ZYXEL
COMMUNICATIONS

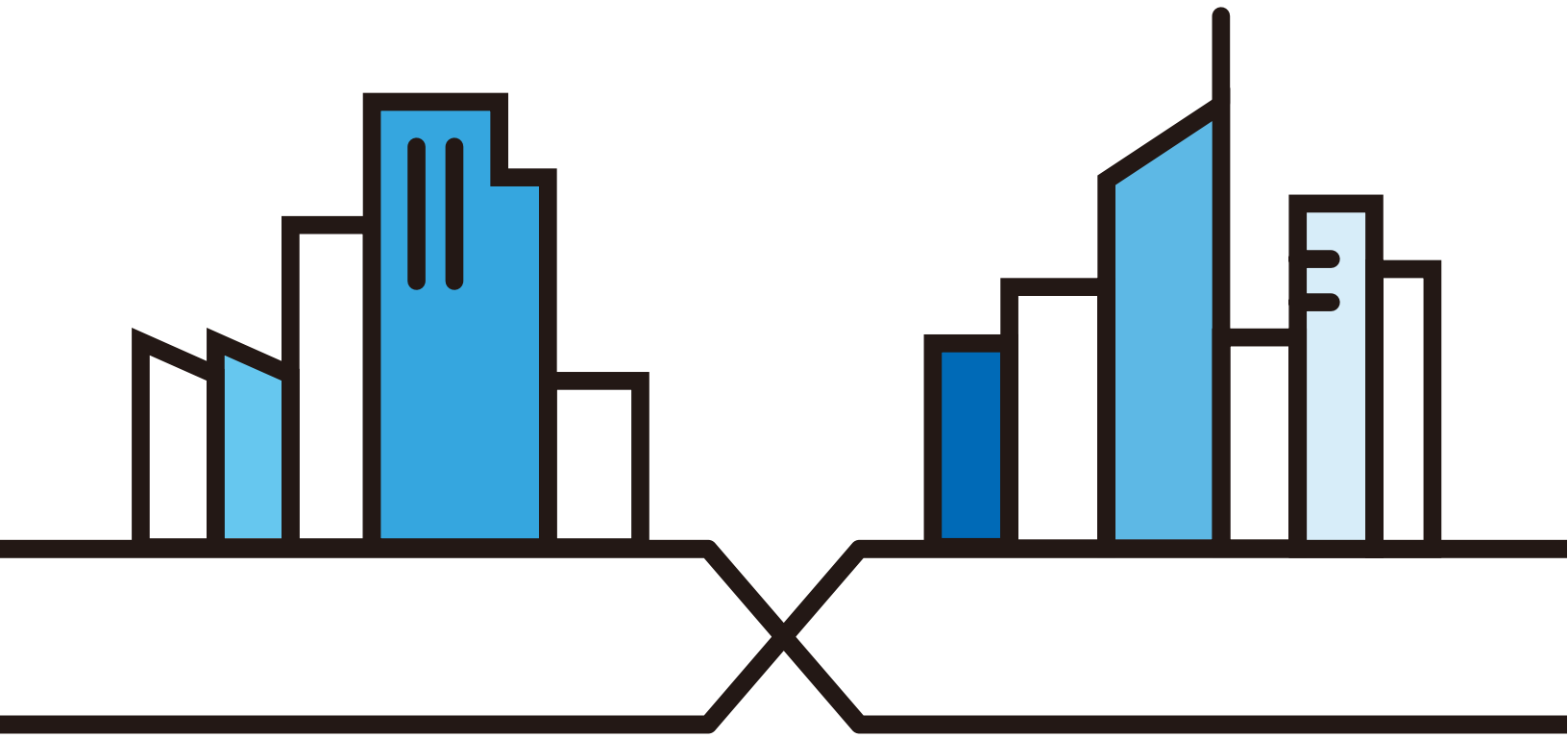
User's Guide

PM Series

XGS-PON SFU with 10GbE LAN

Default Login Details	
LAN IP Address	https://192.168.0.1
User Name	admin
Password	See the device label

Version 5.42/5.61 Ed 2, 04/2024



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the PM Device and get up and running right away.

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

- 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, **Network Setting > Home Networking** means you first click **Network Setting** in the navigation panel, then the **Home Networking** sub menu to get to that screen.

Icons Used in Figures

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

PM Device 	Generic Router 	Desktop 
Switch 	Laptop 	

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

This chapter introduces the main features and applications of the PM Devices. The PM Device is a PON (Passive Optical Network) modem with one 10 Gbps Multi-Gigabit Ethernet LAN port.

The PM Device refers to the following models:

- PM7300-T0
- PM7500-00

Table 1 PM Device Comparison Table

	PM7300-T0	PM7500-00
Port Control Protocol	YES	YES
Fiber Optical Port	XGS-PON	XGS-PON
Maximum Downstream Data Rate	9953.28 Mbps	9953.28 Mbps
Maximum Upstream Data Rate	9953.28 Mbps	9953.28 Mbps
Multi-Gig LAN	1/2.5/5/10 GbE LAN	1/2.5/5/10 GbE LAN
LAN IP Setup	YES	YES
System Log	YES	YES
TFTP	YES (LAN only)	YES (LAN only)
Firmware Upgrade	YES	YES
Certificates	YES	YES
Log Settings	YES	YES
Traffic Status	YES	YES
User Account's Maintenance	YES	YES
Remote Management	HTTP/HTTPS/SSH/PING	HTTP/HTTPS/SSH/PING
Backup/Restore	YES	YES
Wall Mount	YES	YES
Latest Firmware Version	V5.42	V5.61

1.1.1 Multi-Gigabit Ethernet

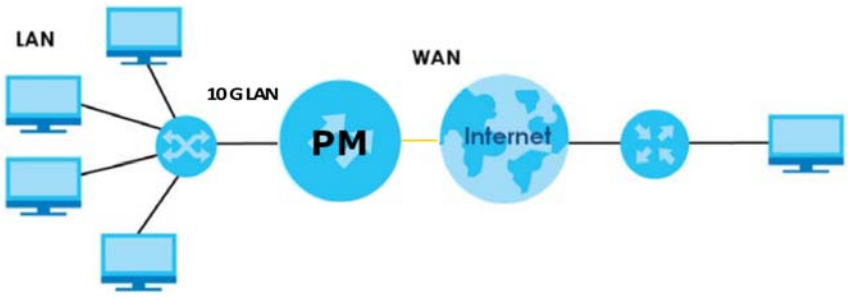
The Multi-Gigabit Ethernet port on the PM Device supports a maximum connection speed of 10 Gbps, dependent on cable type and length. Devices can also connect to the Multi-Gigabit Ethernet port at the following speeds: 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps and 10 Gbps. The following table lists the

maximum transmission speeds and distances for different Ethernet cable types.

Table 2 Ethernet Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100 Mbps	100 m	100 MHz
Category 5e	1 Gbps / 2.5 Gbps / 5 Gbps	100 m	100 MHz
Category 6	5 Gbps / 10 Gbps	50 m	250 MHz
Category 6a	10 Gbps	100 m	500 MHz
Category 7	10 Gbps	100 m	650 MHz

Figure 1 Overview



1.2 Ways to Manage the PM Device

Use any of the following methods to manage the PM Device.

- Web Configurator. This is recommended for management of the PM Device using a (supported) web browser.
- Secure Shell (SSH), Telnet. Use for troubleshooting the PM Device by qualified personnel.
- FTP. Use FTP for firmware upgrades and configuration backup or restore.

1.3 Good Habits for Managing the PM Device

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

- Change the Web Configurator 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.
- Regularly back up the device configuration to a file, and make sure you know how to restore it. Restoring an earlier working configuration may be useful if the device has errors. If you have to reset the PM Device to its factory default settings, for example because you forgot the password, then you can use the backup file to quickly restore your last configuration.

CHAPTER 2
Hardware Panels

2.1 Overview

This chapter describes the LEDs and port panels of the PM Device.

2.2 LEDs

The following figures show the PM Device LED indicators.

None of the LEDs are on if the PM Device is not receiving power.

2.2.1 PM7300-T0 and PM7500-00

The LED indicators are located on the front (top) panel.

Figure 2 PM7300-T0 and PM7500-00's Front Panel

The following are the LED descriptions for your PM Device.

Table 3 PM7300-T0 and PM7500-00's LED Behavior

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The PM Device is ready for use.
		Blinking	The PM Device is booting.
		Off	The PM Device is not receiving power.
	Red	On	There is a system failure.
		Blinking	The firmware upgrade is in progress.
PON	Green	On	The PON connection is ready.
		Blinking	The PM Device is trying to establish a link.
		Off	The fiber link is down.
LOS	Red	On	PON transceiver is powered down.
		Blinking	This is a R(x) low power alarm.
		Off	The PON connection is working normally.
10GbE	Green	On	The Ethernet link is up.
		Blinking	The PM Device is transmitting or receiving data.
		Off	The Ethernet link is down.

2.3 Rear Panel Ports and Buttons

Figure 3 PM7300-T0's Rear Panel

Figure 4 PM7500-00's Rear Panel

The following table describes the ports and buttons on the PM Device.

Table 4 Rear Panel Ports and Buttons

LABELS	DESCRIPTION
RESET	Press for 5 seconds to restore the PM Device to its factory default settings.
PON	Connect the PM Device to the Internet using a fiber cable.
10GbE	Connect the PM Device to an Ethernet device such as a network switch, NAS or server. Connect a computer for initial configuration.
POWER	Connect the power adapter and press the **POWER** button to start the PM Device.
ON/OFF	Press the **ON/OFF** button after connecting the power adapter to start the PM Device.

2.3.1 RESET Button

Insert a thin object into the **RESET** hole of the PM Device to reload the factory-default configuration file if you forget your password or IP address, or you cannot access the Web Configurator. This means that you will lose all configurations that you had previously saved. The password will be reset to **the default (see the PM Device label)** and the IP address will be reset to **192.168.0.1**.

Figure 5 Reset Button (PM7300-T0)

Figure 6 Reset Button (PM7500-00)

1 Make sure the PM Device is connected to power and the **POWER** LED is on.

2 Using a thin item, press the **RESET** button for more than 5 seconds.

CHAPTER 3
The Web Configurator

3.1 Overview

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such as Internet Explorer 11, Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

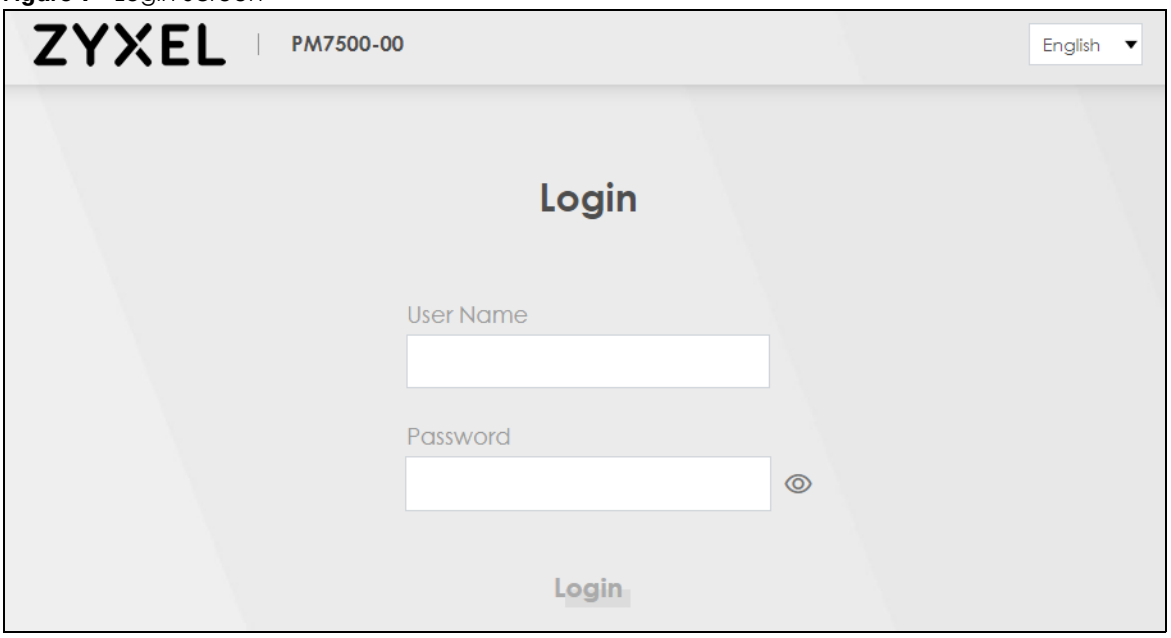
In order to use the Web Configurator you need to allow:

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

3.2 Accessing the Web Configurator

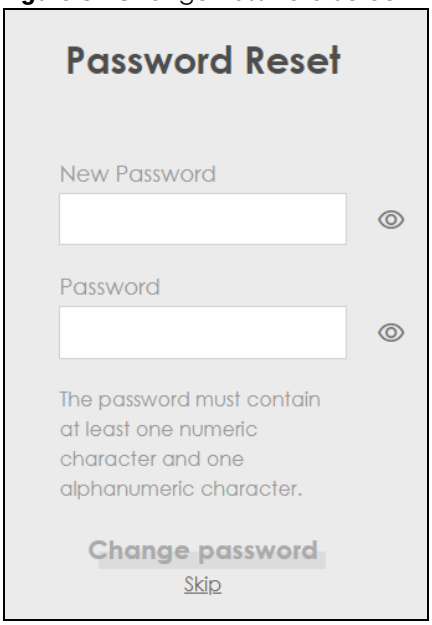
1. Make sure your PM Device hardware is properly connected (refer to the Quick Start Guide).
2. Manually configure your computer's IP address to be in the range 192.168.0.2~192.168.0.254 with subnet mask 255.255.255.0.
3. Manually configure Launch your web browser and go to https://192.168.0.1.
4. A password screen displays. To access the administrative Web Configurator and manage the PM Device, type the default username **admin** and the randomly assigned default password (see the device label) in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 7 Login Screen



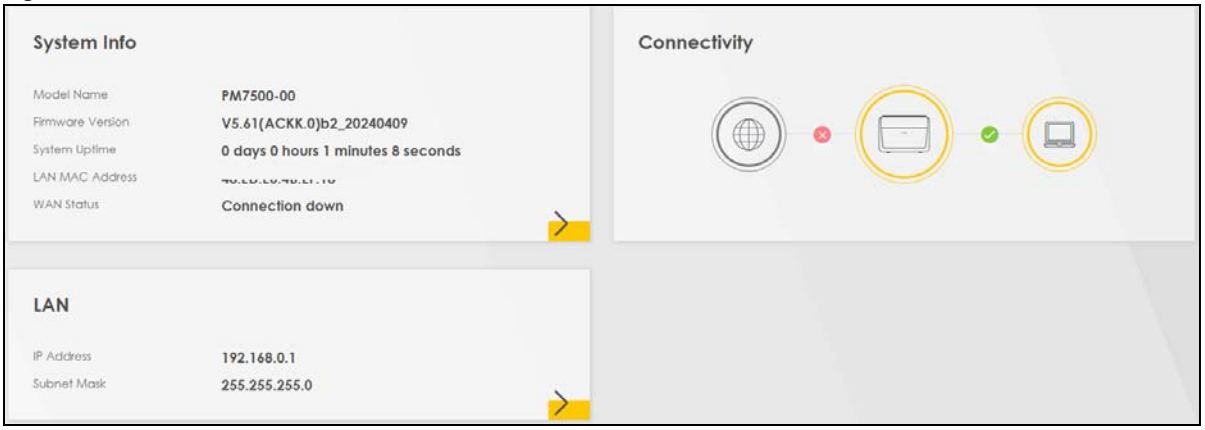
5 The following screen displays if you have not yet changed your password. Enter a new password, retype it to confirm and click **Apply**.

Figure 8 Change Password Screen



6 The **Connection Status** screen displays (see Chapter 4 on page 20 for details about it).

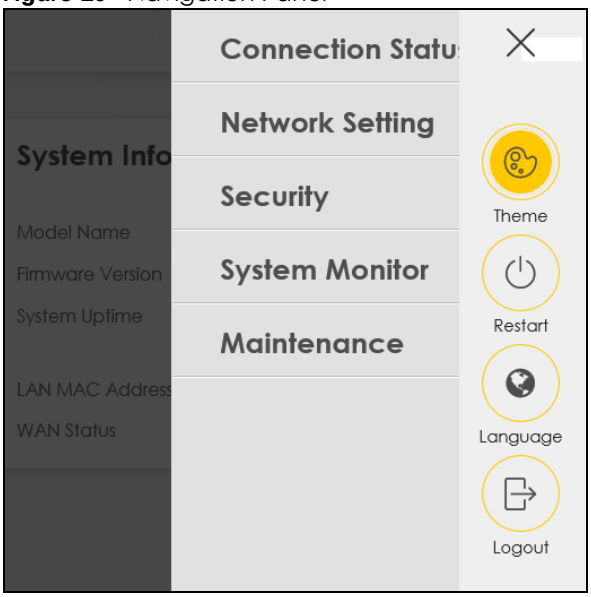
Figure 9 PM Device Connection Status



3.3 Navigation Panel

Click the menu icon ( ) to display a navigation panel as shown next with menu and sub-menu links and quick link icons. Click X to close the navigation panel.

Figure 10 Navigation Panel



The following tables describe each menu item.

Table 5 Navigation Panel Menus Summary

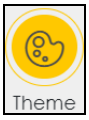
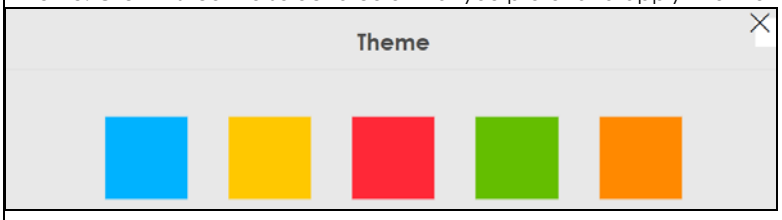
LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the PM Device and connected devices.
Networking Setting		
Broadband	Broadband	Use this screen to view the PM Device's WAN connections.
Home Networking	LAN Setup	Use this screen to configure LAN settings.
Security		

Table 5 Navigation Panel Menus Summary (continued)

LINK	TAB	FUNCTION
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the PM Device. You can export or e-mail the logs.
	Security Log	Use this screen to see the PM Device's security-related logs.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the PM Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the PM Device.
Optical Signal Status	Optical Signal Status	Use this screen to view the fiber transceiver's TX power and RX power level and its temperature.
Maintenance		
System	System	Use this screen to set Host name and Domain name of the PM Device.
User Account	User Account	Use this screen to change the user password or add user accounts on the PM Device.
Remote Management	MGMT Services	Use this screen to configure which services can access the PM Device and which interfaces can allow them.
	Trust Domain	Use this screen to manage a list of IP addresses which are allowed to access the PM Device through the services configured in the **Maintenance > Remote Management** screen.
Time	Time	Use this screen to change your PM Device's time and date settings.
Log Setting	Log Setting	Use this screen to change your PM Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your PM Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your PM Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the PM Device without turning the power off.
Diagnostic	Diagnostic	Use this screen to identify problems with the PON connection. Use ping and traceroute to test whether the PM Device can reach a particular host.

The icons provide the following functions.

Table 6 Navigation Panel Quick Link Icons

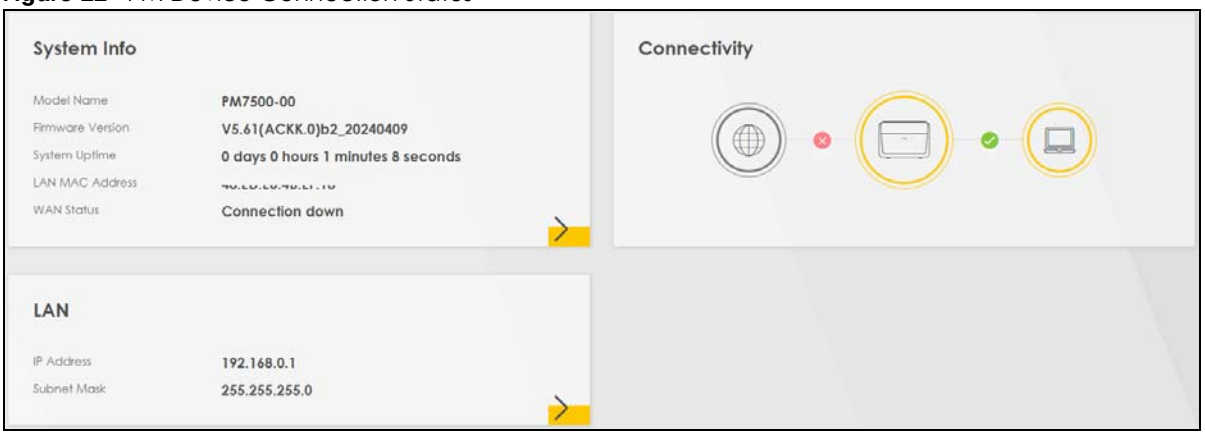
ICON	DESCRIPTION
	**Theme**: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
	**Language**: Select the language you prefer.
	**Restart**: Click this icon to reboot the PM Device without turning the power off.
	**Logout**: Click this icon to log out of the Web Configurator.

CHAPTER 4
Connection Status

4.1 Overview

The **Connection Status** screen appears when you log into the Web Configurator or click **Connection Status** in the navigation panel. This screen shows the network status of the PM Device and information about the connected computers and devices, and lets you configure some basic settings.

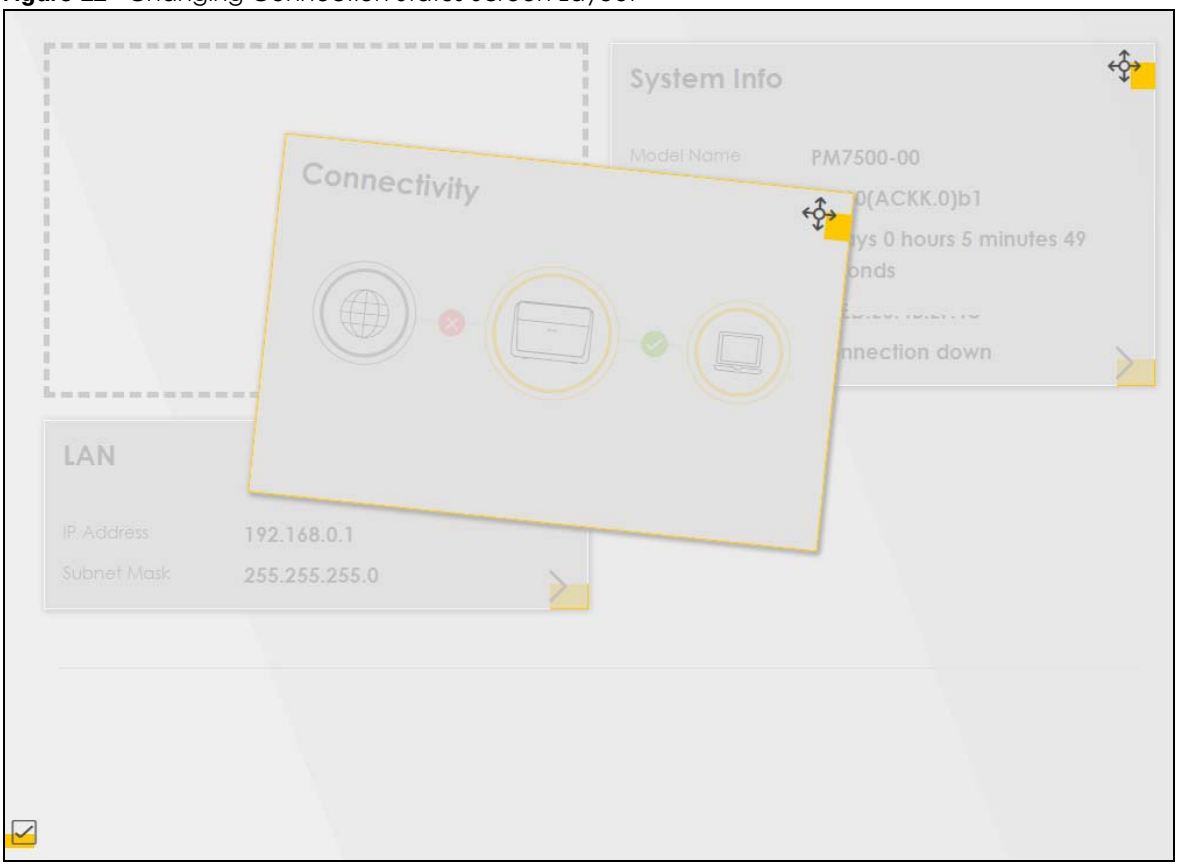
Figure 11 PM Device Connection Status



4.1.1 Layout Icon

Click the layout icon ( ) to arrange the panels. Select a panel and drag it to move it around. Click the check mark icon ( ) in the lower left corner to save the changes.

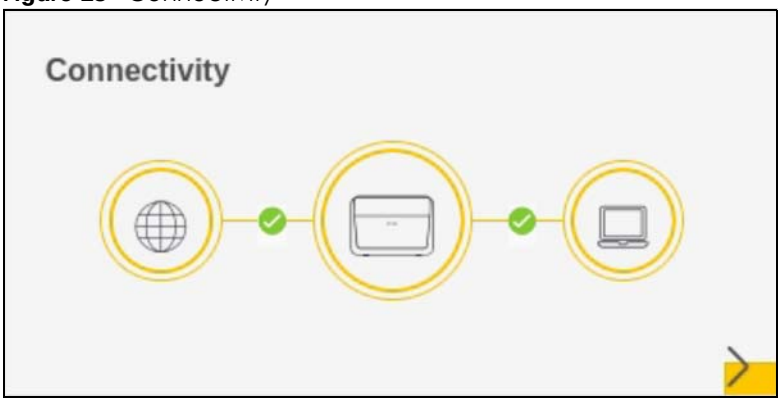
Figure 12 Changing Connection Status Screen Layout



4.2 Connectivity Panel

The **Connectivity** panel displays the status of the PM Device's network connections.

Figure 13 Connectivity

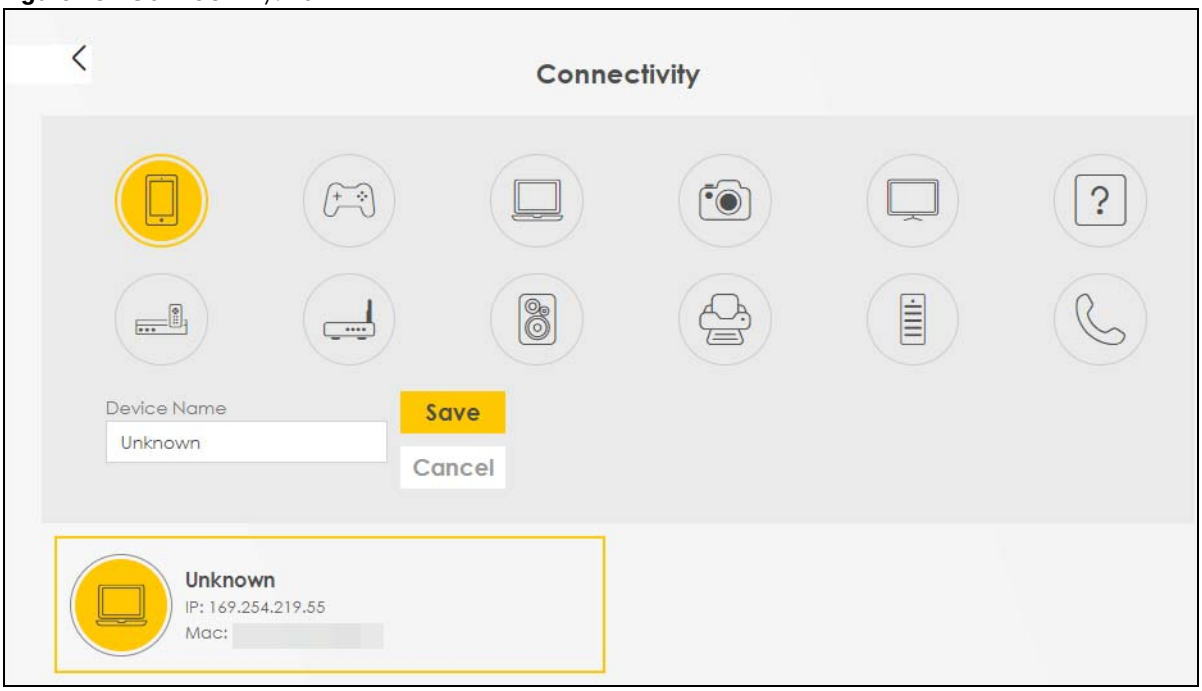


Click the **Arrow** icon ( ) to open the following screen. Use this screen to view the IP addresses and MAC addresses of the devices connected to the PM Device.

Figure 14 Connectivity: Connected Devices

Hover your cursor over a device to display an **Edit** icon ( ). Click the **Edit** icon to change the name or icon for a connected device. Enter a name in the **Device Name** field and/or select an icon for the connected device. Click **Save** to save your changes.

Figure 15 Connectivity: Edit



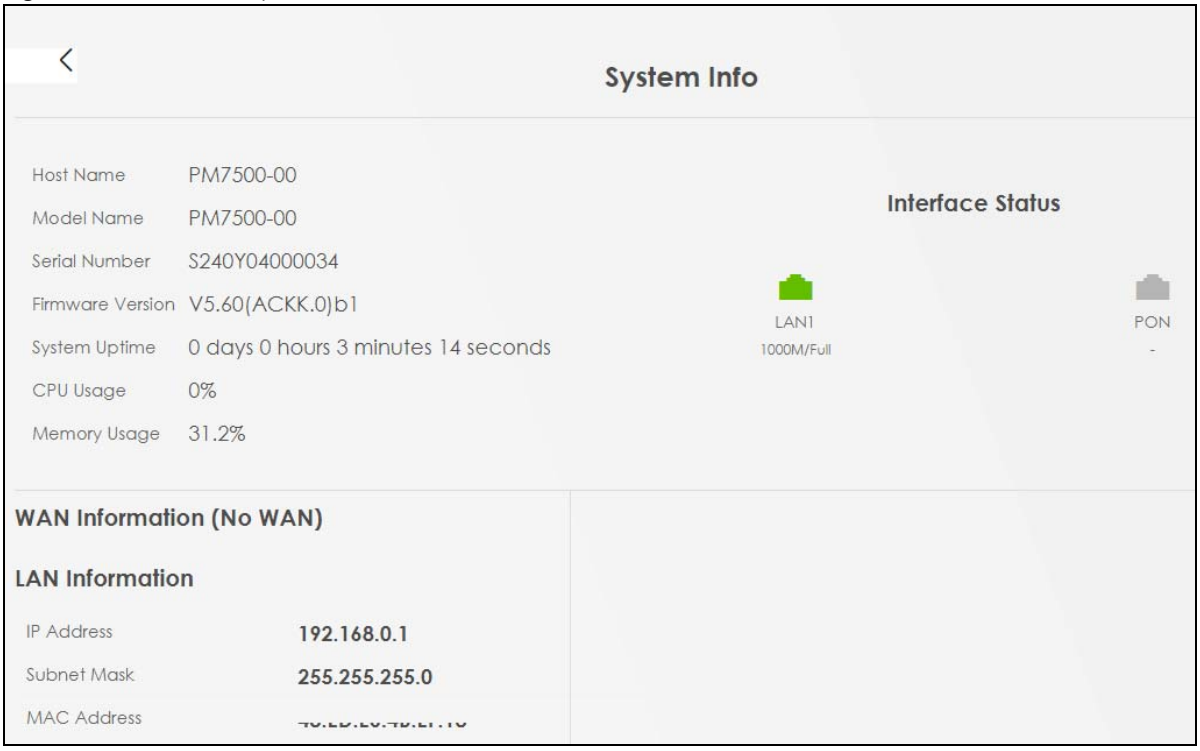
4.3 System Info Panel

The **System Info** panel displays the PM Device's basic system information.

Figure 16 System Info

Click the **Arrow** icon ( ) to open the following screen with more information.

Figure 17 Details for System Information



The following table describes the labels in this screen.

Table 7 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the PM Device system name. It is used for identification.
Model Name	This shows the model number of your PM Device.
Serial number	This field displays the serial number of the PM Device.
Firmware Version	This is the current version of the firmware inside the PM Device.
System Uptime	This field displays how long the PM Device has been running since it last started up. The PM Device starts up when you plug it in and turn it ON, when you restart it (**Maintenance > Reboot**), or when you reset it.
CPU Usage	This displays the current CPU usage percentage.

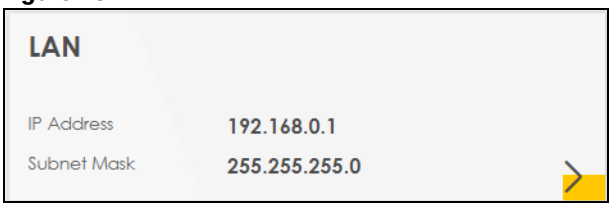
Table 7 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
Memory Usage	This displays the current RAM usage percentage.
Interface Status These virtual ports show whether the ports are in use and their connection or transmission rate.	
WAN Information These fields display when you have a WAN connection. **PON WAN** displays for an IPv4 WAN connection. **Ethernet WAN** displays for an IPv6 WAN connection.	
Name	This field displays the name configured in the PM Device for the WAN connection.
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IPv4 IP address of the PM Device in the WAN.
Release	A **Release** button displays when an IP WAN connection has an IPv4 address. Click **Release** to release the IPv4 address and set the IP address to 0.0.0.0.
Renew	A **Renew** button displays if you release an IP WAN connection's IP address. Click **Renew** to renew the IPv4 address.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
IPv6 Address	This field displays if the PM Device obtains an IPv6 address. It shows the current IPv6 IP address of the PM Device in the WAN.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your PM Device.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
LAN Information	
IP Address	This is the current IP address of the PM Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of the LAN interface.

4.4 LAN Panel

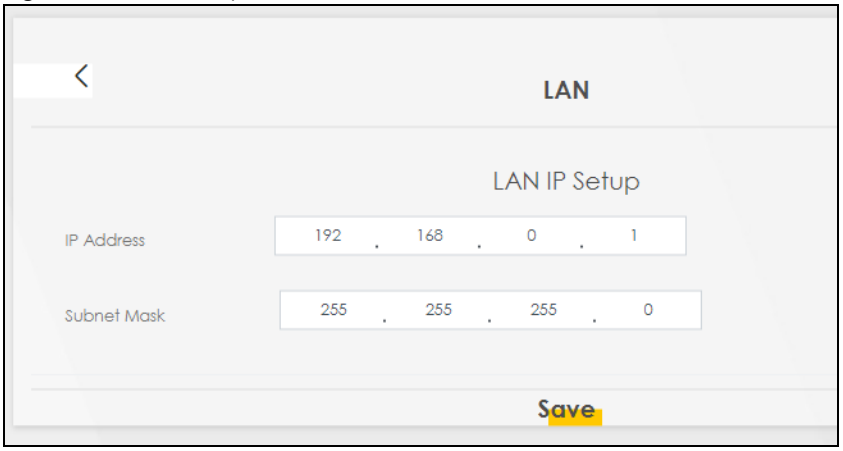
The **LAN** panel displays the PM Device's LAN IP address and subnet mask.

Figure 18 LAN



Click the **Arrow** icon ( ) to open the following screen. Use this screen to configure the PM Device's LAN IP address and subnet mask.

Figure 19 LAN Setup



The following table describes the labels in this screen.

Table 8 LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your PM Device in dotted decimal notation, for example, 192.168.0.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your PM Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.

CHAPTER 5
Broadband

5.1 Overview

This chapter discusses the PM Device's **Broadband** screen. Use this screen to view your PM Device's Internet access settings.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

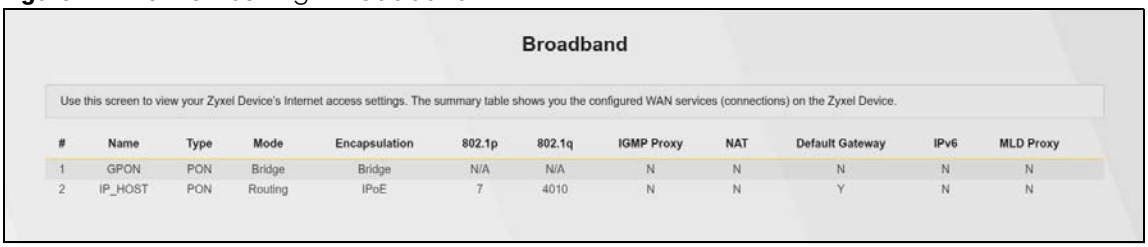
Figure 20 LAN and WAN

5.2 Broadband

Use this screen to view your PM Device's Internet access settings. The summary table shows you the WAN services (connections) on the PM Device.

Click **Network Setting** > **Broadband** to access this screen.

Figure 21 Network Setting > Broadband



The following table describes the labels in this screen.

Table 9 Network Setting > Broadband

LABEL	DESCRIPTION
#	This is the index number of the entry.
Name	This is the service name of the connection.

Table 9 Network Setting > Broadband (continued)

LABEL	DESCRIPTION
Type	This shows the types of the connections the PM Device has.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the PM Device act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the PM Device use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.

CHAPTER 6
Home Networking

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the **Home Networking** screens to help you configure the LAN settings.

6.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address and subnet mask of your PM Device (Section 6.2 on page 29).

6.1.2 What You Need To Know

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

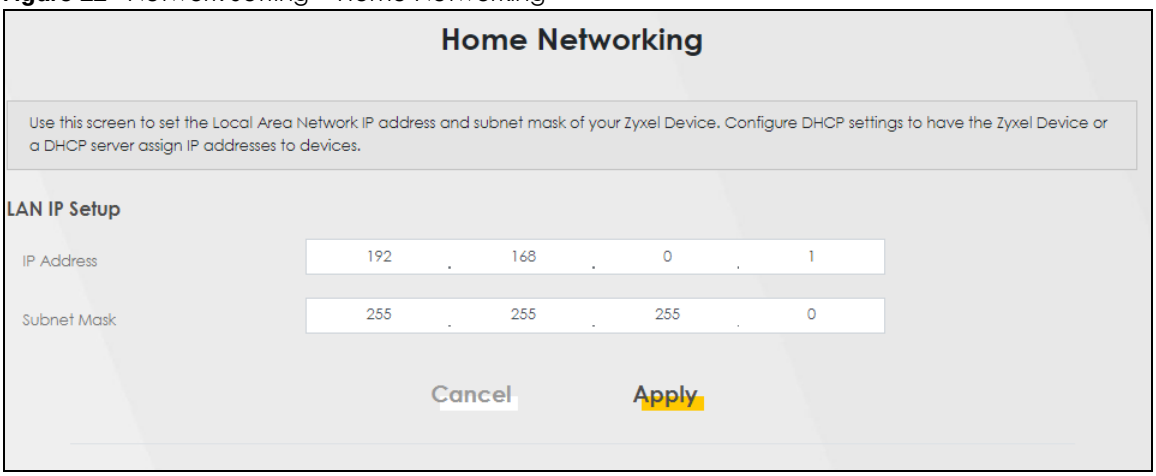
Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

6.2 LAN Setup

Click **Network Setting > Home Networking** to open the **LAN Setup** screen. Use this screen to set the LAN IP address and subnet mask of your PM Device. A LAN IP address is the IP address of a networking device in the LAN. You can use the PM Device's LAN IP address to access its Web Configurator from the LAN.

Figure 22 Network Setting > Home Networking



The following table describes the fields on this screen.

Table 10 Network Setting > Home Networking

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your PM Device in dotted decimal notation, for example, 192.168.0.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your PM Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 7
Certificates

7.1 Certificates Overview

The PM Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

7.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the PM Device's CA-signed certificates (Section 7.3 on page 30).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the PM Device (Section 7.4 on page 34).

7.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

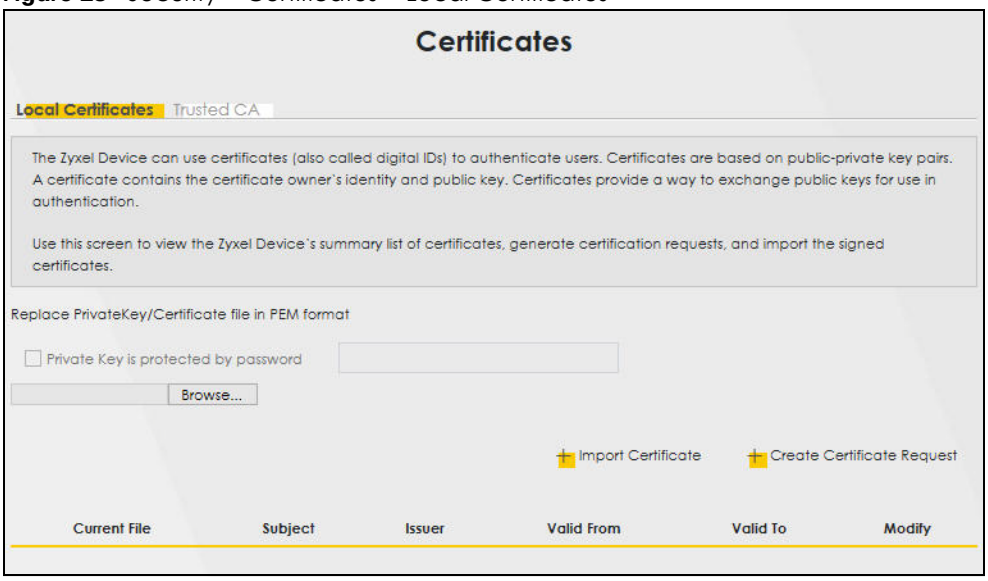
Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the PM Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

7.3 Local Certificates

Click **Security > Certificates** to open the **Local Certificates** screen. Use this screen to view the PM Device's summary list of certificates, generate certification requests, and import signed certificates.

Figure 23 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

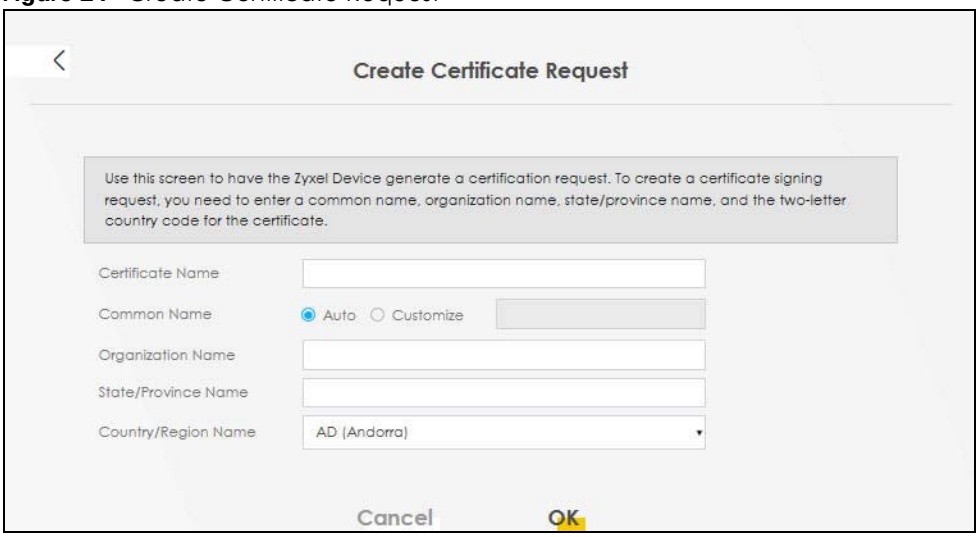
Table 11 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Private Key is protected by a password	Select the check box and enter the private key into the text box to store it on the PM Device. The private key should not exceed 63 ASCII characters (not including spaces).
Browse / Choose File	Click **Browse** or **Choose File** to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the PM Device.
Create Certificate Request	Click this button to go to the screen where you can have the PM Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

7.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the PM Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Figure 24 Create Certificate Request



The following table describes the labels in this screen.

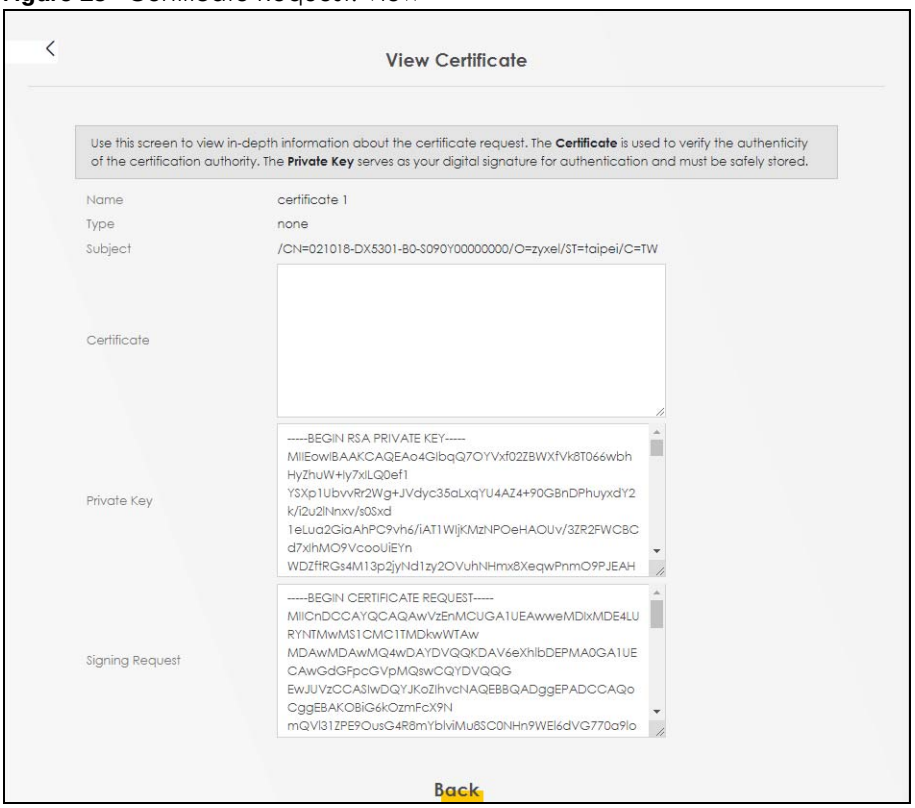
Table 12 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the PM Device configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the PM Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the PM Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

7.3.2 View Certificate Request

Click the **Edit** icon in the **Local Certificates** screen to open the following screen. Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored.

Figure 25 Certificate Request: View



The following table describes the fields in this screen.

Table 13 Certificate Request: View

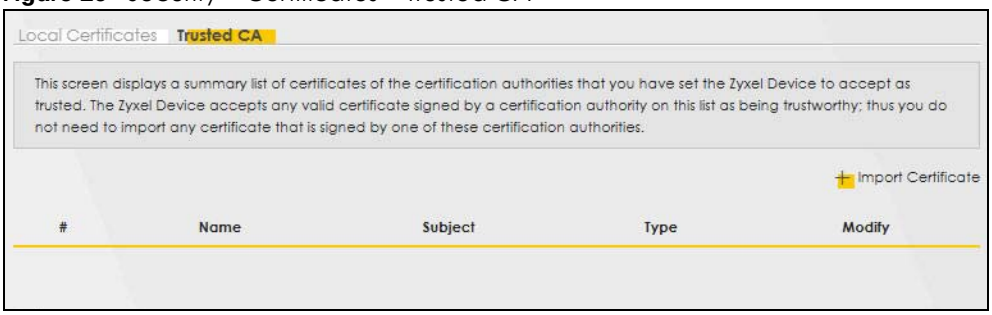
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click **Back** to return to the previous screen.

7.4 Trusted CA

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the PM Device to accept as trusted. The PM Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Note: A maximum of 10 trusted certificates can be added.

Figure 26 Security > Certificates > Trusted CA



The following table describes the fields in this screen.

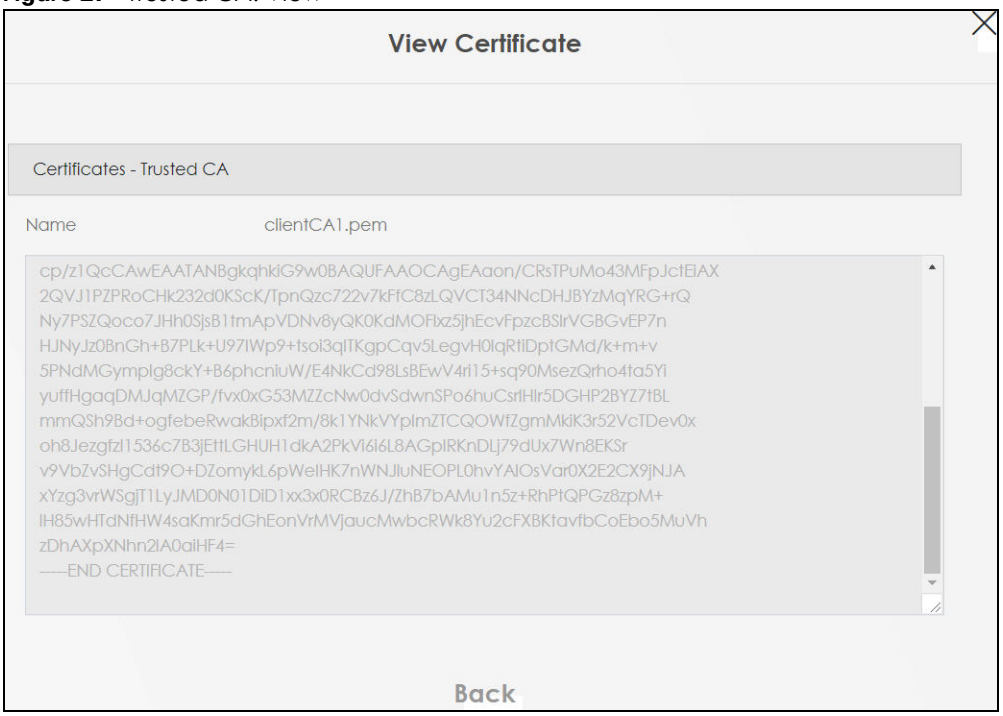
Table 14 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the PM Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

7.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Figure 27 Trusted CA: View



The following table describes the fields in this screen.

Table 15 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.

7.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The PM Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS#7, or PEM (base-64) encoded PKCS#7.

Figure 28 Trusted CA: Import Certificate

The following table describes the fields in this screen.

Table 16 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Click **Browse** or **Choose File** and select the certificate you want to upload.
Choose File/ Browse	Click this button to find the certificate file you want to upload.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 8
Log

8.1 Overview

The Web Configurator allows you to choose which categories of events and/or alerts to have the PM Device log and then display the logs or have the PM Device send them to an administrator (as e-mail) or to a syslog server.

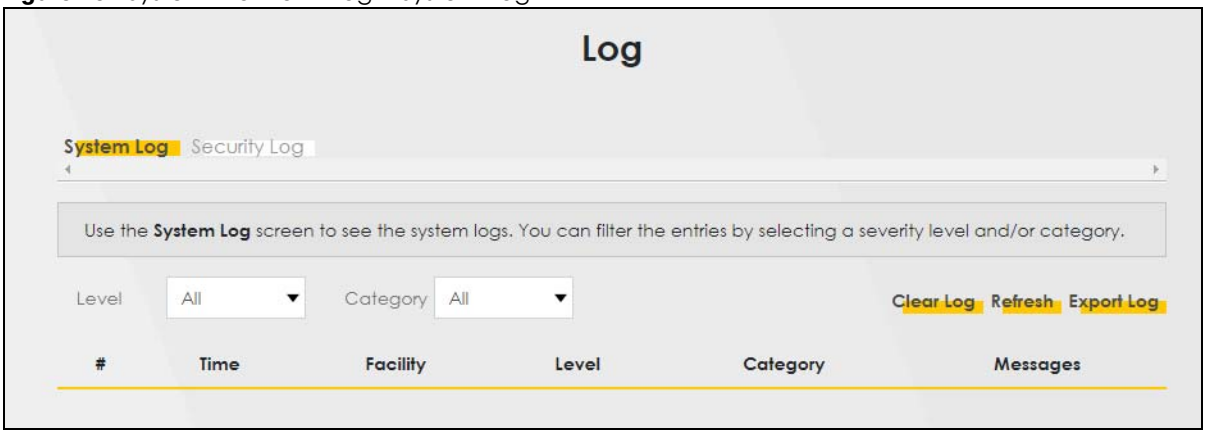
8.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 8.2 on page 37).
- Use the **Security Log** screen to see the security-related logs (Section 8.3 on page 38).

8.2 The System Log Screen

Use the **System Log** screen to see the system logs. Click **System Monitor > Log** to open the **System Log** screen.

Figure 29 System Monitor > Log > System Log



The following table describes the labels in this screen.

Table 17 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box to display only logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the logs.

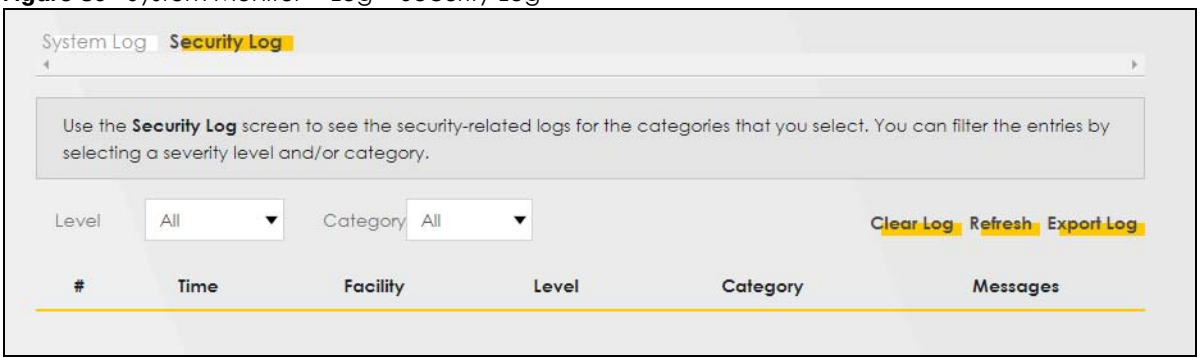
Table 17 System Monitor > Log > System Log (continued)

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

8.3 Security Log

Use the **Security Log** screen to see the security-related logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 30 System Monitor > Log > Security Log



The following table describes the labels in this screen.

Table 18 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box to display only security logs of that severity or higher.
Category	Select the type of security logs to display.
Clear Log	Click this to delete all the security logs.
Refresh	Click this to renew the list of security logs.
Export Log	Click this to export the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

CHAPTER 9
Traffic Status

9.1 Traffic Status Overview

Use the **Traffic Status** screens to look at the network traffic status and statistics of the WAN and LAN interfaces.

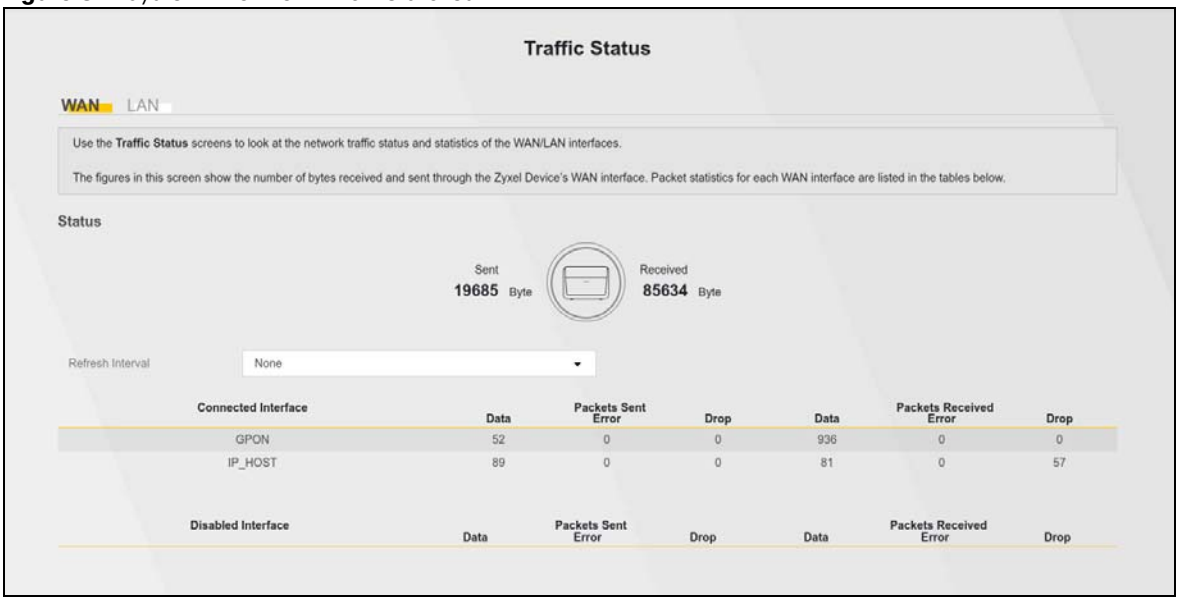
9.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 9.2 on page 39).
- Use the **LAN** screen to view the LAN traffic statistics (Section 9.3 on page 40).

9.2 WAN Traffic Status

Click **System Monitor > Traffic Status** to open the **WAN Traffic Status** screen. This screen shows the total numbers of bytes sent and received through the PM Device's WAN interfaces and each WAN interface's packet statistics.

Figure 31 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

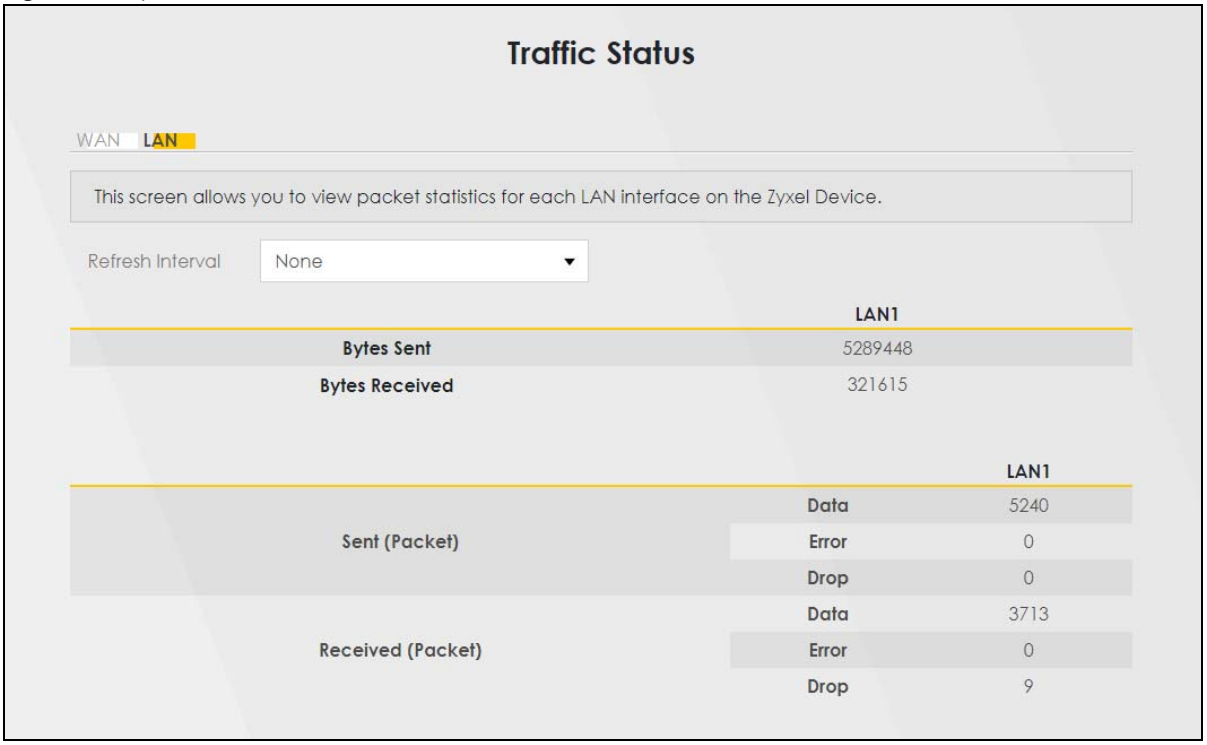
Table 19 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the PM Device to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disabled.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

9.3 LAN Status

Click **System Monitor > Traffic Status > LAN** to open the following screen. This screen allows you to view packet statistics for the LAN interface.

Figure 32 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

Table 20 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the PM Device to update this screen.
Interface	This shows the LAN interface on the PM Device.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN interfaces on the PM Device.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

CHAPTER 10
Optical Signal Status

10.1 Overview

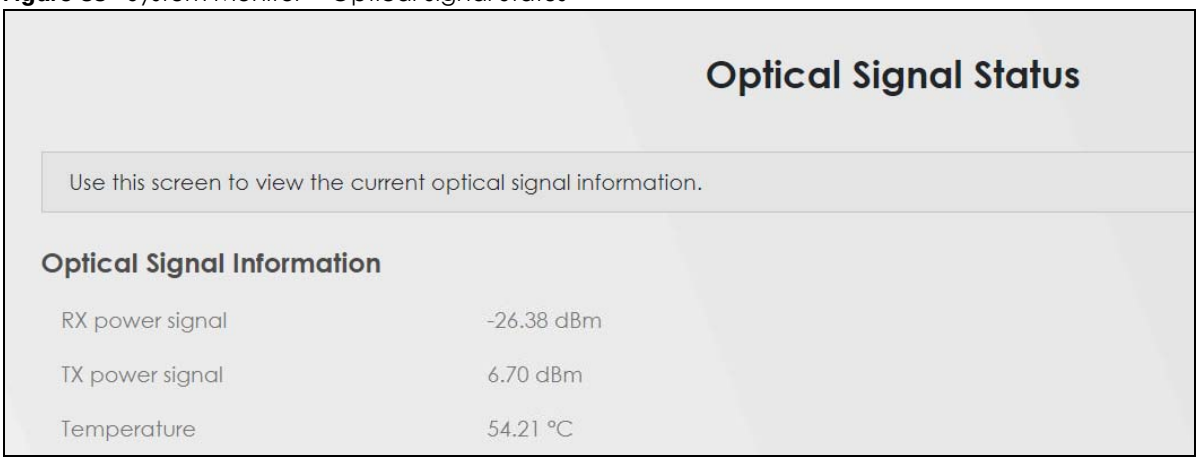
Use this screen to view the PON transceiver's TX power and RX power level and its temperature.

10.2 The Optical Signal Status Screen

Click **System Monitor > Optical Signal Status** to open the **Optical Signal Status** screen to see the real-time DDMI parameters.

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

Figure 33 System Monitor > Optical Signal Status



The following table describes the labels in this screen.

Table 21 System Monitor > Optical Signal Status

LABEL	DESCRIPTION
Optical Signal Information	
RX power signal	This field displays the transceiver's receiving power in dBm. The normal range is -9 to -28 dBm. The lower the value, the stronger the signal as there is less background noise. For example, -28 dBm is a stronger signal than -9 dBm.
TX power signal	This field displays the transceiver's transmitting power in dBm. The normal range is 4 to 9 dBm.
Temperature	This field displays the transceiver's temperature in degrees Celsius. The normal range is 0 to 85 degrees Celsius. (185 degrees Fahrenheit)

Note: Make sure the fiber optic cable is well connected to the PON port.

Note: If the TX and RX power signals of the DDMI are out of range, inspect the fiber optic cable for dirt, any fiber optic cable bends, or excessive curves. If the fiber optic cable is clean and undamaged, use a power meter to measure whether the actual RX power signal of the PM Device falls within the range of -9 to -28 dBm.

CHAPTER 11
System

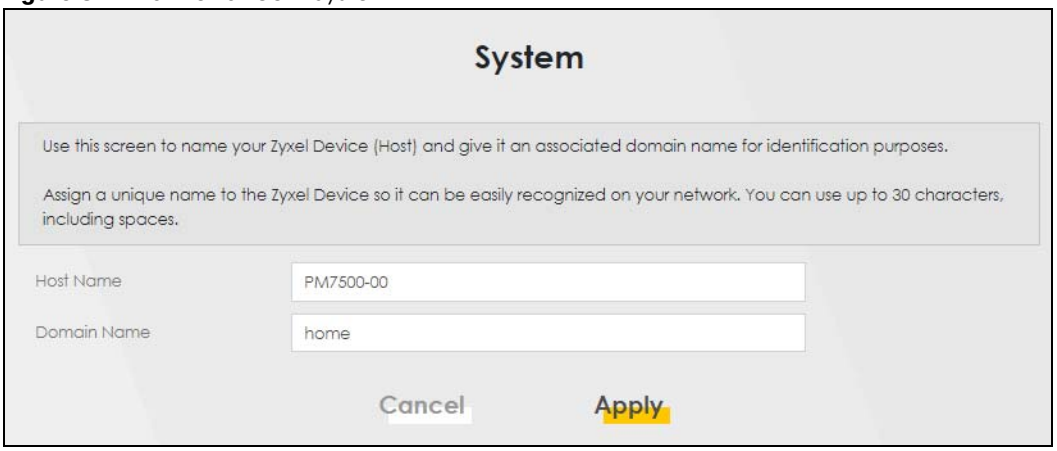
11.1 Overview

On the **System** screen, you can name your PM Device (Host) and give it an associated domain name for identification purposes.

11.2 The System Screen

Click **Maintenance > System** to open the following screen. Assign a unique name to the PM Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 34 Maintenance > System



The following table describes the labels on this screen.

Table 22 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your PM Device. Enter a descriptive name of up to 30 alphanumeric characters, including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your host PM Device for identification purpose. Enter a descriptive name of up to 30 alphanumeric characters. The following special characters listed in the brackets ["`<>^$|&;\/:*?'] are not allowed in the **Domain Name**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to abandon this screen without saving.

CHAPTER 12
User Account

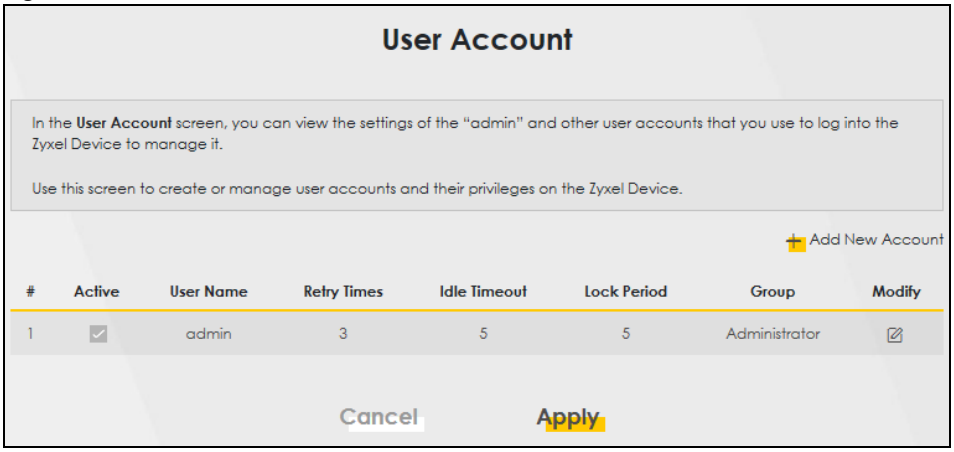
12.1 Overview

In the **User Account** screen, you can view the settings of the "admin" and other user accounts that you use to log in the PM Device.

12.2 The User Account Screen

Click **Maintenance > User Account** to open the following screen.

Figure 35 Maintenance > User Account



Note: The maximum number of the user account is four.

There are two of types of user accounts, Administrator and User. The table below shows the web privilege differences of **Administrator** and **User** at the time of writing.

The following table describes the labels on this screen.

Table 23 Administrator/User privilege differences

LINK	TAB	ADMINISTRATOR	USER
Configuration			
	Connection Status	Yes	Yes
Network			
	Broadband	Yes	No
	Home Networking	Yes	No
Security			
	Certificates	Yes	No

Table 23 Administrator/User privilege differences (continued)

LINK	TAB	ADMINISTRATOR	USER
System Monitor			
	Log	Yes	Yes
	Traffic Status	Yes	Yes
	Optical Signal Status	Yes	Yes
Maintenance			
	System	Yes	No
	User Account	Yes	Yes
	Remote Management	Yes	Yes
	Log Setting	Yes	Yes
	Firmware Upgrade	Yes	Yes
	Backup Restore	Yes	Yes
	Reboot	Yes	Yes

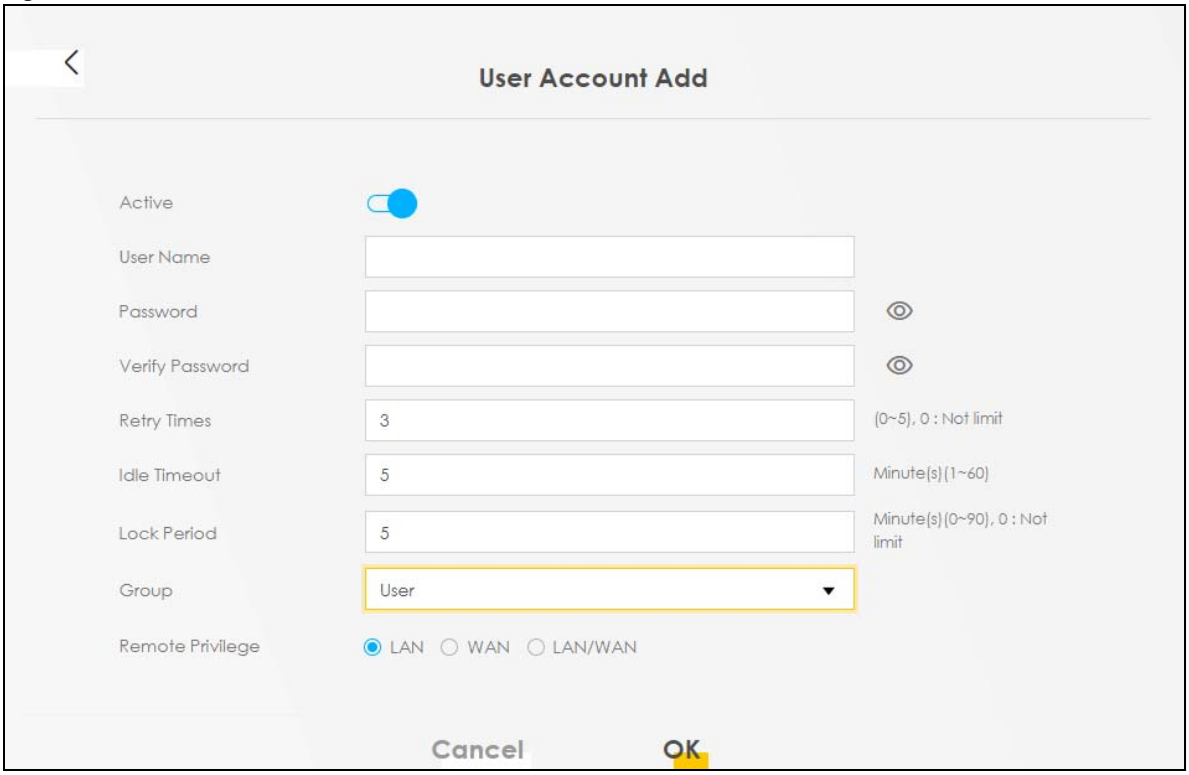
Table 24 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
User Name	This field displays the name of the account used to log into the PM Device Web Configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This field displays the length of inactive time before the PM Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	This field displays whether this user has **Administrator** or **User** privileges.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the PM Device.

12.2.1 The User Account Add/Edit Screen

Click **Add New Account** or the **Modify** icon of an existing account in the **Maintenance > User Account** to open the following screen.

Figure 36 Maintenance > User Account > Add



The following table describes the labels on this screen.

Table 25 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (switch turns blue) or disable (switch turns gray) the user account. This field is grayed out if you are editing the logged-in account.
User Name	Enter a new name for the account (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign ($) vertical bar (|) ampersand (&) semicolon (;)
Old Password	Type the default password or the existing password used to access the PM Device Web Configurator. This field only appears when editing an existing account.
New Password	Type your new system password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. Click the eye icon to view the password. After you change the password, use the new password to access the PM Device.
Verify Password	Type the new password again for confirmation. Click the eye icon to view the password.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the PM Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	Specify whether this user will have **Administrator** or **User** privileges. This field displays when adding a new account.
Remote Privilege	Select whether this user can access the PM Device with HTTPS or SSH through the **WAN**, **LAN** or **LAN/WAN**. Only the Administrator is allowed to use Telnet and SSH for remote management.

Table 25 Maintenance > User Account > Add/Edit (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

CHAPTER 13
Remote Management

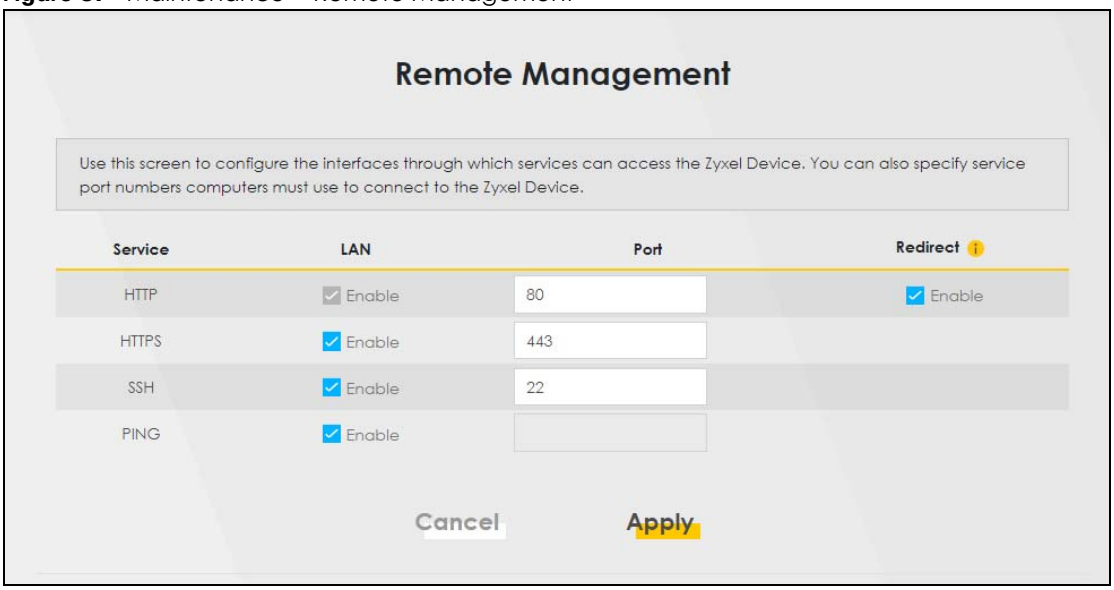
13.1 Overview

Remote management controls through which interfaces, which services can access the PM Device, and from which IP addresses.

13.2 MGMT Services

Use this screen to configure which services can access the PM Device and which interfaces can allow them. You can also specify the port numbers the services must use to connect to the PM Device. Click **Maintenance > Remote Management > MGMT Services** to open the following screen. Use this screen to configure which services can access the PM Device and which interfaces can allow them. You can also specify the port numbers the services must use to connect to the PM Device. Click **Maintenance > Remote Management** to open the following screen.

Figure 37 Maintenance > Remote Management



The following table describes the labels on this screen.

Table 26 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
Service	This is the service you may use to access the PM Device.
LAN	Select the **Enable** check box for the corresponding services that you want to allow access to the PM Device from the LAN.

Table 26 Maintenance > Remote Management > MGMT Services (continued)

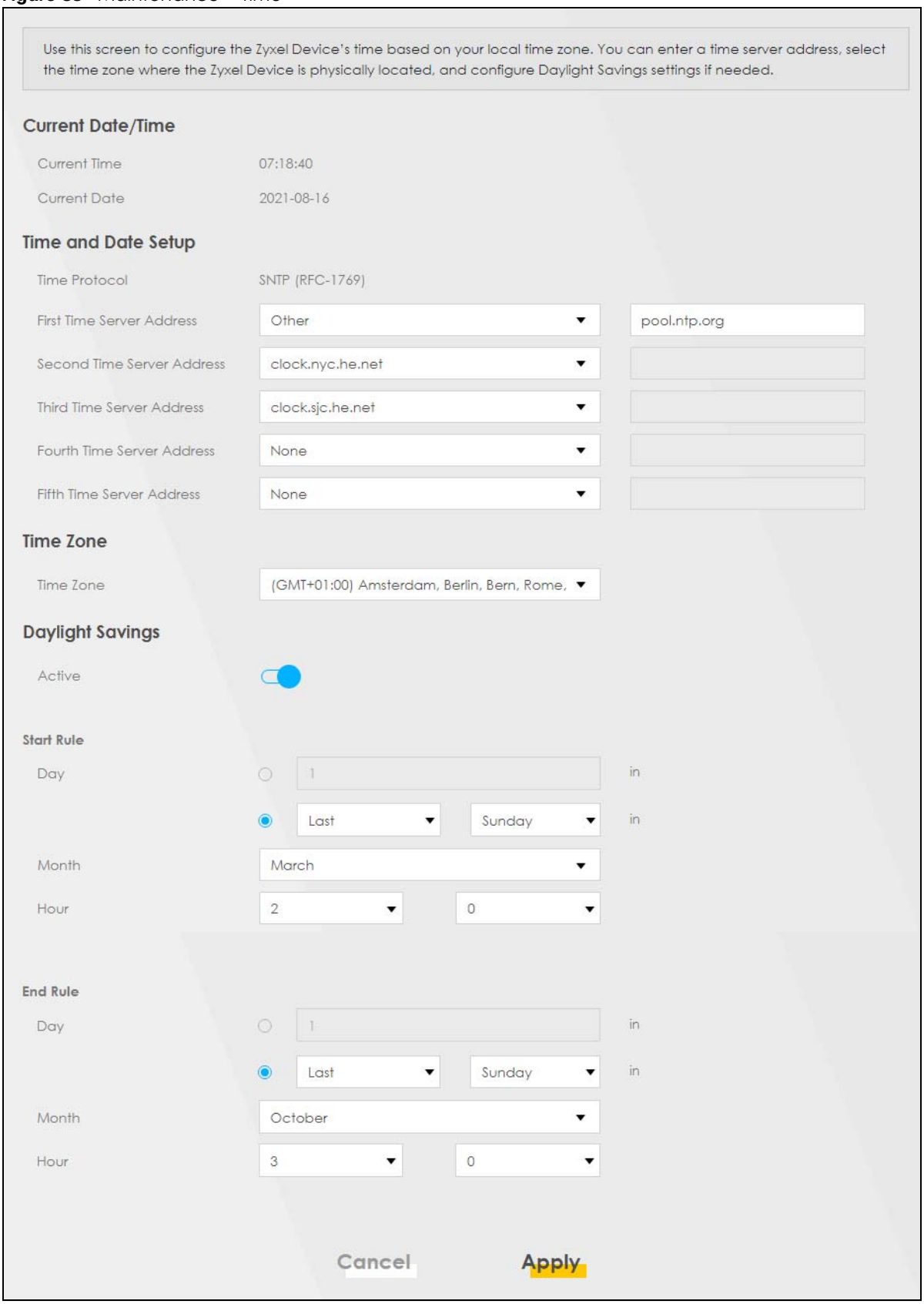
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server. For example, if you enter http://192.168.0.1 in your browser to access the Web Configurator, then the PM Device will automatically change this to the more secure https://192.168.0.1 for access.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the PM Device.

CHAPTER 14
Time

14.1 Time

To change your PM Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the PM Device's time based on your local time zone.

Figure 38 Maintenance > Time



The following table describes the labels on this screen.

Table 27 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your PM Device. Each time you reload this page, the PM Device synchronizes the time with the time server.
Current Date	This field displays the date of your PM Device. Each time you reload this page, the PM Device synchronizes the date with the time server.
Time and Date Setup	
Time Protocol	This displays the time protocol your PM Device uses.
First ~ Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** to not configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Click the switch to move it to the right ( ) to have the PM Device use Daylight Saving Time. Click the switch again to move it to the left ( ) to have the PM Device not use Daylight Saving Time.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Hour** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Time** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select depends on your time zone. In Germany for instance, you would select **2** in the **Time** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 27 Maintenance > Time (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the PM Device.

CHAPTER 15
Log Setting

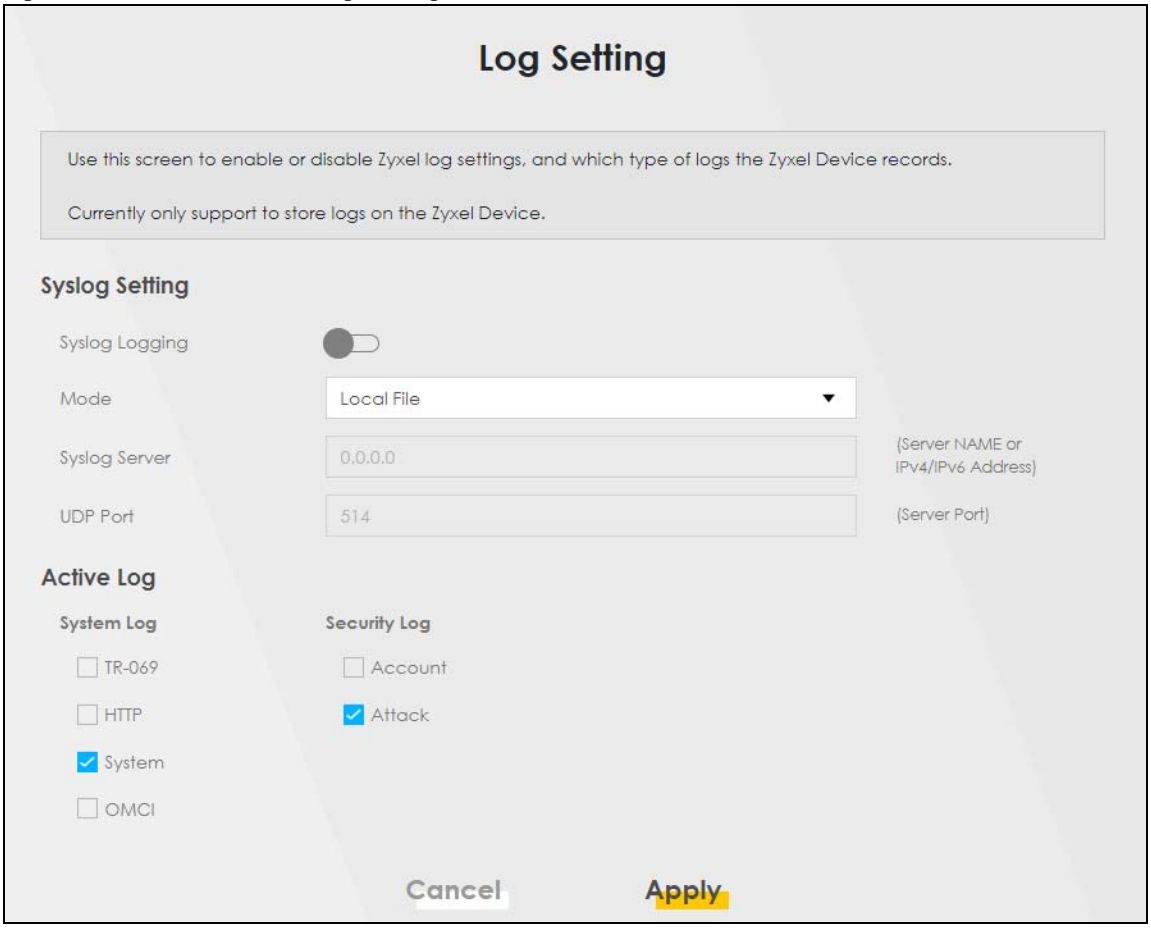
15.1 Overview

You can configure where the PM Device sends logs and which logs and/or immediate alerts the PM Device records in the **Logs Setting** screen.

15.2 Log Setting

To change your PM Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 39 Maintenance > Log Setting



The following table describes the fields on this screen.

Table 28 Maintenance > Log Setting

LABEL	DESCRIPTION
Active Log	
System Log	Select the categories of system logs to record.
TR-069	Select **TR-069** to record information related to the TR-069 auto-configuration service to monitor or troubleshoot problems.
HTTP	Select **HTTP** to record information related to the Internet Information services to monitor or troubleshoot problems.
System	Select **System** to record information related to the system to monitor or troubleshoot problems.
OMCI	Select **OMCI** to record information related to the ONT Interface to monitor or troubleshoot problems.
Security Log	Select the categories of security logs to record.
Account	Select **Account** to record information related to the PM Device's user accounts.
Attack	Select **Attack** to record information related to attacks detected on the PM Device.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 16
Firmware Upgrade

16.1 Overview

This chapter explains how to upload new firmware to your PM Device. You can download new firmware releases from your nearest Zyxel FTP site (or www.zyxel.com) to use to upgrade your device's performance.

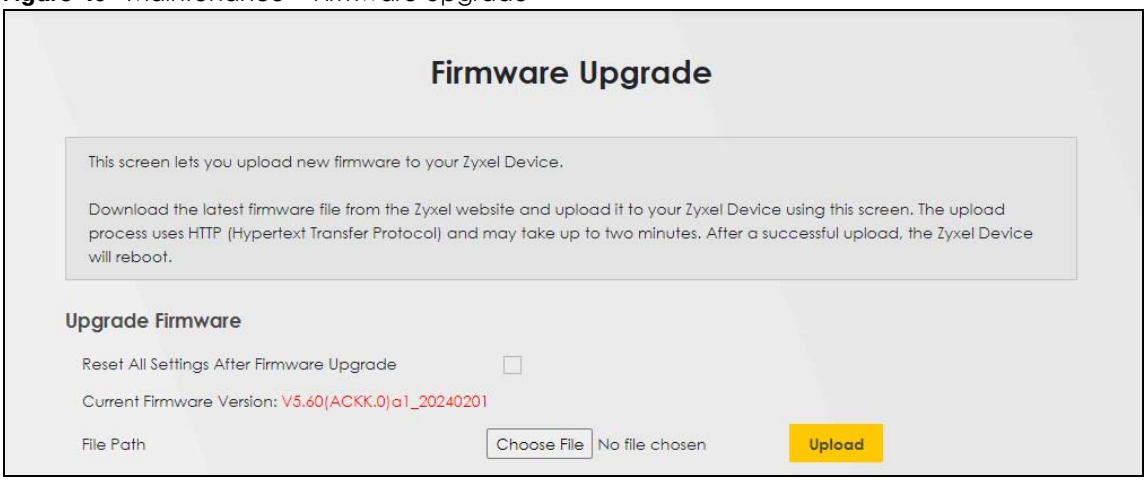
Only use firmware for your device's specific model. Refer to the label on the bottom of your PM Device.

16.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTPS (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the PM Device while firmware upload is in progress.

Figure 40 Maintenance > Firmware Upgrade



The following table describes the labels on this screen. After you see the firmware updating screen, wait two minutes before logging into the PM Device again.

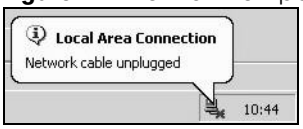
Table 29 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Click the check box to have the PM Device automatically reset itself after the new firmware is uploaded.
Reset All Settings After Firmware Upgrade	Click the check box to have the PM Device automatically reset itself after the new firmware is uploaded.
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you wasn't to upload in this field or click **Browse** to find it.
Browse / Choose File	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

After you see the firmware updating screen, wait a few minutes before logging into the PM Device again.

The PM Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 41 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

CHAPTER 17
Backup/Restore

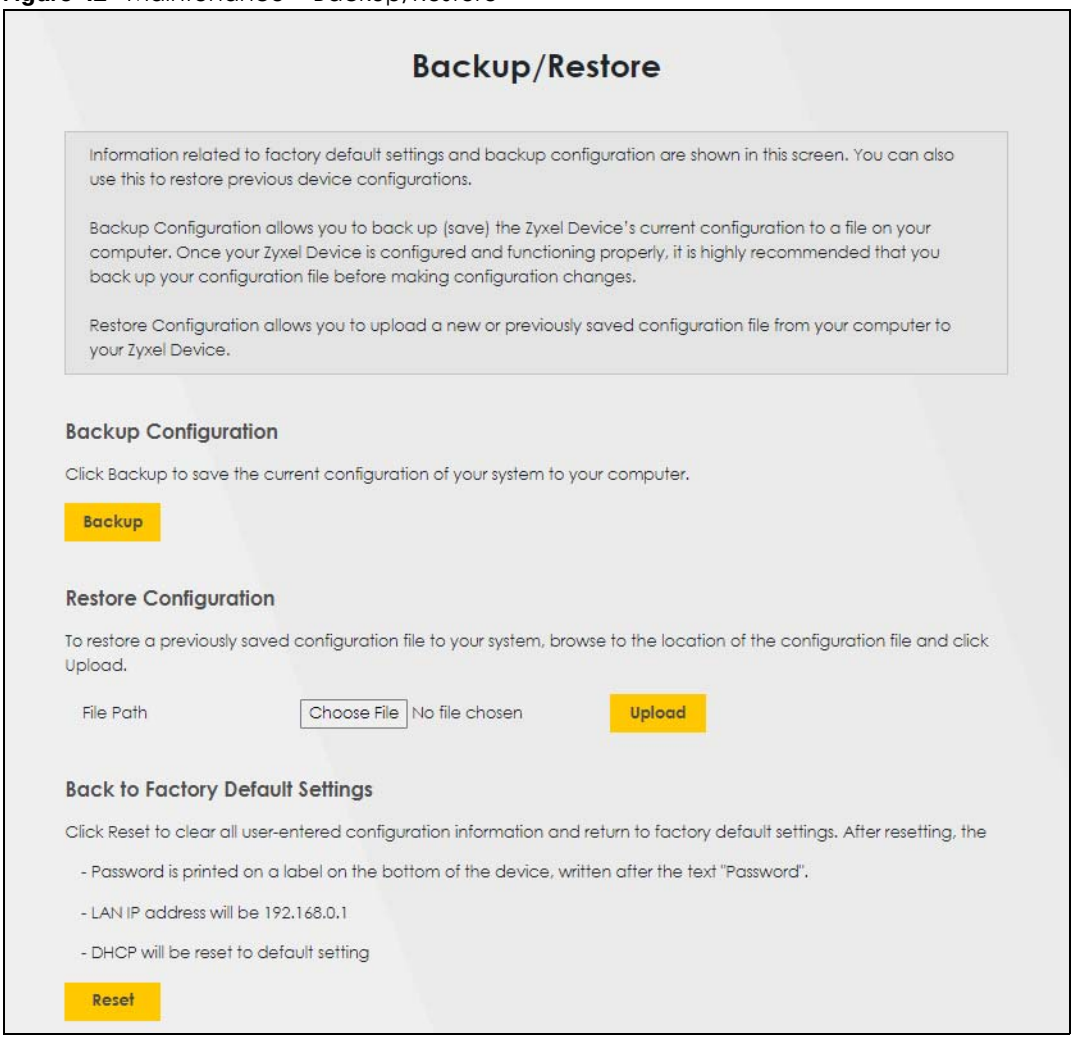
17.1 Overview

The **Backup/Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

17.2 The Backup/Restore Screen

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears on this screen, as shown below.

Figure 42 Maintenance > Backup/Restore



Backup Configuration

Backup Configuration allows you to back up (save) the PM Device's current configuration to a file on your computer. Once your PM Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the PM Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your PM Device.

Table 30 Restore Configuration

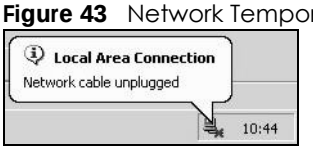
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse / Choose File	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your PM Device settings back to the factory default.

Do not turn off the PM Device while configuration file upload is in progress.

After the PM Device configuration has been restored successfully, the login screen appears. Login again to restart the PM Device.

The PM Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 43 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.0.1).

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen. Reset to Factory Defaults.

Click the **Reset** button to clear all user-entered configuration information and return the PM Device to its factory defaults. The following warning screen appears.

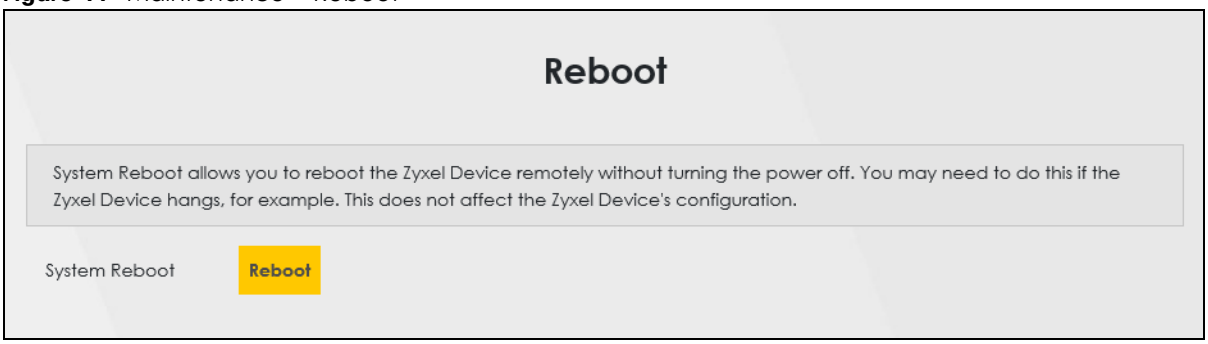
You can also press the **RESET** button on the rear panel to reset the factory defaults of your PM Device. Refer to Section 2.3.1 on page 14 for more information on the **RESET** button.

17.3 The Reboot Screen

System restart allows you to reboot the PM Device remotely without turning the power off. You may need to do this if the PM Device hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the PM Device reboot. This does not affect the PM Device's configuration.

Figure 44 Maintenance > Reboot



CHAPTER 18
Diagnostic

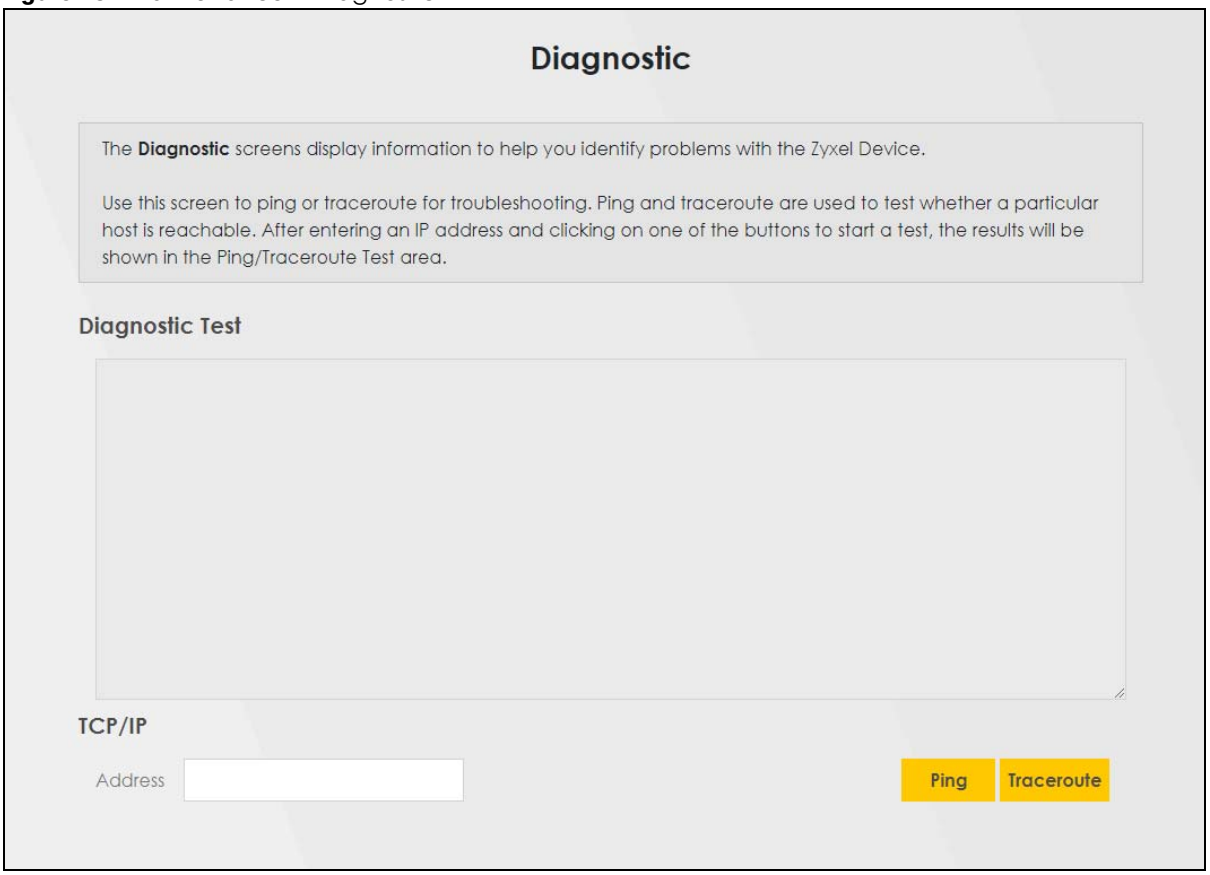
18.1 Overview

The **Diagnostic** screen displays information to help you identify problems with the PM Device.

18.2 Diagnostic

Use this screen to ping or traceroute for troubleshooting. Use ping and traceroute to test whether the PM Device can reach a particular host. After entering an IP address and clicking one of the buttons to start a test, the results display in the **Diagnostic Test** area. Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 45 Maintenance > Diagnostic



The following table describes the fields on this screen.

Table 31 Maintenance > Diagnostic

LABEL	DESCRIPTION
Diagnostic Test	The test results display here.
TCP/IP	
Address	Enter either an IP address or a host name to which to test the connection.
Ping	Click this button to perform a ping test on the IPv4 address or host name in order to test the connection. The ping statistics will show in the info area.
Traceroute	Click this button to check the path and transmission delays between the PM Device and the IPv4 address you entered.

CHAPTER 19
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
- PM Device Access and Login
- Internet Access

19.1 Power, Hardware Connections, and LEDs

The PM Device does not turn on. None of the LEDs turn on.

1. Make sure the PM Device is turned on.
2. Make sure you are using the power adapter or cord included with the PM Device.
3. Make sure the power adapter or cord is connected to the PM Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the PM Device off and on.
5. 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 2.2 on page 12.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the PM Device off and on.
5. If the problem continues, contact the vendor.

19.2 PM Device Access and Login

I forgot the IP address for the PM Device.

1. The default LAN IP address is 192.168.0.1.
2. If you changed the IP address and have forgotten it, you might get the IP address of the PM Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the PM Device (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 2.3.1 on page 14.

I forgot the password.

1. See the label at the bottom of the PM Device for the default login names and associated passwords.
2. If those do not work, you have to reset the device to its factory defaults. See Section 2.2 on page 12.

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 192.168.0.1.
   - If you changed the IP address (Section 6.2 on page 29), 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 PM Device.
2. Make sure your computer uses an IP address within the same subnet as the PM Device.
3. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 2.2 on page 12.
4. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
5. If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).
6. Reset the device to its factory defaults and try to access the PM Device with the default IP address. See Section 2.3.1 on page 14.

7 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the PM Device using another service, such as Telnet. If you can access the PM Device, check the remote management settings to find out why the PM Device does not respond to HTTP / HTTPS.

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

1 Make sure you have entered the password correctly. See the device label for the default login name and associated password. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the Web Configurator while someone is using Telnet to access the PM Device. Log out of the PM Device in the other session, or ask the person who is logged in to log out.

3 Turn the PM Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 19.1 on page 65.

I cannot access the PM Device via Telnet.

See the troubleshooting suggestions for I cannot see or access the **Login screen in the Web Configurator.** Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the **Login screen in the Web Configurator.** Ignore the suggestions about your browser.

19.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 2.2 on page 12.

   The **PON** LED is off if the optical transceiver has malfunctioned or the fiber cable is not connected or is broken or damaged enough to break the PON connection.

   The **LOS** LED turns red if the PM Device is not receiving an optical signal.

   The **LOS** LED turns blinking red if the PM Device is receiving a weak optical signal

   See Section 2.2 on page 12 for details about the other LEDs.

2. Disconnect all the cables from your device and reconnect them.

3. If the problem continues, contact your ISP.

I cannot access the PM Device anymore. I had access to the PM Device, but my connection is not available anymore.

1. Your session with the PM Device may have expired. Try logging into the PM Device again.

2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 2.2 on page 12.

3. Turn the PM Device off and on.

4. If the problem continues, contact your vendor.

PART II
Appendices

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 Communications Corp. office for the region in which you bought the device.

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

For Zyxel Communications Corp. 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 Corp. Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corp. Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corp. Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Communications Corp. Kazakhstan
- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Communications Corp. Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp. Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp. Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp. Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications Corp. Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

Thailand

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

Vietnam

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

Europe

Belarus

- Zyxel Communications Corp. Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Communications Corp. Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Communications Corp. Bulgaria

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

Czech Republic

- Zyxel Communications Corp. Communications Czech s.r.o.
- https://www.zyxel.com/cz/cs

Denmark

- Zyxel Communications Corp. Communications A/S
- https://www.zyxel.com/dk/da

Finland

- Zyxel Communications Corp. Communications
- https://www.zyxel.com/fi/fi

France

- Zyxel Communications Corp. France
- https://www.zyxel.com/fr/fr

Germany

- Zyxel Communications Corp. Deutschland GmbH.
- https://www.zyxel.com/de/de

Hungary

- Zyxel Communications Corp. Hungary & SEE
- https://www.zyxel.com/hu/hu

Italy

- Zyxel Communications Corp. Communications Italy S.r.l.
- https://www.zyxel.com/it/it

Norway

- Zyxel Communications Corp. Communications A/S
- https://www.zyxel.com/no/no

Poland

- Zyxel Communications Corp. Communications Poland
- https://www.zyxel.com/pl/pl

Romania

- Zyxel Communications Corp. Romania
- https://www.zyxel.com/ro/ro

Russian Federation

- Zyxel Communications Corp. Communications Corp.
- https://www.zyxel.com/ru/ru

Slovakia

- Zyxel Communications Corp. Slovakia
- https://www.zyxel.com/sk/sk

Spain

- Zyxel Communications Corp. Iberia
- https://www.zyxel.com/es/es

Sweden

- Zyxel Communications Corp. 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 Communications Corp. Turkey A.S.
- https://www.zyxel.com/tr/tr

UK

- Zyxel Communications Corp. Communications UK Ltd.
- https://www.zyxel.com/uk/en-gb

Ukraine

- Zyxel Communications Corp. Ukraine
- https://www.zyxel.com/ua/uk-ua

South America

Argentina

- Zyxel Communications Corp. Communications Corp.
- https://www.zyxel.com/co/es-co

Brazil

- Zyxel Communications Corp. Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp. Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp. Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp. Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp. Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications Corp. 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

Europe and the United Kingdom

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

Belgium (English) België (Flemish) Belgique (French)	**National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie *http://www.bipt.be* voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez *http://www.bipt.be* pour de plus amples détails.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.

Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check *https://www.mise.gov.it/it/* for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare *https://www.mise.gov.it/it/* per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

- Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

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

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
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 or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.
- CLASS 1 CONSUMER LASER PRODUCT EN 60825-1: 2014+A11:2021 & EN 50689:2021
- CAUTION: Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- 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.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market in compliance 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), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

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

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。
- 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 if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to *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.

Registration

Register your product online at *www.zyxel.com* to receive email notices of firmware upgrades and related information.

Trademarks

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

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: *https://service-provider.zyxel.com/global/en/gpl-oss-software-notice*

Index

M

N

O

P

R

S

T

U

W

Z