ZYXEL
COMMUNICATIONS

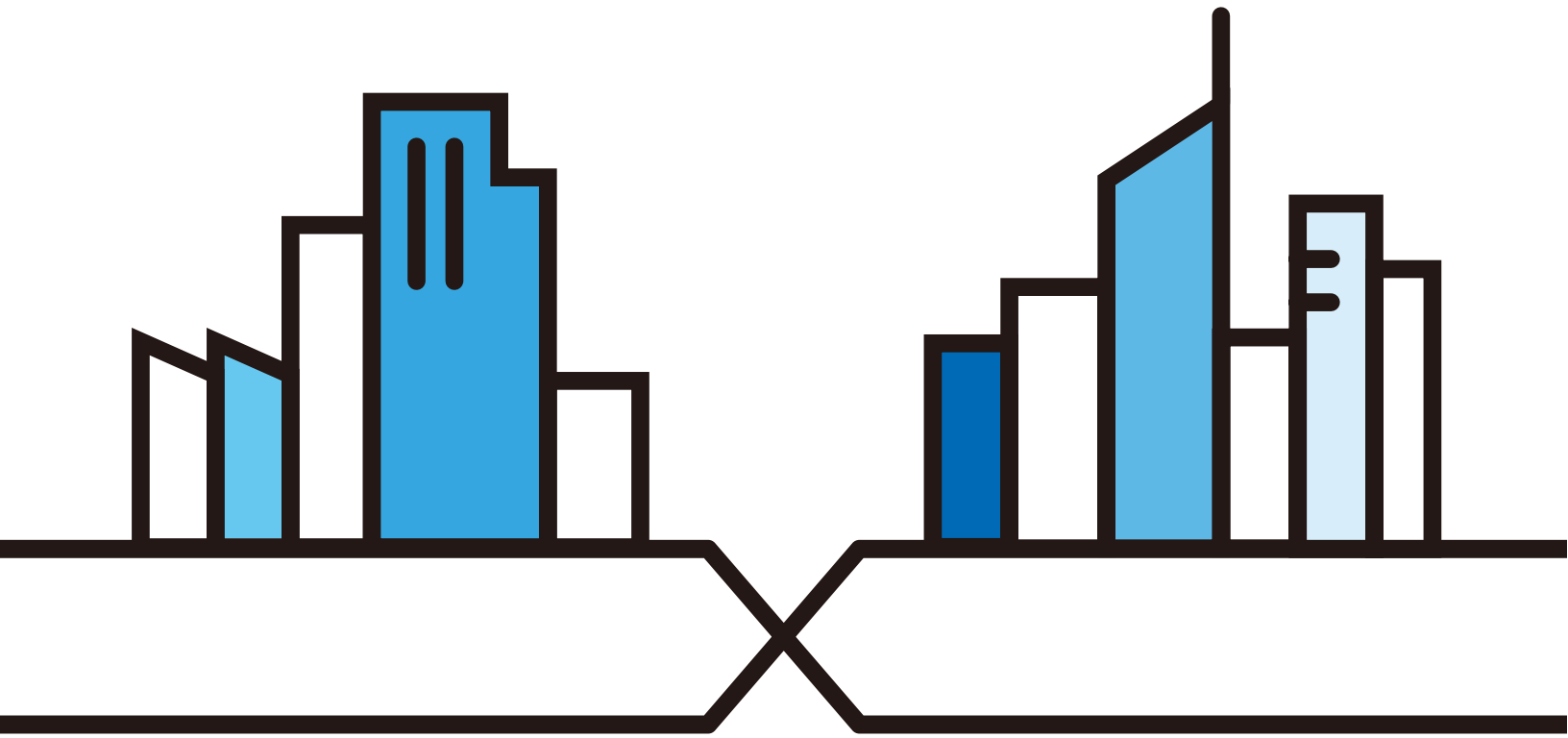
User's Guide

PM Series

G-PON SFU with 2.5G LAN / XGS-PON SFU with 10G LAN /
XGS-PON VoIP Bridge ONT with 10G LAN and UPS

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 4, 04/2025



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This User's Guide is for the platform version listed on the cover. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in product features or Web Configurator brand style. Every effort has been made to ensure that the information in this manual is accurate.

Note: The version number on the cover page refers to the PM Device's latest firmware version to which this User's Guide applies.

Related Documentation

- Quick Start Guide

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

- More Information

  Go to *https://service-provider.zyxel.com/global/en/tech-support* to find other information on the PM Device.

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 	Server 
Game Console 	Apple TV 	Storage 

Accessibility and Compatibility

Introduction

This User's Guide complies with the accessibility requirements set out in EAA (European Accessibility Act) (EU) 2019/882.

Accessibility makes this User's Guide usable for people with disabilities, including those with visual, auditory, motor, and cognitive impairments. Compatibility ensures this User's Guide works well with a wide range of devices, software, and assistive technologies.

Accessibility Feature – Screen Reader Support

The visually impaired may use screen readers, such as NVDA to read contents.

To use the screen reader, do the following:

1. Open your screen reader software.
2. Navigate to this User's Guide; the screen reader should automatically start reading the contents.
3. Use the keyboard shortcuts to navigate through this User's Guide (refer to the screen reader documentation).

Accessibility Feature – Keyboard Navigation

Keyboard navigation allows you to read the contents in this User's Guide without a mouse. Use the following keys.

- **Tab** key: navigate between interactive elements (for example, buttons, links, fields).
- **Enter** key: select or activate the highlighted item.
- Arrow keys: move between options in menus or lists.
- **Esc** (Escape) key: close pop-up windows or cancel actions.

How to Access Support Services

We offer the following ways to contact our Zyxel Communications Corp. support team.

Email Support: support.zyxel.com

Send a detailed description of your issue, including any error messages, screenshots, or steps you have already taken to resolve the problem. The response time is typically within 24 hours.

User Forums and Community Support: https://community.zyxel.com/en

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

This User's Guide is for the platform version listed on the cover. This chapter introduces the main features and applications of the PM Devices. The PM Devices are the PON (Passive Optical Network) modems that connect to the Internet though a fiber cable.

The PM Device refers to the following models:

- PM5100-T1
- PM7300-T0
- PM7500-00
- PM7505-00

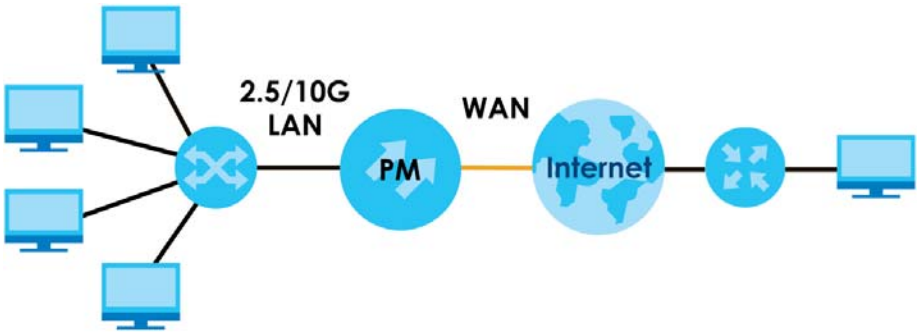
Table 1 PM Device Comparison Table

	PM5100-T1	PM7300-T0	PM7500-00	PM7505-00
Port Control Protocol	YES	YES	YES	YES
Fiber Optical Port	GPON	XGS-PON	XGS-PON	XGS-PON
Maximum Downstream Data Rate	2488 Mbps	9953.28 Mbps	9953.28 Mbps	9953.28 Mbps
Maximum Upstream Data Rate	1244 Mbps	9953.28 Mbps	9953.28 Mbps	9953.28 Mbps
Multi-Gig LAN	100 Mbps, 1 / 2.5 Gbps LAN	1 / 2.5 / 5/ 10 Gbps LAN	1 / 2.5 / 5 /10 Gbps LAN	100 Mbps, 1 / 2.5 / 5 / 10 Gbps LAN
LAN IP Setup	YES	YES	YES	YES
System Log	YES	YES	YES	YES
TFTP	YES (LAN only)	YES (LAN only)	YES (LAN only)	YES (LAN only)
Firmware Upgrade	YES	YES	YES	YES
Certificates	YES	YES	YES	YES
System Log	YES	YES	YES	YES
Security Log	NO	NO	NO	NO
Traffic Status	YES	YES	YES	YES
User Account's Maintenance	YES	YES	YES	YES
Remote Management	HTTP / HTTPS / SSH / PING	HTTP / HTTPS / SSH / PING	HTTP / HTTPS / SSH / PING	HTTP / HTTPS / SSH / PING
Backup/Restore	YES	YES	YES	YES
Diagnostic	NO	NO	NO	NO
Wall Mount	YES	YES	YES	YES

1.2 Example Application

This section shows a an example of using the PM Device in a network environment. Note that the PM Device in the figure is just an example PM Device and not your actual PM Device.

Figure 1 PM Device's Internet Access Application



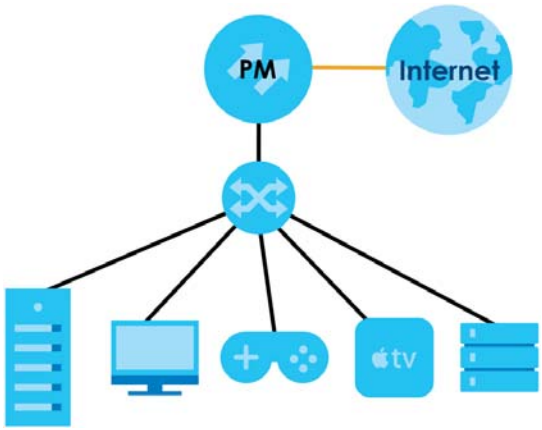
1.2.1 Multi-Gigabit Ethernet

Multi-Gigabit Ethernet supports network speeds of 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps. Not all Multi-Gigabit ports support all speeds. See Table 1 on page 12 for the speeds your PM Device supports.

Some network devices, such as gaming computers, servers, NAS devices, or access points, support 2.5 Gbps or 5 Gbps connectivity. The Multi-Gigabit Ethernet technology enables the PM Device to automatically detect and adjust to the required speed of the connected network device. A non-Multi-Gigabit 10G port would connect to a 2.5 Gbps or 5 Gbps device at just 1 Gbps.

Actual speeds also depend on the type of Ethernet cable used. See Table 2 on page 13 for the correct Ethernet cable type.

Figure 2 Multi-Gigabit Application



See the following table for the cables required and distance limitation to attain the corresponding speed. Please check Table 1 on page 12 for the transmission speeds supported by the PM Device.

Table 2 Ethernet Cable Types

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

Table 2 Ethernet Cable Types (continued)

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 6	5G / 10G	100 m / 55 m	250 MHz
Category 6a	10G	100 m	500 MHz
Category 7	10G	100 m	600 MHz
* A high quality Category 5e cable can support 5 Gbps and up to 100 m with no electromagnetic interference.			

1.3 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). Use for troubleshooting the PM Device by qualified personnel.

1.4 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.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the PM Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the PM Device. You could simply 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 Indicator Panel

The following figures show the PM Device LED indicators and the LED behaviors.

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

2.2.1 PM5100-T1

Figure 3 PM5100-T1

The following are the LED descriptions for your PM5100-T1.

Table 3 PM5100-T1 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.
2.5GbE	Green	On	The Ethernet link is up.
		Blinking	The PM Device is transmitting or receiving data.
		Off	The Ethernet link is down.

2.2.2 PM7300-T0 and PM7500-00

Figure 4 PM7300-T0 and PM7500-00

The following are the LED descriptions for your PM7300-T0 and PM7500-00.

Table 4 PM7300-T0 and PM7500-00 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.

2.2.3 PM7505-00

Figure 5 PM7505-00

The following are the LED descriptions for your PM7505-00.

Table 5 PM7505-00 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.
UPS	Green	On	The AC power is off and the UPS (battery backup) is providing power normally.
		Blinking	The battery is functioning abnormally. For example, the voltage exceeds the expected range.
		Off	The battery is not in use or cannot be charged.
PON	Green	On	The PON connection is ready.
		Blinking	The PM Device is trying to establish a link.
	Red	Blinking	The PON connection is ready but receiving low optical signal strength.
VoIP	Green	On	A SIP account for outgoing calls is enabled and registered. The phone is on-hook and idle.
		Blinking	The phone is off-hook or ringing for an incoming call.
	Amber	On	A SIP account is registered. The phone is on-hook and idle, and there is a voice message.
		Blinking	A SIP account is registered. The phone is off-hook or ringing for an incoming call and there is a voice message.
		Off	The VoIP function is turned-off (deactivated) or no SIP account is registered.

2.3 Rear/Bottom Panel Ports and Buttons

The following shows the PM Device rear panel with ports and buttons.

Place the PM Device with the ports and buttons facing you and the two wall-mounting holes at the bottom.

Figure 6 PM5100-T1

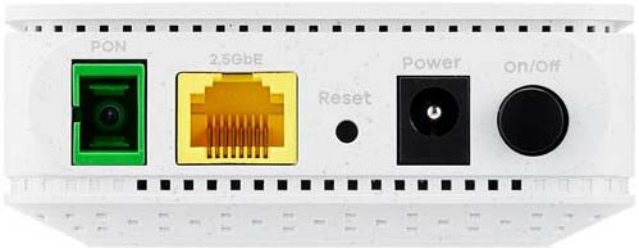


Figure 7 PM7300-T0

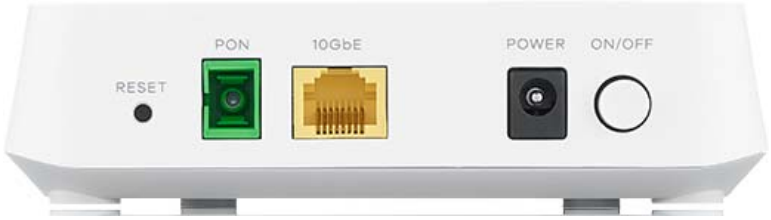


Figure 8 PM7500-00

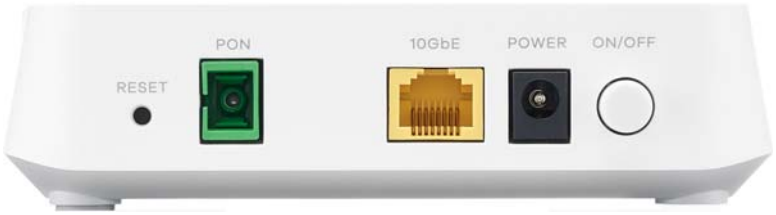
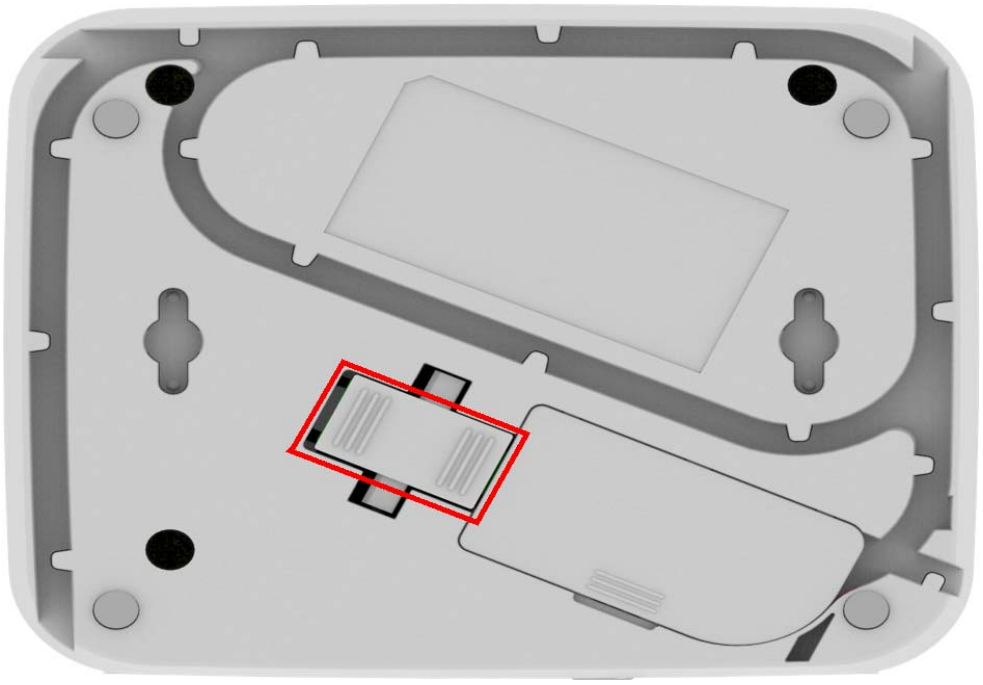


Figure 9 PM7505-00

Figure 10 PM7505-00 PON Port



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

Table 6 Rear/Bottom 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.
2.5 GbE / 10GbE / 1G LAN / 10G LAN	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 **ON/OFF** button to start the PM Device. Note: The ON/OFF button is not available for PM7505-00.
ON/OFF (except PM7505-00)	Press the **ON/OFF** button after connecting the power adapter to start the PM Device.
UPS (PM7505-00 only)	Connect a UPS (Uninterruptible Power Supply) to have a backup power source when the main power fails.
VoIP (PM7505-00 only)	Connect a VoIP (Voice over Internet Protocol) phone, softphone, or VoIP server for transmitting voice/audio data over the Internet instead of traditional phone lines.

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**.

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

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

The following figures shows the location of PM Device **RESET** button.

Figure 11 Reset Button (PM5100-T1)

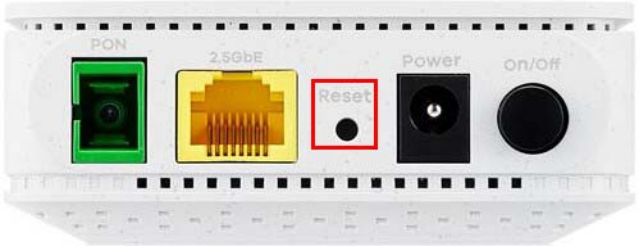


Figure 12 Reset Button (PM7300-T0)

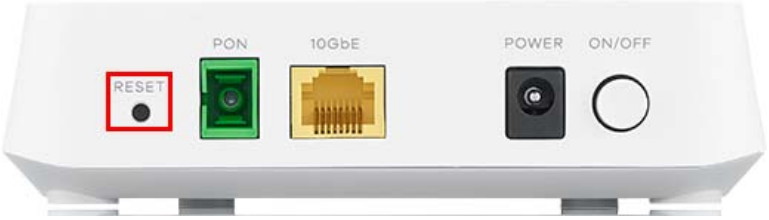


Figure 13 Reset Button (PM7500-00)

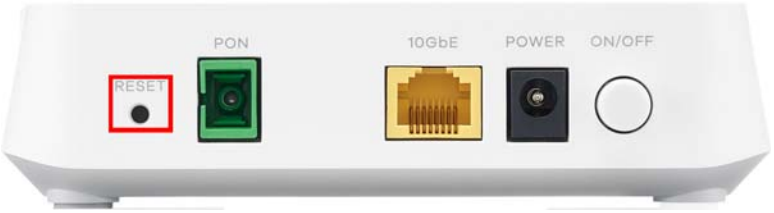


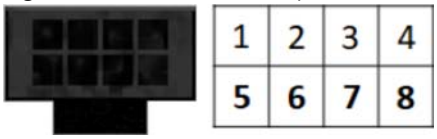
Figure 14 Reset Button (PM7505-00)

2.3.2 UPS Port

You can connect a UPS to the **UPS** port to keep the PM Device running in case the main power fails.

The following diagram and chart show the pin assignments of the **UPS** port on the PM Device.

Figure 15 UPS Port Pin Layout



The following table describes the **UPS** port's pin assignments.

Table 7 UPS Port Pin Assignment

PIN	ASSIGNMENT
1	Power Input +12V.
2	On Battery.
3	Missing Battery.
4	12V Power Return.
5	12V Power Return.
6	Replace Battery.
7	Low Battery.
8	No Connection (unused).

CHAPTER 3
The Web Configurator

3.1 Overview

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

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

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

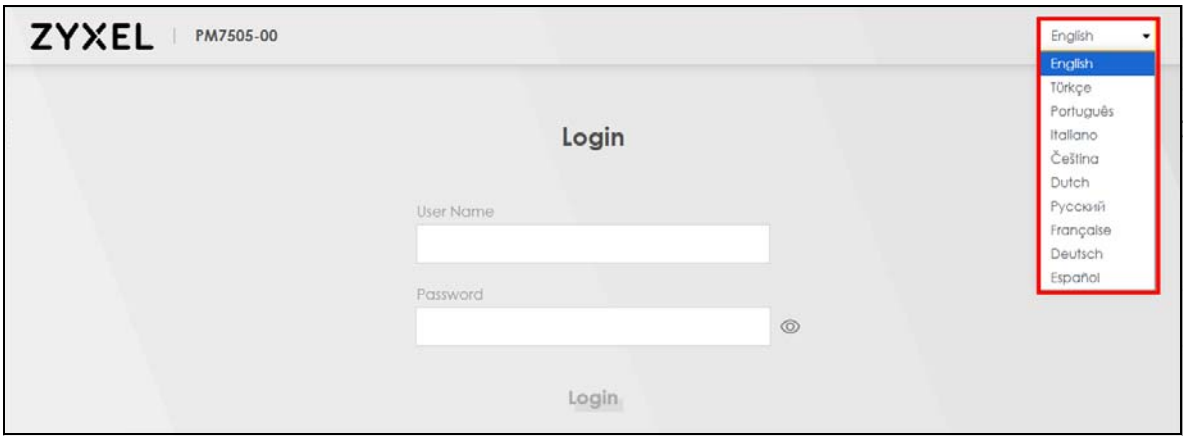
3.2 Accessing the Web Configurator

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 to 192.168.0.254 with subnet mask 255.255.255.0.

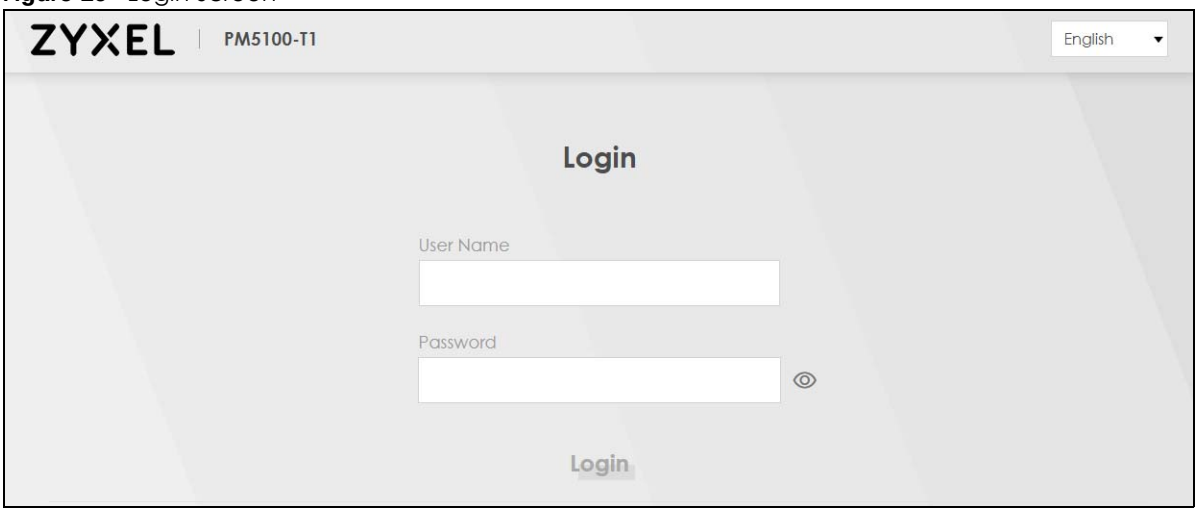
3 Launch your web browser and go to https://192.168.0.1.

4 A **Login** screen displays. Select the language you prefer (upper right).



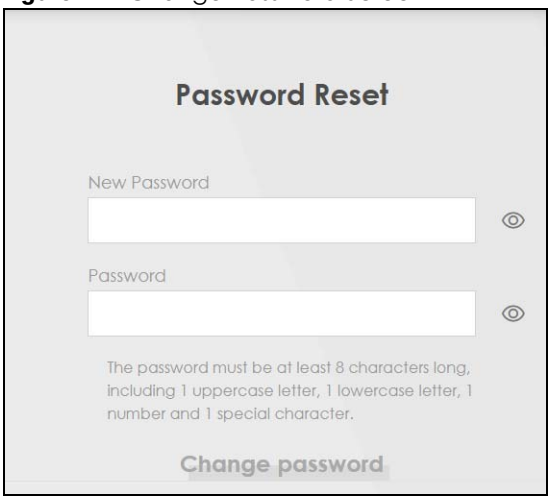
5 To access the administrative Web Configurator and manage the PM Device, type the default username **admin** and the randomly assigned default password (see the device label) in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 16 Login Screen



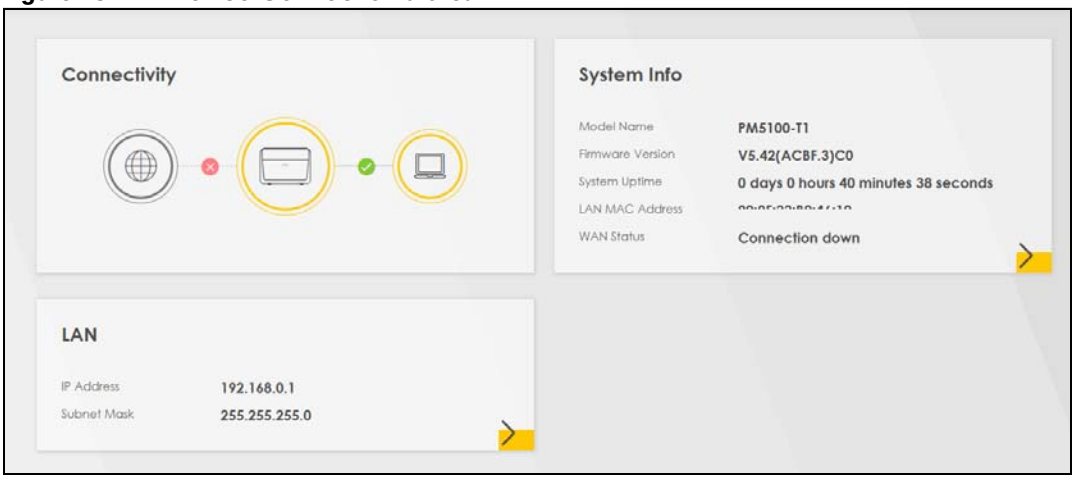
6 The following screen displays if you have not yet changed your password. Enter a new password, retype it to confirm and click **Apply**.

Figure 17 Change Password Screen



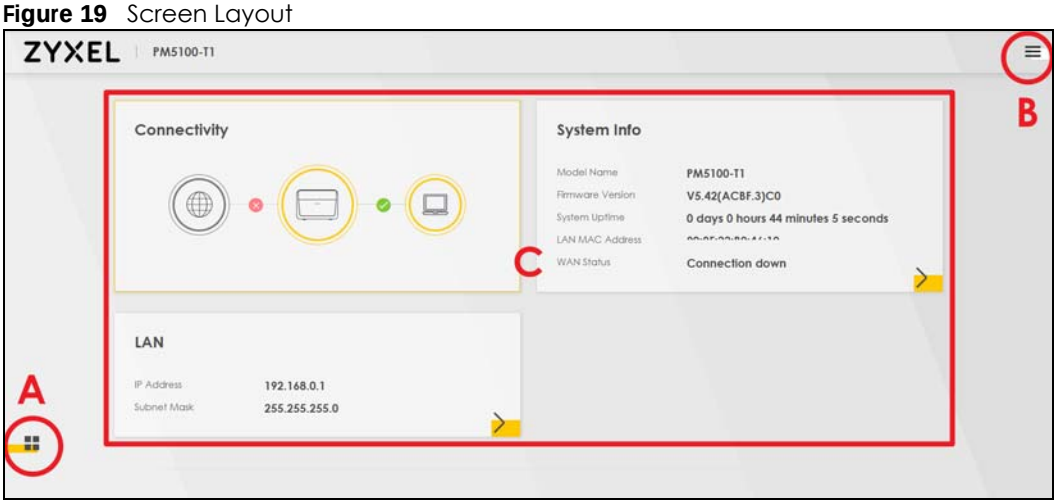
7 The **Connection Status** screen displays (see Chapter 4 on page 29 for details about it).

Figure 18 PM Device Connection Status



3.3 Web Configurator Layout

Figure 19 Screen Layout



All illustrated above, the main screen is divided into these parts:

- **A** – Settings Icon (Navigation Panel and Side bar)
- **B** – Layout Icon
- **C** – Main Window

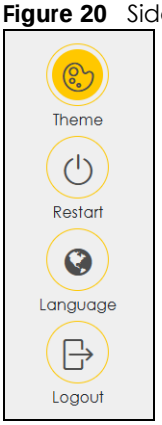
3.3.1 Setting Icon

Click the menu icon ( ) to see the side bar a navigation panel. Click **X** to close the side bar and navigation panel

3.3.1.1 Side Bar

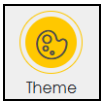
The side bar provides some icons on the right hand side.

Figure 20 Side Bar



The icons provide the following functions.

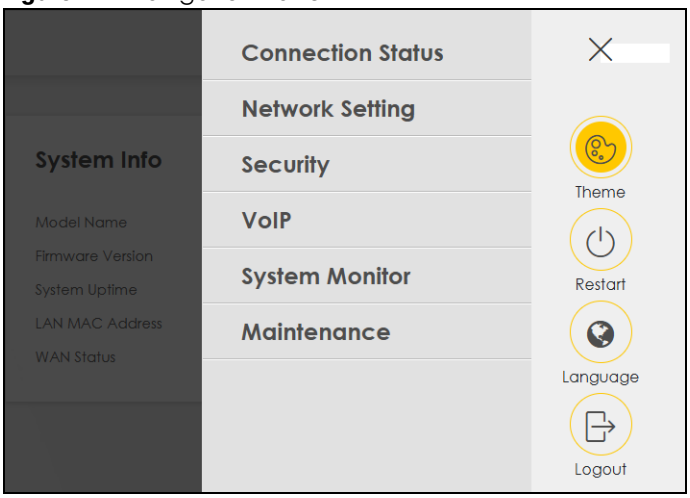
Table 8 Navigation Panel Quick Link Icons

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

3.3.1.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure PM Device features. The following tables describe each menu item.

Figure 21 Navigation Panel



The following tables describe each menu item.

Table 9 Navigation Panel Menus Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the PM Device and connected devices.
Networking Setting		

Table 9 Navigation Panel Menus Summary (continued)

LINK	TAB	FUNCTION
Broadband	Broadband	Use this screen to view the PM Device's WAN connections.
Home Networking	LAN IP Setup	Use this screen to configure LAN settings.
Security		
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.
VoIP		
SIP	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the PM Device.
	SIP Service Provider	Use this screen to configure the SIP server information, and other SIP settings, such as QoS for VoIP calls, outbound proxy, DTMF mode and SIP timers.
	SIP TLS Common	Use this screen to change the default TLS local port if you need to, and select a local certificate for the SIP server to verify the PM Device.
Phone	Phone Device	Use this screen to control which SIP accounts each phone uses to handle outgoing and incoming calls.
	Region	Use this screen to select your location and call service mode.
Call Rule	Call Rule	Use this screen to configure speed dial for SIP phone numbers that you often call.
Call History	Call History	Use this screen to view detailed information for each outgoing call you made or each incoming call from someone calling you. You can also view a summary list of received, dialed and missed calls.
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.
VoIP Status	VoIP Status	Use this screen to view VoIP registration, current call status and phone numbers for the phone ports.
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 Settings	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.

Table 9 Navigation Panel Menus Summary (continued)

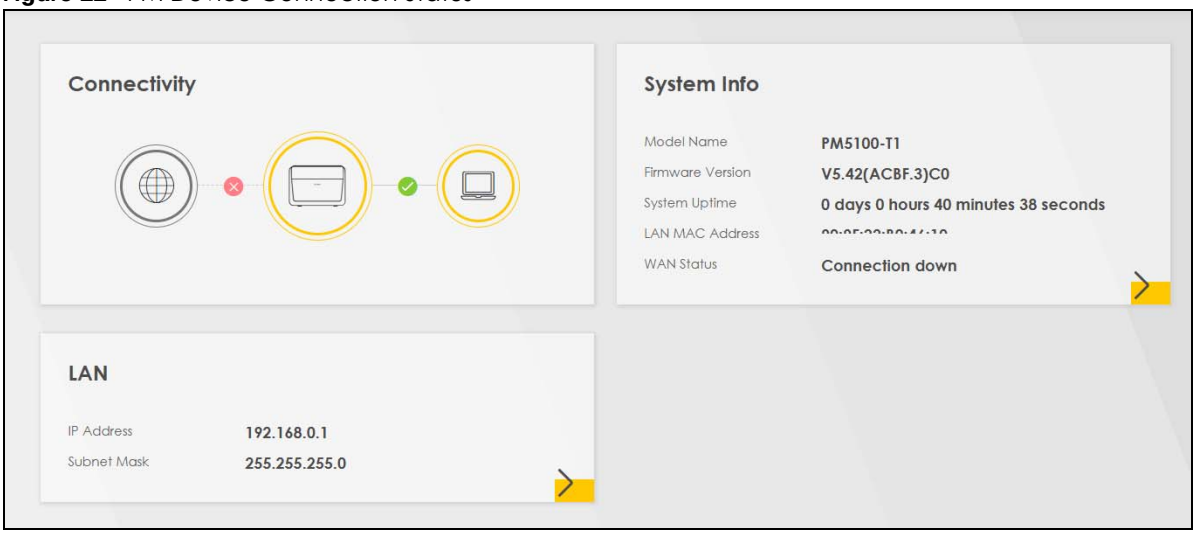
LINK	TAB	FUNCTION
Backup/Restore	Backup/Restore	Use this screen to backup and restore your PM Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the PM Device without turning the power off.
Diagnostic	Diagnostic	Use this screen to identify problems with the PON connection. Use ping and traceroute to test whether the PM Device can reach a particular host.

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.

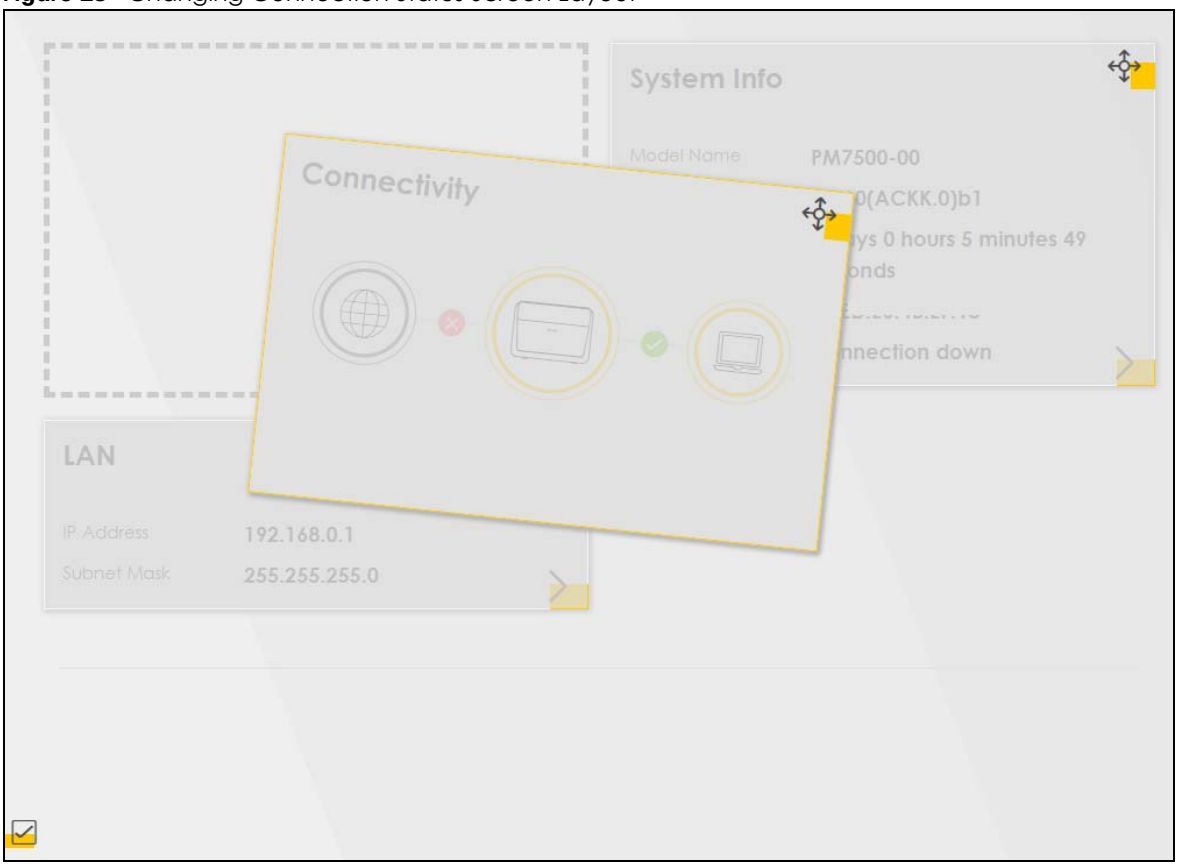
Figure 22 PM Device Connection Status



4.1.1 Layout Icon

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

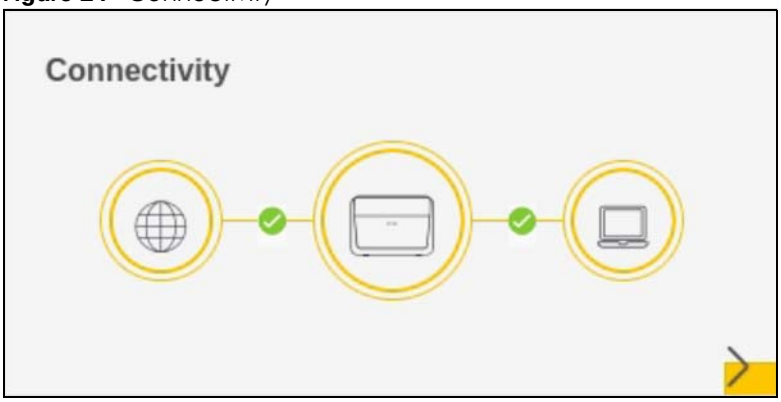
Figure 23 Changing Connection Status Screen Layout



4.2 Connectivity Panel

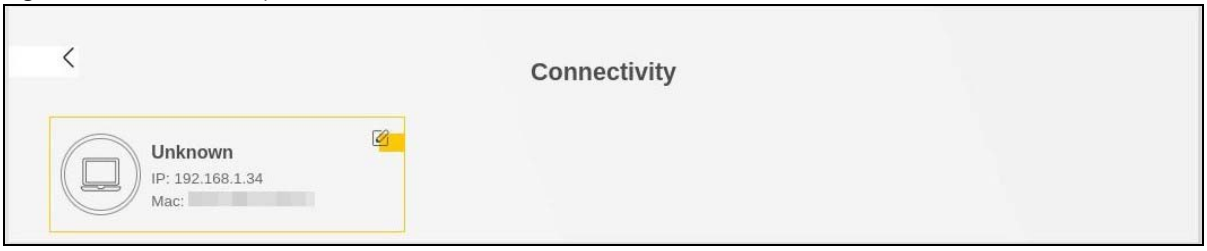
The **Connectivity** panel displays the status of the PM Device's network connections.

Figure 24 Connectivity



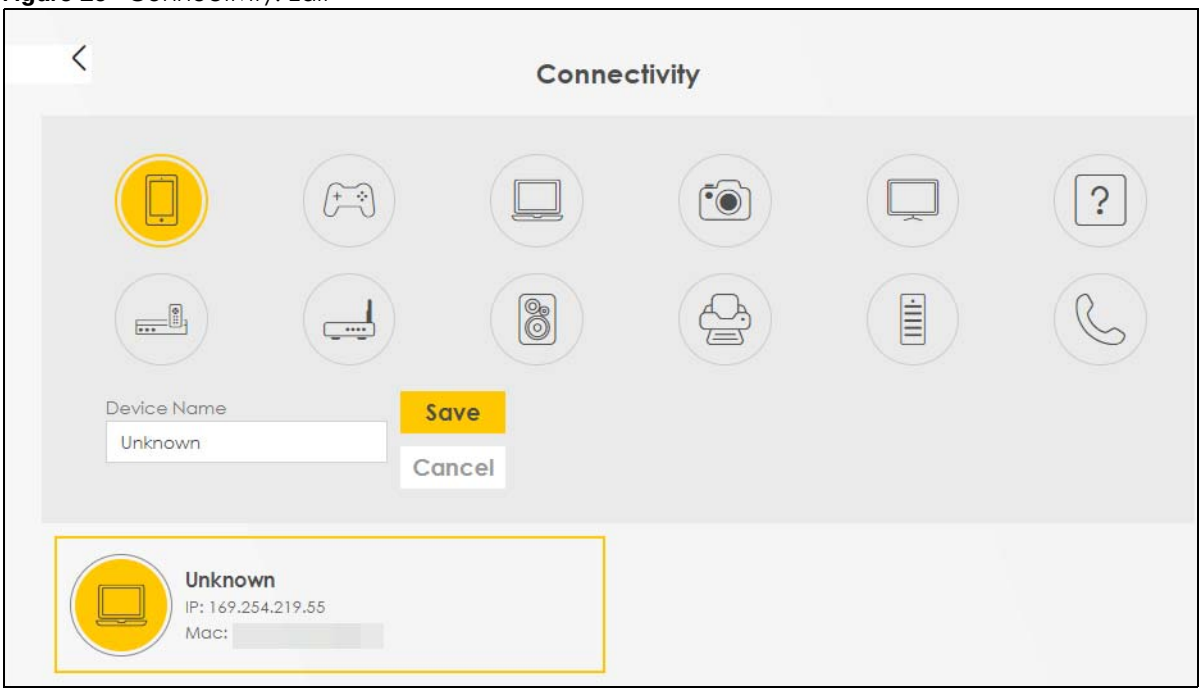
Click the **Arrow** icon ( ) to open the following screen. Use this screen to view the IP addresses and MAC addresses of the devices connected to the PM Device.

Figure 25 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 26 Connectivity: Edit



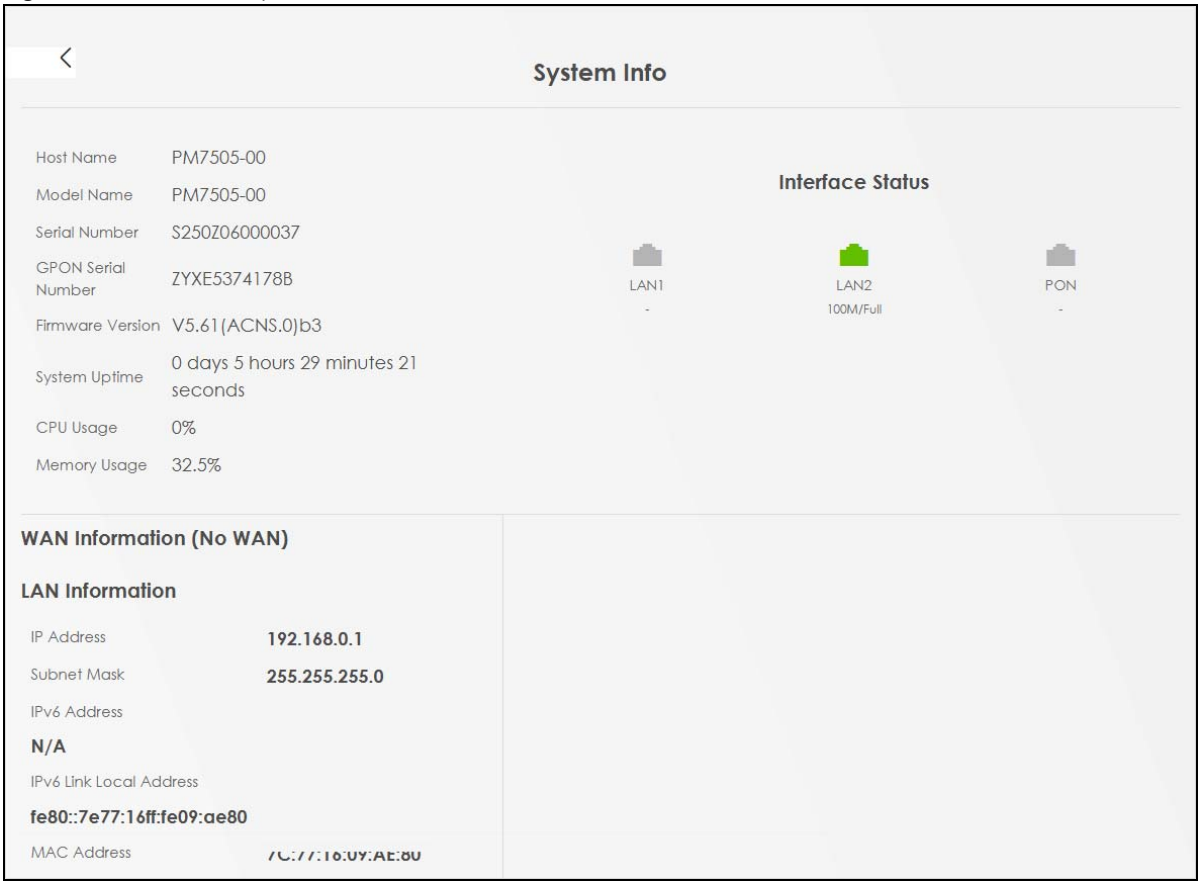
4.3 System Info Panel

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

Figure 27 System Info

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

Figure 28 Details for System Information



The following table describes the labels in this screen.

Table 10 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.

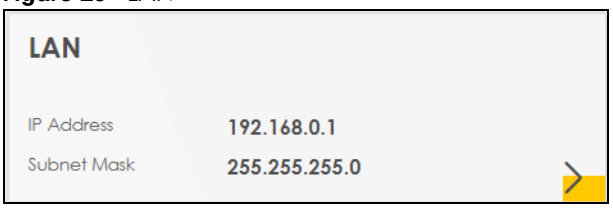
Table 10 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
GPON Serial Number	This field displays the unique identifier assigned to an ONU (Optical Network Unit) by the manufacturer. It is used for authentication and provisioning in a GPON network.
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.
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.
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 LAN. Otherwise, it shows **N/A**.
IPv6 Link Local Address	This field displays the current link-local address of the PM Device for the LAN interface. A link-local address is a special type of the IP address that is only valid for communication within the local network segment or broadcast domain of the device. Typically, link-local addresses are used for automatic address configuration and neighbor discovery protocols.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of the LAN interface.

4.4 LAN Panel

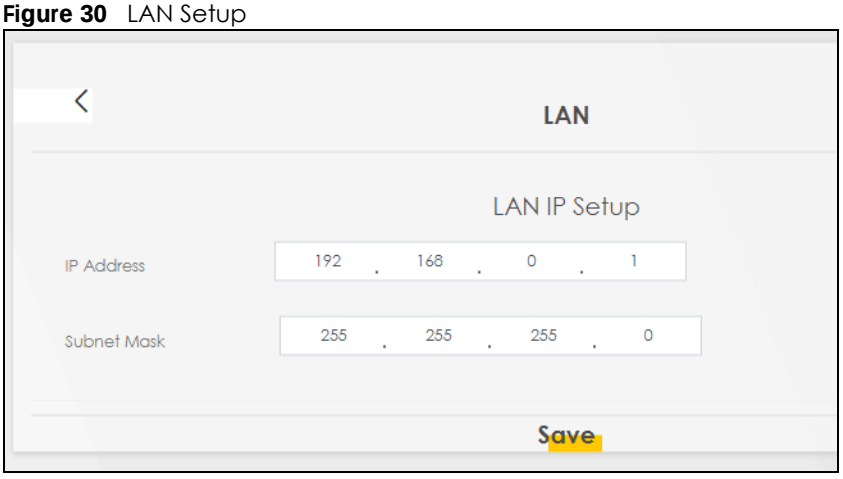
The **LAN** panel displays the PM Device's LAN IP address and subnet mask.

Figure 29 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 30 LAN Setup



The following table describes the labels in this screen.

Table 11 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	Enter 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
Web Tutorials

5.1 Overview

This chapter shows you how you use the PM Device various features.

- How to Change an Interface IP
- How to Rename Your Device
- How to Change the Admin Password
- How to View the Interface Status
- How to View the WAN Station Status
- How to View the LAN Station Status
- How to Upgrade the Firmware
- How to Back Up the Device Configuration
- How to Restore the Device Configuration
- How to Reset the PM Device to the Factory Defaults
- How to View Logs

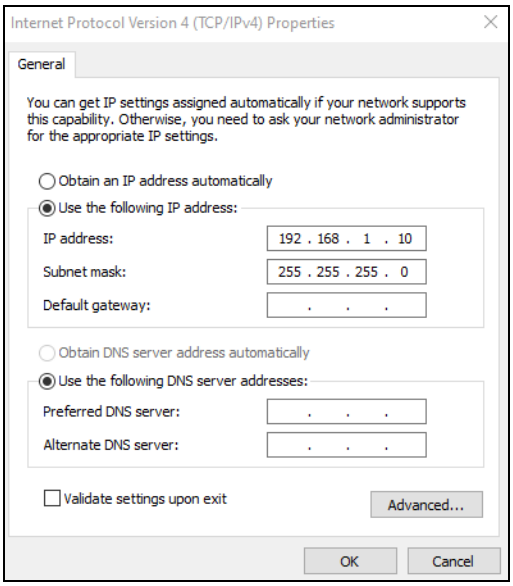
5.2 Device Settings

This section shows you how to change an interface IP, rename your device, and change the admin password.

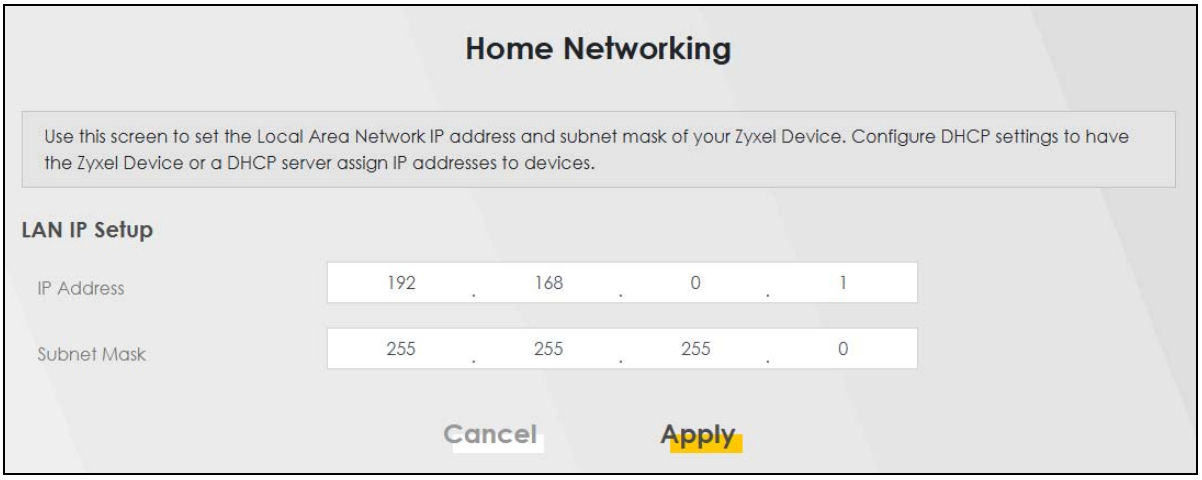
5.2.1 How to Change an Interface IP

Duplicated IP addresses in the network environment may cause failure to connect to the PM Device. To change the interface IP of your PM Device, please follow the steps below:

1 Change your computer's IP address to the same subnet mask as the PM Device. For example, if the default static IP address of the PM Device is 192.168.0.1. Set your computer IP address between 192.168.0.2 and 192.168.0.254.



2 Log into the PM Device using the default IP address "192.168.0.1". Go to **Network Setting** > **Home Networking**. Enter your preferred IPv4 address in the **IP Address** field. For instance, "192.168.0.15". Click Apply and the Web Configurator will be disconnected due to the IP address change.

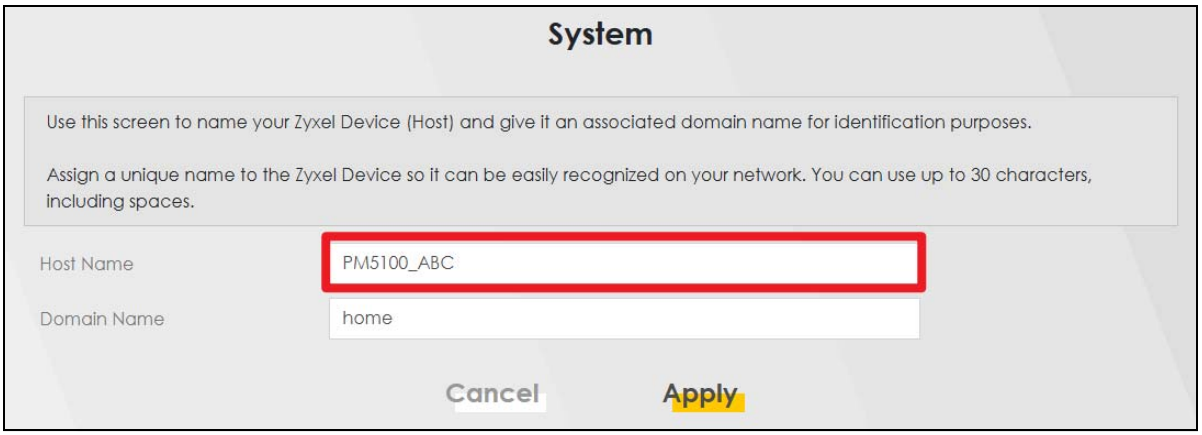


3 Enter the new IP address "192.168.0.15" in the address bar to see if you can access the PM Device's Web Configurator.

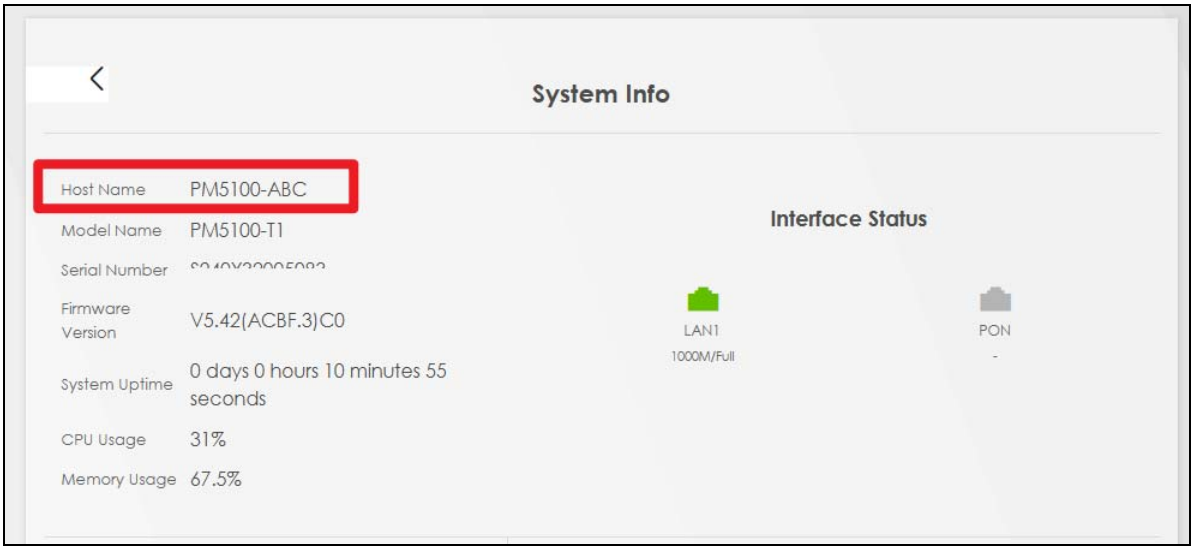
5.2.2 How to Rename Your Device

Duplicated device names may confuse network administrators. To change the host name, please follow the steps below:

1 Go to the **Maintenance** > **System** screen. Enter a new host name. Click **Apply** to save the new host name.



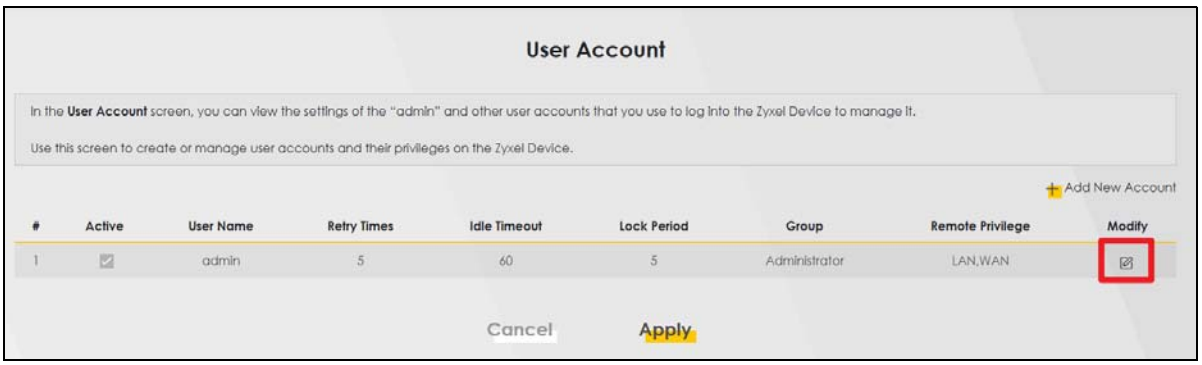
2 Go to the **Connection Status** > **System Info**. Check if the new host name has been applied successfully.



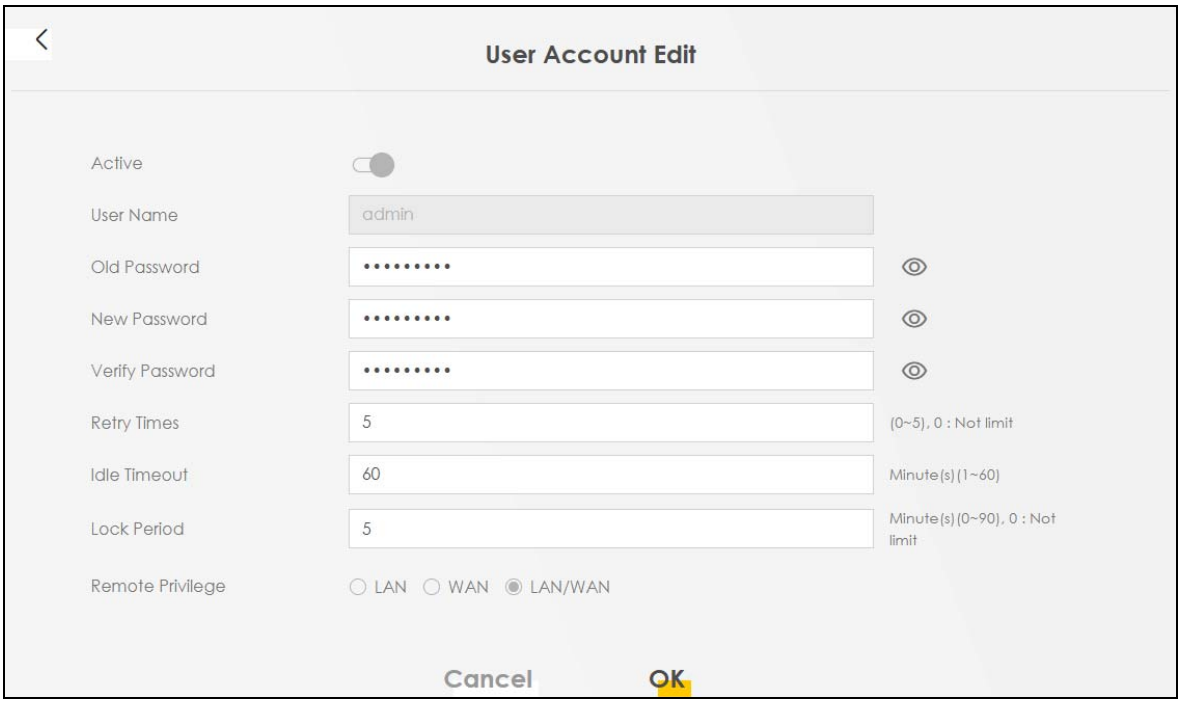
5.2.3 How to Change the Admin Password

Change the Web Configurator login password regularly to secure your account. To change the admin password, follow the steps below:

1 Go to the **Maintenance** > **User Account** screen. Click the **Edit** icon.



2 The **User Account** Edit screen appears. Enter your old and new passwords in the corresponding field. Click **OK**.

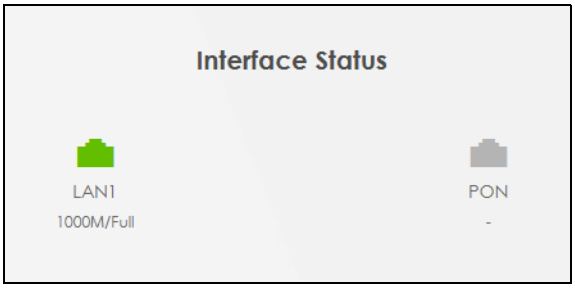


5.3 Traffic Usage

A low transmission rate or packet loss may impact network performance and reliability. Check the transmission rate and packet statistics to see if there are any connectivity issues.

5.3.1 How to View the Interface Status

Go to **Connection Status** > **System Info**. You can view the transmission rate on the PM Device's connections and transmission rate from **Interface Status**.

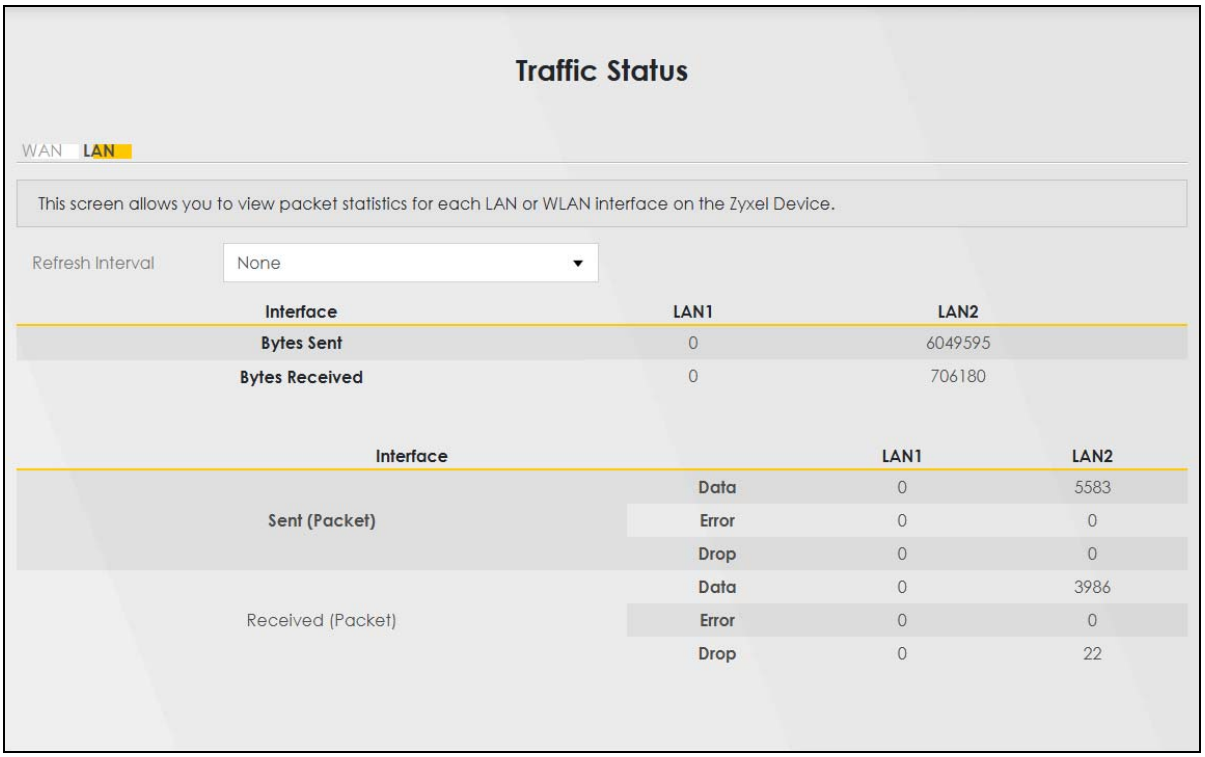


5.3.2 How to View the WAN Station Status

Go to **System Monitor** > **Traffic Status** > **WAN**. Check the total numbers of bytes sent and received through the PM Device WAN interfaces and each WAN interface's packet statistics.

5.3.3 How to View the LAN Station Status

Go to System **Monitor** > **Traffic Status** > **LAN**. Check the total numbers of bytes sent and received through the PM Device LAN interface the interface's packet statistics.



5.4 Device Maintenance

This section shows you how to upgrade the PM Device firmware, back up the configuration and restore the PM Device to its previous or default settings.

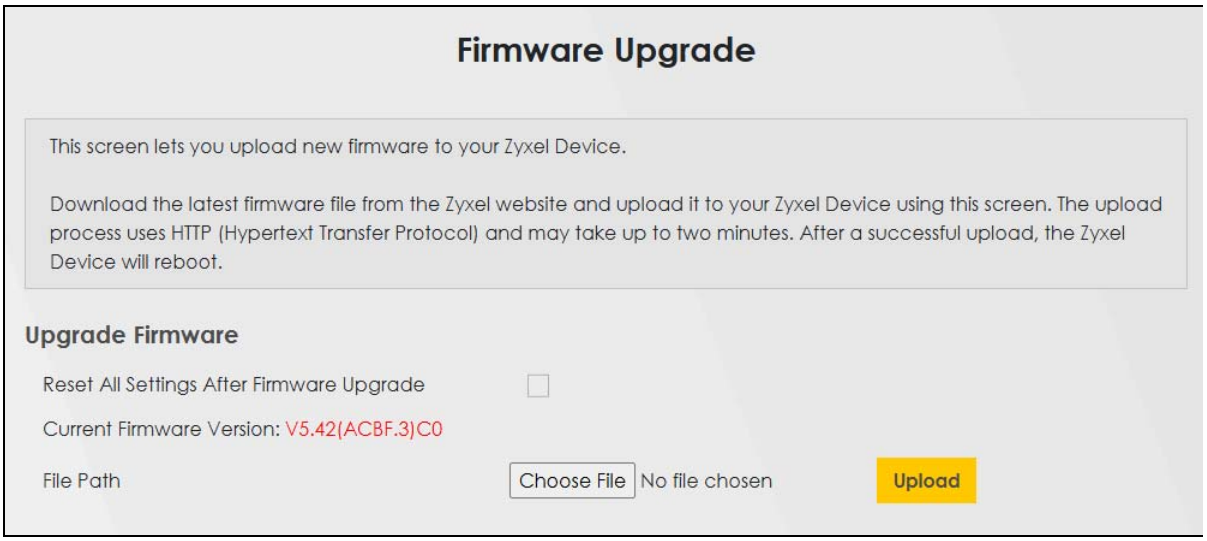
5.4.1 How to Upgrade the Firmware

Upload the router firmware to the PM Device for feature enhancements.

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

2 Go to the **Maintenance** > **Firmware Upgrade** screen.

3 Click **Choose File** and select the file with a ".bin" extension to upload. Click **Upload**.



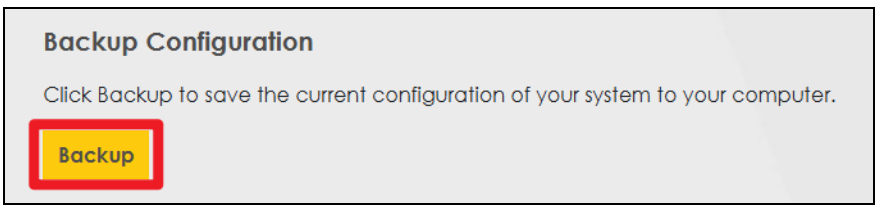
4 This process may take up to 2 minutes to finish. After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

5.4.2 How to Back Up the Device Configuration

Back up a configuration file allows you to return to your previous settings.

1 Go to the **Maintenance** > **Backup/Restore** screen.

2 Click **Backup** in the **Backup Configuration** section, and a configuration file will be saved to your computer.

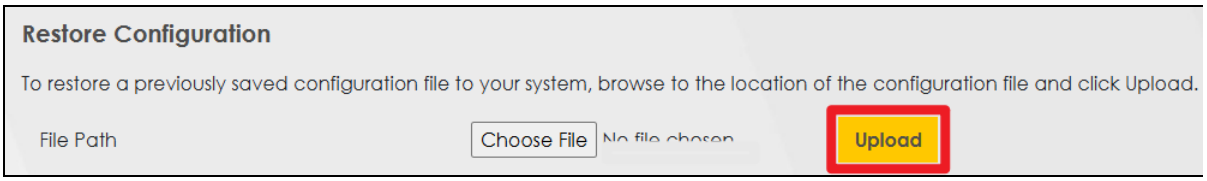


5.4.3 How to Restore the Device Configuration

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

1 Go to the **Maintenance** > **Backup/Restore** screen.

2 Click **Choose File** in **Restore Configuration** section, and select the configuration file that you want to upload. Click **Upload**.

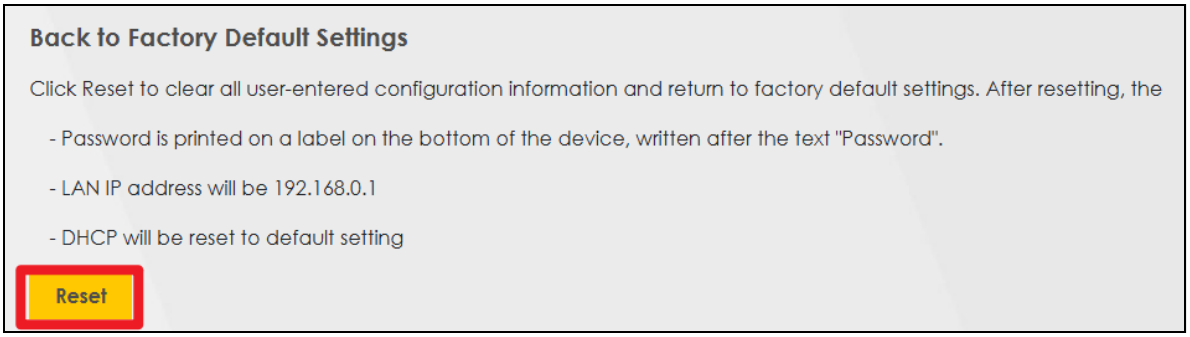


3 The PM Device will restart automatically after the configuration file is successfully uploaded. Wait for one minute before logging into the PM Device again.

5.4.4 How to Reset the PM Device to the Factory Defaults

To reset the PM Device, you can press the **RESET** button on the rear panel for more than 5 seconds. Alternatively, you can use the web configurator to reset the PM Device.

Go to **Maintenance** > **Backup/Restore** and click the **Reset**. The PM Device will reset to factory defaults and the LAN IP address will be set to the default IP address.

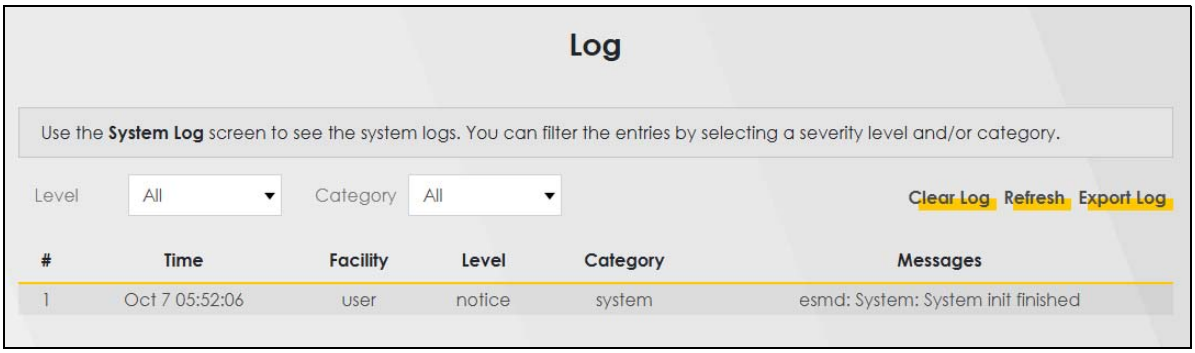


5.5 System Log

5.5.1 How to View Logs

To view the system log of the PM Device, go to **System Monitor** > **Log**.

Select the **Level** to filter the log by severity. Select the **Category** to filter the log by different features. If you want to download the Log file on your local computer, click **Export Log** to download the PM Device's system log to your local computer.


Log
Use the System Log screen to see the system logs. You can filter the entries by selecting a severity level and/or category.
Level
All
Category
All
Clear Log
Refresh
Export Log
Time Facility Level Category Messages
1 Oct 7 05:52:06 user notice system esmd: System: System init finished

PART II
Technical Reference

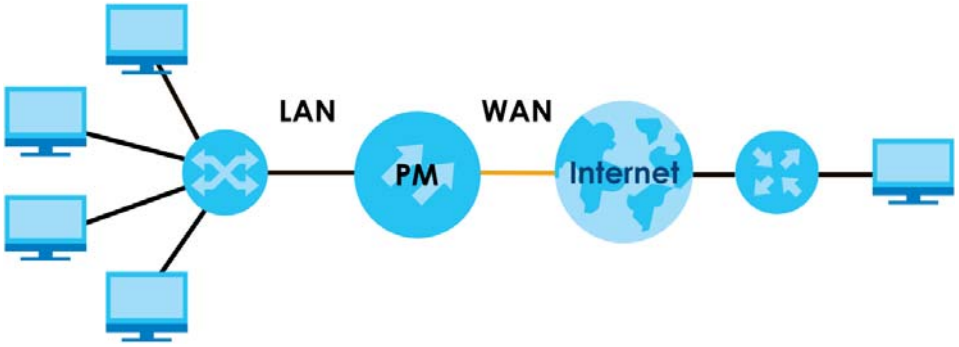
CHAPTER 6
Broadband

6.1 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 31 LAN and WAN



6.1.1 What You Can Do in this Chapter

Use Broadband screens to view, remove or add a WAN interface. You can also configure the WAN settings on the PM Device for Internet access.

Table 12 WAN Setup Overview

INTERNET CONNECTION		
MODE	**ENCAPSULATION**	**CONNECTION SETTINGS**
Routing	IPoE	VLAN, MTU, WAN IP address, DNS Server, Routing Feature, DHCP Option
	PPPoE	PPP Information, VLAN, MTU, WAN IP address, DNS Server, Routing Feature, DHCP Option
Bridge	N/A	VLAN and MTU

6.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter. For more details on IPv6, see Appendix B on page 142.

WAN IP Address

The WAN IP address is an IP address for the PM Device, which makes it accessible from an outside network. It is used by the PM Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the PM Device tries to access the Internet.

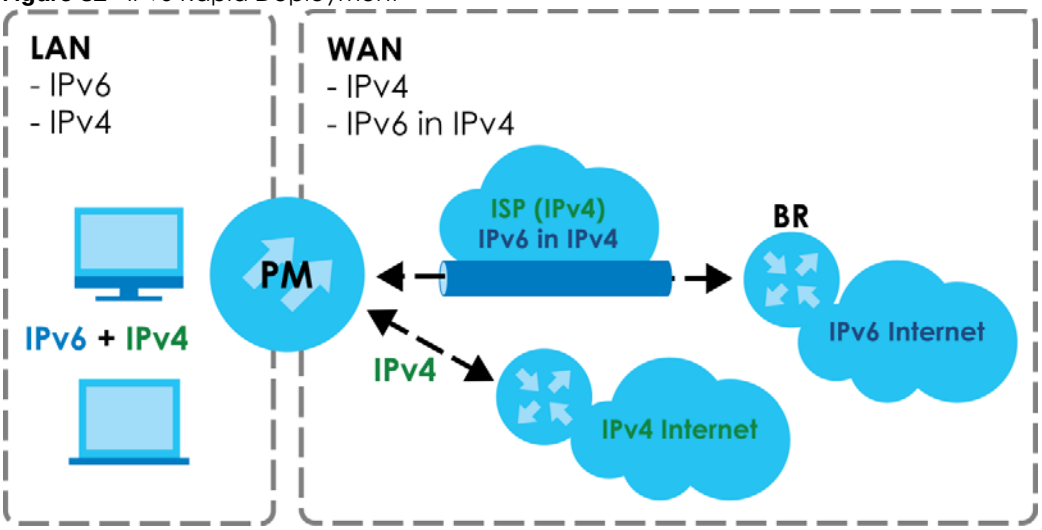
If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP addresses.

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6RD) when the local network uses IPv6 and the ISP has an IPv4 network. When the PM Device has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6RD to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The PM Device generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (**BR** in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The PM Device uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 32 IPv6 Rapid Deployment

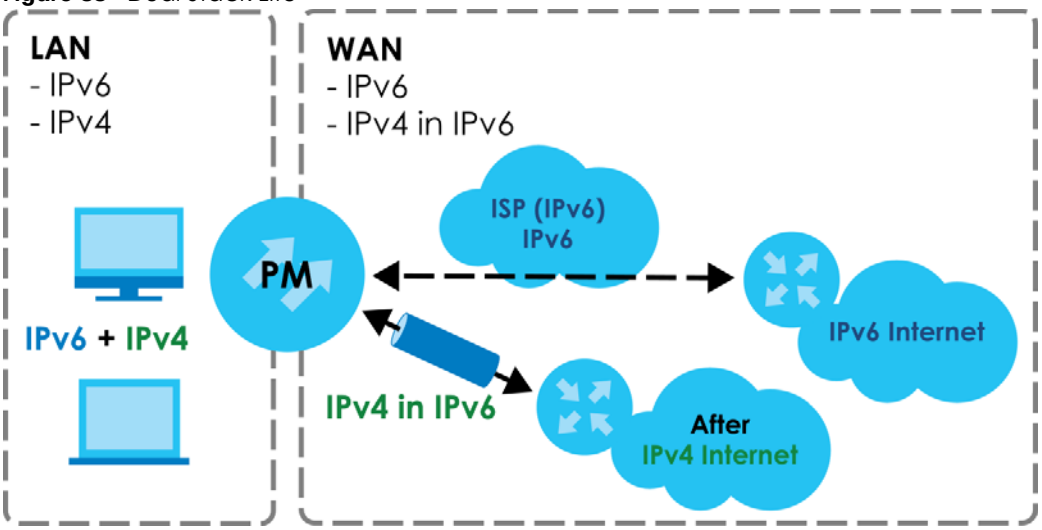


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the PM Device has an IPv6 WAN address and you set **IPv6/IPv4 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The PM Device tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP's Address Family Transition Router (**After** in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The PM Device uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 33 Dual Stack Lite



Carrier-Grade NAT (CGNAT)

CGNAT allows an Internet Service Provider (ISP) to use a single public WAN IP address for multiple customers with different Internet access devices.

6.1.3 Before You Begin

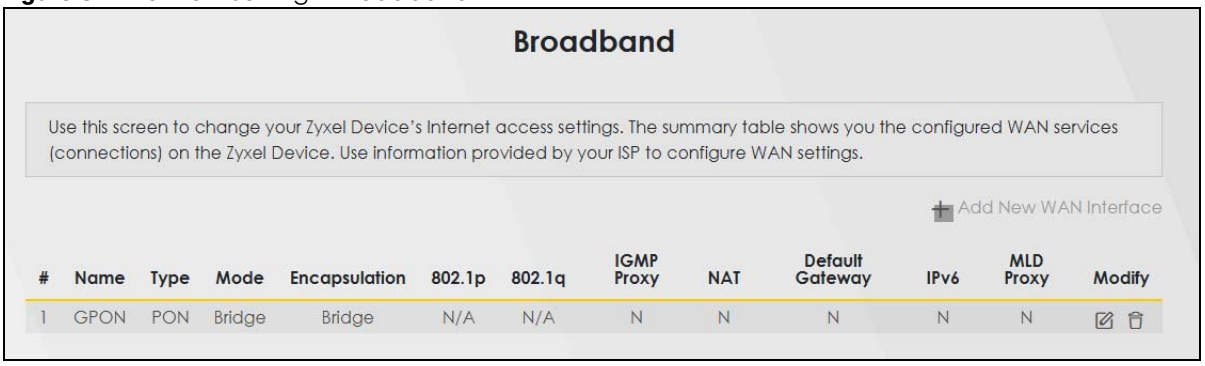
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

6.2 Broadband

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

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

Figure 34 Network Setting > Broadband



The following table describes the labels in this screen.

Table 13 Network Setting > Broadband

LABEL	DESCRIPTION
#	This is the index number of the entry.
Name	This is the service name of the connection.
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.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

6.2.1 Add or Edit Internet Connection

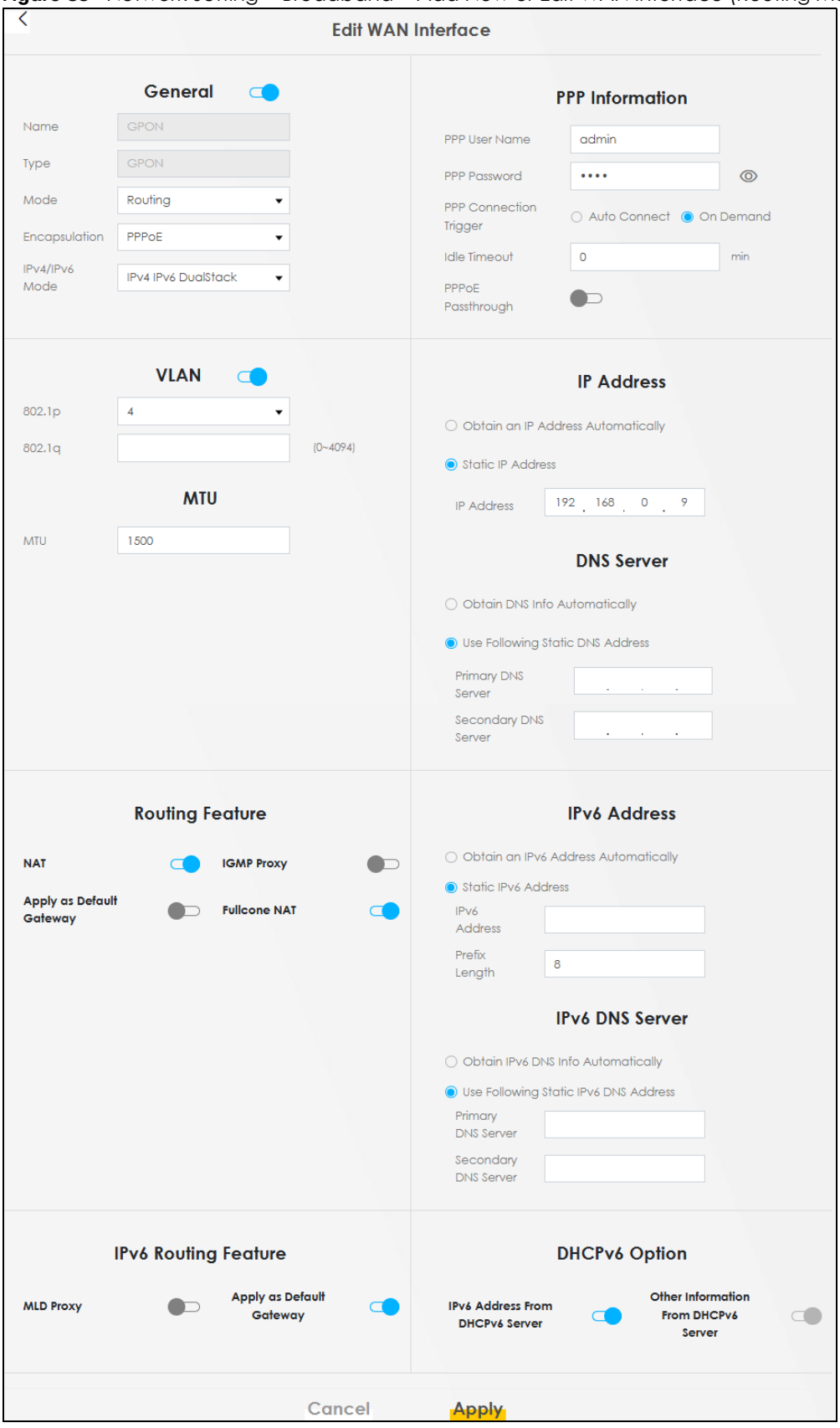
Click **Add New WAN Interface** in the Broadband screen or the **Edit** icon next to an existing WAN interface to open the following screen. Use this screen to configure a WAN connection. The screen varies depending on the mode, encapsulation, and IPv6 or IPv4 mode you select.

Routing Mode

Use **Routing** mode if your ISP give you one IP address only and you want multiple computers to share an Internet account.

The following example screen displays when you select the **Routing** mode and **PPPoE** encapsulation. The screen varies when you select other **Encapsulation** and **IPv6/IPv4 Mode**

Figure 35 Network Setting > Broadband > Add New or Edit WAN Interface (Routing Mode)



The following table describes the labels in this screen.

Table 14 Network Setting > Broadband > Add New or Edit WAN Interface (Routing Mode)

LABEL	DESCRIPTION
General Click the switch to enable this WAN interface.	
Name	Specify a descriptive name for this connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. This field is read-only if you are editing the WAN interface.
Type	This field shows the types of available connections. This field is read-only if you are editing the WAN interface.
Mode	Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. The choices are **PPPoE** and **IPoE.**
IPv4/IPv6 Mode	Select **IPv4 Only** if you want the PM Device to run IPv4 only. Select **IPv4 IPv6 DualStack** to allow the PM Device to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the PM Device to run IPv6 only.
PPP Information (This is available only when you select **Routing** in the **Mode** field and **PPPoE** in the **Encapsulation** field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Click the eye icon to enable password unmask to show your entered password in plain text.
PPP Connection Trigger	Select when to have the PM Device establish the PPP connection. **Auto Connect** – select this to not let the connection time out. **On Demand** – select this to automatically bring up the connection when the PM Device receives packets destined for the Internet.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not available if you select **Auto Connect in the PPP Connection Trigger field**.
PPPoE Passthrough	In addition to the PM Device's built-in PPPoE client, you can enable PPPoE Passthrough to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP through the PM Device. Each host can have a separate account and a public WAN IP address. PPPoE Passthrough is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE Passthrough if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
VLAN Click this switch to enable VLAN on this WAN interface.	
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Enter the VLAN ID number (from 0 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.

Table 14 Network Setting > Broadband > Add New or Edit WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
IP Address (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed. the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP. This is available only when you set the **Encapsulation** to **IPoE**.
Gateway IP Address	Enter the gateway IP address provided by your ISP. This is available only when you set the **Encapsulation** to **IPoE**.
DNS Server (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Obtain DNS Info Automatically	Select **Obtain DNS Info Automatically** if you want the PM Device to use the DNS server addresses assigned by your ISP.
Use Following Static DNS Address	Select **Use Following Static DNS Address** if you want the PM Device to use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Routing Feature (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
NAT	Click this switch to activate NAT on this connection.
IGMP Proxy	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group – it is not used to carry user data. Click this switch to have the PM Device act as an IGMP proxy on this connection. This allows the PM Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Click this switch to have the PM Device use this WAN interface of this connection as the system default gateway.
Fullcone NAT	Click this switch to enable full cone NAT on this WAN connection. This field is available only when you activate **NAT**. In full cone NAT, the PM Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The PM Device also maps packets coming to that external IP address and port to the internal IP address and port.
6RD The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 45 for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.	
Automatically configured by DHCPC	The **Automatically configured by DHCPC** option is configurable only when you set the method of encapsulation to **IPoE**.
Manually Configured	Select **Manually Configured** if you have the IPv4 address of the relay server. Otherwise, select **Automatically configured by DHCPC** to have the PM Device detect it automatically through DHCP.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.

Table 14 Network Setting > Broadband > Add New or Edit WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
IPv4 Mask Length	Enter the subnet mask number (1 – 32) for the IPv4 network.
Border Relay IPv4 Address	When you select **Manually Configured**, specify the relay server's IPv4 address in this field.
DHCPC Options (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field and **IPoE** in the **Encapsulation** field.) Note: The available DHCP options may differ by model.	
Request Options	Select **Option 42** to have the PM Device get NTP time server information from DHCP packets sent from the DHCP server. Select **Option 43** to have the PM Device get vendor specific information from DHCP packets sent from the DHCP server. Select **Option 120** to have the PM Device get static route information from DHCP packets sent from the DHCP server. Select **Option 121** to have the PM Device get SIP server information from DHCP packets sent from the DHCP server.
Sent Options	
option 12	To identify the PM Device to the DHCP server, select this to automatically add the hostname of the PM Device in the DHCP discovery packets that go to the DHCP server.
option 60	Select this and enter the device identity you want the PM Device to add in the DHCP discovery packets that go to the DHCP server.
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.
option 61	Select this and enter any string that identifies the device.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID	Enter the hardware type, a time value and the MAC address of the device.
option 125	Select this to have the PM Device automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
IPv6 Address (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.)	
Obtain an IPv6 Address Automatically	Select **Obtain an IPv6 Address Automatically** if you want to have the PM Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select **Static IPv6 Address** if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your PM Device's interfaces. The gateway helps forward packets to their destinations. This is available only when you set the **Encapsulation** to **IPoE**.
IPv6 DNS Server (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. Configure the IPv6 DNS server in the following section.)	
Obtain IPv6 DNS Info Automatically	Select **Obtain IPv6 DNS Info Automatically** to have the PM Device get the IPv6 DNS server addresses from the ISP automatically.

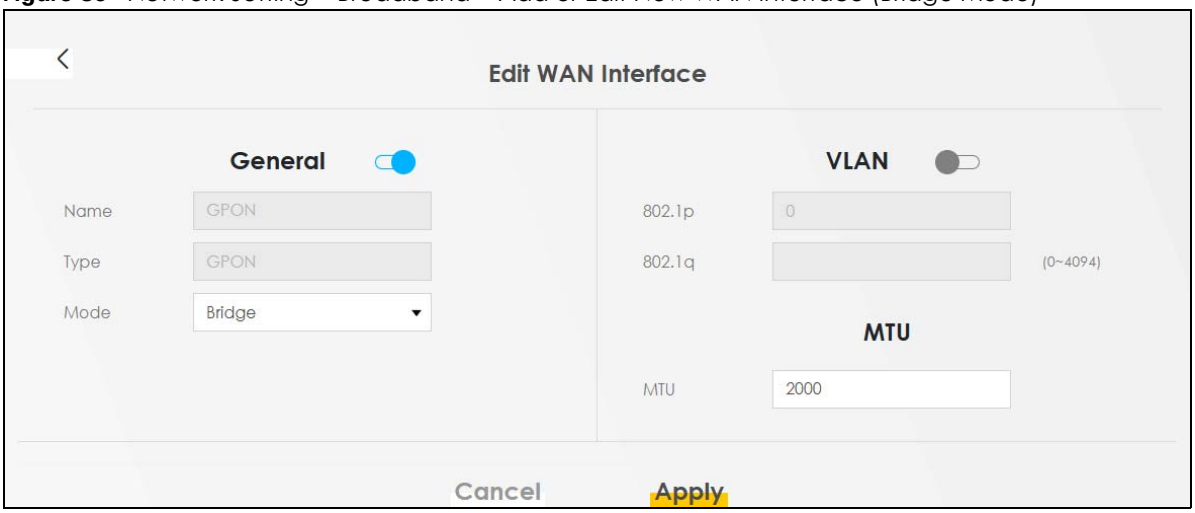
Table 14 Network Setting > Broadband > Add New or Edit WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Use Following Static IPv6 DNS Address	Select **Use Following Static IPv6 DNS Address** to have the PM Device use the IPv6 DNS server addresses you configure manually.
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
IPv6 Routing Feature (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. You can enable IPv6 routing features in the following section.)	
MLD Proxy Enable	Select this checkbox to have the PM Device act as an MLD proxy on this connection. This allows the PM Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the PM Device use the WAN interface of this connection as the system default gateway.
DS-Lite	This is available only when you select **IPv6 Only** in the **IPv4/IPv6 Mode** field. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 45 for more information. Click this switch to enable DS-Lite to let local computers use IPv4 through an ISP's IPv6 network.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
DHCPv6 Option (This is available only when you select **IPv6 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
IPv6 Address From DHCPv6 Server	Click the switch to let the PM Device send DHCP requests to the DHCPv6 server to obtain an IPv6 address.
Other Information From DHCPv6 Server	Click the switch to have the PM Device get other information, such as DNS information, from DHCPv6 packets sent from the DHCPv6 server. This will be enabled if **IPv6 Address From DHCPv6 Server** is enabled.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. The following example screen displays when you select **Bridge** mode.

Figure 36 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)



The following table describes the labels in this screen.

Table 15 Network Setting > Broadband

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Name	**Enter a service name of the connection.** **This field is read-only is you are editing the WAN interface.**
Type	This field shows the connection type. This field is read-only is you are editing the WAN interface.
Mode	Select **Bridge** if your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as DHCP server and NAT on traffic from the selected LAN ports.
VALN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right, the function is enabled. Otherwise, it is not.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Enter the VLAN ID number (from 0 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

6.3 Technical Reference

The following section contains additional technical information about the PM Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The PM Device can work in bridge mode or routing mode. When the PM Device is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, WiFi, and so on) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the PM Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the PM Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However, the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

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

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

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

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges – they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and 2 bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The PM Device can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the PM Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

CHAPTER 7
Home Networking

7.1 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.

7.1.1 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 7.2 on page 56).

7.1.2 What You Need To Know

IP Address

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

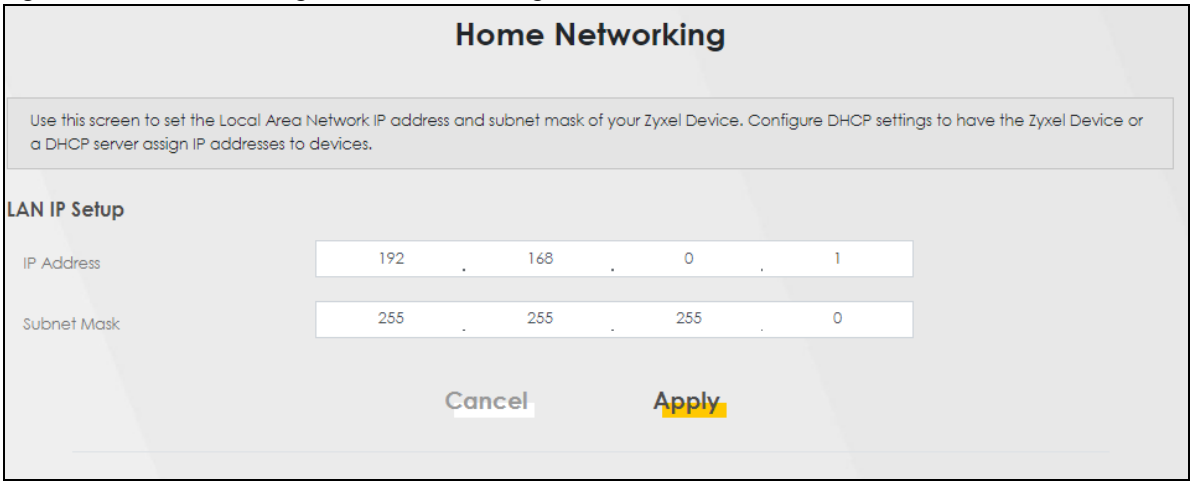
Subnet Mask

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.

7.2 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 37 Network Setting > Home Networking



The following table describes the fields on this screen.

Table 16 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	Enter 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 8
Certificates

8.1 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.

8.1.1 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 8.2 on page 58).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the PM Device (Section 8.3 on page 62).

8.1.2 What You Need to Know

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

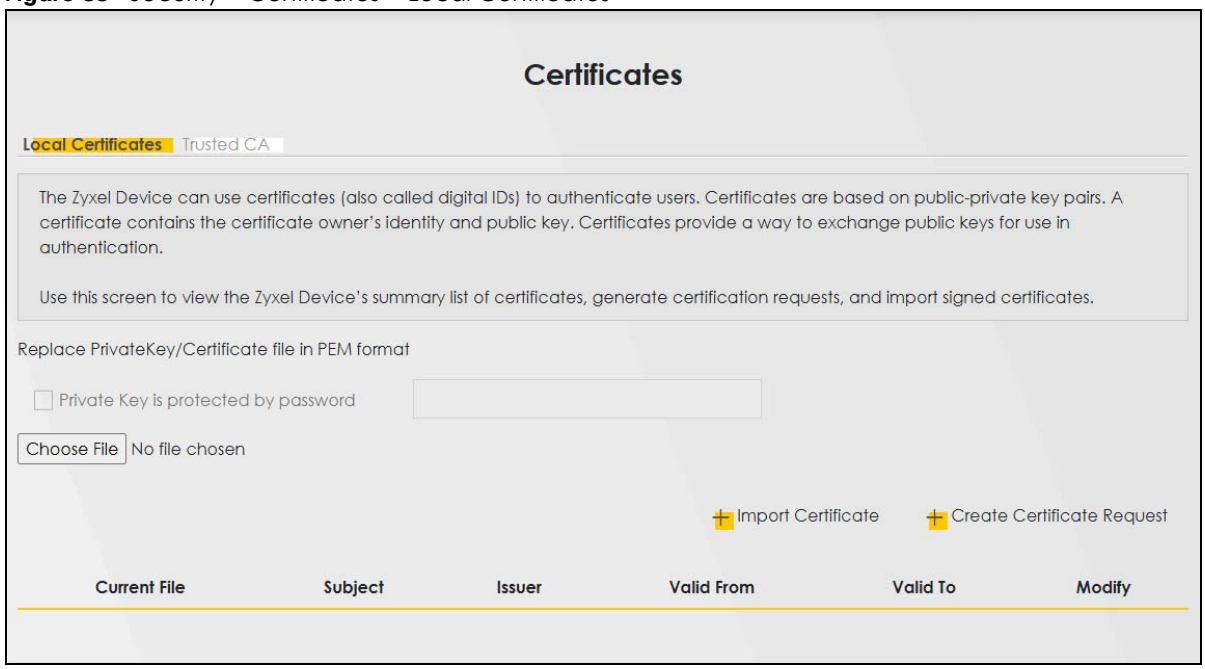
Certification Authority

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.

8.2 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 38 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

Table 17 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. You can use up to 63 alphanumeric (0-9, a-z, A-Z) and special characters, 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 information that identifies the owner of the certificate, such as Common Name (**CN**), Organization Name (**O**), State/Province Name (**ST**), and Country/Region Name (**C**). 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.

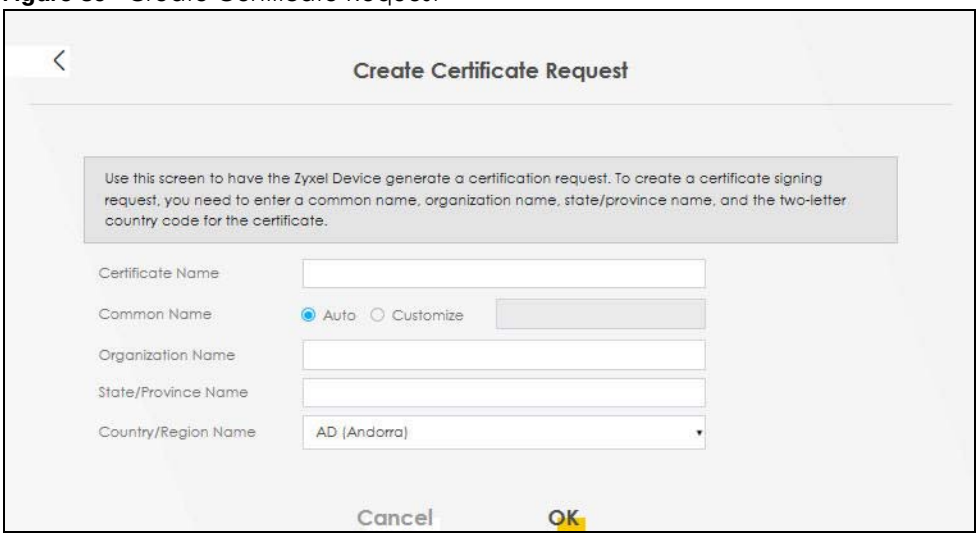
Table 17 Security > Certificates > Local Certificates (continued)

LABEL	DESCRIPTION
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.

8.2.1 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 39 Create Certificate Request



The following table describes the labels in this screen.

Table 18 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Enter a descriptive name to identify this certificate. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Common Name	Select **Auto** to have the PM Device configure this field automatically. Or select **Customize** to enter it manually. Enter the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Enter up to 32 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	Enter 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.

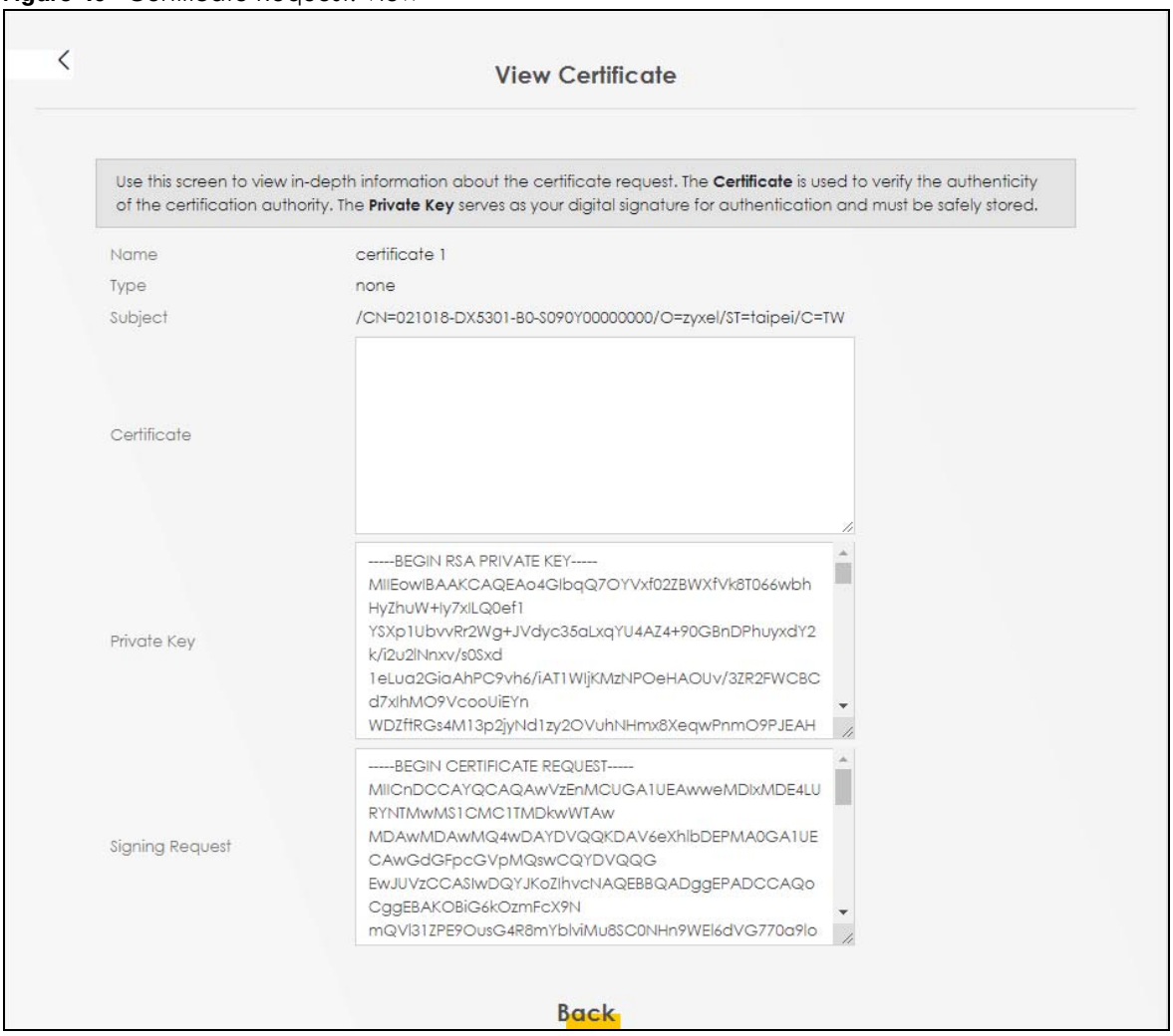
Table 18 Create Certificate Request (continued)

LABEL	DESCRIPTION
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.

8.2.2 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 40 Certificate Request: View



The following table describes the fields in this screen.

Table 19 Certificate Request: View

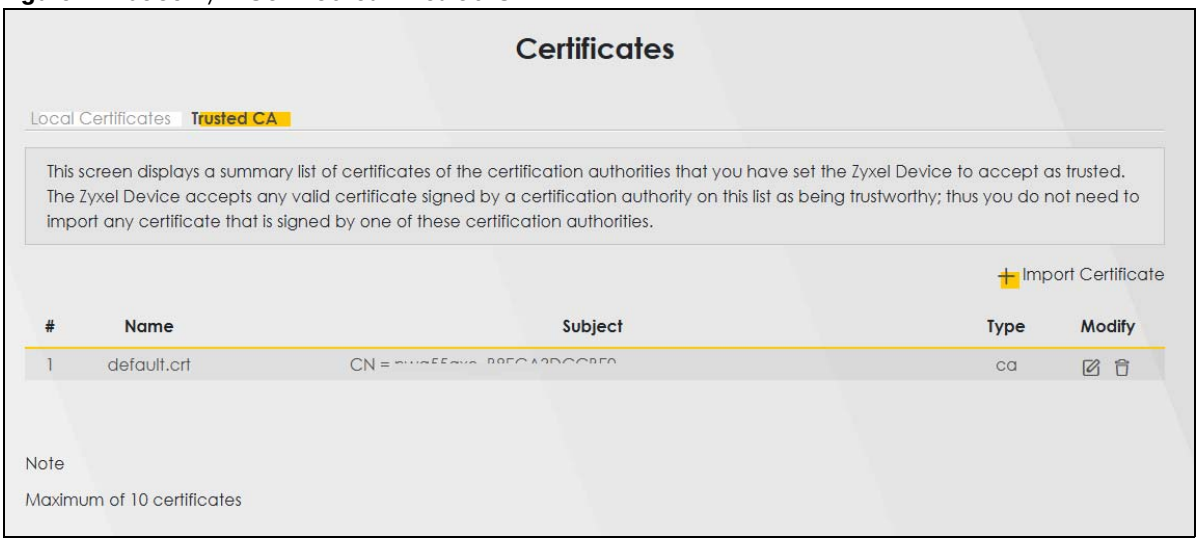
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (**CN**), Organization Name (**O**), State/Province Name (**ST**), and Country/Region Name (**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.

8.3 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 41 Security > Certificates > Trusted CA



The following table describes the fields in this screen.

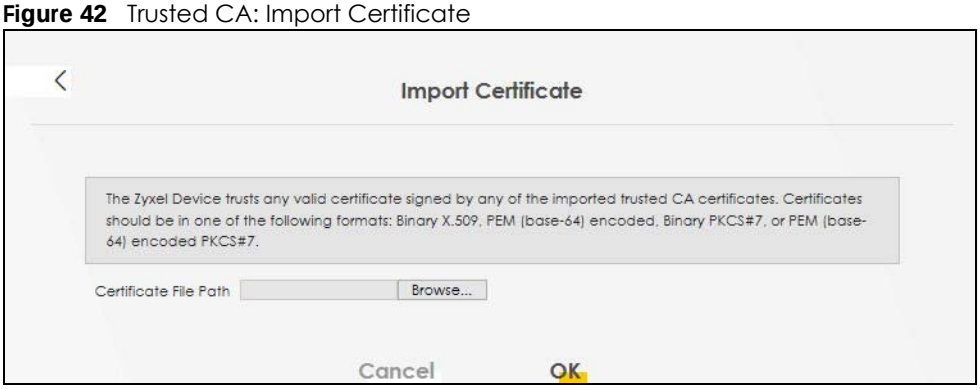
Table 20 Security > Certificates > Trusted CA

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**), Organization Name (**O**), State/Province Name (**ST**), and Country/Region Name (**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.

8.3.1 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 42 Trusted CA: Import Certificate



The following table describes the fields in this screen.

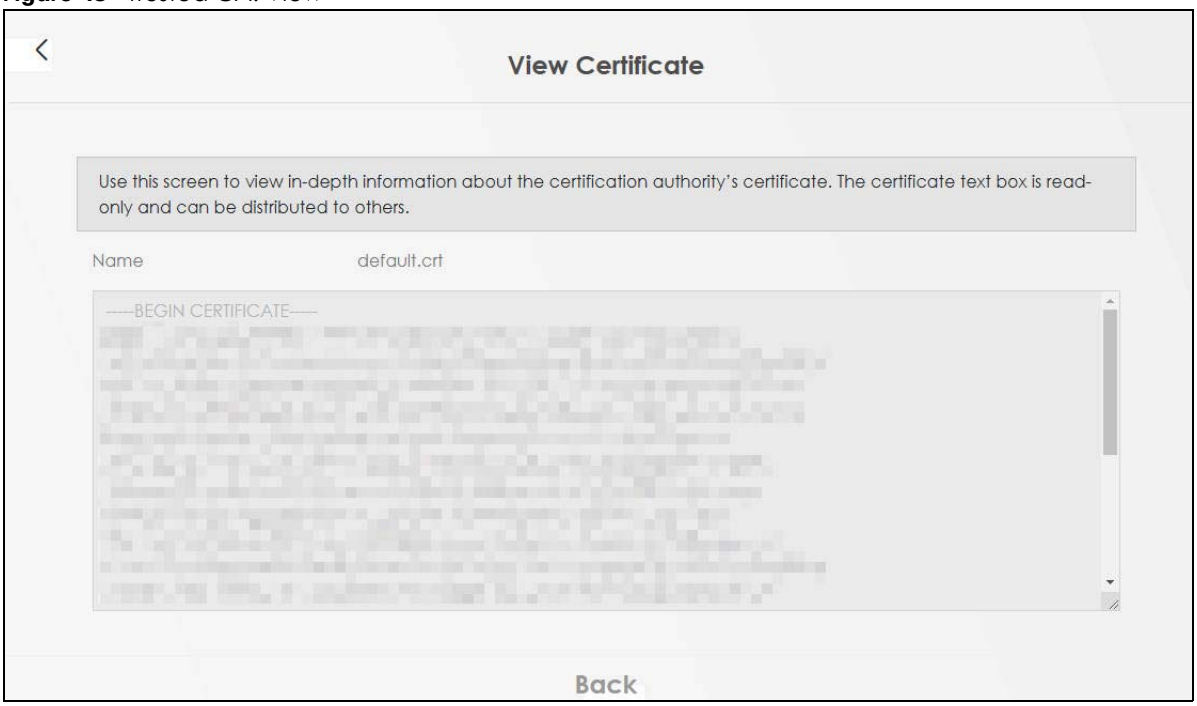
Table 21 Trusted CA: Import Certificate

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.

8.3.2 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 43 Trusted CA: View



The following table describes the fields in this screen.

Table 22 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 (through USB thumb drive for example).
Back	Click **Back** to return to the previous screen.

8.4 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

Certification Authorities

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.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The PM Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Advantages of Certificates

Certificates offer the following benefits.

- The PM Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Format

The certification authority certificate that you want to import has to be in PEM (Base-64) encoded X.509 file format. This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

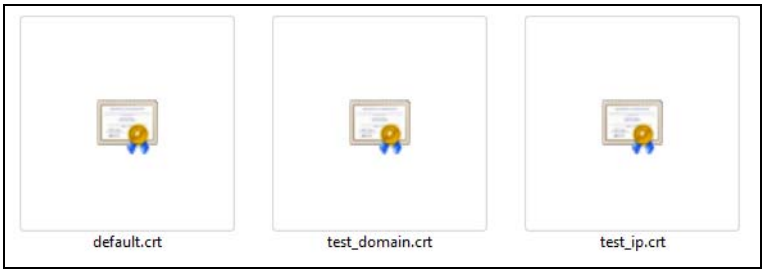
8.4.1 Verify a Certificate

Before you import a trusted CA or trusted remote host certificate into the PM Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the PM Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

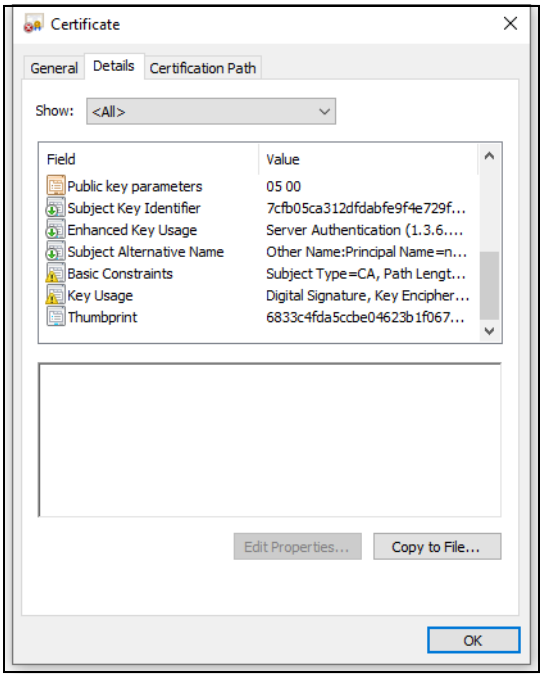
You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.



Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

CHAPTER 9
VoIP

9.1 VoIP Overview

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider.

Use this chapter to:

- Connect an analog phone to the PM Device.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

5G only supports all-IP based packet-switched telephony services. When Voice service is enabled, the PM Device supports Circuit Switched FallBack (CSFB) to deliver or receive circuit-switched voice calls and text messages through a 3G mobile network and then goes back to the 5G network to transmit data packets.

With the voice service, users do not need a SIP account and SIP server to make phone calls over the Internet.

Note: This feature is only available on certain models. For details, see the features comparison table at Table 1 on page 12.

9.1.1 What You Can Do in this Chapter

These screens allow you to configure your PM Device to make phone calls over the Internet and your regular phone line, and to set up the phone you connect to the PM Device.

- Use the **SIP Account** screen to set up information about your SIP account, control which SIP accounts the phones connected to the PM Device use, and configure audio settings such as volume levels for the phones connected to the PM Device (Section 9.3 on page 69).
- Use the **SIP Service Provider** screen to configure the SIP server information, and the numbers for certain phone functions (Section 9.4 on page 75).
- Use the **SIP TLS Common** screen to change the default TLS local port if you need to, and select a local certificate for the SIP server to verify the PM Device.(Section 9.5 on page 81).
- Use the **Phone** screens to change settings that depend on which region of the world the PM Device is in (Section 9.6 on page 82).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 9.8 on page 85).
- Use the **Call History** screen to view a call history list (Section 9.9 on page 86).

You do not necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

9.1.2 What You Need to Know About VoIP

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signaling standard that lets one network device (like a computer or the PM Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your PM Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call. To access this screen, click **VoiceVoIP** > **SIP**.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the PM Device to use your SIP account to make calls, the PM Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you do not need a SIP account. It is possible for one SIP device (like the PM Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup – figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

SIP Address

A SIP address is a URI (Uniform Resource Identifier) that resembles an email address, using the format: user@domain. It uniquely identifies a telephone extension over a VoIP system. A SIP address of 123-45-67@voip-provider.net tells a client to connect to voip-provider.net and request a connection to 123-45-67. While VoIP can only send voice messages over the Internet, SIP (though strictly speaking is a type of VoIP) can send voice, data, video, and other media. VoIP phones also need to be connected to a computer to function, whereas SIP phones only need to be connected to a modem.

9.2 Before You Begin

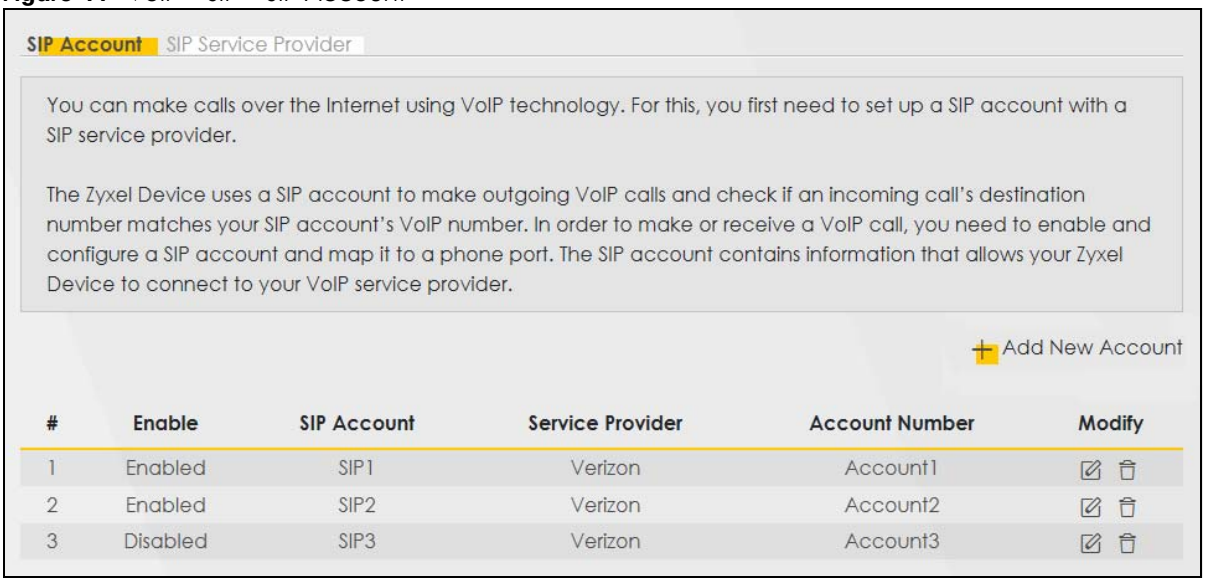
- Before you can use these screens, you need to have a VoIP account already set up. If you do not have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the PM Device.

9.3 SIP Account

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider. The PM Device uses a SIP account to make outgoing VoIP calls, and to check if an incoming call's destination number matches your SIP account's VoIP number. In order to make and receive VoIP calls, you need to enable and configure a SIP account, and then map it to a phone port. The SIP account contains information that allows your PM Device to connect to your VoIP service provider.

To access this screen, click **VoIP** > **SIP** > **SIP Account.**

Figure 44 VoIP > SIP > SIP Account



The following table describes the labels in this screen.

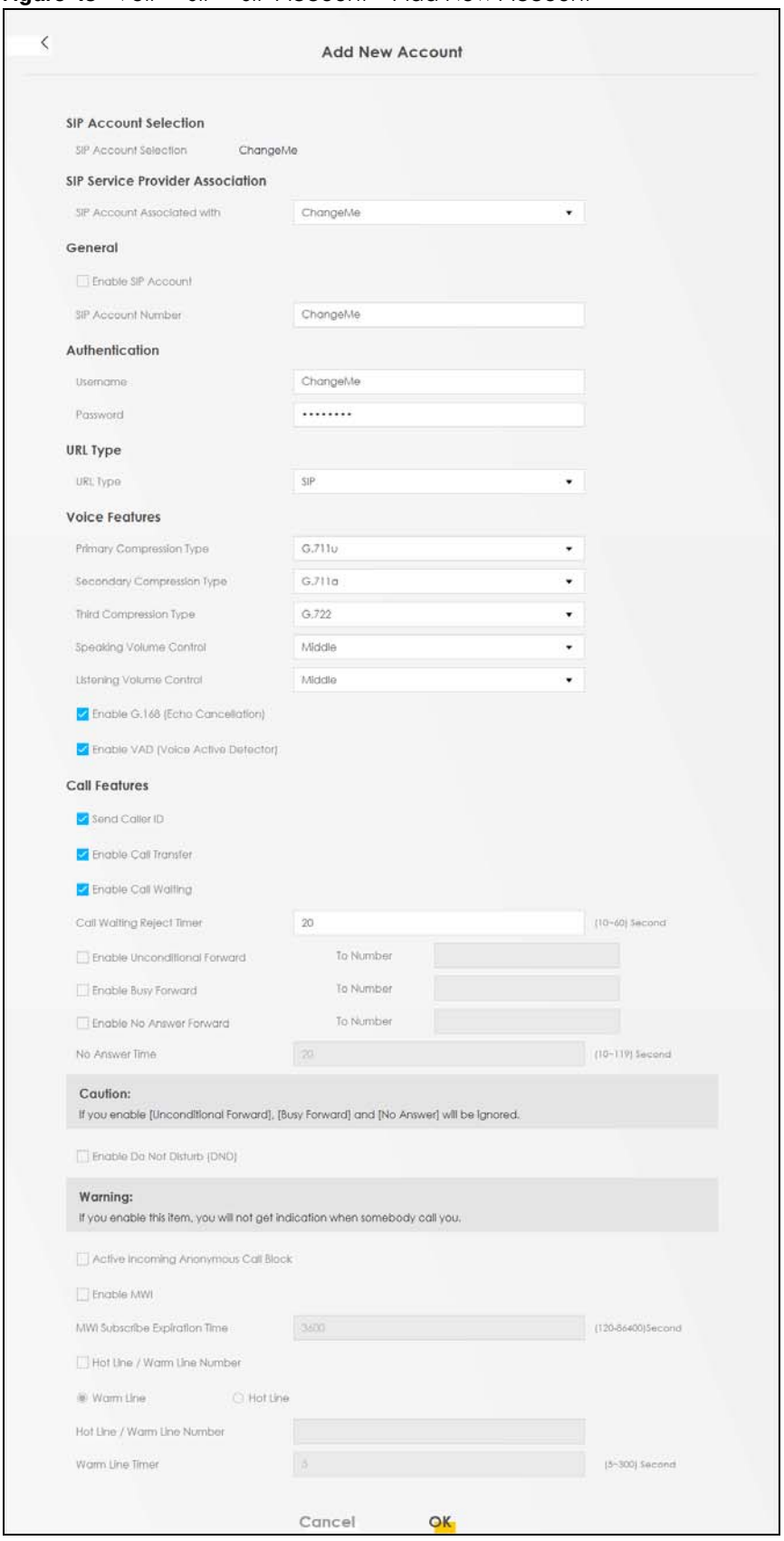
Table 23 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
Add New Account	Click this to configure a SIP account.
#	This is the index number of the entry.
Enable	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
Service Provider	This shows the name of the SIP service provider.
Account Number	This shows the SIP number.
Modify	Click the **Modify** icon to configure the SIP account.

9.3.1 Add or Edit SIP Account

Use this screen to configure a SIP account and map it to a phone port in the **Phone Device** screen. To access this screen, click the **Add New Account** button in the **VoIP** > **SIP** > **SIP Account** screen.

Figure 45 VoIP > SIP > SIP Account > Add New Account

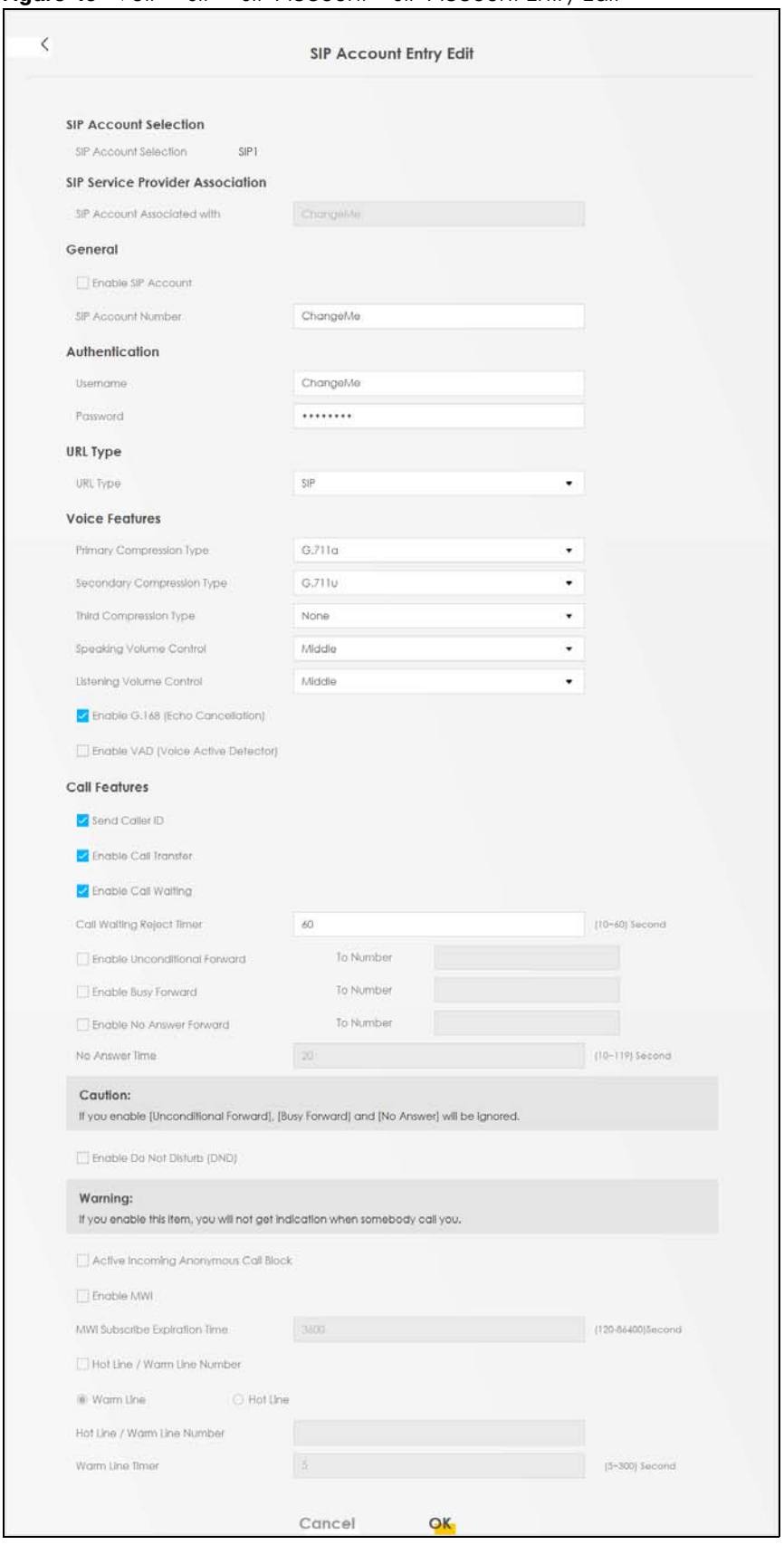


9.3.2 SIP Account Entry Edit

You can configure an SIP account. To access this screen, click the Modify icon of an entry in the **VoIP** > **SIP** > **SIP Account** screen.

Note: You do not necessarily need to use all these fields to set up your account.

Figure 46 VoIP > SIP > SIP Account > SIP Account Entry Edit



The following table describes the labels in this screen.

Table 24 VoiceVoIP > SIP > SIP Account > Add New Account or SIP Account Entry Edit

LABEL	DESCRIPTION
SIP Account Selection	
SIP Account Selection	This field displays **ChangeMe** if you are creating a new SIP account or the SIP account you are modifying.
SIP Service Provider Association	
SIP Account Associated with	Select the SIP service provider profile to use for the SIP account you are configuring in this screen. You should already have configured a SIP service provider profile in the **SIP Service Provider** screen. This field is read-only when you are modifying an existing SIP account.
General	
Enable SIP Account	Select this if you want the PM Device to use this account. Clear it if you do not want the PM Device to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable characters and spaces.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 alphanumeric (0-9, a-z, A-Z), printable special characters and spaces.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 alphanumeric (0-9, a-z, A-Z), printable special characters and spaces.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the PM Device sends the SIP number. **SIP** – include the SIP service domain name. **TEL** – do not include the SIP service domain name.
Voice Features	
Primary/Secondary/Third Compression Type	Select the type of voice coder or decoder (codec) that you want the PM Device to use. • **G.711** provides higher voice quality but requires more bandwidth (64 kbps). • **G.729** provides good sound quality and reduces the required bandwidth to 8 kbps. • **G.711a** is typically used in Europe. • **G.711u** is typically used in North America and Japan. • **G.726-32** operates at 16, 24, 32 or 40 kbps. • **G.722** operates at 6.3 kbps or 5.3 kbps. When two SIP devices start a SIP session, they must agree on a codec. Select the PM Device's first choice for voice coder or decoder. Select the PM Device's second choice for voice coder or decoder. Select **None** if you only want the PM Device to accept the first choice. Select the PM Device's third choice for voice coder or decoder. Select **None** if you only want the PM Device to accept the first or second choice.
Speaking Volume Control	Select the loudness that the PM Device uses for speech that it sends to the peer device. Choices are **Minimum**, **Middle**, and **Maximum**.
Listening Volume Control	Select the loudness that the PM Device uses for speech that it receives from the peer device. Choices are **Minimum**, **Middle**, and **Maximum**.

Table 24 VoiceVoIP > SIP > SIP Account > Add New Account or SIP Account Entry Edit (continued)

LABEL	DESCRIPTION
Enable G. 168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Enable VAD (Voice Active Detector)	Select this if the PM Device should stop transmitting when you are not speaking. This reduces the bandwidth the PM Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Enable Call Transfer	Select this to enable call transfer on the PM Device. This allows you to transfer an incoming call (that you have answered) to another phone.
Enable Call Waiting	Select this to enable call waiting on the PM Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Call Waiting Reject Timer	Specify a time of seconds that the PM Device waits before rejecting the second call if you do not answer it.
Enable Unconditional Forward	Select this if you want the PM Device to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Enable Busy Forward	Select this if you want the PM Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Enable No Answer Forward	Select this if you want the PM Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the PM Device should wait for you to answer an incoming call before it considers the call unanswered.
Enable Do Not Disturb (DND)	Select this to turn the do not disturb feature on. This has the PM Device reject all calls destined to the phone line.
Active Incoming Anonymous Call Block	Select this to have the phone not ring for incoming calls with caller ID deactivated.
Enable MWI	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
MWI Subscribe Expiration Time	Keep the default value of this field unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the PM Device subscribes to the service. Before this time passes, the PM Device automatically subscribes again.
Hot Line / Warm Line Number	Select this to enable the hot line or warm line feature on the PM Device.
Warm Line	Select this to have the PM Device dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line	Select this to have the PM Device dial the specified hot line number immediately when you pick up the telephone.
Hot Line / Warm Line Number	Enter the number of the hot line or warm line that you want the PM Device to dial.

Table 24 VoiceVoIP > SIP > SIP Account > Add New Account or SIP Account Entry Edit (continued)

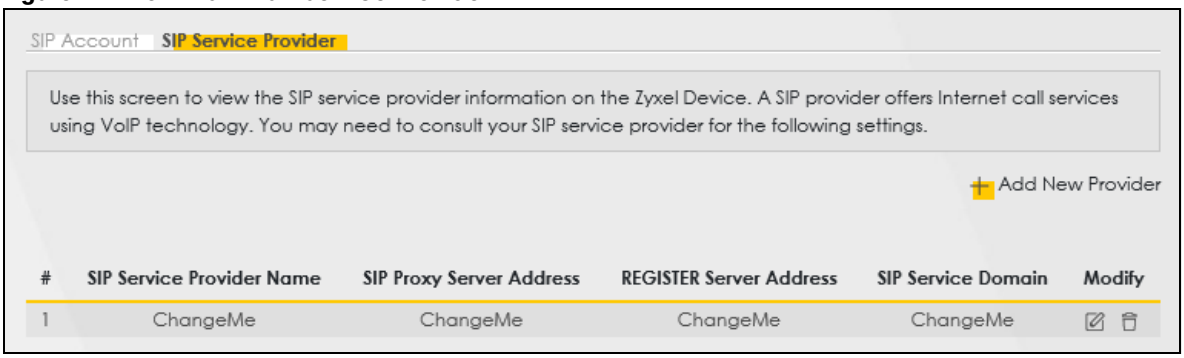
LABEL	DESCRIPTION
Warm Line Timer	Enter a number of seconds that the PM Device waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

9.4 SIP Service Provider

Use this screen to view the SIP service provider information on the PM Device. A SIP provider offers Internet call services using VoIP technology. You may need to consult your SIP service provider for the following settings.

To access this screen, click **VoIP** > **SIP** > **SIP Service Provider**.

Figure 47 VoIP > SIP > SIP Service Provider



The following table describes the labels in this screen.

Table 25 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
Add New Provider	Click this button to add a new SIP service provider.
#	This is the index number of the entry.
SIP Service Provider Name	This shows the name of the SIP service provider.
SIP Proxy Server Address	This shows the IP address or domain name of the SIP server.
REGISTER Server Address	This shows the IP address or domain name of the SIP register server.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @symbol. You can use up to 127 printable ASCII Extended set characters.
Modify	Click the **Edit** icon to configure the SIP service provider. Click the **Delete** icon to delete this SIP service provider from the PM Device.

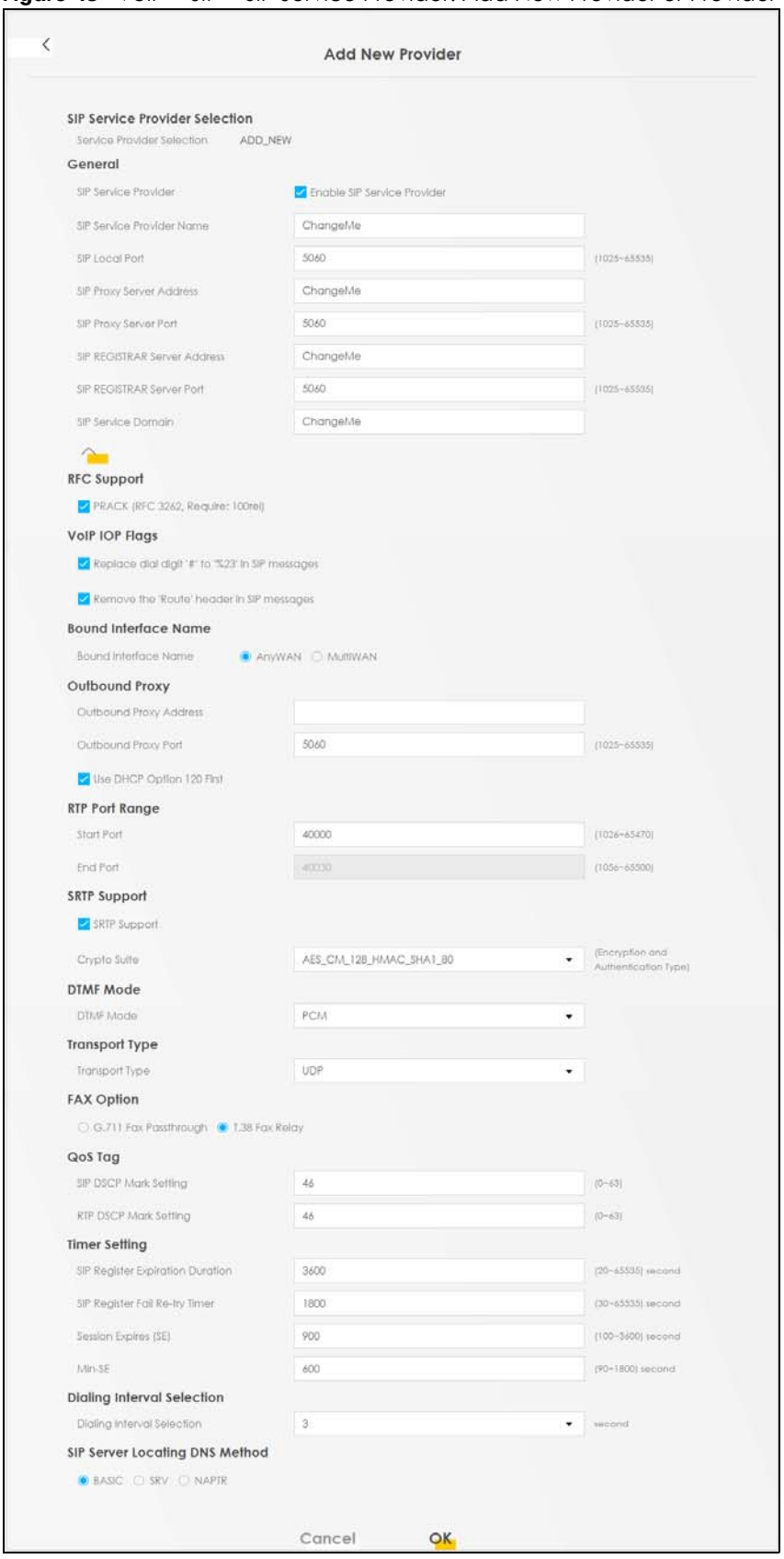
9.4.1 Provider Entry Add/Edit

Use this screen to configure the SIP server information, the numbers for certain phone functions and dialing plan for a SIP service provider.

Click the Modify icon next to a profile of SIP service provider settings in the **VoIP** > **SIP** > **SIP Service Provider** to open the following screen.

Note: Click this ( ) to see all the fields in the screen. You do not necessarily need to use all these fields to set up your account. Click again to see and configure only the fields needed for this feature.

Figure 48 VoIP > SIP > SIP Service Provider: Add New Provider or Provider Entry Edit



The following table describes the labels in this screen.

Table 26 VoIP > SIP > SIP Service Provider > Add New Provider or Provider Entry Edit

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	This field displays **ADD_NEW** if you are creating a new SIP service provider profile or the SIP service provider name you are modifying.
General	
SIP Service Provider	Select this if you want the PM Device to use this SIP provider. Clear it if you do not want the PM Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the PM Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Proxy Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Proxy Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP REGISTRAR Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].
SIP REGISTRAR Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].
RFC Support	
PRACK (RFC 3262, Require: 100rel)	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select **Supported** or **Required** to have the PM Device include a SIP Require or Supported header field with the option tag 100rel in all INVITE requests. When the PM Device receives a SIP response message indicating that the phone it called is ringing, the PM Device sends a PRACK message to have both sides confirm the message is received. If you select **Supported**, the peer device supports the option tag 100rel to send provisional responses reliably. If you select **Required**, the peer device requires the option tag 100rel to send provisional responses reliably. Select **Disabled** to turn off this function.

Table 26 VoIP > SIP > SIP Service Provider > Add New Provider or Provider Entry Edit (continued)

LABEL	DESCRIPTION
PRACK (RFC 3262, Require: 100rel)	During a call session, there are two types of SIP responses used – final and provisional. Final responses convey the result of a request and require a confirmation response. Provisional responses only convey the request processing progress and does not require a confirmation response, and are therefore considered unreliable. RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Which is, the PM Device includes a SIP Require header field with the option tag 100rel in all INVITE requests. When the PM Device receives a SIP response message indicating that the phone it called is ringing, the PM Device sends a PRACK message to have both sides confirm the message is received. Select this to have the caller require the option tag 100rel to send provisional responses reliably.
VoIP IOP Flags – Select VoIP inter-operability settings.	
Replace dial digit '#' to '%23' in SIP messages	Replace a dial digit "#" with "%23" in the INVITE messages.
Remove the 'Route' header in SIP messages	Remove the 'Route' header in SIP packets.
Bound Interface Name	
Bound Interface Name	If you select **AnyWAN**, the PM Device automatically activates the VoIP service when any WAN connection is up. If you select **MultiWAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the PM Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the PM Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
Use DHCP Option 120 first	Select this to have the PM Device use DHCP Option 120 first.
RTP Port Range	
Start/End Port	Enter the listening port numbers for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
SRTP Support	

Table 26 VoIP > SIP > SIP Service Provider > Add New Provider or Provider Entry Edit (continued)

LABEL	DESCRIPTION
SRTP Support	When you make a VoIP call using SIP, the Real-time Transport Protocol (RTP) is used to handle voice data transfer. The Secure Real-time Transport Protocol (SRTP) is a security profile of RTP. It is designed to provide encryption and authentication for the RTP data in both unicast and multicast applications. The PM Device supports encryption using AES with a 128-bit key. To protect data integrity, SRTP uses a Hash-based Message Authentication Code (HMAC) calculation with Secure Hash Algorithm (SHA)-1 to authenticate data. HMAC SHA-1 produces a 80 or 32-bit authentication tag that is appended to the packet. Both the caller and callee should use the same algorithms to establish an SRTP session.
Crypto Suite	Select the encryption and authentication algorithm set used by the PM Device to set up an SRTP media session with the peer device. Select **AES_CM_128_HMAC_SHA1_80** or **AES_CM_128_HMAC_SHA1_32** to enable both data encryption and authentication for voice data. Select **AES_CM_128_NULL** to use 128-bit data encryption but disable data authentication. Select **NULL_CIPHER_HMAC_SHA1_80** to disable encryption but require authentication using the default 80-bit tag.
DTMF Mode	Control how the PM Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** – send the DTMF tones in RTP packets. **PCM** – send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIP INFO** – send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the protocol used to transport the SIP packets. For **UDP** and **TCP**, see the Service appendix for more information on the example services and the required protocol and port number.
FAX Option	This field controls how the PM Device handles fax messages.
G711 Fax Passthrough	Select this if the PM Device should use G.711 to send fax messages. You have to also select which operating codec (**G.711Mulaw** or **G.711Alaw**) to use for encoding/ decoding FAX data. The peer devices must use the same settings.
T38 Fax Relay	Select this if the PM Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
QoS Tag	
SIP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The PM Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The PM Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
SIP Register Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The PM Device automatically tries to re-register your SIP account when one-half of this time has passed (The SIP register server might have a different expiration).

Table 26 VoIP > SIP > SIP Service Provider > Add New Provider or Provider Entry Edit (continued)

LABEL	DESCRIPTION
SIP Register Fall Re-try timer	Enter the number of seconds the PM Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires [SE]	Enter the number of seconds the PM Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the PM Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the PM Device accepts.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the PM Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
SIP Server Location DNS Method	Select the method that the PM Device used to query the ISP's DNS server for SIP server address. The PM Device will use the query result to locate the SIP server for phone service registration. Select **BASIC** to have the PM Device query the DNS server for a DNS A record that contains the IP address of the SIP server. Select **SRV** to have the PM Device query the DNS server for a DNS Service (SRV) record. The SRV record is a list of all available SIP servers information that the DNS server maintains. The PM Device will then use the SRV record to perform A query to get the SIP server IP. This is useful if your primary SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls. Select **NAPTR** to have the PM Device query the DNS server for DNS Name Authority Pointer (NAPTR) records in order to find the available services (transport protocols) supported by the SIP server. The PM Device will then perform an SRV or A query to get the SIP server information.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

9.5 SIP TLS Common

Encrypt SIP traffic between the PM Device and the SIP server using TLS (Transport Layer Security). Configure this screen if the SIP server requires it.

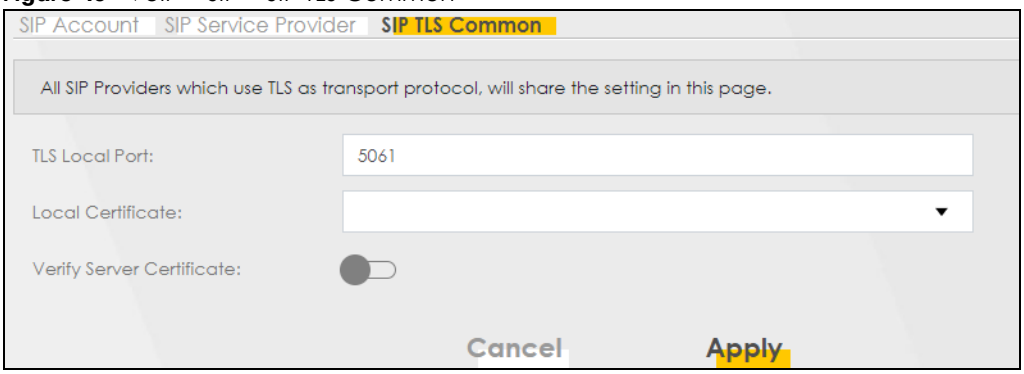
Use this screen to:

- Change the default TLS local port.
- Select a local certificate for the SIP server to verify the PM Device.

Note: To activate **SIP TLS Common**, select **TLS** in **Transport Type** in the **SIP Service Provider** screen.

To access this screen, click **VoIP** > **SIP** > **SIP TLS Common**.

Figure 49 VoIP > SIP > SIP TLS Common



The following table describes the labels in this screen.

Table 27 VoIP > SIP > SIP TLS Common

LABEL	DESCRIPTION
TLS Local Port	Port 5061 is typically used for SIP over TLS. Enter the PM Device's TLS local port number if your VoIP service provider gave you one. Otherwise, keep the default value.
Local Certificate	This is the certificate the SIP server uses to verify the PM Device. Go to **Certificate** > **Local Certificate** and import a PM Device certificate that the SIP server can use to verify the PM Device, if required. Then select the certificate you imported in this field.
Verify Server Certificate	Click to enable this if you want the PM Device to verify the certificate from the SIP server. If required or if your VoIP service provider gave you a certificate, import the dedicated CA in **Certificate** > **Trusted CA** in order for the PM Device to authenticate the SIP server.

9.6 Phone

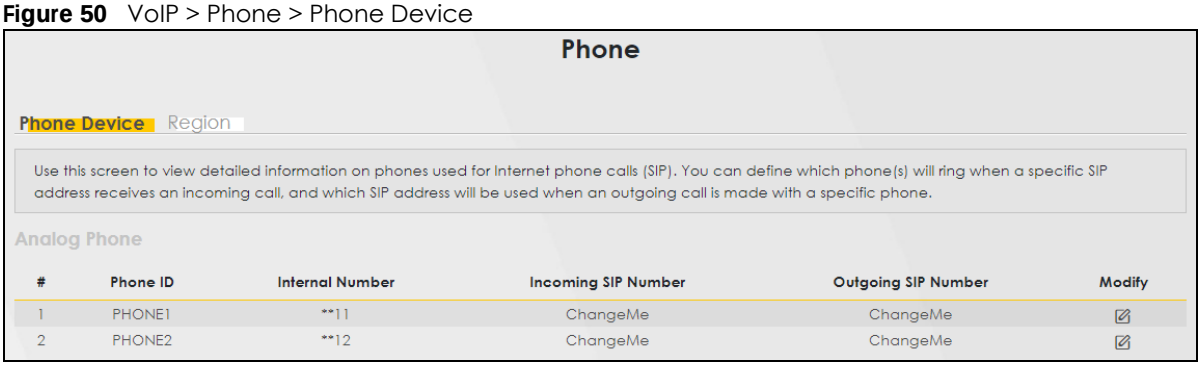
Use these screens to configure SIP numbers and regions for IP phones that are connected to the PM Device.

9.6.1 Phone Device

Use this screen to view detailed information on phones used for Internet phone calls (SIP). You can define which phones will ring when a specific SIP address receives an incoming call, and which SIP address will be used when an outgoing call is made with a specific phone.

To access this screen, click **VoIP** > **Phone** > **Phone Device**.

Figure 50 VoIP > Phone > Phone Device



Each field is described in the following table.

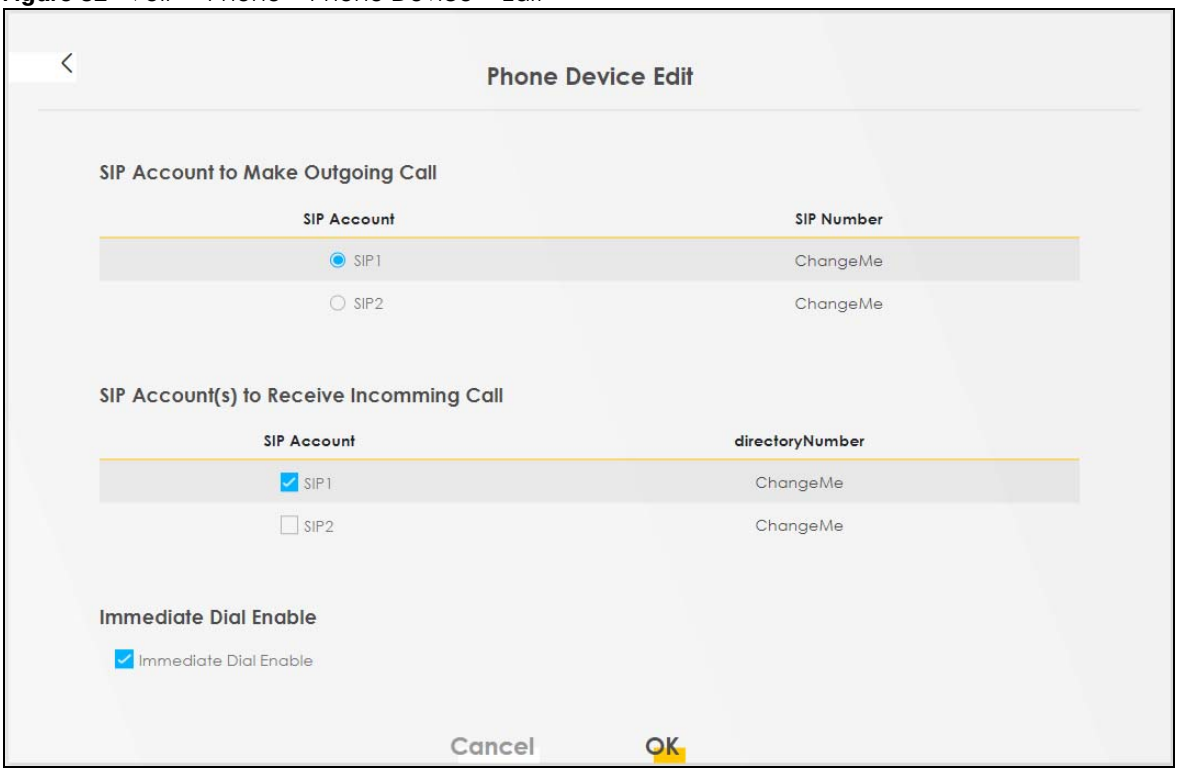
Table 28 VoIP > Phone > Phone Device

LABEL	DESCRIPTION
#	This displays the index number of the phone device.
Phone ID	This field displays the name of a phone port on the PM Device.
Internal Number	This field displays the internal call prefix of a phone port on the PM Device.
Incoming SIP Number	This field displays the SIP address that you use to receive calls on this phone port.
Outgoing SIP Number	This field displays the SIP address that you use to make calls on this phone port.
Modify	Click the Edit icon to configure the SIP account.

9.6.2 Phone Device Edit

Use this screen to control which SIP account and PSTN line each phone uses. Click an Edit icon in **VoIP** > **Phone** > **Phone Device** to open the following screen.

Figure 51 VoIP > Phone > Phone Device > Edit



Each field is described in the following table.

Table 29 VoIP > Phone > Phone Device > Edit

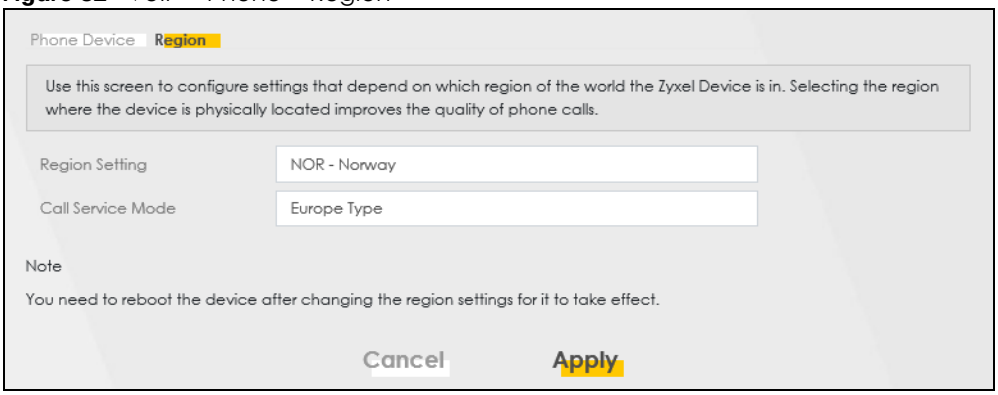
LABEL	DESCRIPTION
SIP Account to Make Outgoing Call	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Account(s) to Receive Incoming Call	Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port. If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
Immediate Dial Enable	Select this if you want to use the pound key (#) to tell the PM Device to make the phone call immediately, instead of waiting for the number of second you selected in the **Dialog Interval Selection** field of the **VoIP** > **SIP** > **SIP Service Provider** > **Add New Provider** or **Edit** screen. If you select this, dial the phone number, and then press the pound key. The PM Device makes the call immediately instead of waiting. You can still wait, if you want.
Cancel	Click **Cancel** to exit this screen without saving
OK	Click **OK** to save your changes.

9.7 Phone Region

Use this screen to configure settings that depend on which region of the world the PM Device is in. Selecting the region where the device is physically located improves the quality of phone calls.

To access this screen, click **VoIP** > **Phone** > **Region**.

Figure 52 VoIP > Phone > Region



The following table describes the labels in this screen.

Table 30 VoIP > Phone > Region

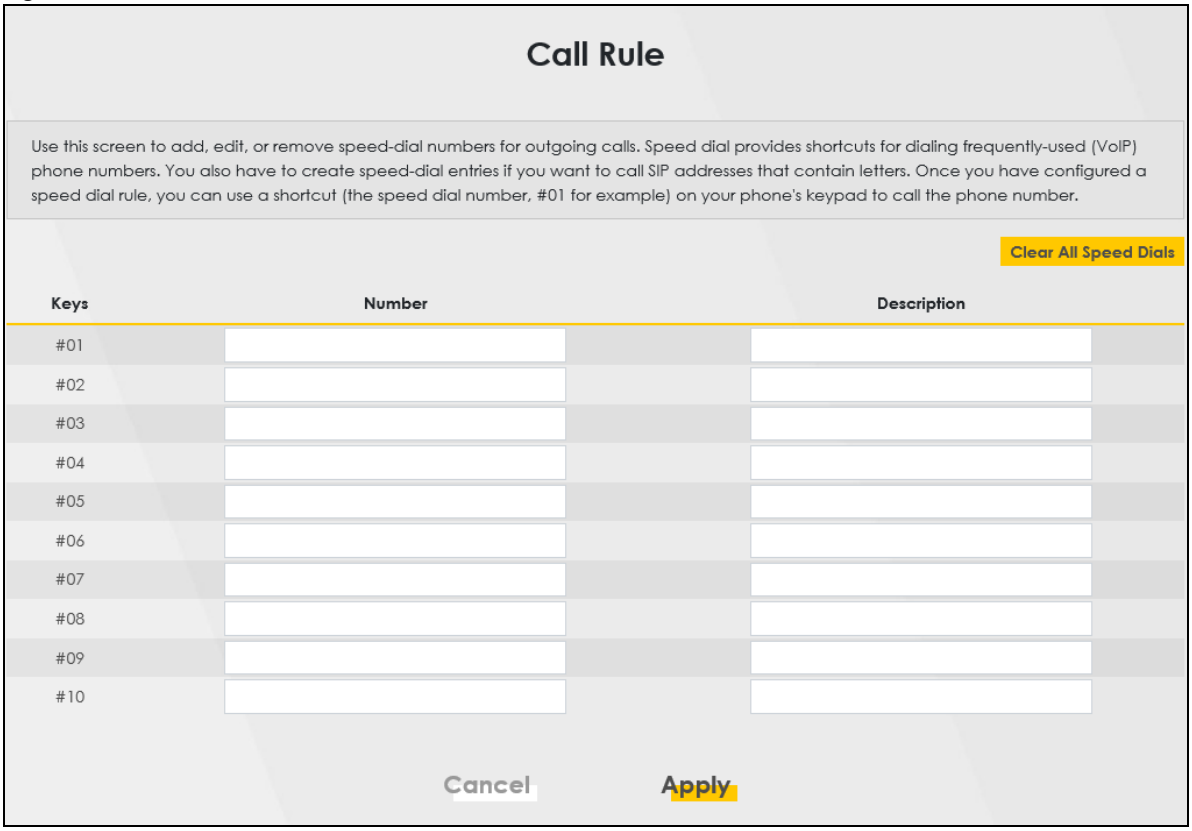
LABEL	DESCRIPTION
Region Setting	Select the place in which the PM Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. • **Europe Type** – use supplementary phone services in European mode. • **USA Type** – use supplementary phone services American mode. You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the PM Device.
Cancel	Click this to set every field in this screen to its last-saved value.

Note: You need to reboot the PM Device after changing the region settings for it to take effect.

9.8 Call Rule

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number. To access this screen, click **VoIP** > **Call Rule**.

Figure 53 VoIP > Call Rule



The following table describes the labels in this screen.

Table 31 VoIP > Call Rule

LABEL	DESCRIPTION
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the PM Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Clear All Speed Dials	Click this button to remove all speed dials saved.
Apply	Click this to save your changes and to apply them to the PM Device.
Cancel	Click this to set every field in this screen to its last-saved value.

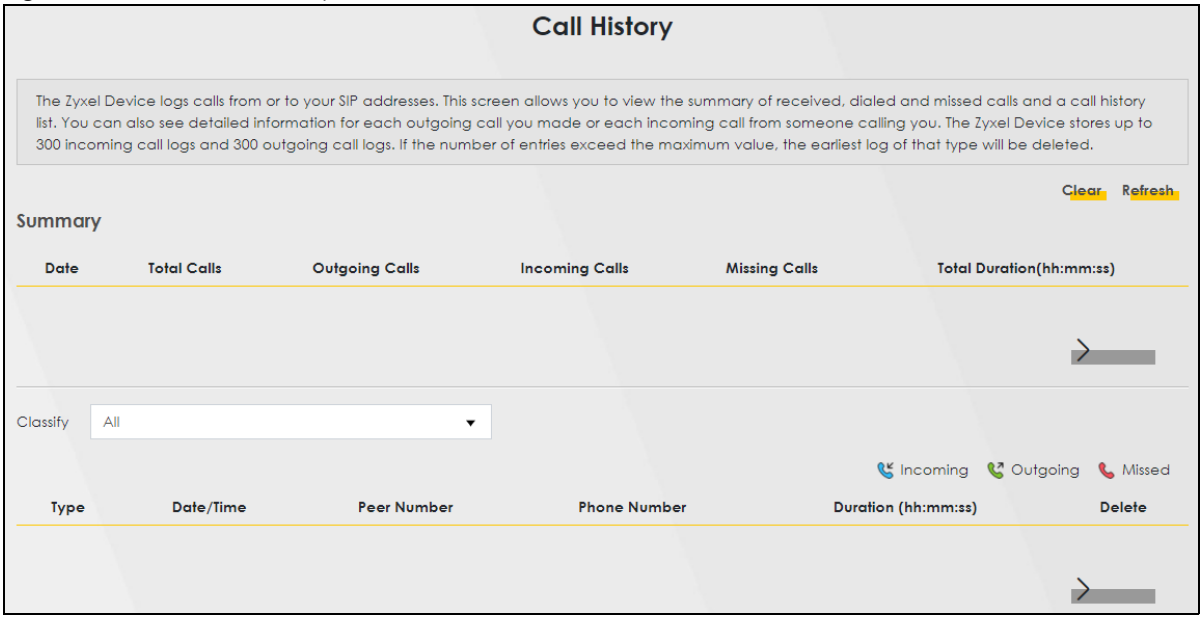
9.9 Call History

The PM Device logs calls from or to your SIP addresses. This screen allows you to view a summary of received, dialed and missed calls and a call history list. You can also view detailed information on each outgoing and incoming call.

9.9.1 Call History Screen

To access this screen, click **VoIP** > **Call History**.

Figure 54 VoIP > Call History



Each field is described in the following table.

Table 32 VoIP > Call History

LABEL	DESCRIPTION
Clear List	Click this button to remove all entries from the call history list.
Clear	Click this button to remove all entries from the call history list.
Refresh	Click this button to renew the call history list.
Export	Click this button to download a call history list.
Summary	
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP addresses that day.
Outgoing Calls	This displays how many calls originated from you that day.
Incoming Calls	This displays how many calls you received that day.
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration (hh:mm:ss)	This displays how long all calls lasted that day.
Classify	Select the type of the calls. The call types are: **All**, **Incoming**, **Outgoing** and **Missed**.
Type	This displays the type of the calls.
Date/Time	This displays the date and time when the calls were made.
Peer Number	This displays the SIP address that called you or you called.
Phone Number	This displays the phone number of the call.
Duration (hh:mm:ss)	This displays how long the call lasted.
Delete	Click the **Delete** icon to remove the call history.

9.10 Technical Reference

This section contains background material relevant to the **VoIP** screens.

VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an email address identifies an email account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an email address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

SIP Registration

Each PM Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the PM Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The PM Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the PM Device attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated through a challenge / response system using the HTTP digest mechanism (as detailed in RFC 3261, "SIP: Session Initiation Protocol").

SIP Servers

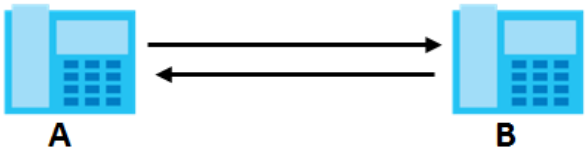
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP SIP user agent to receive the call.

Figure 55 SIP User Agent



SIP Proxy Server

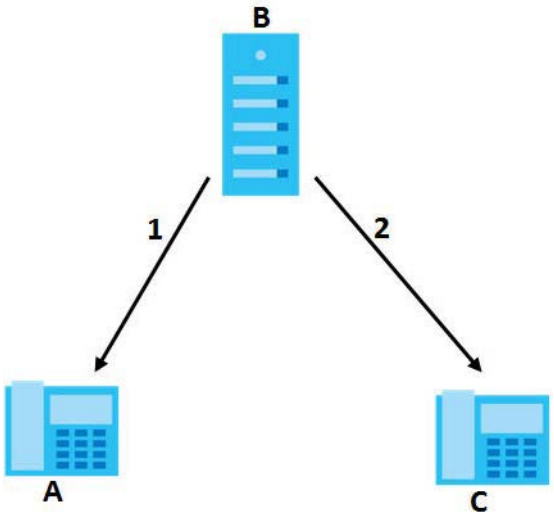
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).

2 The SIP proxy server forwards the call invitation to **C**.

Figure 56 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

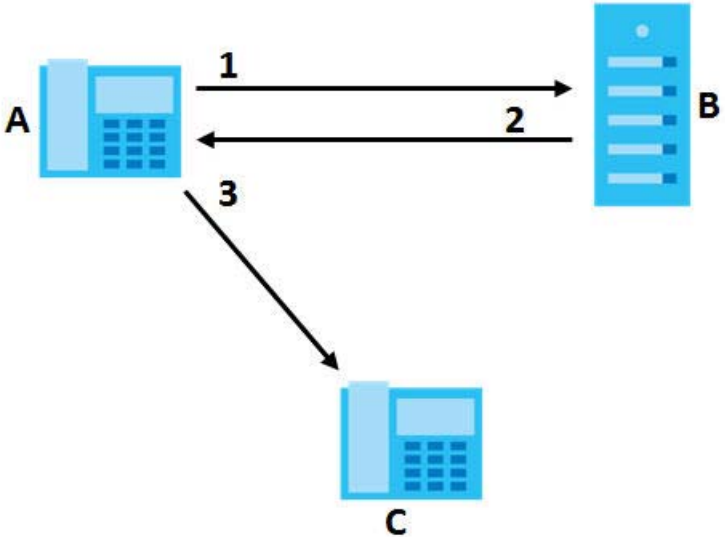
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).

2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

Figure 57 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

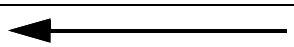
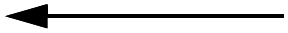
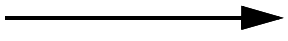
Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 33 SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK
4. ACK		
	5.Dialogue (voice traffic)	
6. BYE		
		7. OK

1. **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.
2. **B** sends a response indicating that the telephone is ringing.
3. **B** sends an OK response after the call is answered.
4. **A** then sends an ACK message to acknowledge that **B** has answered the call.
5. Now **A** and **B** exchange voice media (talk).
6. After talking, **A** hangs up and sends a BYE request.
7. **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

SIP Call Progression Through Proxy Servers

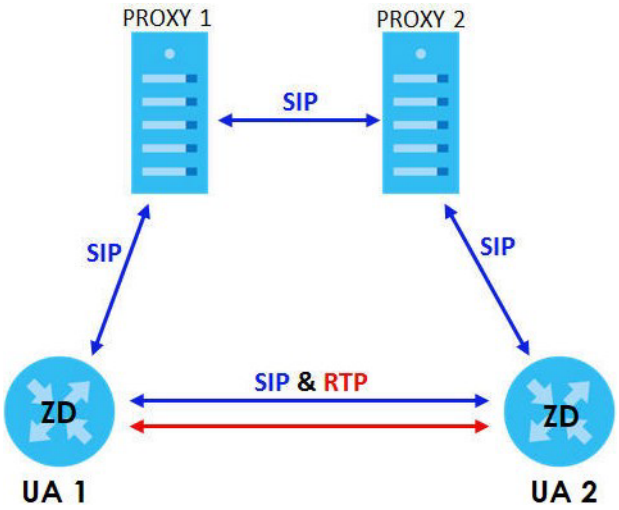
Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested

by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

Figure 58 SIP Call Through Proxy Servers



The following table shows the SIP call progression.

Table 34 SIP Call Progression

UA 1		PROXY 1		PROXY 2		UA 2
Invite	→					
		Invite	→			
		100 Trying	←			
				Invite	→	
				100 Trying	←	
						180 Ringing ←
				180 Ringing	←	
		180 Ringing	←			
						200 OK ←
				200 OK	←	
		200 OK	←			
ACK	→					
RTP	↔					RTP
						BYE ←
200 OK	→					

1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.

2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.

3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** through **Proxy 1**.

5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** through **Proxy 1**.

6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.

7 When **User Agent 2** hangs up, he sends a BYE request.

8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The PM Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the PM Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

Comfort Noise Generation

When using VAD, the PM Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the PM Device. The PM Device allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 35 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	900 seconds for all custom tones combined
Maximum Time per Individual Tone	180 seconds
Total Number of Tones Recordable	5 You can record up to 5 different custom tones but the total time must be 900 seconds or less.

Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1101 – 1105 on your phone followed by the "#" key.
3. Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.
4. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Listening to Custom Tones

Do the following to listen to a custom tone:

1. Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.
2. Press a number from 1201 to 1208 followed by the "#" key to listen to the tone.
3. You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Deleting Custom Tones

Do the following to delete a custom tone:

1 Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1301 – 1308 followed by the "#" key to delete the tone of your choice. Press 14 followed by the "#" key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

9.10.1 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the PM Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[1]

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 59 DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

1. The PM Device does not support DiffServ at the time of writing.

9.10.2 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The PM Device supports the following services:

- Call Return
- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb
- IVR
- Call Completion
- CCBS
- Outgoing SIP

Note: To take full advantage of the supplementary phone services available through the PM Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

9.10.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the PM Device.

You can invoke all the supplementary services by using the flash key.

9.10.2.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 36 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.

Table 36 European Flash Key Commands (continued)

COMMAND	SUB-COMMAND	DESCRIPTION
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press "0".
- Disconnect the first call and answer the second call.

  Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then "2".

European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press "3" to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

9.10.2.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 37 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1 Press the flash key to put the caller on hold.

2 When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.

3 After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference

Use the following steps to make three-way conference calls.

1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.

2 Dial a phone number directly to make another call (to party B).

3 When party B answers the second call, press the flash key to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.

6 If you want to go back to the three-way conversation, press the flash key again.

7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

9.10.2.4 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

Table 38 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
*98#	Call transfer	Transfer a call to another phone. See Section 9.10.2.2 on page 96 (Europe type) and Section 9.10.2.3 on page 98 (USA type).
*66#	Call return	Place a call to the last person who called you.
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off.
#95#	Disable Do Not Disturb	
*41#	Enable Call Waiting	Use these to allow you to put a call on hold when you are answering another, or to turn this function off.
#41#	Disable Call Waiting	
****	IVR	Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold).
####	Internal Call	Call the phone(s) connected to the PM Device.
*82	One Shot Caller Display Call	Activate or deactivate caller ID for the next call only.
*67	One Shot Caller Hidden Call	

CHAPTER 10
Log

10.1 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.

10.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 10.2 on page 101).
- Use the **Security Log** screen to see the security-related logs (Section 10.3 on page 102).

10.1.2 What You Need To Know

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

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as System Errors consist of both logs and alerts. You may differentiate them by their color in the View Log screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

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

Table 39 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.

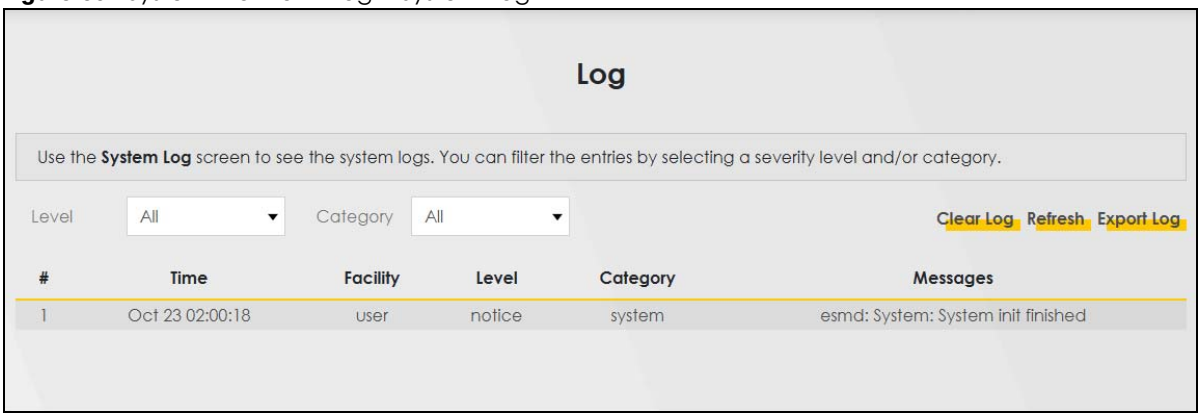
Table 39 Syslog Severity Levels (continued)

CODE	SEVERITY
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

10.2 System Log

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

Figure 60 System Monitor > Log > System Log



The following table describes the labels in this screen.

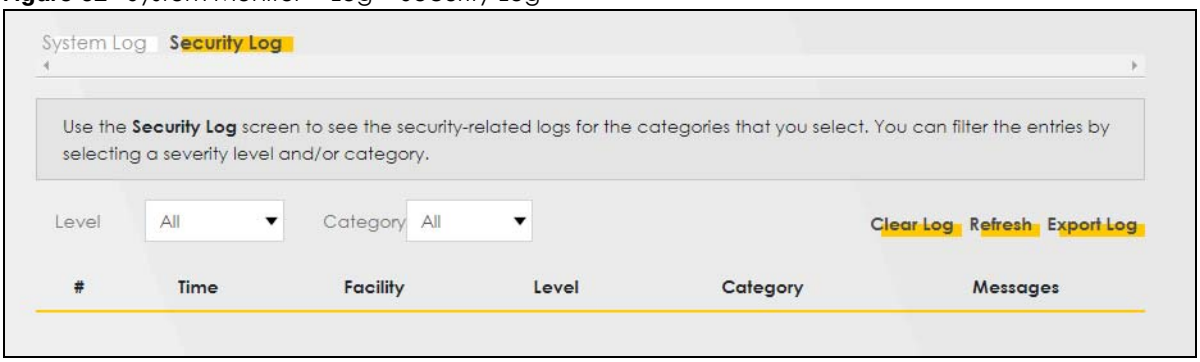
Table 40 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the PM Device searches through all 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.
#	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.

10.3 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 61 System Monitor > Log > Security Log



The following table describes the labels in this screen.

Table 41 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 11
Traffic Status

11.1 Overview

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

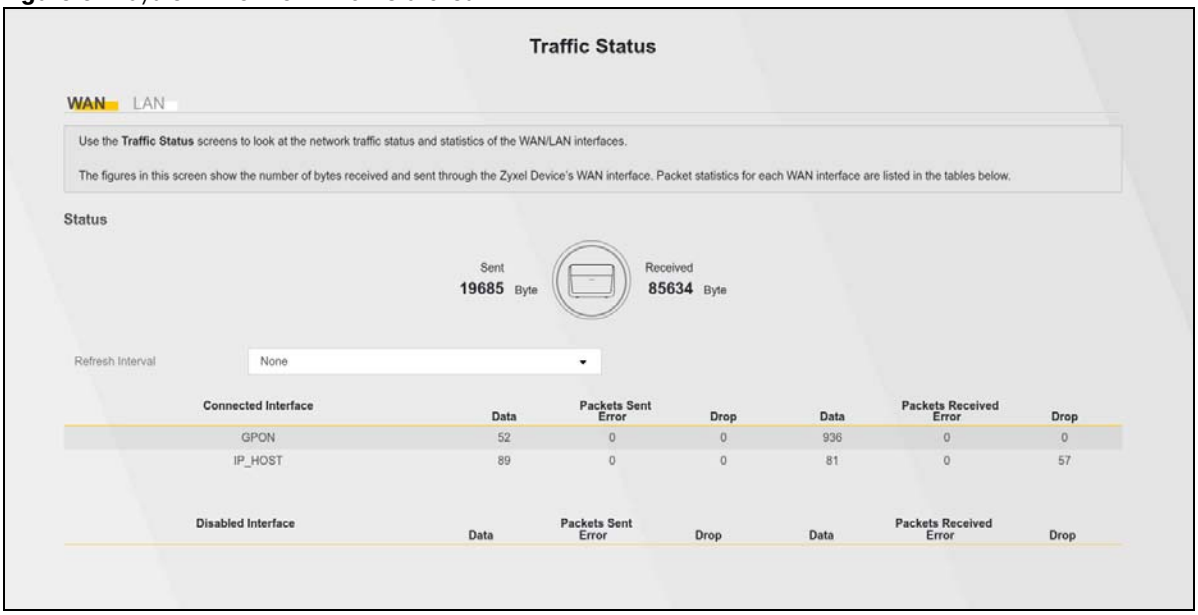
11.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 11.2 on page 103).
- Use the **LAN** screen to view the LAN traffic statistics (Section 11.3 on page 104).

11.2 WAN Traffic Status

Click **System Monitor** > **Traffic Status** > **WAN** to open the **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 62 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

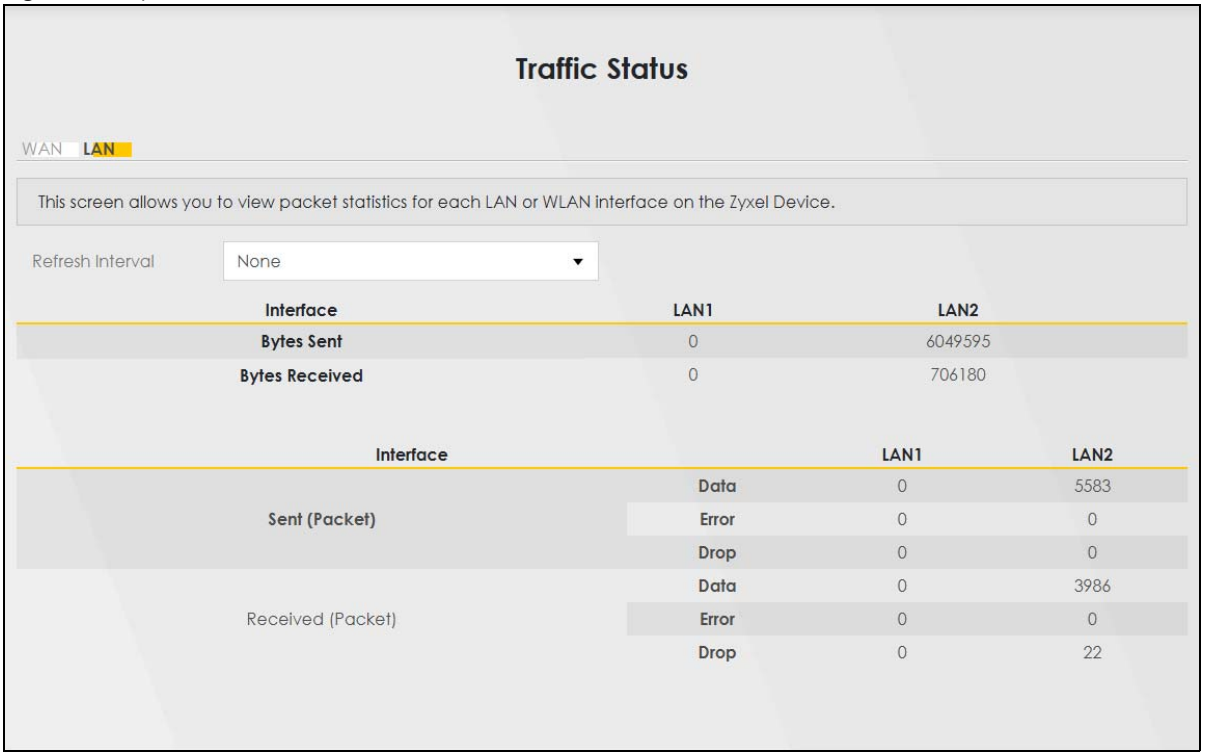
Table 42 System Monitor > Traffic Status > WAN

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.

11.3 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 63 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

Table 43 System Monitor > Traffic Status > LAN

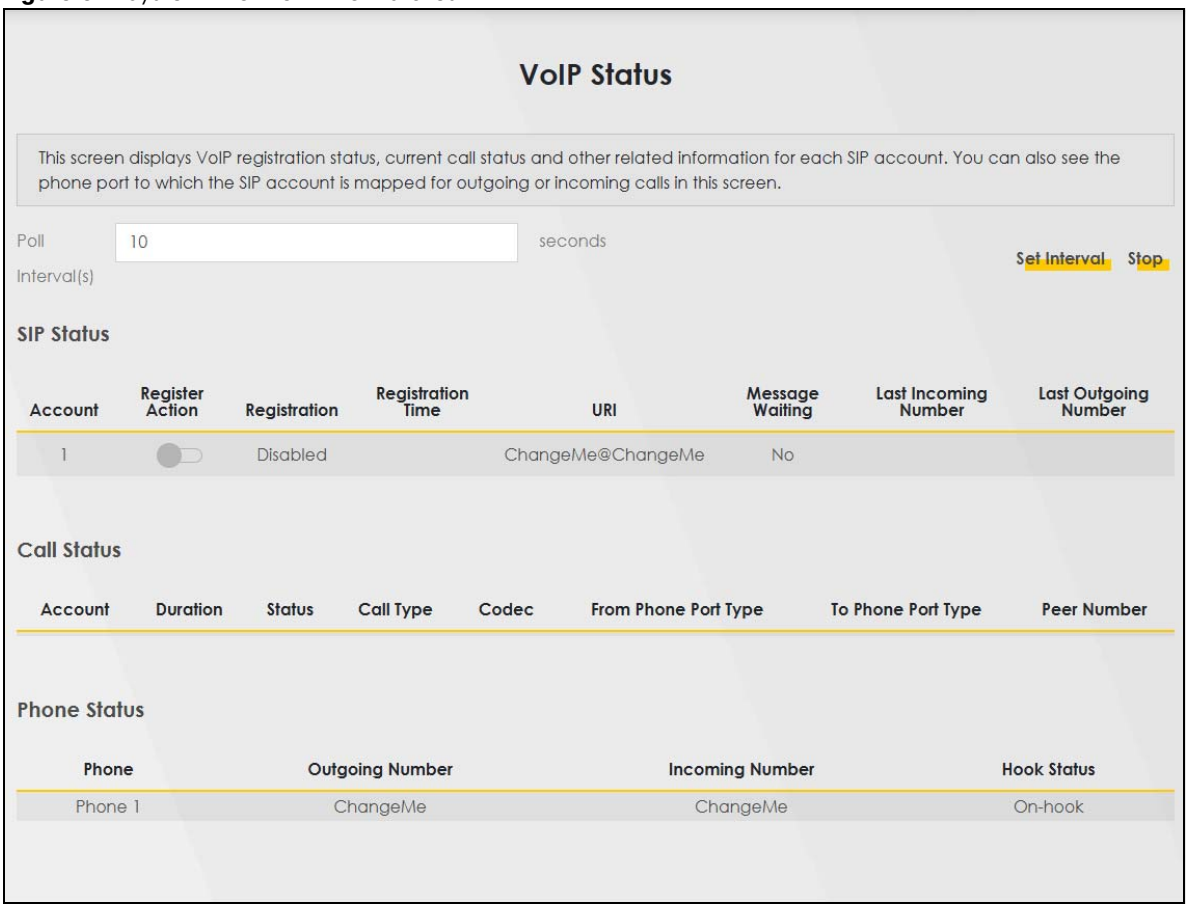
LABEL	DESCRIPTION
Refresh Interval	Select how often you want the PM Device to update this screen.
Interface	This shows the LAN interface on the PM Device.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
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 12
VoIP Status

12.1 VoIP Status Screen

Click **System Monitor** > **VoIP Status** to open the following screen. You can view the Voice over IP (VoIP) registration, current call status and phone numbers in this screen.

Figure 64 System Monitor > VoIP Status



The following table describes the labels in this screen.

Table 44 System Monitor > VoIP Status

LABEL	DESCRIPTION
Poll Interval	Enter the number of seconds the PM Device needs to wait before updating this screen and then click **Set Interval**. Click **Stop** to have the PM Device stop updating this screen.
SIP Status	
Account	This column displays each SIP account in the PM Device.

Table 44 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Register Action	Click on this switch to register/unregister the SIP account. This switch will turn blue if a registration attempt is successful; otherwise, it will revert to its unregistered setting. Unregistering an account does not delete the SIP account itself, but removes the mapping between your SIP identity and your IP address or domain name,
Registration	This field displays the current registration status of the SIP account. **Registered** – The SIP account is activated and has been registered with a SIP server. You can use it to make a VoIP call. **Unregistered** – The SIP account is activated, but the last time the PM Device tried to register the SIP account with the SIP server, the attempt failed. Use the **Register Action** switch to register the account again. The PM Device will also automatically try to register the SIP account again after a period of time that you configured in **VoIP** > **SIP** > **SIP Service Provider** > **Add/Edit** > **SIP Register Fail Re-Try Timer**. **Disabled** – The SIP account is not active. Make sure the corresponding SIP Service Provider and SIP Account are both enabled in **VoIP** > **SIP** > **SIP Service Provider** > **Add/Edit** and **VoIP** > **SIP** > **SIP Account** > **Add/Edit**.
Registration Time	This field displays the last time the PM Device successfully registered the SIP account. The field is blank if the PM Device has never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP** > **SIP** screen.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the PM Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** – There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** – The callee's phone is ringing. **Ring** – The phone is ringing for an incoming VoIP call. **Process** – There is a VoIP call in progress. **DISC** – The callee's line is busy, the callee hung up or your phone was left off the hook.

Table 44 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Call Type	This field displays the call direction type of the current VoIP call. **Outgoing Call** – It is a SIP VoIP call made by local phone ports, and this SIP account is able to issue a (SIP-based) call setup to the SIP account of remote peers for a VoIP call establishment. This (SIP-based) call setup signal is sent to the SIP server first, and then the SIP server would relay it to the target peer after correctly resolving and locating the target peer. During the call setup (signaling) phase, Calling state is displayed in the Status field, and it turns to InCall state once the call is successfully established. **Incoming Call** – It is a SIP VoIP call made or originated by remote SIP accounts to connect to this local SIP account. One or more local phone ports can be configured to receive this type of call, see the **Incoming Number** below, and all of them should begin to ring during the call setup (signaling phase), see the **Status** above. Once some remote SIP accounts start to ring one local phone, answer by off-hook to the call, and the call is successfully established. The other ringing local phone ports will stop ringing and turning to InCall state in the **Status** field. **Internal Call** – It is a local VoIP call between two different local phone ports. No SIP signaling is needed and thus no SIP server is involved to establish this type of call. This type of call is established through the Internal and Non-SIP local setup signaling procedure between the call-originating and call-terminating local phone ports. In general, one or more local phone ports can be designed to receive this type of call, and once any of the ringing phones answer the call, the other ringing ones will stop ringing. During the call setup phase (signaling phase), Calling state is displayed in **Status** field, and turns to InCall state once the call is successfully established.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
From Phone Port Type	This field displays the phone ports type used to originate, start, or create the current VoIP call. Two possible type values will be displayed here: SIP – For the current call which is categorized as **Incoming Call** in the **Call Type** field. This field will show the type SIP. FXS – As for the other cases: **Outgoing Call** and **Internal Call**. This field will show the corresponding local phone port type: FXS, the legacy analog phone port on the PM Device.
To Phone Port Type	This field displays the phone ports type used to receive the current VoIP call. Three possible type values will be displayed here: SIP – For the current call which is categorized as **Outgoing Call** in the **Call Type** field. This field will show the type SIP. FXS and Unknown – As for the other cases: **Incoming Call** and **Internal Call**, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the PM Device. While the call is established, this field displays **Unknown** during the call setup phase (signaling phase). This is because one or more local phone ports can be configured or designed to receive these two types of calls, see the **Call Type** above, and the local phone port will answer the call that has not been determined yet at that time.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays the name of a phone port on the PM Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Hook Status	This field displays whether the phone is in the on or off hook status. **Off-Hook** means a telephone connected to one of the phone port has its receiver off the hook. **On-Hook** means a telephone connected to one of the phone port has its receiver on the hook.

CHAPTER 13
Optical Signal Status

13.1 Overview

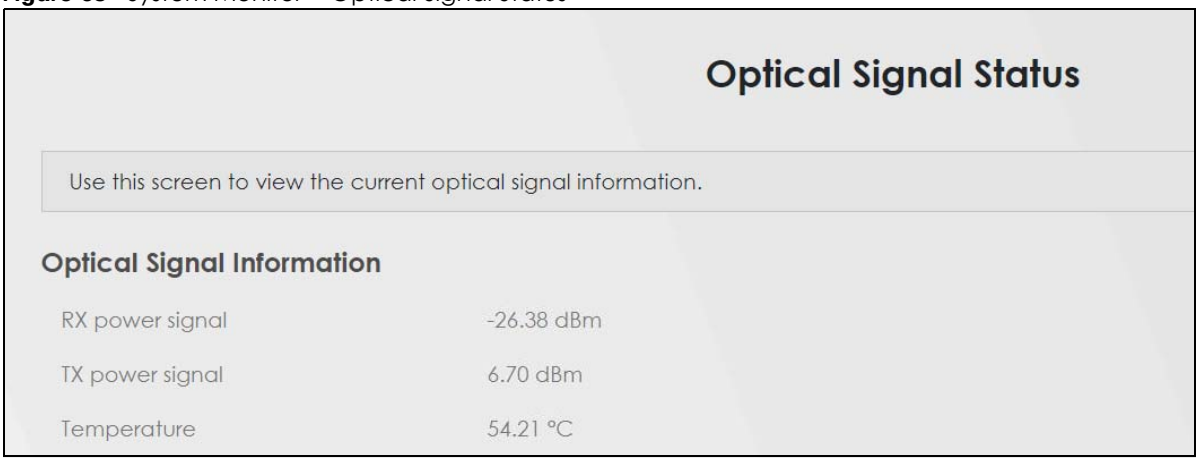
Use this screen to view the PON transceiver's TX power and RX power level and its temperature.

13.2 Optical Signal Status

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 65 System Monitor > Optical Signal Status



The following table describes the labels in this screen.

Table 45 System Monitor > Optical Signal Status

LABEL	DESCRIPTION
Optical Signal Information	
RX power signal	This displays the PON transceiver's receiving power in dBm. The normal range is –9 to –28 dBm. The higher the value, the stronger the signal as there is less background noise. For example, –9 dBm is a stronger signal than –28 dBm.
TX power signal	This field displays the transceiver's transmitting power in dBm.
Temperature	This field displays the transceiver's temperature in degrees Celsius.

The following table shows the normal range of optical signal information.

LABEL	NORMAL RANGE
RX power signal	–9 to –28 dBm
TX power signal	2 to 7 dBm
Temperature	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 –8 to –27 dBm.

CHAPTER 14
System

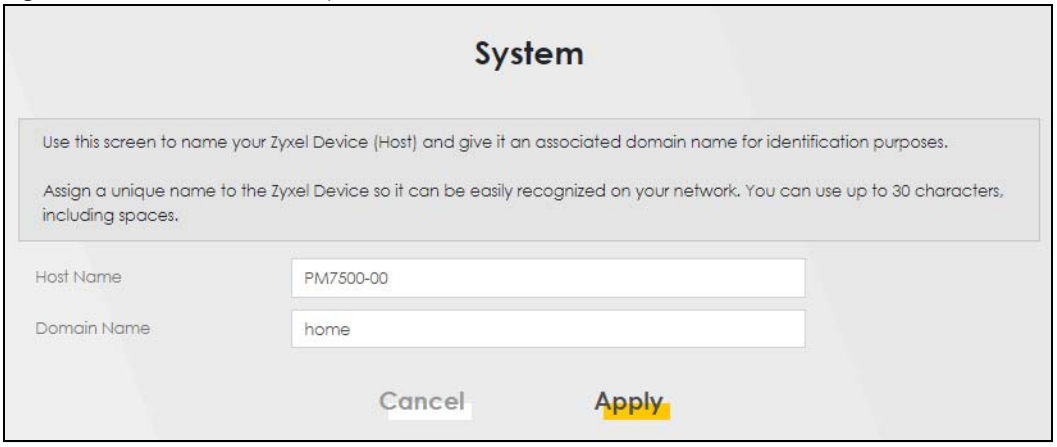
14.1 Overview

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

14.2 System

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 66 Maintenance > System



The following table describes the labels on this screen.

Table 46 Maintenance > System

LABEL	DESCRIPTION
Host Name	Enter a host name for your PM Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Domain Name	Enter a Domain name for your host PM Device for identification purpose. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Cancel	Click **Cancel** to abandon this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 15
User Account

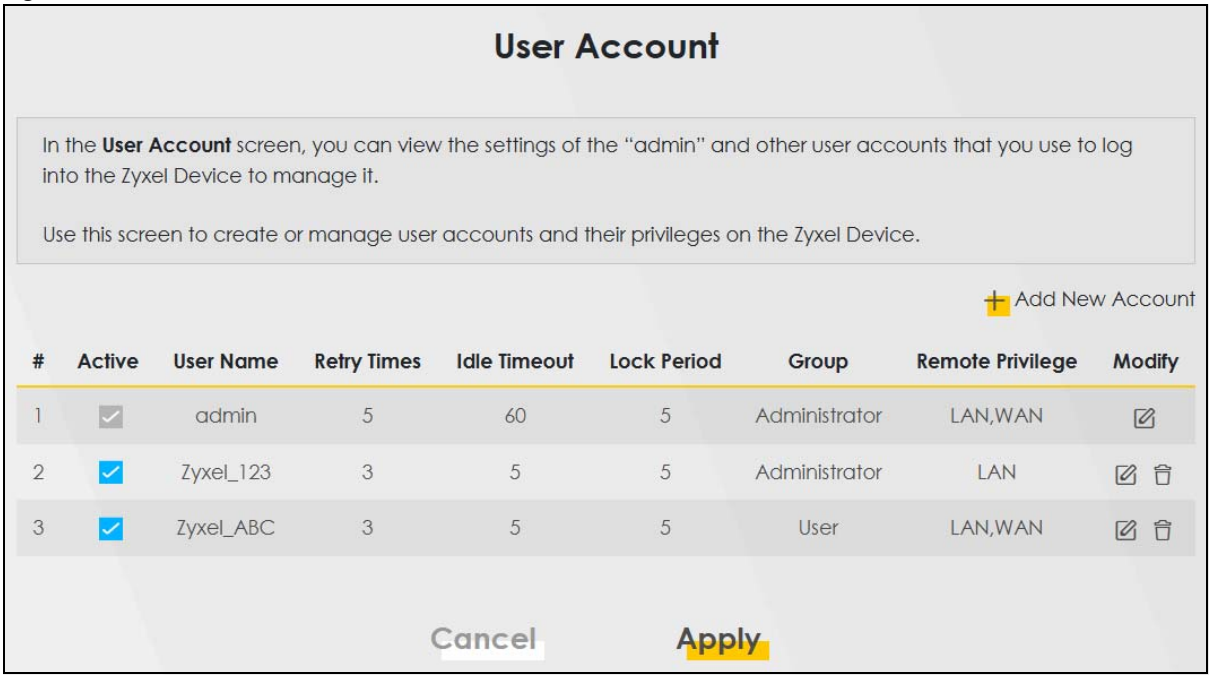
15.1 Overview

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.

15.2 User Account

Click **Maintenance** > **User Account** to open the following screen. Use this screen to create and manage user accounts and their privileges on the PM Device.

Figure 67 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 47 Administrator/User Privilege Differences

LINK	TAB	ADMINISTRATOR	USER
Connection Status			
	Connection Status	Yes	Yes
Network			
	Broadband	Yes	No
	Home Networking	Yes	No
Security			
	Certificates	Yes	No
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
	Time	Yes	Yes
	Log Setting	Yes	Yes
	Firmware Upgrade	Yes	Yes
	Backup/Restore	Yes	Yes
	Reboot	Yes	Yes

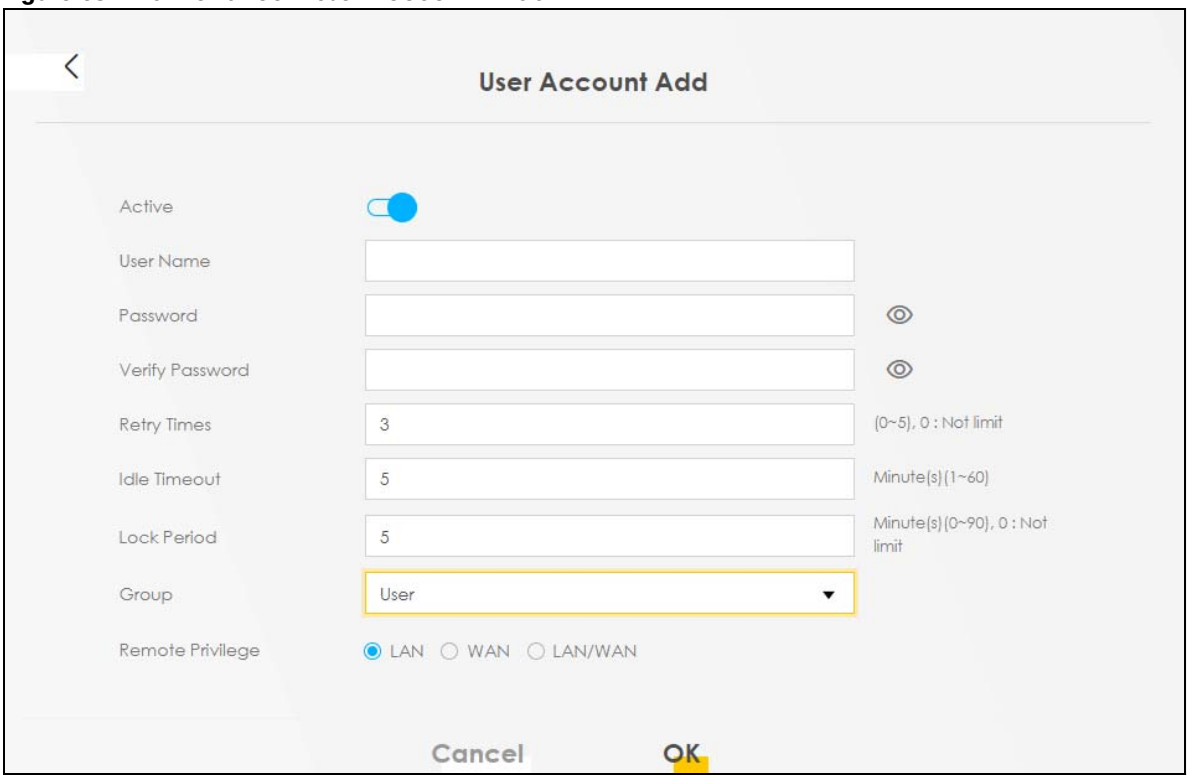
Table 48 Maintenance > User Account

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 checkbox to disable the user account. Select the checkbox 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.
Remote Privilege	This field displays whether this user can access the PM Device through the **WAN**, **LAN** or **LAN/ WAN**.
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.

15.2.1 User Account Add/Edit

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

Figure 68 Maintenance > User Account > Add



The following table describes the labels on this screen.

Table 49 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 name for this account. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Password	Enter your new system password. The password must contain at least one numeric and one alphabetic character. You can use 6 – 64 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. Note that as you enter a password, the screen displays a (*) for each character you enter. Click the eye icon to view the password. After you change the password, use the new password to access the PM Device. If you are changing your existing password, you have to first enter your **Old Password** then enter your **New Password**.
Verify Password	Enter 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.

Table 49 Maintenance > User Account > Add/Edit (continued)

LABEL	DESCRIPTION
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. An Administrator account can access all Web Configurator menus. A User account can only access Monitor and Maintenance menus. See the Administrator/User Privilege Differences on page 113 for the privileges of **Administrator** and **User**.
Remote Privilege	Select whether this user can access the PM Device through the **WAN**, **LAN** or **LAN/WAN**. Only the Administrator is allowed to use Telnet and SSH for remote management.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

CHAPTER 16
Remote Management

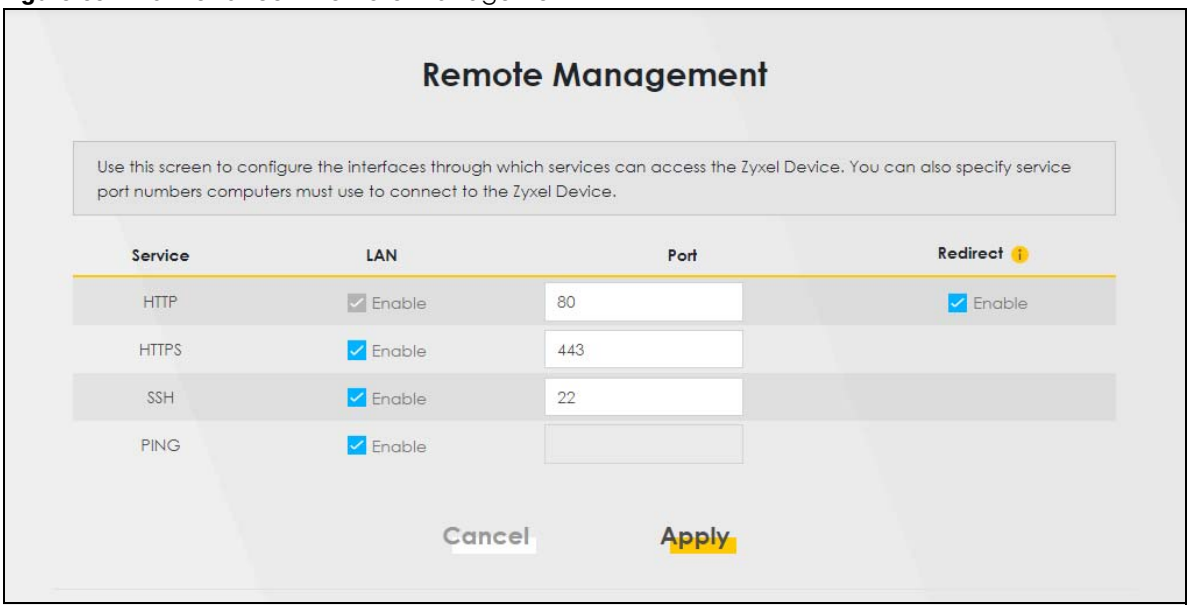
16.1 Overview

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

16.2 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** to open the following screen.

Figure 69 Maintenance > Remote Management



The following table describes the labels on this screen.

Table 50 Maintenance > Remote Management

LABEL	DESCRIPTION
Service	This is the service you may use to access the PM Device. • **HTTP** allows you to access the PM Device through a web browser. • **HTTPS** is a secured version of HTTP that provides a secure connection through encryption. • **SSH** is a secure protocol for remote command-line access. • **PING** can test if the PM Device is reachable and measure response time.
LAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the PM Device from the LAN.
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 17
Time

17.1 Overview

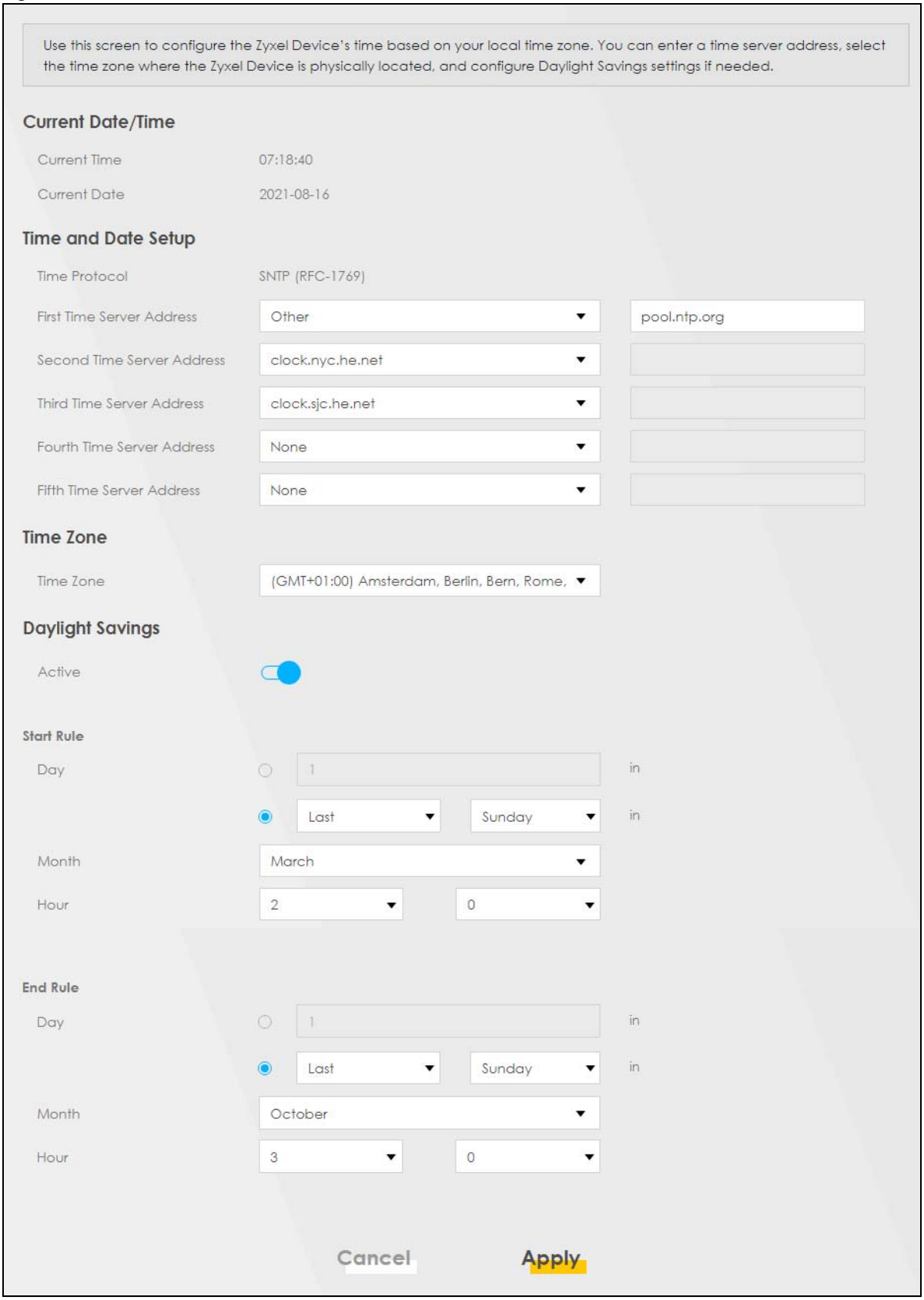
This chapter shows you how to configure the PM Device's system date and time.

17.2 Time

For effective scheduling and logging, the PM Device's system time must be accurate. Use this screen to configure the PM Device's time based on your local time zone. You can enter a time server address, select the time zone where the PM Device is physically located, and configure Daylight Savings settings if needed.

Click **Maintenance** > **Time** to open the following screen.

Figure 70 Maintenance > Time



The following table describes the labels on this screen.

Table 51 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 40 printable 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 51 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 18
Log Setting

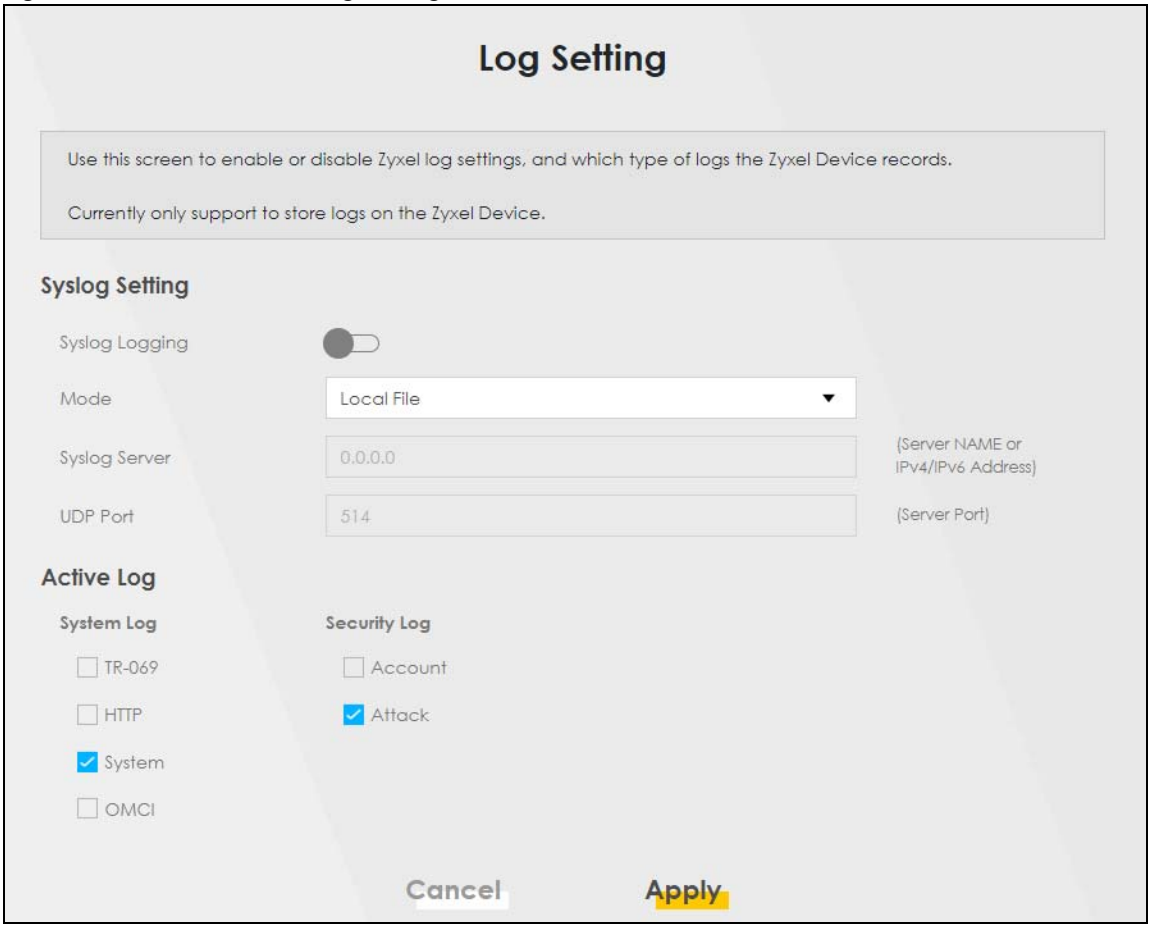
18.1 Overview

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.

18.2 Log Setting

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

Figure 71 Maintenance > Log Setting



The following table describes the fields on this screen.

Table 52 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Slide the switch to the right to enable syslog logging.
Mode	Select **Remote** to have the PM Device send it to an external syslog server. Select **Local File** to have the PM Device save the log file on the PM Device itself. Select **Local File and Remote** to have the PM Device save the log file on the PM Device itself and send it to an external syslog server. Note: A warning appears upon selecting **Remote** or **Local File and Remote**. Just click **OK** to continue.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
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.
Voice	Select **Voice** to record information related to VoIP 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 19
Firmware Upgrade

19.1 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 PM Device's performance.

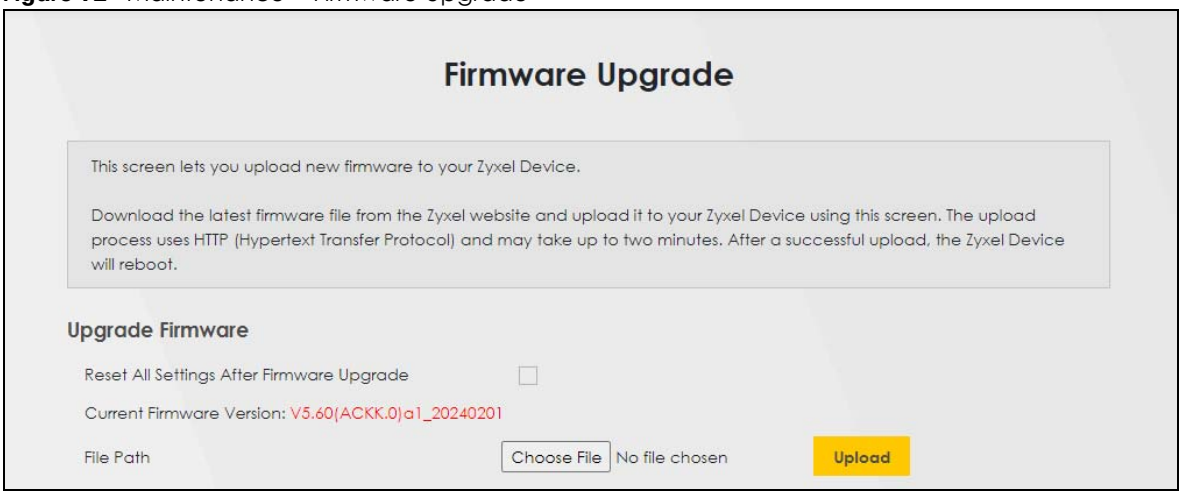
Only use firmware for your device's specific model. Refer to the label on the bottom of your PM Device.

19.2 Firmware

Click **Maintenance** > **Firmware Upgrade** to open the following screen. The upload process uses HTTPS (Hypertext Transfer Protocol) and may take up to 2 minutes. After a successful upload, the system will reboot.

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

Figure 72 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.

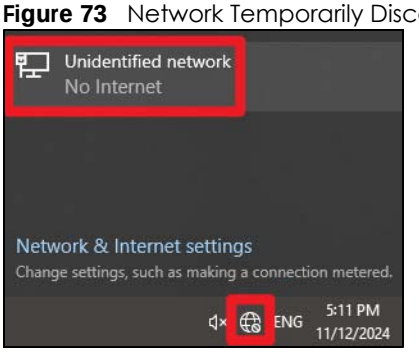
Table 53 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Reset All Settings After Firmware Upgrade	Click the checkbox 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	Enter the location of the file you want to upload in this field or click **Choose File** / **Browse** to find it.
Choose File / Browse	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 2 minutes.

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

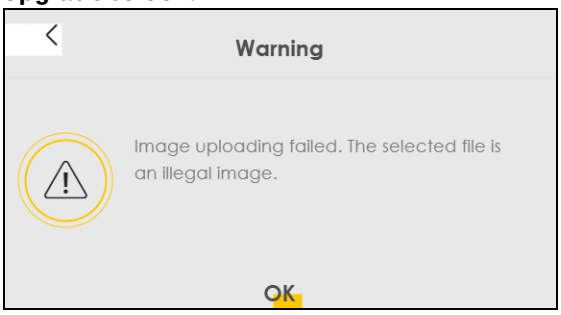
The PM Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 73 Network Temporarily Disconnected



After few 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 20
Backup/Restore

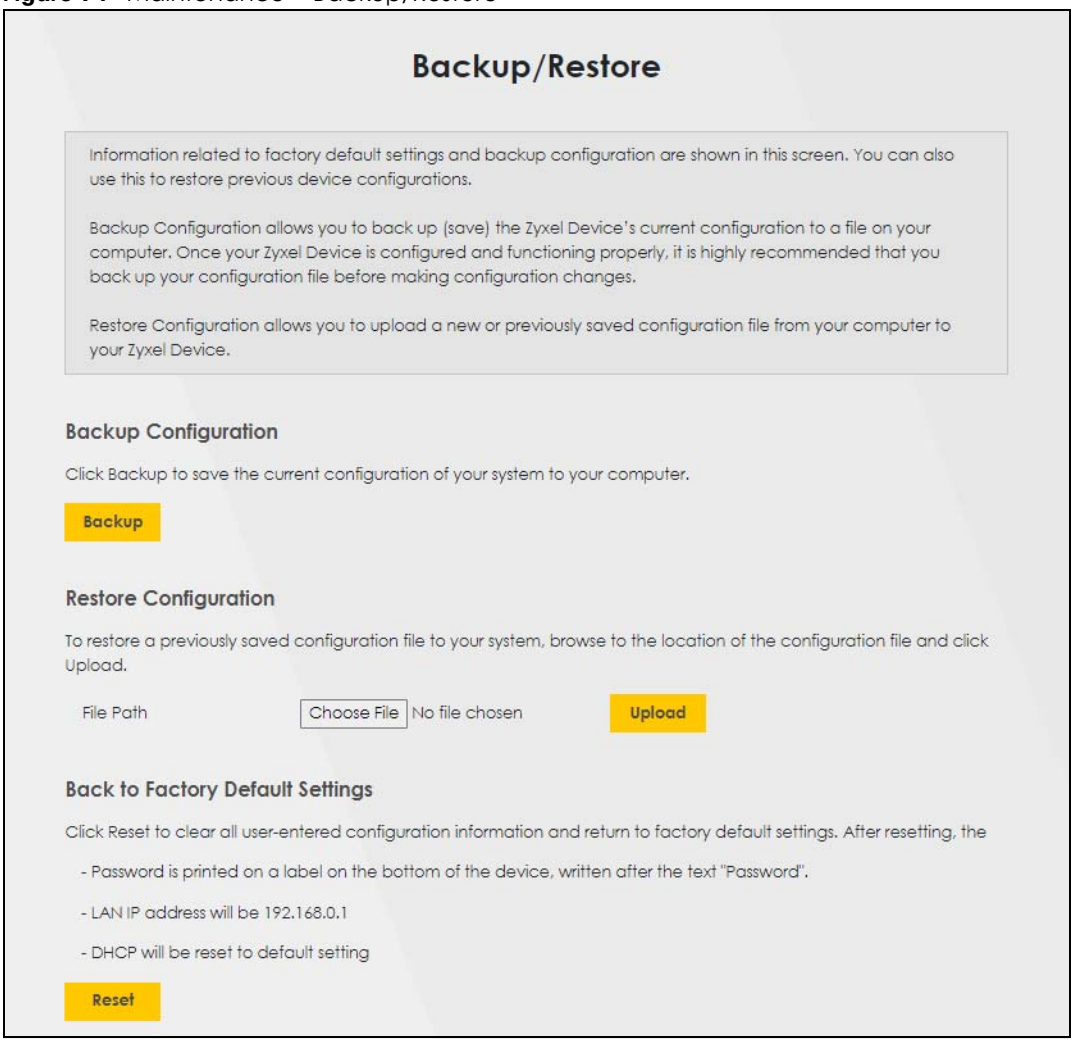
20.1 Overview

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

20.2 Backup/Restore

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

Figure 74 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 54 Restore Configuration

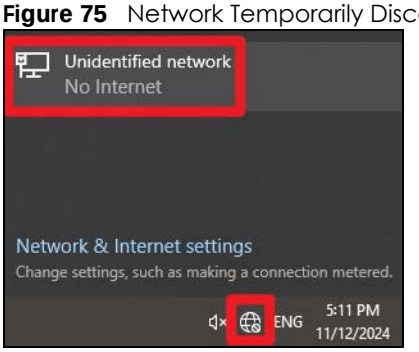
LABEL	DESCRIPTION
File Path	Enter the location of the file you want to upload in this field or click **Choose File / Browse** to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click 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 75 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.

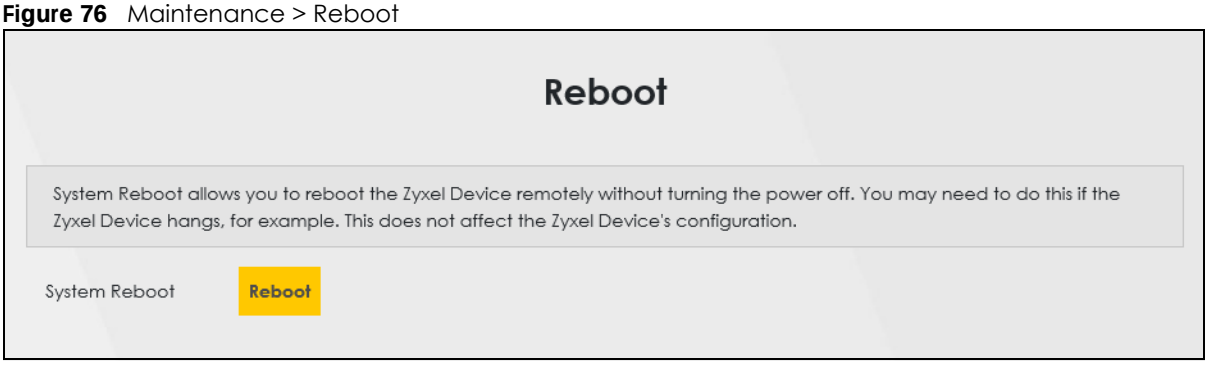
You can also press the **RESET** button on the rear panel to reset the factory defaults of your PM Device. Refer to Section 2.3.1 on page 20 for more information on the **RESET** button.

20.3 Reboot

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 76 Maintenance > Reboot



CHAPTER 21
Diagnostic

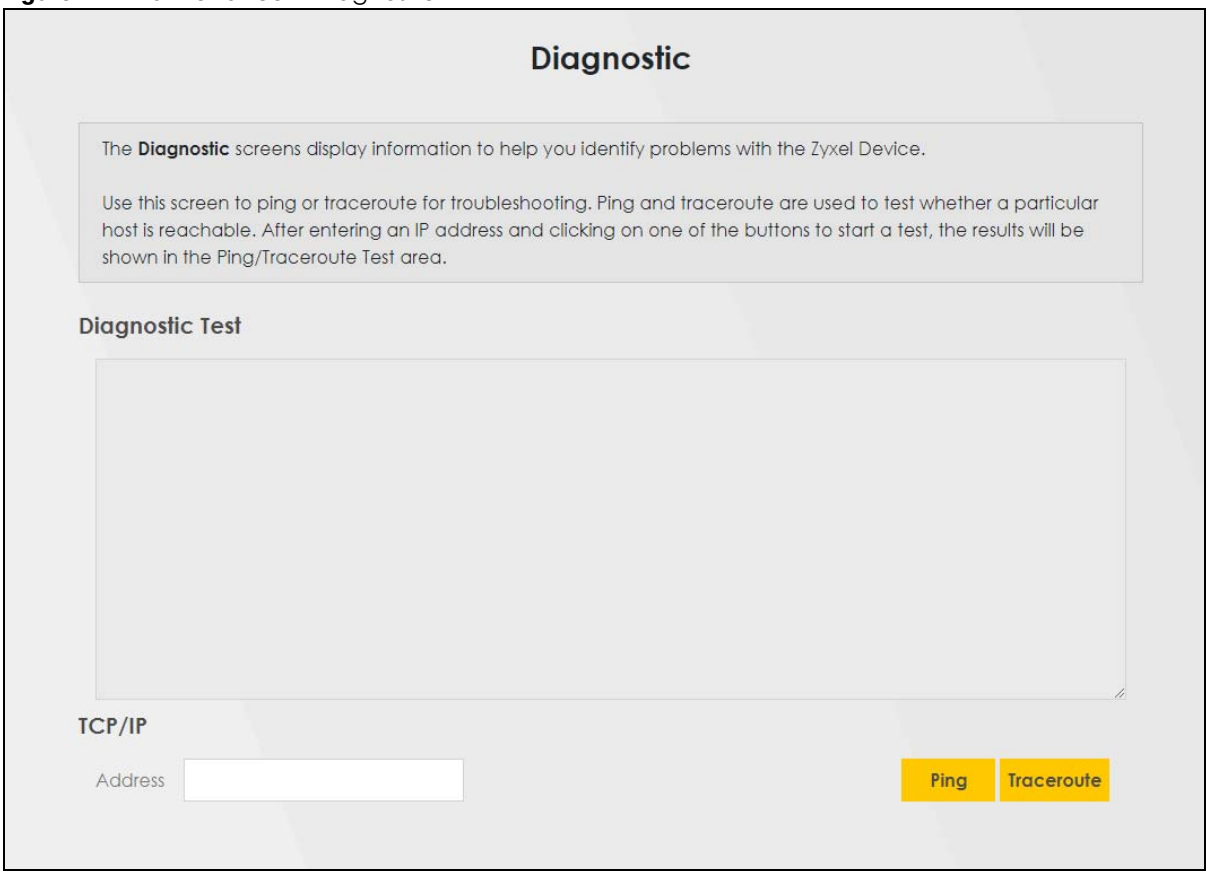
21.1 Overview

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

21.2 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 77 Maintenance > Diagnostic



The following table describes the fields on this screen.

Table 55 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.

PART III
Appendices

CHAPTER 22
Troubleshooting

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

- Accessibility and Compatibility
- Power, Hardware Connections, and LEDs
- PM Device Access and Login
- Internet Access

22.1 Accessibility and Compatibility

Screen reader not reading content

- Ensure the latest version of the screen reader is installed.
- Check if the screen reader's accessibility settings are enabled.

Web browser not displaying correctly

- Clear your web browser cache.
- Ensure that JavaScript is enabled.
- Try using a different supported web browser.

22.2 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 15.

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.

22.3 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 20.

I forgot the admin 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 15.

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 7.2 on page 56), 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. Your computer should have an IP address from192.168.0.2 to 192.168.0.254. See Section 5.2.1 on page 35.

3 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 2.2 on page 15.

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 PM Device to its factory defaults and try to access the PM Device with the default IP address. See Section 2.3.1 on page 20.

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.

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 SSH 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 22.2 on page 133.

I cannot access the PM Device through 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.

22.4 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** or Section 2.2 on page 15.

   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 15 for details about the other LEDs.

2. Disconnect all the cables from your device and reconnect them.
3. If that does not work, restart your PM Device.
4. 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 15.
3. Turn the PM Device off and on.
4. If the problem continues, contact your vendor.

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 PM 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 PM Device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

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

Korea

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

Malaysia

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Belarus

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

Belgium (Netherlands)

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

Bulgaria

- Zyxel Bulgaria

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

Czech Republic

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

Denmark

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Norway

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

Poland

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

Romania

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

Russian Federation

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

Slovakia

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

Spain

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

Sweden

- Zyxel Communications A/S
- https://www.zyxel.com/se/sv

Switzerland

- Studerus AG
- https://www.zyxel.com/ch/de-ch
- https://www.zyxel.com/fr/fr

Turkey

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

UK

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

Ukraine

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

South America

Argentina

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

Brazil

- Zyxel Communications Brasil Ltda.

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

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

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

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX B
IPv6

Overview

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

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

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

Table 56 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and cannot be assigned to a multicast group.

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

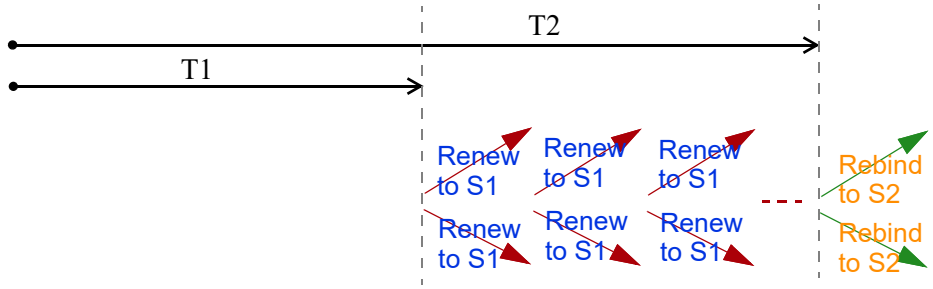
The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC	00	:	13	:	49	:	12	:	34	:	56

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The PM Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the PM Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The PM Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the PM Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the PM Device also sends out a neighbor solicitation message. When the PM Device receives a

neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the PM Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The PM Device creates an entry in the default router list cache if the router can be used as a default router.

When the PM Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the PM Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the PM Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the PM Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the PM Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

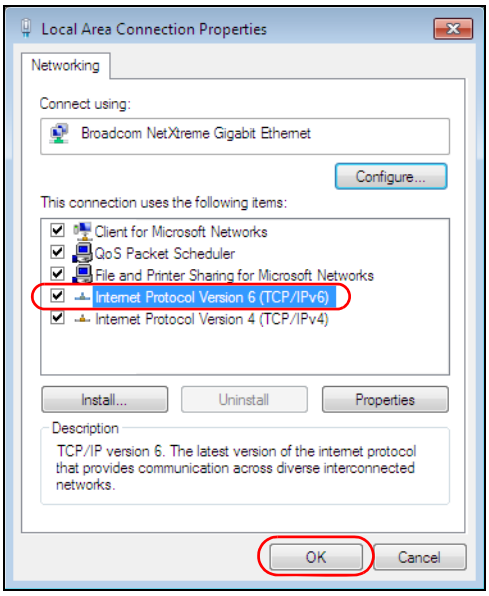
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1. Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.
2. Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
3. Click **OK** to save the change.



4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

APPENDIX C
Legal Information

Copyright

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America

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

FCC EMC Statement

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

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

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Caution

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.

Canada

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

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES(B) / NMB(B)

Europe and the United Kingdom

The following information applies if you use the product within the European Union 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.ibpt.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 cerințele esențiale 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
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.
- The Power Supply is not waterproof, avoid contact with liquid. Handle the Power Supply with care; do not pry open, nor pull or press the pins on it.
- 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. 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.

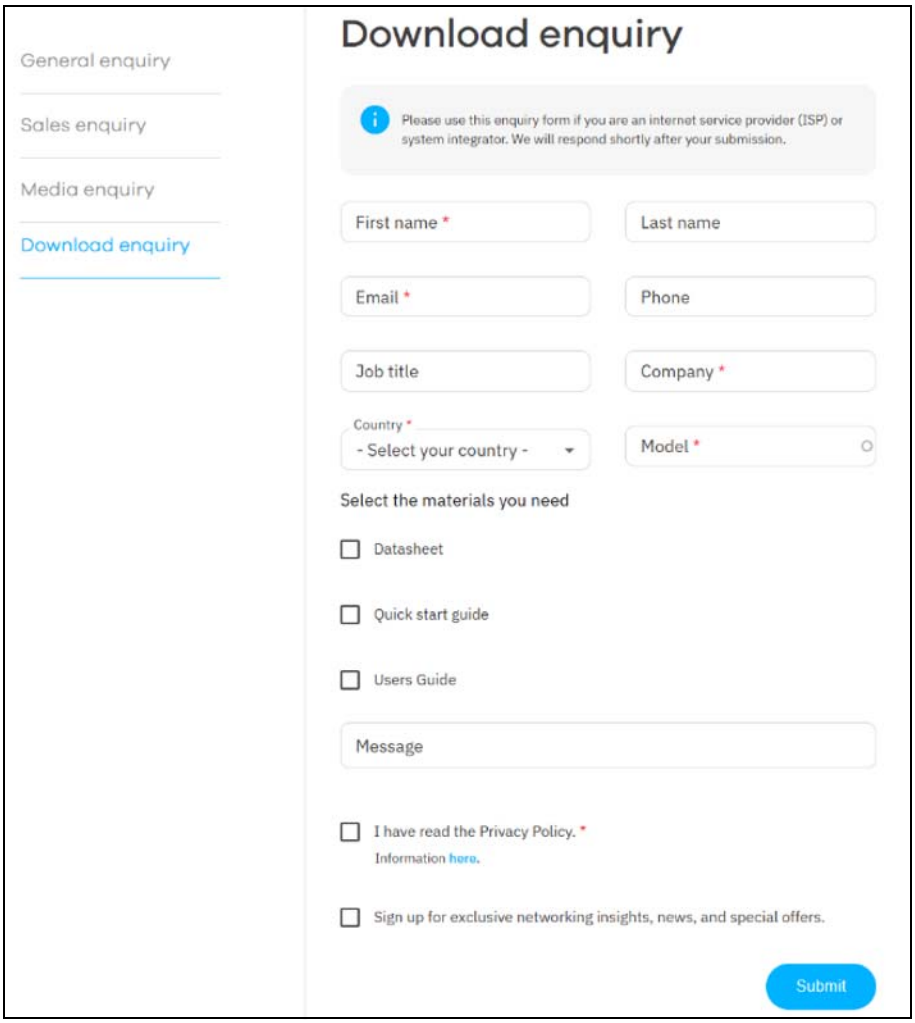
Note

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.

Enquiries

Go to *https://www.zyxel.com/service-provider/global/en/download-enquiry* to request a User's Guide for configuration assistance and related safety warnings.



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

Numbers

A

B

C

D

E

F

G

I

K

L

M

N

O

P

Q

R

S

T

U

V

W