need to Know

Read this section to know more about **Loop Prevention**, **Broadcast Storm Control**, **Port Isolation**, **Bandwidth Control**, and **PoE**.

8.1.1.1 Loop Prevention

A switch loop happens if there is more than one connection between two ports on the same switch or between two switches connected together. If this happens, broadcasts are continually rebroadcast and could flood the network. You must break the loop by stopping multiple paths between two switch ports.

Figure 37 The Switch Has Two Ports Connected with the Same Cable

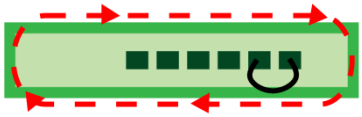


Figure 38 The Connected Switch Has Two Ports Connected with the Same Cable

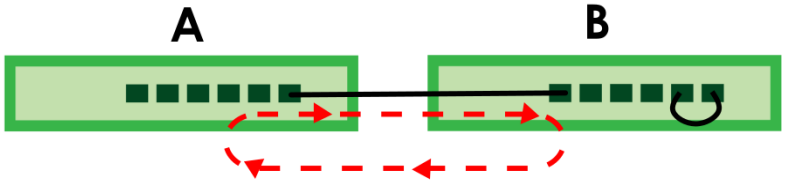
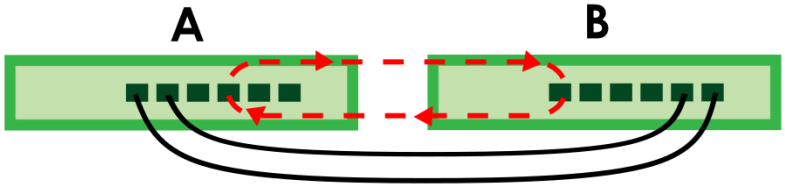


Figure 39 Two Connections between Switches without using the Spanning Tree Protocol (STP)



Loop Prevention allows the Switch to shut down a port automatically if it discover a loop on that port.

8.1.1.2 Broadcast Storm Control

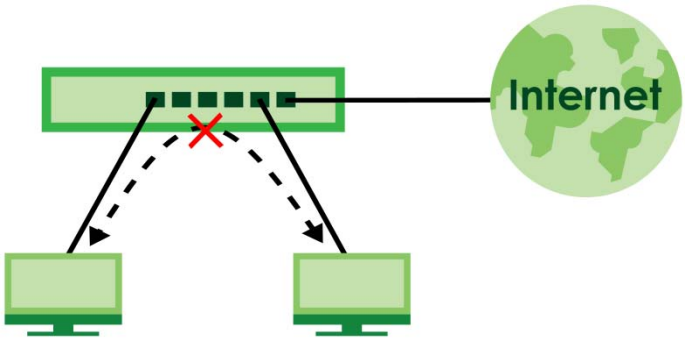
Broadcast storm control limits the number of broadcast packets the Switch receives per second on the ports. When the maximum number of allowable broadcast packets is reached per second, the subsequent

packets are discarded. Enable this feature to reduce broadcast packets in your network. You can specify limits on each port.

8.1.1.3 Port Isolation

Port isolation means that each port can only communicate with the uplink (out-going) port and cannot communicate with each other. All incoming ports are selected while only the uplink port is selected. An uplink port is a port through which a data packet leaves. An incoming port is a port through which a data packet enters. This option is the most limiting but also the most secure.

Figure 40 Port Isolation



For example, if you have computers grouped together in a VLAN that communicates with servers in other networks. These computers have no need to communicate together, so it is best to block unwanted communication.

Note: You cannot configure port isolation settings and link aggregation settings on the same port.

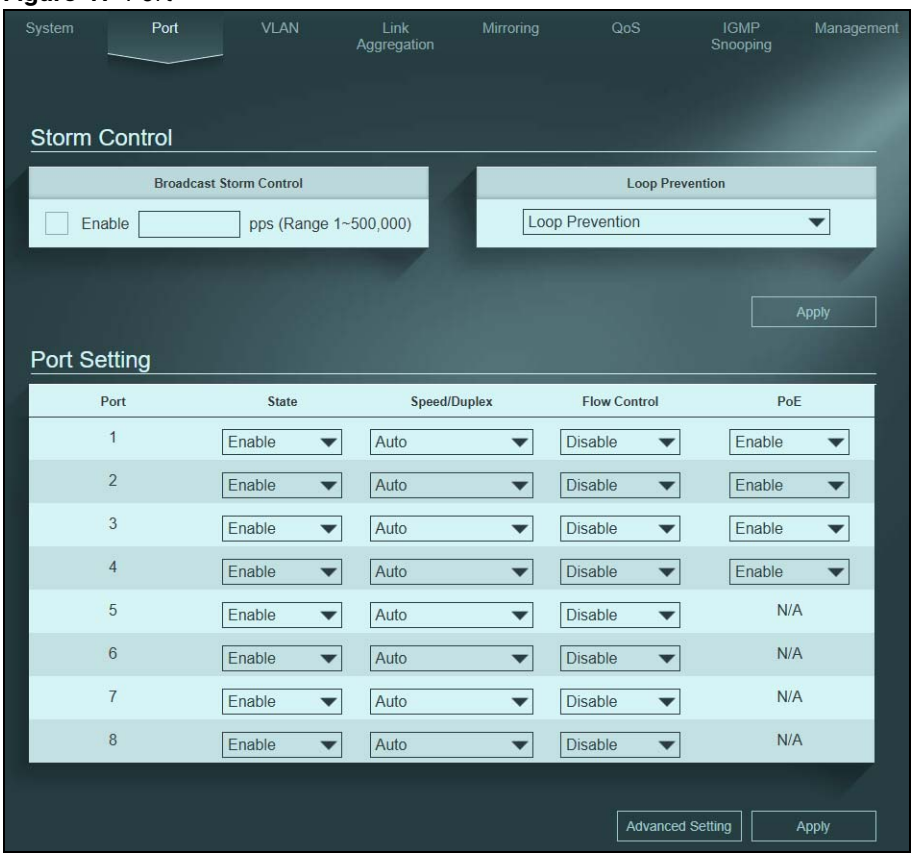
8.1.1.4 Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

8.2 Port Settings

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

Figure 41 Port



The following table describes the labels in this screen.

Table 11 Port

LABEL	DESCRIPTION
Storm Control	
Broadcast Storm Control	**Enable** traffic storm control on the Switch by specifying how many broadcast packets a port receives per second (**pps**).
Loop Prevention	Select **Loop Prevention** to allow the Switch to shut down a port automatically when it detects a loop on the port. The port becomes active when the loop disappears. Select **Off** to disable this feature.
Apply	Click this button to save your changes to the Switch.
Port Setting	
Port	This identifies the Ethernet port on the Switch.
State	Select **Enable** to enable the port or **Disable** to disable it.

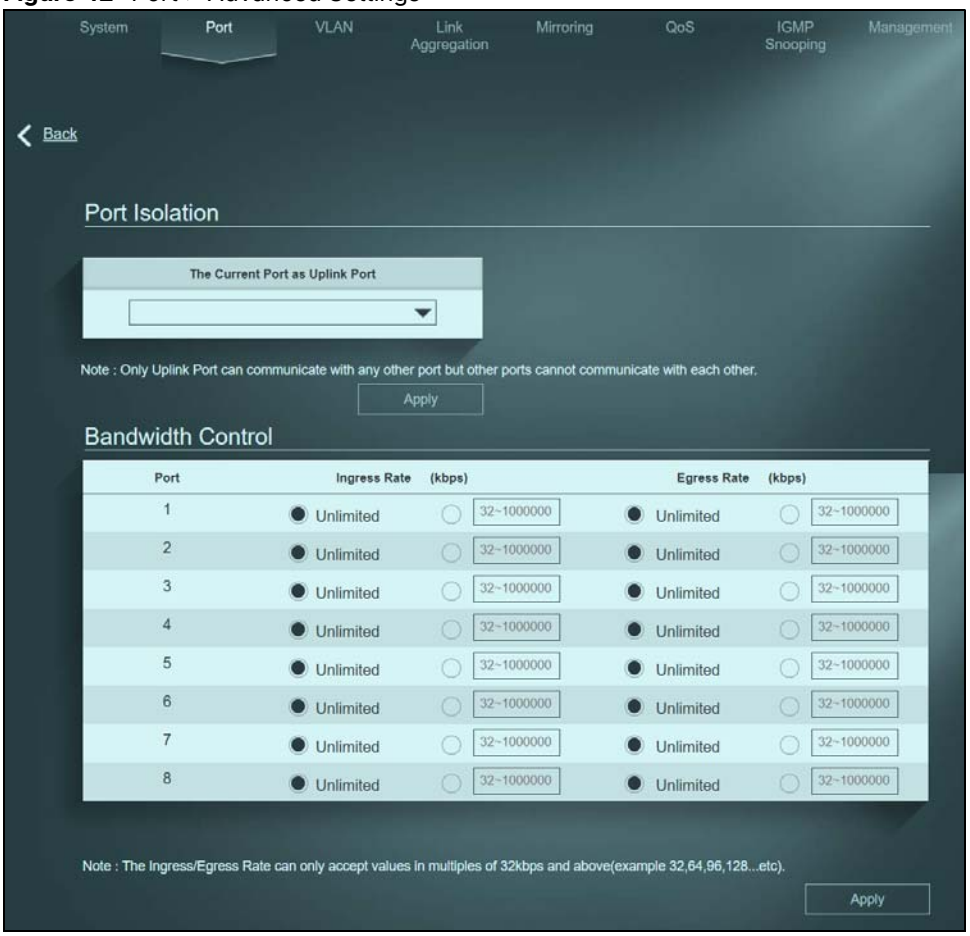
Table 11 Port (continued)

LABEL	DESCRIPTION
Speed/Duplex	Select the speed of the Ethernet connection on this port. The options are: • **Auto**(Default) • **1G-Full Duplex** (Gigabit connections only) • **100M-AN** (100M/auto-negotiation) • **100M-Full Duplex** • **10M-AN** (10M/auto-negotiation) • **10M-Full Duplex** For ports 9 and 10 on the GS1200-10v3, the available options are limited to the following: • **Auto**(Default) • **1G-Full Duplex** (Gigabit connections only) • **100M-Full Duplex** Select **Auto** (auto-negotiation) to allow one port to negotiate with a peer port automatically to obtain the connection speed 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. 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. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed 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 IEEE 802.3x flow control in full duplex mode and backpressure flow control in half 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. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select the check box to enable it.
PoE (GS1200-5HPv3 / GS1200-8HPv3)	Select **Enable** to provide power to a PoE-enabled device connected to the port or **Disable** so the port cannot receive power from the Switch. See Section 1.1.1 on page 11 for more information on PoE.
Advanced Settings	Click this button to set up **Port Isolation** and **Bandwidth Control**.
Apply	Click this button to save your changes to the Switch.

8.2.1 Advanced Settings

Click **Advanced Settings** to open the following screen.

Figure 42 Port > Advanced Settings



The following table describes the labels in this screen.

Table 12 Port > Advanced Settings

LABEL	DESCRIPTION
Back	Click this button to return to the main **Port** (previous) screen.
Port Isolation	
The Current Port as Uplink Port	Select a port to be the uplink (out-going) port. Each port can only communicate with the uplink port and cannot communicate with each other. All incoming ports are selected while only the uplink port is selected. See Section 8.1.1.3 on page 51 for more details. Otherwise, select **Disabled**.
Apply	Click this button to save your changes to the Switch.
Bandwidth Control	
Port	This identifies the Ethernet port on the Switch.
Ingress Rate (kbps)	Specify the maximum bandwidth allowed in kilobits per second (kbps) for the incoming traffic flow on a port. Select **Unlimited** to have the Switch obtain the connection speed of up to 1000 Mbps.
Egress Rate (kbps)	Specify the maximum bandwidth allowed in kilobits per second (kbps) for the out-going traffic flow on a port. Select **Unlimited** to have the Switch obtain the connection speed of up to 1000 Mbps.
Apply	Click this button to save your changes to the Switch.

CHAPTER 9 VLAN

9.1 Overview

The primary function of a VLAN is to separate network traffic. A host in one VLAN cannot communicate with a host in another VLAN. While hosts on the same VLAN can communicate, even if they are not on the same switch. A VLAN is like a virtual switch.

Advantages of putting hosts in separate VLANs:

- To limit the amount of broadcasts across the network.
- To hide a client's data from another client.

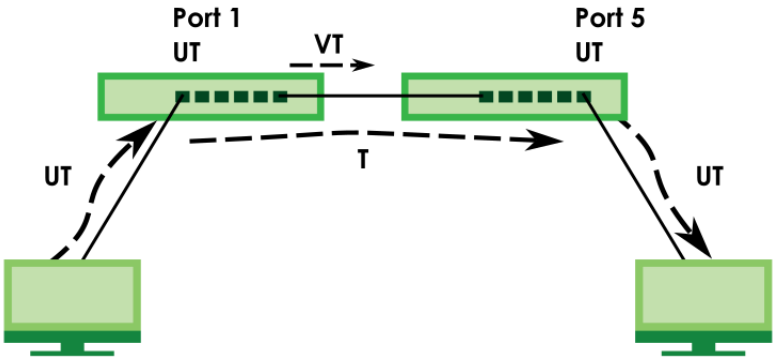
This chapter shows you how to configure VLAN settings.

9.1.1 IEEE 802.1Q Tagged VLANs

Each port on the Switch is capable of passing tagged (**T**) or untagged (**UT**) 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 (**VT**). 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 incoming 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 incoming port itself), thus confining the broadcast to a specific domain.

Figure 43 Tagged VLAN

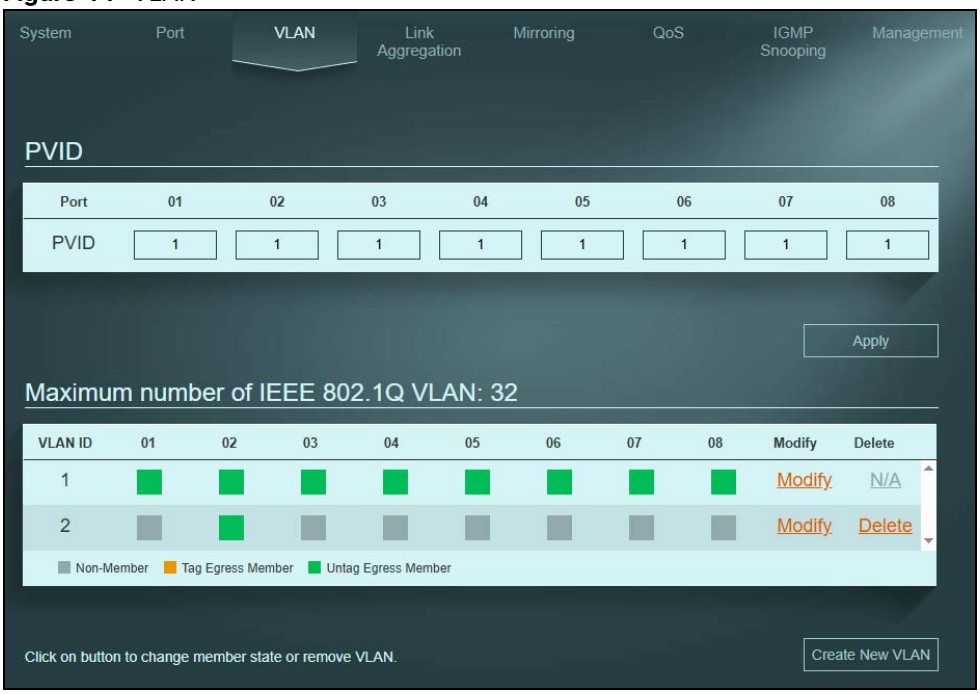


9.2 VLAN Settings

Use this screen to view and configure VLAN settings for the Switch. Click **VLAN** in the navigation panel to open the following screen.

Note: You could block yourself (and all others) from managing the Switch if you remove all ports from VLAN1 and you do not configure other VLAN groups. In case this happens, reset the Switch to the default settings (see Section 4.6 on page 32 for more information).

Figure 44 VLAN



The following table describes the labels in this screen.

Table 13 VLAN

LABEL	DESCRIPTION
PVID	
Port	This field displays the port number.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1 and 4094 as the port VLAN ID.
Apply	Click this button to save your PVID settings to the Switch.
Maximum number of IEEE 802.1Q VLAN	This shows the maximum number of IEEE 802.1Q VLANs you can have on the Switch.
VLAN ID	This is the ID number of the VLAN group.

Table 13 VLAN (continued)

LABEL	DESCRIPTION
01 – 10 01 – 08 01 – 05	This displays the ports that are participating in a VLAN. A tagged port is orange, an untagged port is green and ports not participating in a VLAN are gray. Multiple ports in a VLAN can be configured as tagged or untagged or not participating. A port is a 'tagged port' when the interface is expecting frames containing VLAN tags. An example of this is when the sender will send a frame with a VLAN tag. The receiving switch will see the VLAN tag, and if the VLAN is allowed, it will forward the frame.
Modify	Click **Modify** to edit the VLAN settings.
Delete	Click **Delete** to remove the VLAN group. You cannot delete the default VLAN.
Create New VLAN	Click this button to configure a new IEEE 802.1Q VLAN for the Switch.

CHAPTER 10
Link Aggregation

10.1 Overview

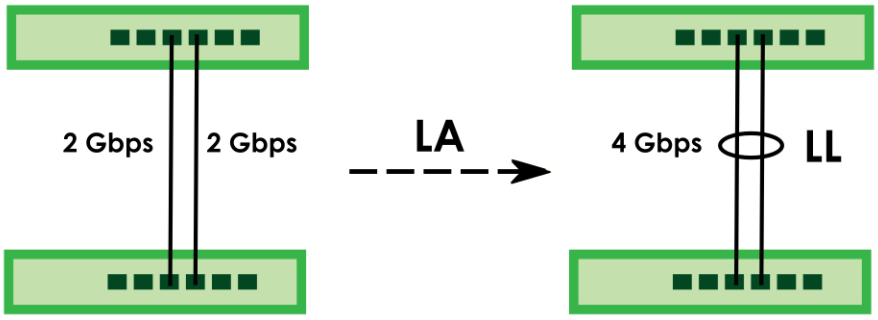
This chapter shows you how to logically aggregate physical links to form one logical and higher bandwidth link.

Link aggregation (**LA**) (trunking) is the grouping of physical ports into one logical higher-capacity link (**LL**). You may want to trunk (link) 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.

Note: You cannot configure port isolation settings and link aggregation settings on the same port.

Note: Configure link aggregation before physically connecting the cable to the ports to avoid network topology loops.

Figure 45 Link Aggregation



10.2 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.

Static Link Aggregation

In static link aggregation, the trunk group is manually configured on both ends of the devices. It does not use any protocol for negotiation between devices. The configurations on both ends must be matched to enable the trunk group.

Dynamic Link Aggregation

In dynamic link aggregation, the trunk group is configured by using Link Aggregation Control Protocol (LACP) which is defined by IEEE 802.3ad/802.1AX. The configurations on both ends must be matched to enable the trunk group.

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.

Note: LACP only works on full-duplex links.

Link Aggregation ID

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

Table 14 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 15 Link Aggregation ID: Peer Switch

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

Difference between Static and Dynamic Link Aggregation

The physical connections for both static and dynamic link aggregation are the same. The difference lies in how the link aggregation is configured and managed.

The following table shows the difference between static and dynamic link aggregation.

Table 16 Difference Between Static and Dynamic Aggregation

FEATURE	STATIC LINK AGGREGATION	DYNAMIC LINK AGGREGATION
Configuration	Manually	Through LACP
Protocol	None	LACP (IEEE 802.3ad/802.1AX)
Fault Tolerance	Limited The traffic still flows to the failed link, potentially leading to dropped packets.	Automatic LACP detects the failure and dynamically adjusts the trunking group to exclude the failed link.
Automatic Detection and Correction	None	YES

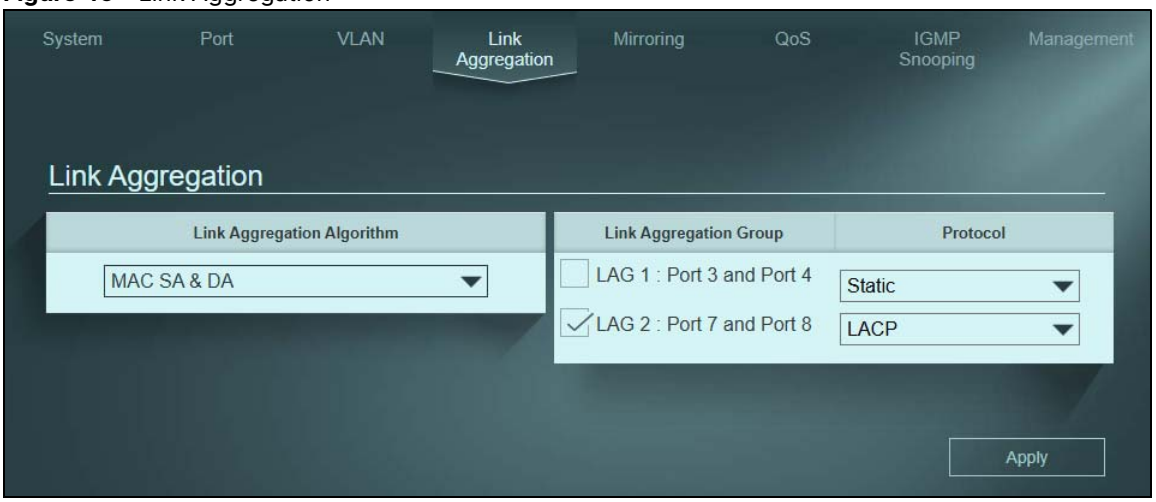
1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

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

10.3 Link Aggregation

Use this screen to configure link aggregation.

Figure 46 Link Aggregation



The following table describes the labels in this screen.

Table 17 Link Aggregation

LABEL	DESCRIPTION
Link Aggregation	
Link Aggregation Algorithm	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **MAC SA & DA** 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 **MAC SA** to distribute traffic based on the packet's source MAC address. Select **MAC DA** to distribute traffic based on the packet's destination MAC address. Select **MAC SA & DA** to distribute traffic based on a combination of the packet's source and destination MAC addresses.
Link Aggregation Group	The field identifies the default link aggregation groups the Switch supports. Select which link aggregation group supports your choice in the previous **Link Aggregation Algorithm** field. For example, enabling **LAG 1: Port 3 and Port 4** will allow packets from the same source and/or to the same destination to go through ports 3 and 4 for a maximum throughput of 2 Gbps. This allows for faster speed compared to passing packets through ports 3 and 4 individually (maximum 1 Gbps). Note: See Table 1 on page 10 for details on the number of link aggregation groups supported by your switch and the specific ports that support link aggregation. Note: Make sure the ports in a link aggregation group have the same PVID and VLAN ID.

Table 17 Link Aggregation (continued)

LABEL	DESCRIPTION
Protocol	Select the link aggregation protocol to apply to the selected group. Select **Static** (default) to configure the ports as static members of a trunk group without using any negotiation protocol. Select **LACP** to configure the ports as members of a trunk group using the Link Aggregation Control Protocol (LACP), which dynamically negotiates and maintains the aggregation.
Apply	Click this button to save your changes to the Switch.

CHAPTER 11 Mirroring

11.1 Overview

This chapter discusses port mirroring setup screens.

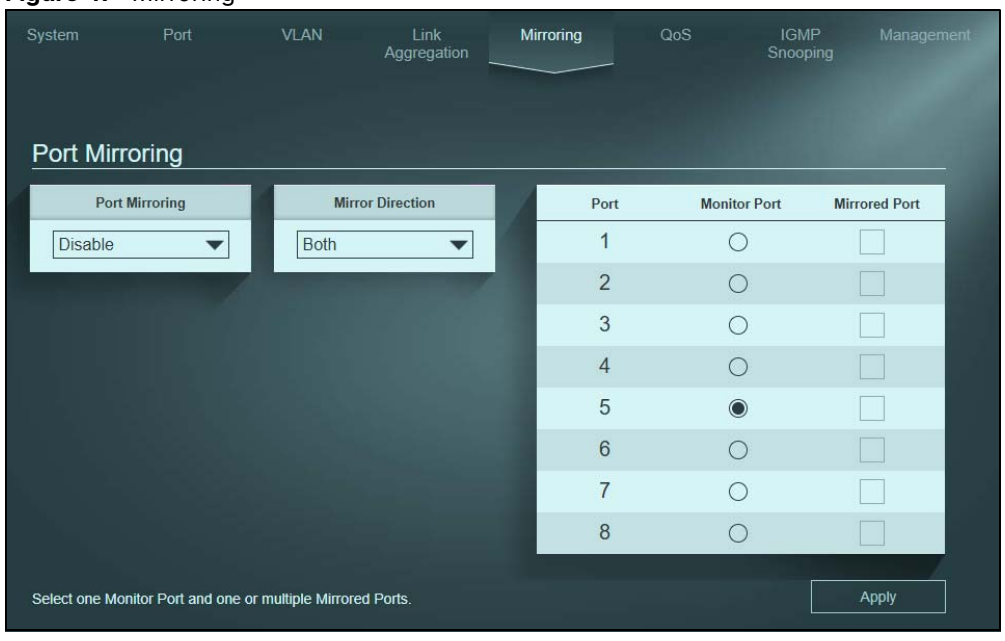
Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) to examine the traffic from the monitor port without interference.

11.2 Mirroring Settings

Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Note: A port cannot be the monitor port and the mirrored port at the same time.

Figure 47 Mirroring



The following table describes the labels in this screen.

Table 18 Mirroring

LABEL	DESCRIPTION
Port Mirroring	
Port Mirroring	Select **Enable** to activate port mirroring on the Switch, or **Disable** to disable the feature.
Mirror 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**.
Port	This field displays the port number.
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. Note: Select one monitor port.
Mirrored Port	Select this option to mirror the traffic on a port. Note: Select one or multiple mirrored ports.
Apply	Click this button to save your changes to the Switch.

CHAPTER 12 QoS

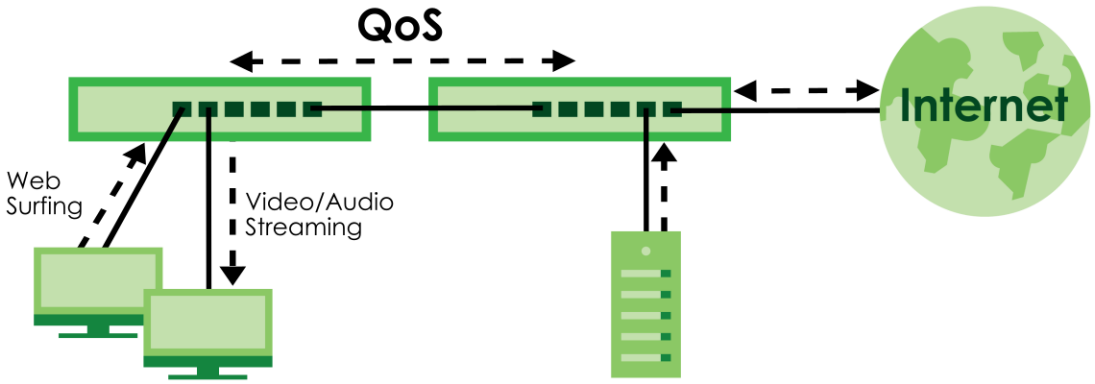
12.1 Overview

This chapter introduces the configuration and functions of the **QoS** (Quality of Service) screen.

Occasionally, data might be delayed, depending on the volume of traffic and the capacity of the equipment. Numeric and text data are usually not affected by delays, because they are reassembled at the destination. However, when VoIP and streaming videos are reassembled, they might have some troublesome gaps. 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 applications such as VOD (Video on Demand).

You can enable QoS to have the Switch assign each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

Figure 48 QoS



12.2 What You Need to Know

The Switch can put packets into the queues according to the port on which the packet is received or the priority tag in the packet.

12.2.1 Port-Based QoS

The Port-Based QoS feature assigns priority to data transmitted through a particular port. When the data arrives to a port it begins a queue. Therefore the Switch has a queue for each port. If data arrives at the same time to all ports, ports with higher priority will be first to transmit the data received. The higher the priority of the port, the less delays the data passing through will have.

12.2.2 IEEE 802.1p QoS

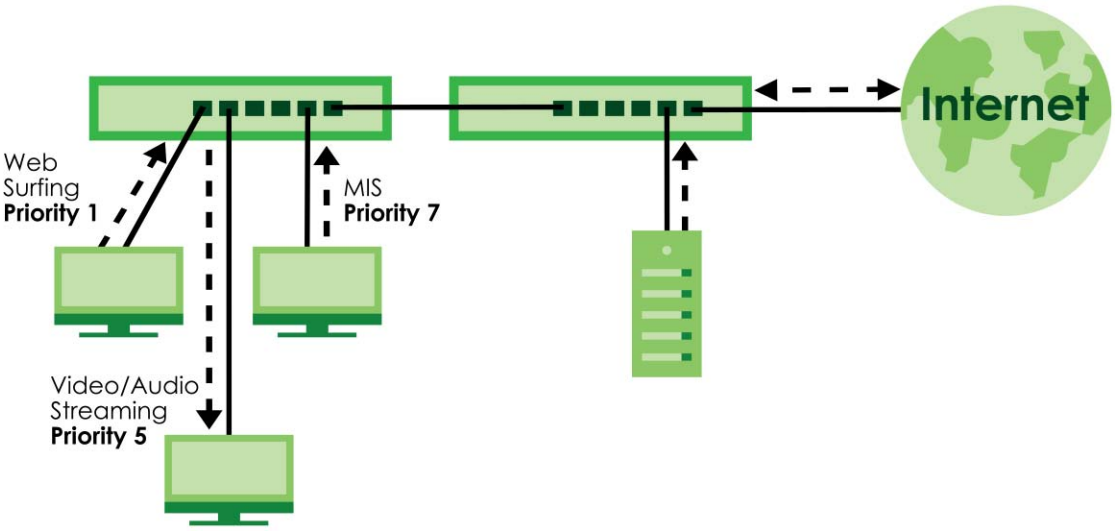
IEEE 802.1p defines a 3-bit field called PCP (Priority Code Point) within the IEEE 802.1Q VLAN tag, which is also referred to as a CoS (Class of Service) value and indicates the frame priority level. IEEE 802.1p QoS uses the priority value (from 0 to 7) to define up to eight traffic types. That is, each priority level defines a class of service. The table below shows the IEEE recommendations for traffic types, these may vary or be reassigned.

Table 19 IEEE Priority to Traffic Type Mapping Recommendations

PCP	PRIORITY	ACRONYM	TRAFFIC TYPES
1	0 (lowest)	BK	Background
0	1 (default)	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

Note: Frames without an explicit priority tag are treated as system traffic and assigned to **Queue0**.

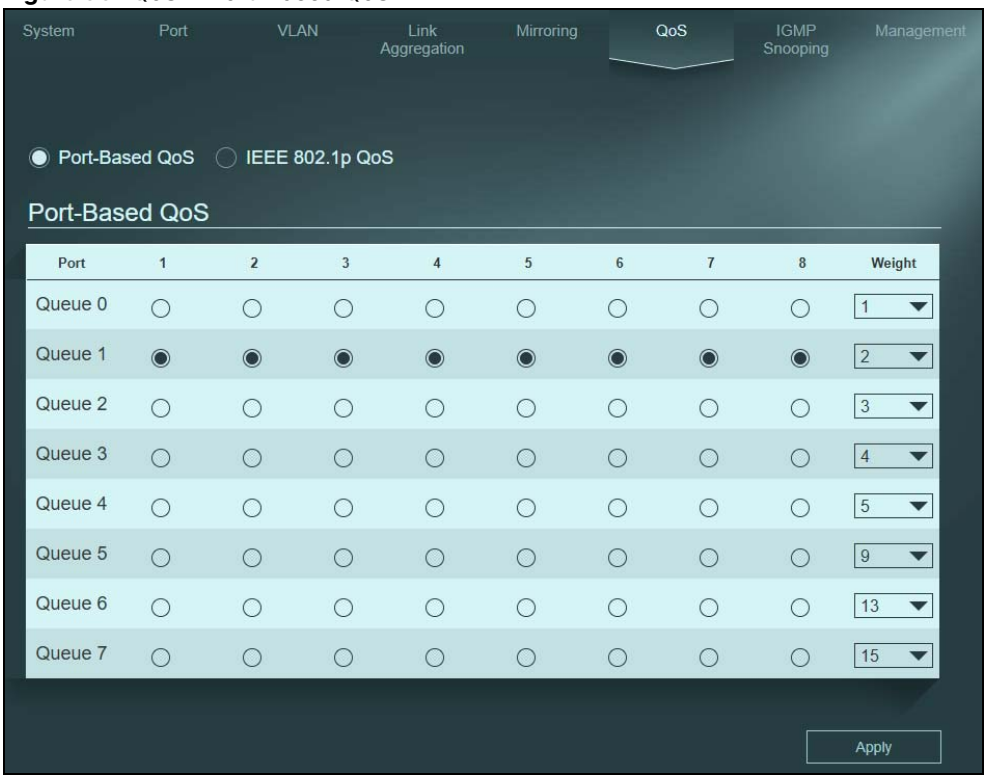
Figure 49 IEEE 802.1p QoS



12.3 Port-Based QoS Screen

The Switch's default settings for Port-Based QoS are shown in the next figure.

Figure 50 QoS > Port-Based QoS



The following table describes the labels in this screen.

Table 20 QoS > Port-Based QoS

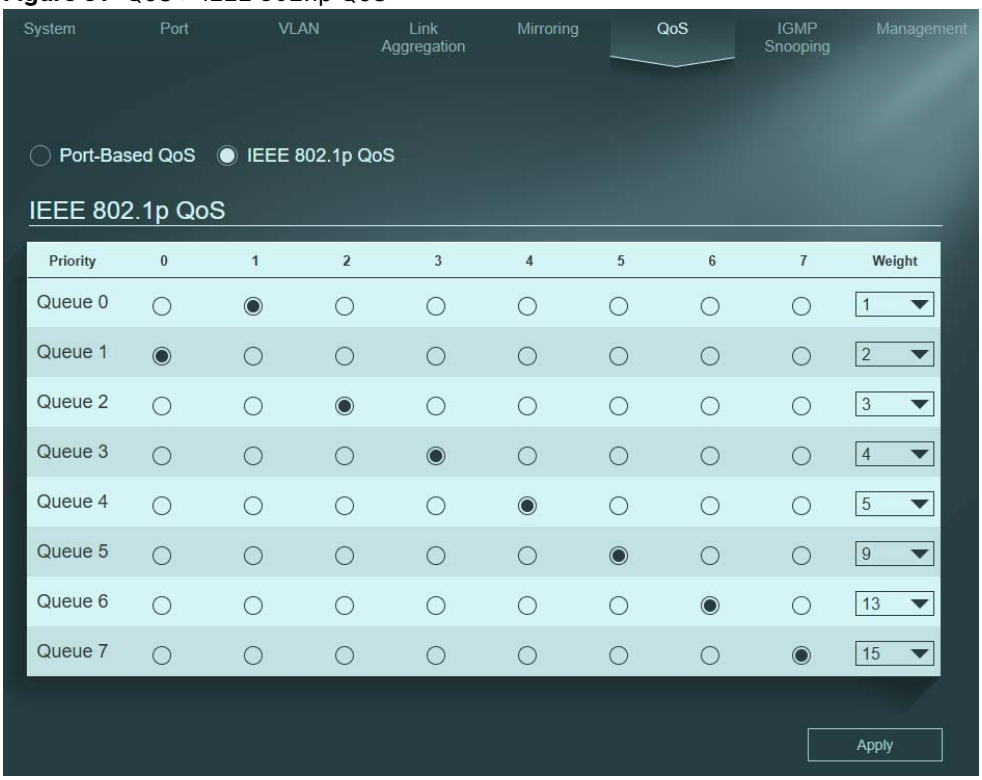
LABEL	DESCRIPTION
Port-Based QoS	
Port 1 – 5 Port 1 – 8 Port 1 – 10	Select which ports will carry the sensitive data, using the priority queuing levels given. Click on each port's radio button to assign a priority queue.
Weight	Assign the weight (the number you select in the queue **Weight** field) to each priority. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click **Apply** to save your changes to the Switch.

12.4 IEEE 802.1P QoS Screen

Both Port-Based QoS and IEEE 802.1P QoS use the same priority queuing levels. Remember the difference amongst both features relies on how the priority queuing is assigned. Port-Based QoS assigns priority queuing by port, whereas IEEE 802.1P QoS assigns queuing by PCP priority tags.

The Switch's default settings for IEEE 802.1P QoS are shown in the next figure. The numbers from 0 to 7 refer to the priority tags for each traffic type.

Figure 51 QoS > IEEE 802.1p QoS



The following table describes the labels in this screen.

Table 21 QoS > IEEE 802.1p QoS

LABEL	DESCRIPTION
IEEE 802.1p QoS	
Priority 0 – 7	Select which priority tags will carry the sensitive data, using the priority queuing levels given. Click each priority tag's radio button to assign a priority queue.
Weight	Assign the weight (the number you select in the queue **Weight** field) to each priority. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click **Apply** to save your changes to the Switch.

CHAPTER 13
IGMP Snooping

13.1 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.

Note: You must enable IGMP snooping to use the IPTV service.

The 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. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch. It checks the 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.

13.2 IGMP Snooping Settings

Click **IGMP Snooping** in the navigation panel to display the screen as shown next.

Figure 52 IGMP Snooping

The following table describes the labels in this screen.

Table 22 IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping	
Enable IGMP Snooping	Select this option to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Unknown Multicast Drop	Select this option to discard the frame when the Switch receives an unknown multicast frame. Otherwise, the Switch sends the frame to all ports.
IGMP Static Router Port	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 a port to be used as an IGMP query port. Or, select **Auto** to allow any port to be used as an IGMP router port after receiving an IGMP query. Note: If link aggregation is enabled, the ports in a link aggregation group will not be available in this field.
Apply	Click **Apply** to save your changes to the Switch.

CHAPTER 14 Management

14.1 Overview

This chapter explains how to use the **Management** screen to configure settings on the Switch, such as login password change, firmware upgrade, configuration backup and restore, system reset or reboot, IP address change, and so on.

14.1.1 What You Need to Know

Read on for an overview of IEEE 802.3az Energy Efficient Ethernet (EEE) and SNMP concepts that can help you configure the screens in this chapter.

IEEE 802.3az Energy Efficient Ethernet (EEE)

IEEE 802.3az allows both sides of a link to support EEE. When 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.

SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to 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 monitor the Switch through the network through SNMP version 2. SNMP is only available if TCP/IP is configured. See Section 14.3.1 on page 74 for more information.

14.2 Management Settings

Use this screen to upload the latest firmware, upload a stored device configuration file, save your configurations for later use, change the administrator system password, change the IP address, enable DHCP client, or reboot/reset the system.

An administrator is someone who can both view and configure Switch changes. The default administrator password is on the device label.

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

Figure 53 Management

The following table describes the labels in this screen.

Table 23 Management

LABEL	DESCRIPTION
Device Setting	
Reset	Click this button to clear all Switch configuration information you configured and return to the factory defaults. 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 IP address.
Reboot	Click this button to restart the Switch without physically turning the power off.
Firmware Upgrade	Click this button to upgrade the latest firmware to the Switch.

Table 23 Management (continued)

LABEL	DESCRIPTION
DHCP Client	Select **Enable** 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. Otherwise, select **Disable**.
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 192.168.1.3. This is the IP address of the Switch in an IP routing domain.
Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.255.0.
Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Apply	Click this button to save your changes for **DHCP Client**, **IP Address**, **Subnet Mask**, and **Gateway** to the Switch.
HTTPS	The Switch always allows access through HTTPS. See Section 14.3.2 on page 75 for more information.
HTTP	Select **Enable** to also allow access using the HTTP protocol. Otherwise, select **Disable**.
Timeout	Enter how many minutes (from 1 to 30) a session can be left idle before the session times out. After it times out, you have to log in with your password again. A very long timeout setting may has security risks.
Apply	Click this button to save your changes for **HTTP Timeout** to the Switch.
Management VID	This is the ID number of the management VLAN. Enter a number between 1 and 4094 as the management VLAN ID.
Apply	Click this button to save your changes for **Management VID** to the Switch.
IEEE 802.3az EEE	Select **Enable** to activate Energy Efficient Ethernet globally. Otherwise, select **Disable**.
Apply	Click this button to save your changes for **IEEE 802.3az EEE** to the Switch.
LED ECO Mode	Select **Enable** to turn off all the Switch LINK/ACT port LEDs. Select **Disable** to turn on all the Switch LINK/ACT port LEDs.
Apply	Click this button to save your changes to the Switch.
Configuration Restore/Backup	Enter the path and file name of the configuration file you wish to restore in the text box or click **path** to locate it.
Restore	Click **Restore** to restore a previously saved configuration from your computer to the Switch. Note: “config” is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.
Backup	Click **Backup** to save and store your current Switch settings.
Change Password	
Old Password	Enter the existing system password.
New Password	Enter your new system password using keyboard characters (a – z, A – Z, and 0 – 9). The password must be 8 to 15 characters long
Confirm Password	Reenter your new system password for confirmation.
SNMP	
SNMPv2	Select **Enable** to allow the SNMP manager to retrieve an object variable from the Switch. Otherwise, select **Disable**.
Get Community	The SNMP manager sends requests, and the switch responds using '**public**' as the default Get community string.
Apply	Click this button to save your changes for **Change Password** to the Switch.

14.2.1 Firmware Upgrade

Firmware upgrades contain bug fixes and fixes for security vulnerabilities. It is recommended to keep the Switch's firmware up to date.

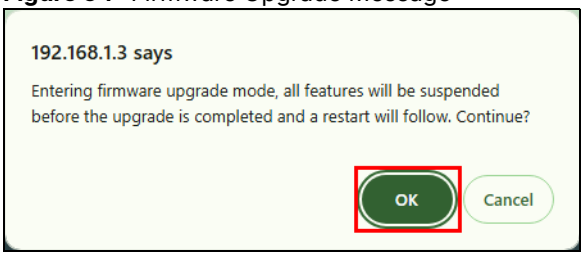
Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the Switch.

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

Do NOT disconnect or turn off power to the Switch while firmware upload is in progress!

The following message will appear after you click the **Firmware Upgrade** button. You will not be able to configure other settings during the firmware upgrade process to avoid system crashes on the Switch. Click **OK**.

Figure 54 Firmware Upgrade Message

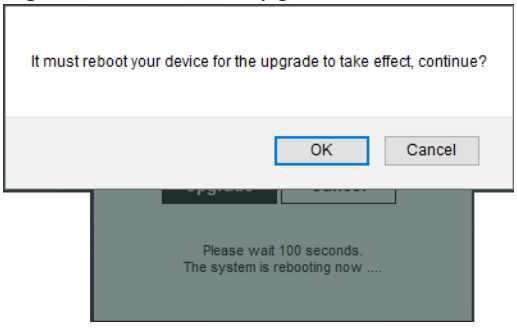


Enter the path and file name of the firmware file you wish to upload to the Switch in the text box or click **path** to locate it. After you select the firmware file, click the **Upgrade** button to load the new firmware.

Figure 55 Firmware Upgrade Path

After a successful upload, the system will reboot, and you will need to log into the Switch again.

Figure 56 Firmware Upgrade Confirmation



If you click the **Cancel** button in the **Firmware Upgrade** page, the Switch will reboot, and you will be directed to the login screen.

14.3 Technical Reference

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

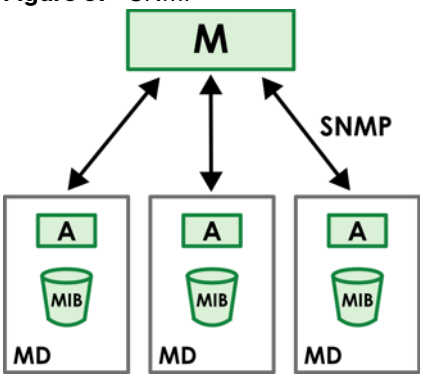
14.3.1 SNMP

An SNMP managed network consists of two main components: agents (**A**) and a manager (**M**). An agent is a management software module that resides in a managed 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 (**MD**). 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 itself is a simple request or response protocol based on the manager or agent model. The SNMP manager sends a request, and the agent returns a response using the Get operation, which allows the manager to retrieve an object variable from the agent.

Figure 57 SNMP



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).

MIBs let administrators collect statistics and monitor status and performance. The Switch uses both standard public (RFC-defined) MIBs for standard functionality.

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**).

14.3.2 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).

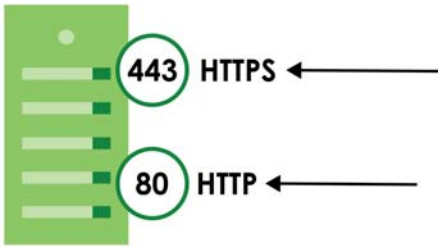
It relies upon certificates, public keys, and private keys.

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.

- **HTTPS** connection requests from an SSL-aware web browser go to port **443** (by default) on the Switch's web server.
- **HTTP** connection requests from a web browser go to port **80** (by default) on the Switch's web server.

Figure 58 HTTPS/HTTP Implementation



CHAPTER 15 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

15.1 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 3.1.1 on page 19.
2. Check the hardware connections. See Section 15.1 on page 76.
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.

A loop is detected.

1 To restore a port in a loop state, disconnect it, check the network connections, and reconnect it.

2 You can log into the Web Configurator. Go to **System** in the Web Configurator to check your port status. Note that you can do this when you enable **Loop Prevention** (default) in the **Port** screen.

15.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default IP address is **192.168.1.3**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 32.

I forgot the password.

1 The default password is on the device label.

2 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 32.

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 192.168.1.3.
- 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 3.1.1 on page 19.

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

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

5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See Section 4.6 on page 32.

6 If the problem continues, contact the vendor.

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

1 Make sure you have entered the password correctly. The default password is on the device label.

2 Disconnect and re-connect the power cord to the Switch.

3 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 32.

Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

15.3 Switch Configuration

After upgrading firmware on the Switch, the login screen does not display.

When one of the following should happen during the firmware upgrade process, a failure may occur.

During the firmware upgrade process:

- The Switch loses power.
- The computer from which you uploaded the firmware file to the Switch is turned off.
- The Ethernet cable connecting the Switch and the computer comes loose. This is the computer from where you uploaded the firmware file to the Switch.

When any of the above occurs, and you are directed to the **Firmware Upgrade** screen, follow the steps below:

1 Make sure the power supply is sufficient in your environment.

2 Make sure your computer’s Ethernet cable is securely connected to the Switch.

3 Select the firmware file that you tried to upload to the Switch before and try upgrading the firmware again in the **Firmware Upgrade** screen.

4 Wait for the firmware upgrade process to complete. After a successful upload, the system will reboot, and you will need to log into the Switch again.

15.4 PoE Supply

My Powered Devices (PDs) are not receiving power.

1 Check the PoE usage of the Switch through the following methods. When the total power requested by the PoE-enabled devices exceeds the **PoE Total Power** on the **System**, the last PoE-enabled device connected to the Switch will not be powered up. You can add another PoE-capable Switch for additional PDs.

- Check the **PoE Total Power Left** on the **System**. This field displays the remaining power the Switch can provide to connected PDs.
- Check the **PoE MAX** LED on the front panel of your Switch.
- Check the **PoE (W)** field for the port to which your PD is connected on the **System** screen. Make sure that the port is suppling power to the PD.

2 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.
- If the connected PDs do not fully comply with the Switch's supported PoE standard (See Section 1.1.1 on page 11 for the Switch's supported PoE standards), replace the PDs with PoE standard-compliant devices for better compatibility.

3 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 1.1.1 on page 11 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.

4 Disconnect and re-connect the power adapter to the Switch.

5 If the problem continues, contact Zyxel technical support.

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 Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network 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
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.

Federal Communications Commission (FCC) EMC Statement

- The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

- This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the equipment and receiver
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
  - Consult the dealer or an experienced radio/TV technician for assistance

Canada

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES statement

CAN ICES(B)/NMB(B)

Europe and the United Kingdom

The following information applies if you use the product within the European Union or United Kingdom.

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (For indoor devices only) (2) Do not install or service this device during a thunderstorm.
- 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.
- Connect ONLY suitable accessories to the device.
- Do not open the device. Opening or removing the device 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 connected cables carefully so that no one will step on them or stumble over them.
- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.

- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect the power adaptor or cord 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 the damaged power adaptor or cord from the device and the power source. Do not try to repair the power adaptor or cord by yourself. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device.

  – For a permanently connected device, a readily accessible method to disconnect the device shall be incorporated externally to the device;

  – For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas. (For devices with a battery)
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas. (For devices with a battery)
- This product is intended to be supplied by a DC power source marked 'L.P.S' or `Limited Power Source', rated 12 Vdc, 3.0 A and Tma 40 °C (min.).
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating. (For devices with a fuse)
- To avoid possible eye injury, do not look into an operating fiber-optic module’s connector. (For devices with fiber)
- Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019. (For devices with fiber)
- Conforme à 21 CFR 1040.10 et 1040.11 sauf pour la conformité à la norme CEI 60825-1 Ed. 3., comme décrit dans la notice laser Numéro 56 du 8 mai 2019. (For devices with fiber)
- CLASS 1 LASER PRODUCT & "IEC 60825-1:2014" (For devices with fiber)
- APPAREIL À LASER DE CLASS 1 (For devices with fiber)
- CLASS 1 CONSUMER LASER PRODUCT & “EN 50689:2021” (For devices with fiber)

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Caution! Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.

- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.
- Attention: L'utilisation des commandes ou reglages ou l'execution des procedures autres que celles specifiees dans les presents exigences peuvent etre la cause d'une exposition a un rayonnement dangereux).

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market comply with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), the so called "ErP Directive (Energy-related Products directive), as well as ecodesign requirements laid down in applicable implementation measures. Power consumption has satisfied the regulation requirements which are:

- Network standby power consumption < 8 W (watts), and/or
- Off mode power consumption < 0.5 W (watts), and/or
- Standby mode power consumption < 0.5 W (watts).

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

安全警告 - 為了您的安全，請先閱讀以下警告及指示 :

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸 :
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。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。(僅限室內產品)
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用 :
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置;
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is 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 *http://www.zyxel.com* to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at *https://www.zyxel.com/global/en/support/warranty-information*.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. The trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z