

User's Guide

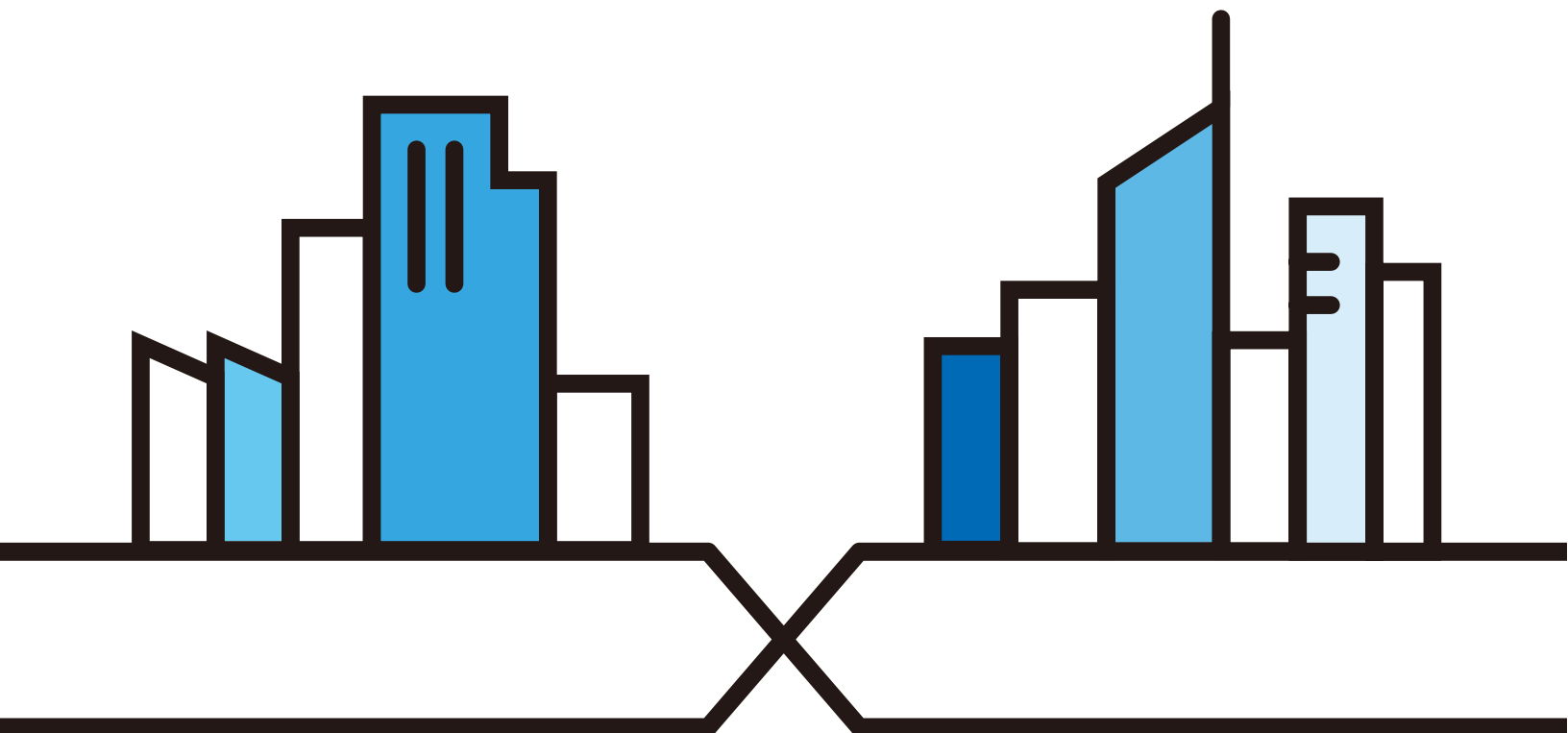
PM Series

XGS-PON SFU with 10G LAN / G-PON SFU with 2.5G LAN

Default Login Details

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

Version 5.42/5.61 Ed 3, 11/2024



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

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

- More Information

Go to <https://service-provider.zyxel.com/global/en/tech-support> to find other information on 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 

Contents Overview

User's Guide	10
Introduction	11
Hardware Panels	14
The Web Configurator	19
Connection Status	26
Web Tutorials	32
Technical Reference	39
Broadband	40
Home Networking	52
Certificates	54
Log	63
Traffic Status	66
Optical Signal Status	69
System	71
User Account	72
Remote Management	76
Time	78
Log Setting	82
Firmware Upgrade	84
Backup/Restore	86
Diagnostic	90
Appendices	92
Troubleshooting	93

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	5
 Part I: User's Guide.....	 10
Chapter 1	
Introduction	11
1.1 Overview	11
1.2 Example Application	12
1.2.1 Multi-Gigabit Ethernet	12
1.3 Ways to Manage the PM Device	13
1.4 Good Habits for Managing the PM Device	13
Chapter 2	
Hardware Panels.....	14
2.1 Overview	14
2.2 LEDs Indicator Panel	14
2.2.1 PM7300-T0 and PM7500-00	14
2.2.2 PM5100-T1	15
2.3 Rear Panel Ports and Buttons	16
2.3.1 RESET Button	17
Chapter 3	
The Web Configurator.....	19
3.1 Overview	19
3.2 Accessing the Web Configurator	19
3.3 Web Configurator Layout	21
3.3.1 Setting Icon	21
Chapter 4	
Connection Status.....	26
4.1 Overview	26
4.1.1 Layout Icon	26
4.2 Connectivity Panel	27
4.3 System Info Panel	28

4.4 LAN Panel	30
Chapter 5	
Web Tutorials	32
5.1 Overview	32
5.2 Device Settings	32
5.2.1 How to Change an Interface IP	32
5.2.2 How to Rename Your Device	33
5.2.3 How to Change the Admin Password	34
5.3 Traffic Usage	35
5.3.1 How to View the Interface Status	35
5.3.2 How to View the WAN Station Status	36
5.3.3 How to View the LAN Station Status	36
5.4 Device Maintenance	36
5.4.1 How to Upgrade the Firmware	37
5.4.2 How to Back Up the Device Configuration	37
5.4.3 How to Restore the Device Configuration	37
5.4.4 How to Reset the PM Device to the Factory Defaults	38
5.5 System Log	38
5.5.1 How to View Logs	38
 Part II: Technical Reference.....	 39
Chapter 6	
Broadband.....	40
6.1 Overview	40
6.1.1 What You Can Do in this Chapter	40
6.1.2 What You Need to Know	40
6.1.3 Before You Begin	42
6.2 Broadband	42
6.2.1 Add or Edit Internet Connection	43
6.3 Technical Reference	49
Chapter 7	
Home Networking.....	52
7.1 Overview	52
7.1.1 What You Can Do in this Chapter	52
7.1.2 What You Need To Know	52
7.2 LAN Setup	52
Chapter 8	
Certificates	54

8.1 Overview	54
8.1.1 What You Can Do in this Chapter	54
8.1.2 What You Need to Know	54
8.2 Local Certificates	54
8.2.1 Create Certificate Request	56
8.2.2 View Certificate Request	56
8.3 Trusted CA	58
8.3.1 Import Trusted CA Certificate	58
8.3.2 View Trusted CA Certificate	59
8.4 Technical Reference	60
8.4.1 Verify a Certificate	61
Chapter 9	
Log.....	63
9.1 Overview	63
9.1.1 What You Can Do in this Chapter	63
9.1.2 What You Need To Know	63
9.2 System Log	64
9.3 Security Log	65
Chapter 10	
Traffic Status.....	66
10.1 Overview	66
10.1.1 What You Can Do in this Chapter	66
10.2 WAN Traffic Status	66
10.3 LAN Status	67
Chapter 11	
Optical Signal Status.....	69
11.1 Overview	69
11.2 Optical Signal Status	69
Chapter 12	
System.....	71
12.1 Overview	71
12.2 System	71
Chapter 13	
User Account.....	72
13.1 Overview	72
13.2 User Account	72
13.2.1 User Account Add/Edit	74

Chapter 14	
Remote Management	76
14.1 Overview	76
14.2 MGMT Services	76
Chapter 15	
Time	78
15.1 Overview	78
15.2 Time	78
Chapter 16	
Log Setting	82
16.1 Overview	82
16.2 Log Setting	82
Chapter 17	
Firmware Upgrade	84
17.1 Overview	84
17.2 Firmware	84
Chapter 18	
Backup/Restore	86
18.1 Overview	86
18.2 Backup/Restore	86
18.3 Reboot	89
Chapter 19	
Diagnostic.....	90
19.1 Overview	90
19.2 Diagnostic	90
Part III: Appendices	92
Chapter 20	
Troubleshooting.....	93
20.1 Power, Hardware Connections, and LEDs	93
20.2 PM Device Access and Login	94
20.3 Internet Access	95
Appendix A Customer Support	97
Appendix B IPv6.....	102

Appendix C Legal Information	108
Index	113

PART I

User's Guide

CHAPTER 1

Introduction

1.1 Overview

This chapter introduces the main features and applications of the PM Devices. The PM Devices are the PON (Passive Optical Network) modems that connect to the Internet through a fiber cable.

The PM Device refers to the following models:

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

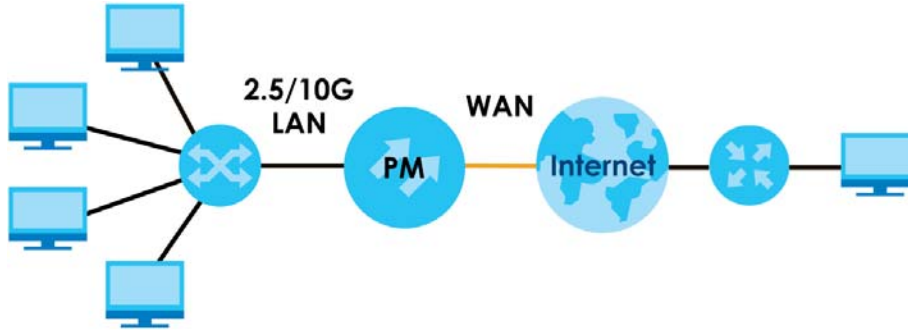
Table 1 PM Device Comparison Table

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



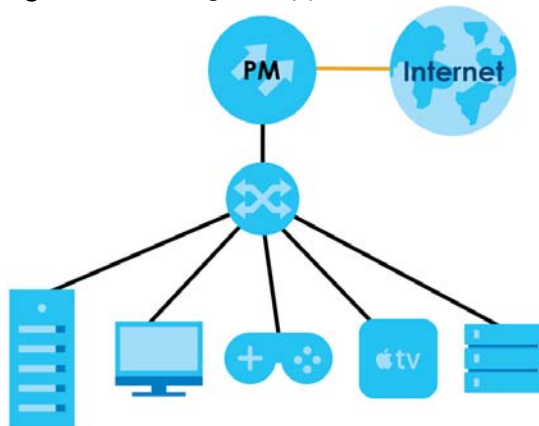
1.2.1 Multi-Gigabit Ethernet

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 11](#) 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 12](#) 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 11](#) 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

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 100m 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 PM7300-T0 and PM7500-00

Figure 3 PM7300-T0 and PM7500-00



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

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

LED	COLOR	STATUS	DESCRIPTION
Power 	Green	On	The PM Device is ready for use.
		Blinking	The PM Device is booting.
		Off	The PM Device is not receiving power.
	Red	On	There is a system failure.
		Blinking	The firmware upgrade is in progress.
PON 	Green	On	The PON connection is ready.
		Blinking	The PM Device is trying to establish a link.
		Off	The fiber link is down.
LOS 	Red	On	PON transceiver is powered down.
		Blinking	This is a R(x) low power alarm.
		Off	The PON connection is working normally.
10GbE 10GE 	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 PM5100-T1

Figure 4 PM5100-T1



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

Table 4 PM5100-T1's LED Behavior

LED	COLOR	STATUS	DESCRIPTION
Power 	Green	On	The PM Device is ready for use.
		Blinking	The PM Device is booting.
		Off	The PM Device is not receiving power.
	Red	On	There is a system failure.
		Blinking	The firmware upgrade is in progress.
PON 	Green	On	The PON connection is ready.
		Blinking	The PM Device is trying to establish a link.
		Off	The fiber link is down.
LOS 	Red	On	PON transceiver is powered down.
		Blinking	This is a R(x) low power alarm.
		Off	The PON connection is working normally.
2.5GbE 	Green	On	The Ethernet link is up.
		Blinking	The PM Device is transmitting or receiving data.
		Off	The Ethernet link is down.

2.3 Rear Panel Ports and Buttons

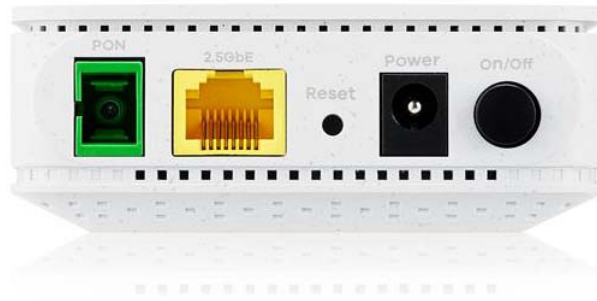
The following shows the PM Device rear panel with ports and buttons.

Figure 5 PM7300-T0



Figure 6 PM7500-00



Figure 7 PM5100-T1

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

Table 5 Rear Panel Ports and Buttons

LABELS	DESCRIPTION
RESET	Press for 5 seconds to restore the PM Device to its factory default settings.
PON	Connect the PM Device to the Internet using a fiber cable.
10GbE / 2.5 GbE	Connect the PM Device to an Ethernet device such as a network switch, NAS or server. Connect a computer for initial configuration.
POWER	Connect the power adapter and press the POWER button to start the PM Device.
ON/OFF	Press the ON/OFF button after connecting the power adapter to start the PM Device.

2.3.1 RESET Button

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

- 1 Make sure the PM Device is connected to power and the **POWER** LED is on.
- 2 Using a thin item, press the **RESET** button for more than 5 seconds.

The following shows the PM Device **RESET** buttons.

Figure 8 Reset Button (PM7300-T0)

Figure 9 Reset Button (PM7500-00)

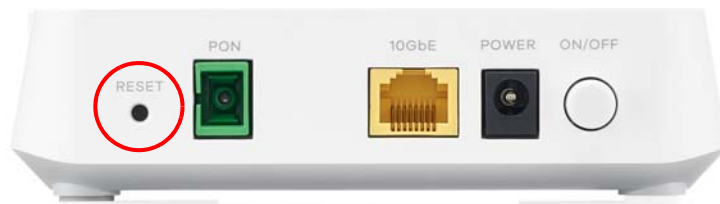
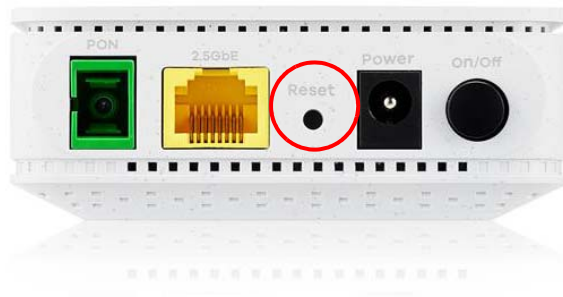


Figure 10 Reset Button (PM5100-T1)



CHAPTER 3

The Web Configurator

3.1 Overview

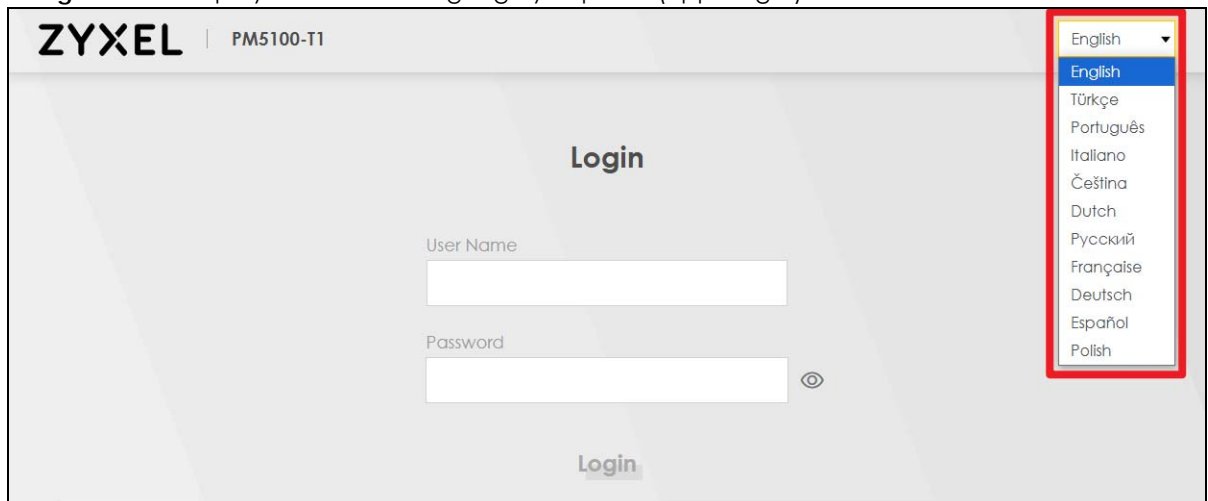
The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Internet Explorer 11, Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768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

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

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

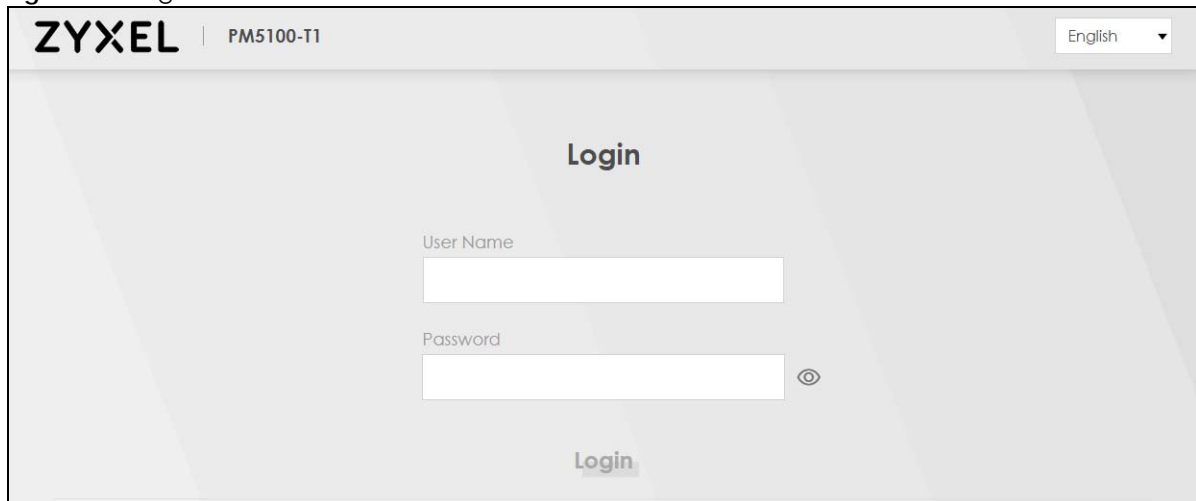
3.2 Accessing the Web Configurator

- 1 Make sure your PM Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Manually configure your computer's IP address to be in the range 192.168.0.2~192.168.0.254 with subnet mask 255.255.255.0.
- 3 Manually configure Launch your web browser and go to <https://192.168.0.1>.
- 4 A **Login** screen displays. Select the language you prefer (upper right).



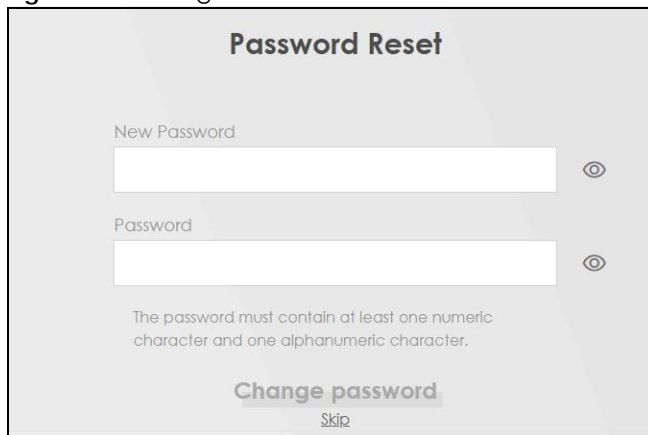
- 5 To access the administrative Web Configurator and manage the PM Device, type the default username **admin** and the randomly assigned default password (see the device label) in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 11 Login Screen

The image shows the login screen of a ZyXEL PM5100-T1 device. At the top left, the 'ZYXEL' logo is displayed next to the model number 'PM5100-T1'. At the top right, there is a language dropdown menu set to 'English'. The main heading in the center is 'Login'. Below this, there are two input fields: 'User Name' and 'Password'. The 'Password' field has a toggle icon (an eye) to its right. At the bottom center, there is a 'Login' button.

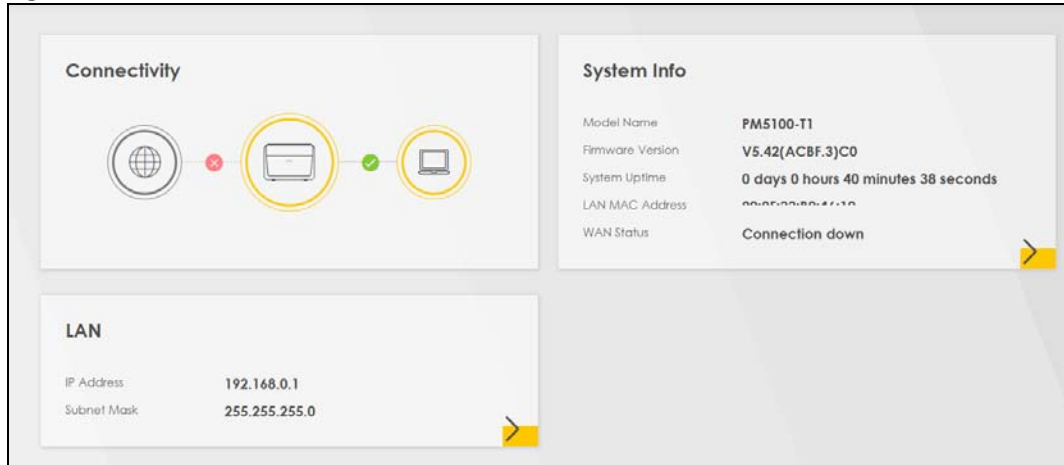
- 6 The following screen displays if you have not yet changed your password. Enter a new password, retype it to confirm and click **Apply**.

Figure 12 Change Password Screen

The image shows the 'Password Reset' screen. The title 'Password Reset' is at the top. Below it, there are two input fields: 'New Password' and 'Password'. Both fields have toggle icons (eyes) to their right. Below the 'Password' field, there is a note: 'The password must contain at least one numeric character and one alphanumeric character.' At the bottom, there are two buttons: 'Change password' and 'Skip'.

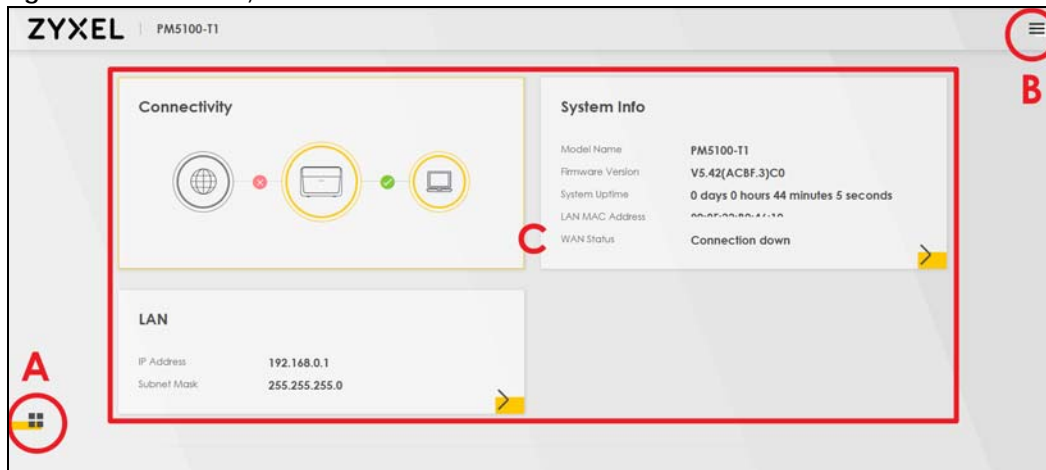
- 7 The **Connection Status** screen displays (see [Chapter 4 on page 26](#) for details about it).

Figure 13 PM Device Connection Status



3.3 Web Configurator Layout

Figure 14 Screen Layout



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

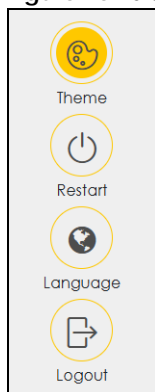
- **A** - Settings Icon (Navigation Panel and Side bar)
- **B** - Layout Icon
- **C** - Main Window

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


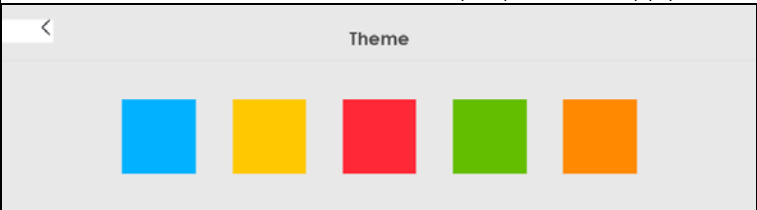



3.3.1.1 Side Bar

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

Figure 15 Side Bar

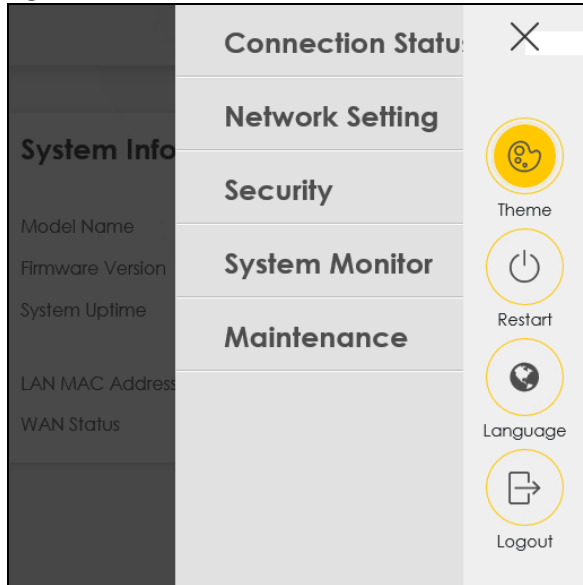
The icons provide the following functions.

Table 6 Navigation Panel Quick Link Icons

ICON	DESCRIPTION
 Theme	Theme: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
 Restart	Restart: Click this icon to reboot the PM Device without turning the power off.
 Language	Language: Select the language you prefer.
 Logout	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 16 Navigation Panel

The following tables describe each menu item.

Table 7 Navigation Panel Menus Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the PM Device and connected devices.
Networking Setting		
Broadband	Broadband	Use this screen to view the PM Device's WAN connections.
Home Networking	LAN 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.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the PM Device. You can export or e-mail the logs.
	Security Log	Use this screen to see the PM Device's security-related logs.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the PM Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the PM Device.
Optical Signal Status	Optical Signal Status	Use this screen to view the fiber transceiver's TX power and RX power level and its temperature.
Maintenance		
System	System	Use this screen to set Host name and Domain name of the PM Device.
User Account	User Account	Use this screen to change the user password or add user accounts on the PM Device.

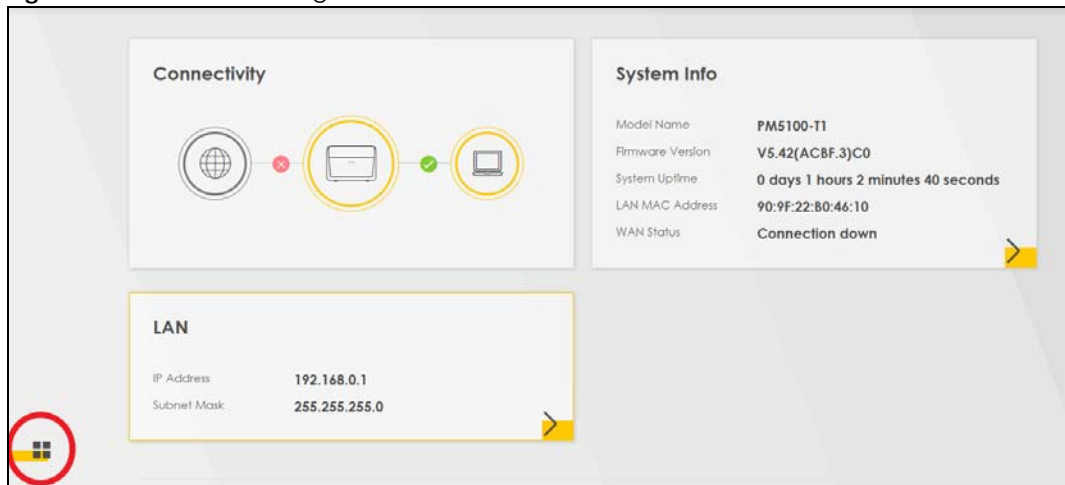
Table 7 Navigation Panel Menus Summary (continued)

LINK	TAB	FUNCTION
Remote Management	MGMT Services	Use this screen to configure which services can access the PM Device and which interfaces can allow them.
	Trust Domain	Use this screen to manage a list of IP addresses which are allowed to access the PM Device through the services configured in the Maintenance > Remote Management screen.
Time	Time	Use this screen to change your PM Device's time and date settings.
Log Setting	Log Setting	Use this screen to change your PM Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your PM Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your PM Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the PM Device without turning the power off.
Diagnostic	Diagnostic	Use this screen to identify problems with the PON connection. Use ping and traceroute to test whether the PM Device can reach a particular host.

3.3.1.3 Widget Icon

Click the Widget icon (🧩) in the lower left corner to arrange the screen order.

Figure 17 Dashboard Widget



The following screen appears. Select a block and hold it to move around. Click the Check icon (✅) in the lower left corner to save the changes.

Figure 18 Check Icon



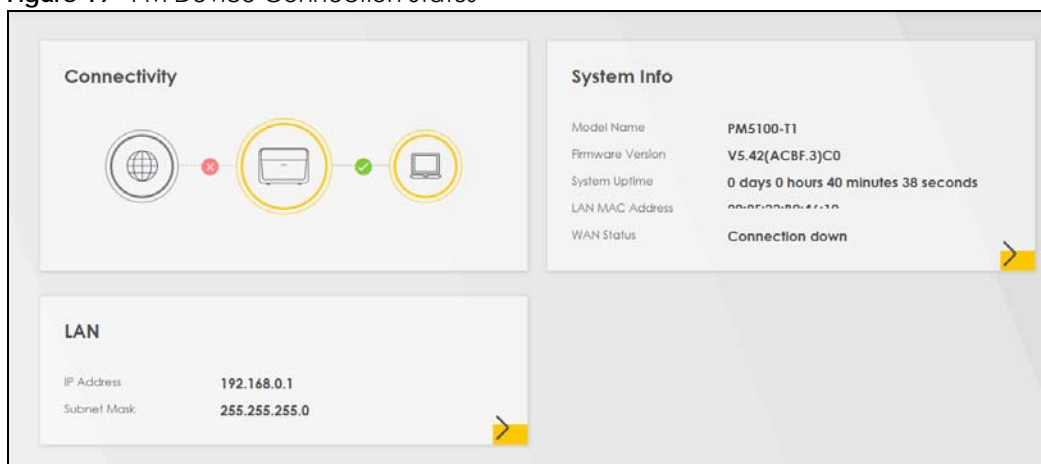
CHAPTER 4

Connection Status

4.1 Overview

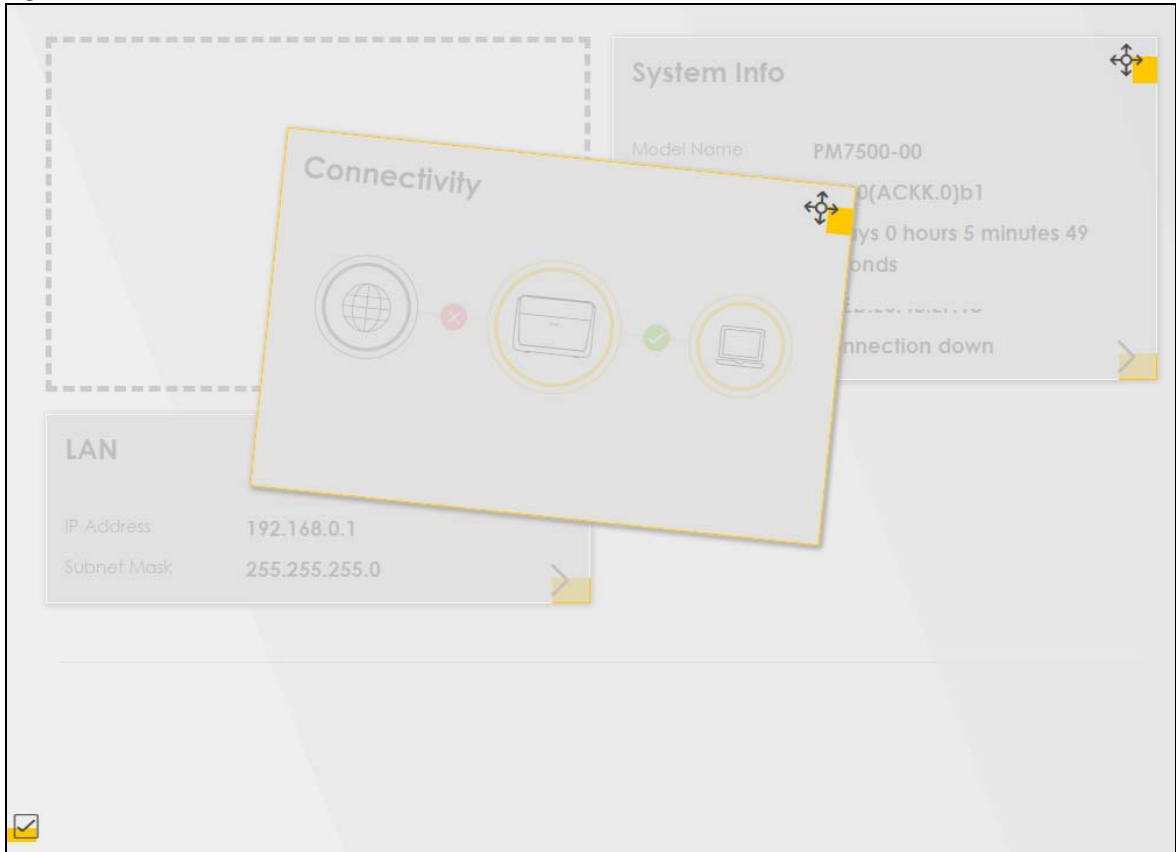
The **Connection Status** screen appears when you log into the Web Configurator or click **Connection Status** in the navigation panel. This screen shows the network status of the PM Device and information about the connected computers and devices, and lets you configure some basic settings.

Figure 19 PM Device Connection Status



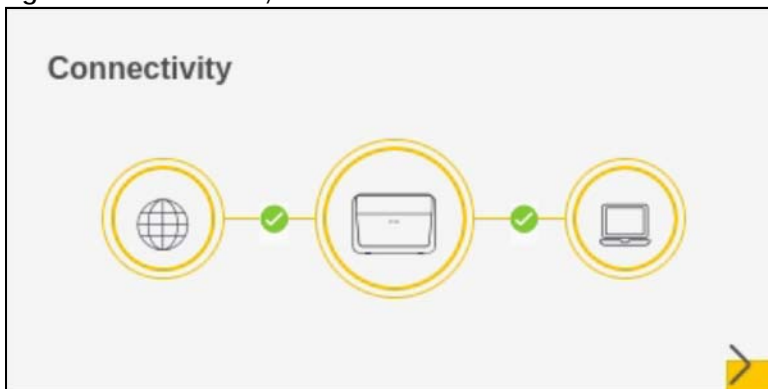
4.1.1 Layout Icon

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 20 Changing Connection Status Screen Layout

4.2 Connectivity Panel

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

Figure 21 Connectivity


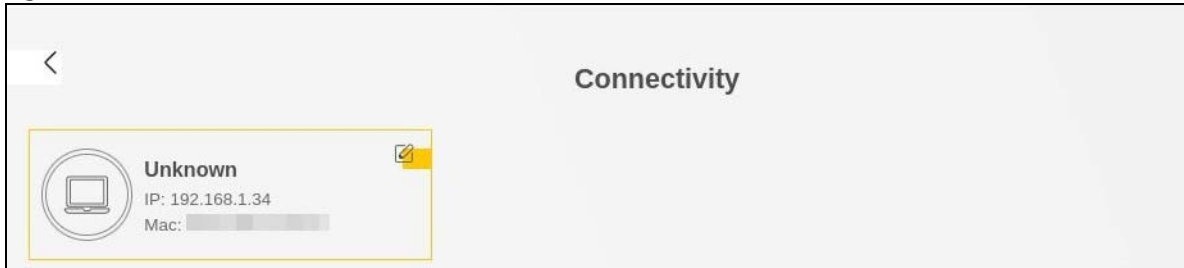
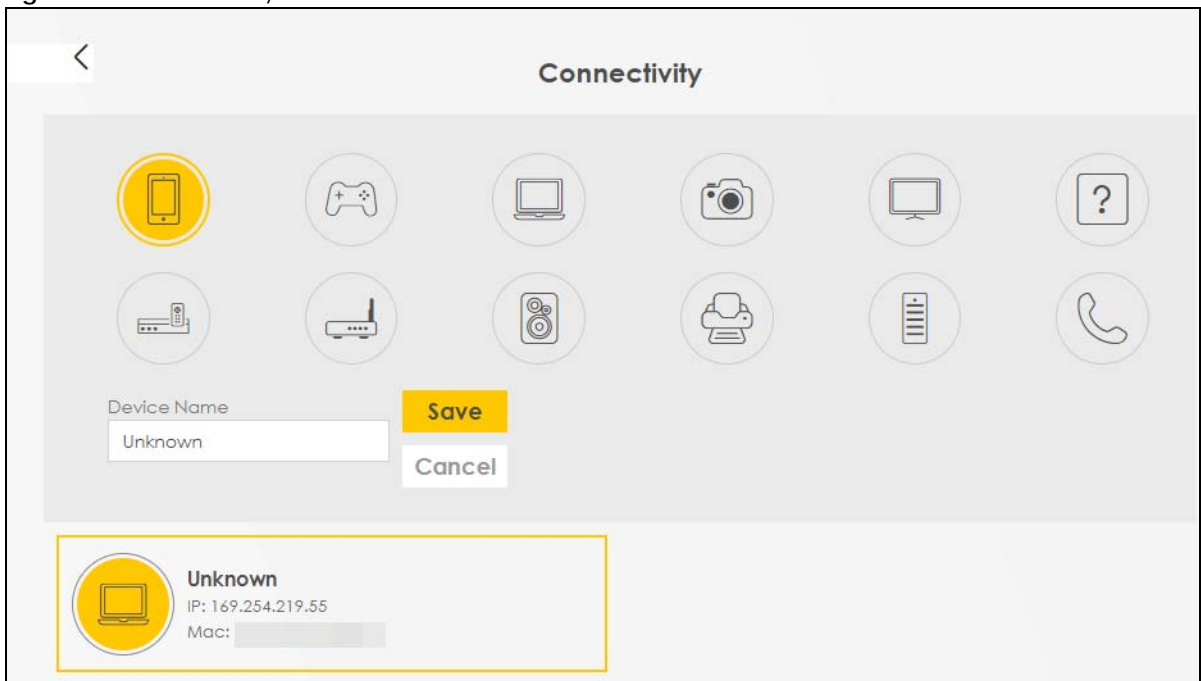
Click the **Arrow** icon () to open the following screen. Use this screen to view the IP addresses and MAC addresses of the devices connected to the PM Device.

Figure 22 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 23 Connectivity: Edit

4.3 System Info Panel

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

Figure 24 System Info


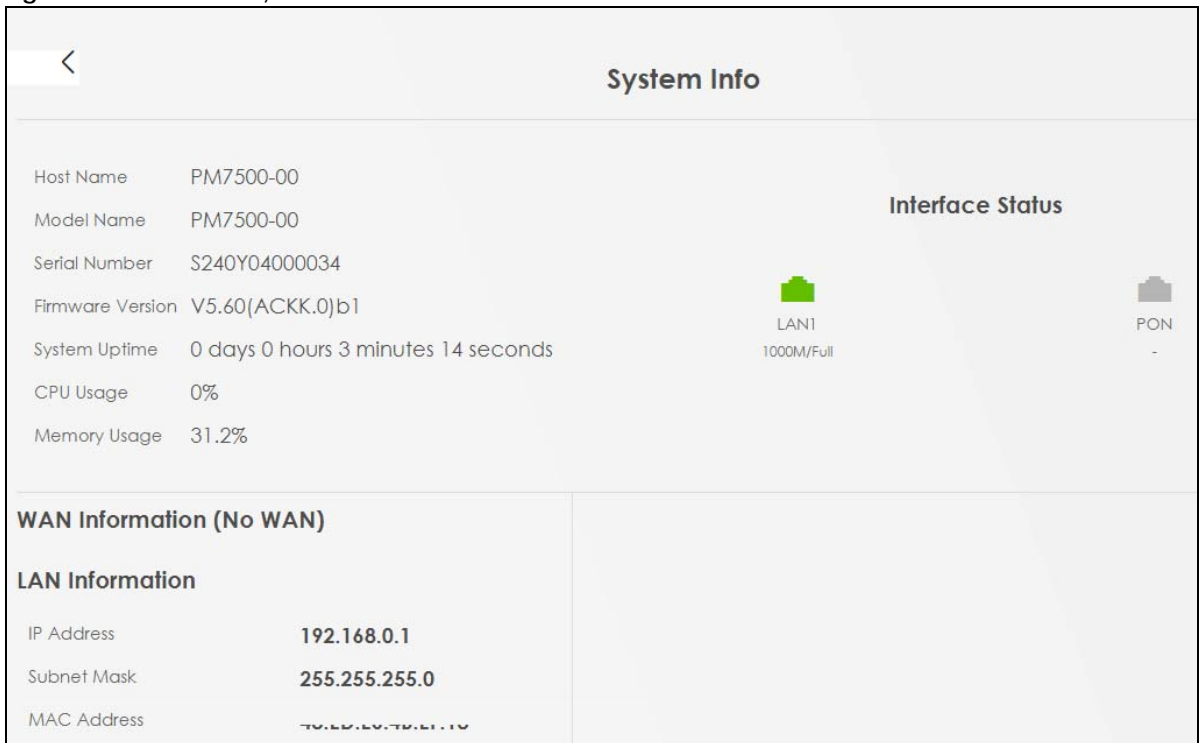
Click the **Arrow** icon () to open the following screen with more information.

Figure 25 Details for System Information

The following table describes the labels in this screen.

Table 8 System Info: Detailed Information

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

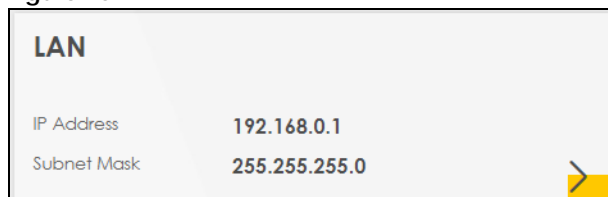
Table 8 System Info: Detailed Information (continued)

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

4.4 LAN Panel

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

Figure 26 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 27 LAN Setup

The screenshot shows a web interface for LAN setup. At the top, there is a back arrow and the title 'LAN'. Below this is a section titled 'LAN IP Setup'. It contains two input fields: 'IP Address' with the value '192 . 168 . 0 . 1' and 'Subnet Mask' with the value '255 . 255 . 255 . 0'. At the bottom right, there is a yellow 'Save' button.

The following table describes the labels in this screen.

Table 9 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](#)

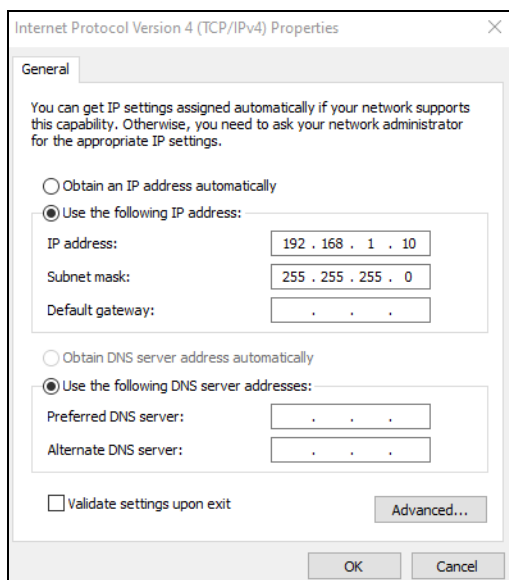
5.2 Device Settings

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

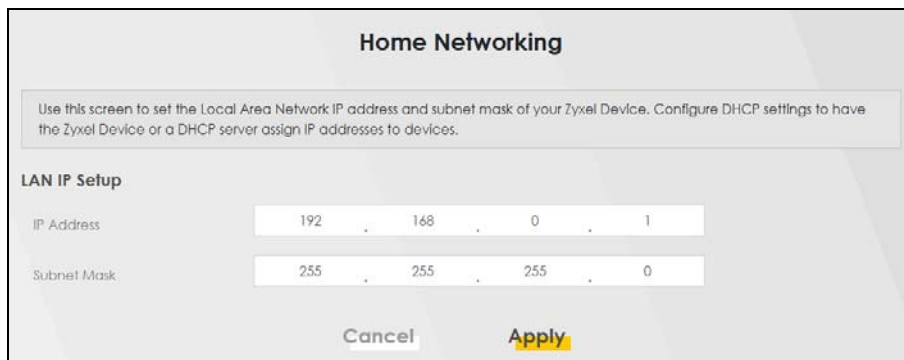
5.2.1 How to Change an Interface IP

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.

System

Use this screen to name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Host Name: PM5100_ABC

Domain Name: home

Cancel Apply

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

System Info

Host Name: PM5100-ABC

Model Name: PM5100-T1

Serial Number: 000000000000

Firmware Version: V5.42(ACBF.3)C0

System Uptime: 0 days 0 hours 10 minutes 55 seconds

CPU Usage: 31%

Memory Usage: 67.5%

Interface Status

LAN1: 1000M/Full

PON: -

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.

User Account

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

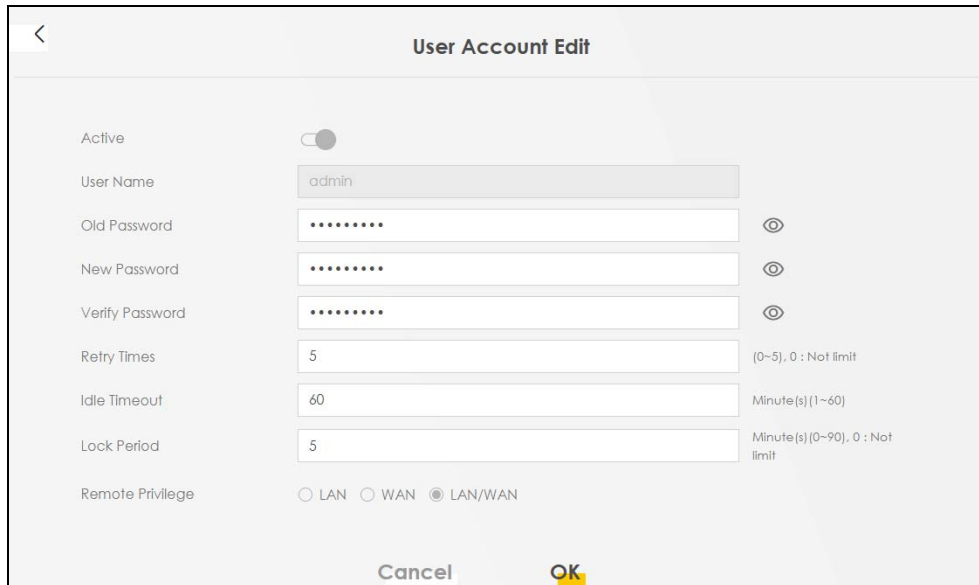
Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

+ Add New Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Remote Privilege	Modify
1	<input checked="" type="checkbox"/>	admin	5	60	5	Administrator	LAN, WAN	

Cancel Apply

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



The 'User Account Edit' form contains the following fields and options:

- Active:** A toggle switch currently turned on.
- User Name:** A text field containing 'admin'.
- Old Password:** A password field with masked characters and a visibility icon.
- New Password:** A password field with masked characters and a visibility icon.
- Verify Password:** A password field with masked characters and a visibility icon.
- Retry Times:** A text field with '5', with a note '(0~5), 0 : Not limit'.
- Idle Timeout:** A text field with '60', with a note 'Minute(s) (1~60)'.
- Lock Period:** A text field with '5', with a note 'Minute(s) (0~90), 0 : Not limit'.
- Remote Privilege:** Radio buttons for LAN, WAN, and LAN/WAN (which is selected).

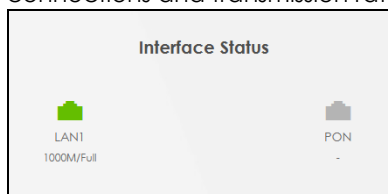
At the bottom are 'Cancel' and 'OK' buttons.

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.

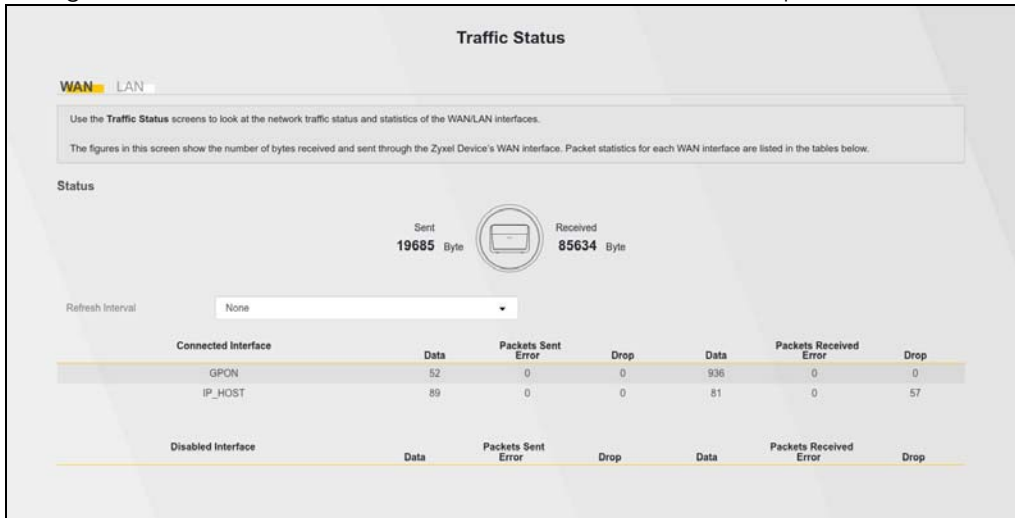
5.3.1 How to View the Interface Status

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



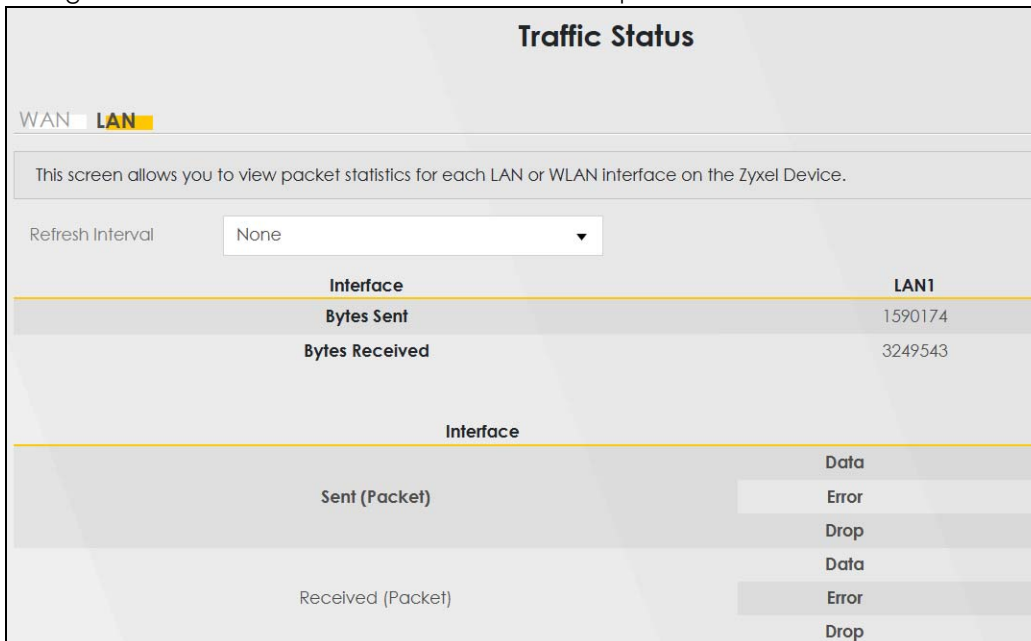
5.3.2 How to View the WAN Station Status

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.



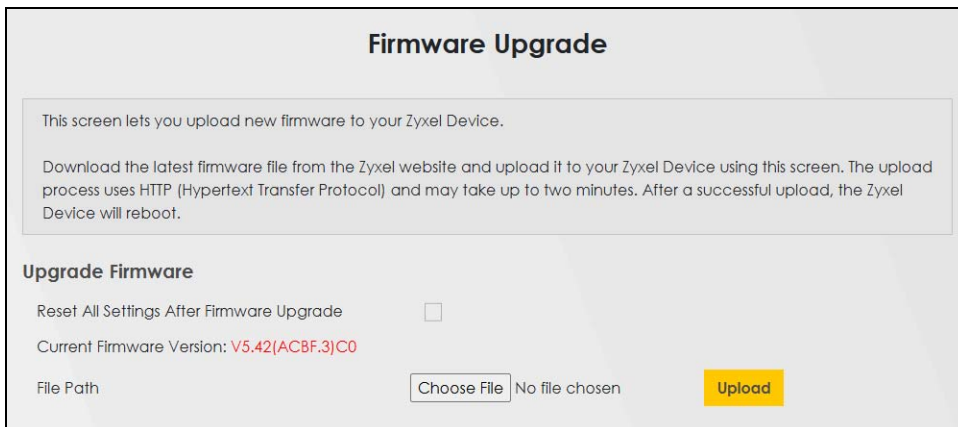
5.4 Device Maintenance

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**.

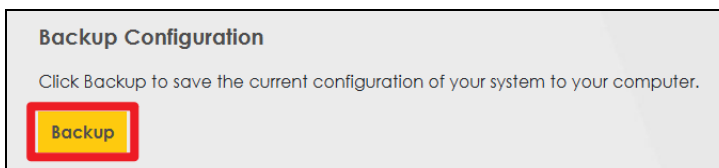


- 4 This process may take up to 2 minutes to finish. After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

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**.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path

Choose File
No file chosen

Upload

- 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.

Back to Factory Default Settings

Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.0.1
- DHCP will be reset to default setting

Reset

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

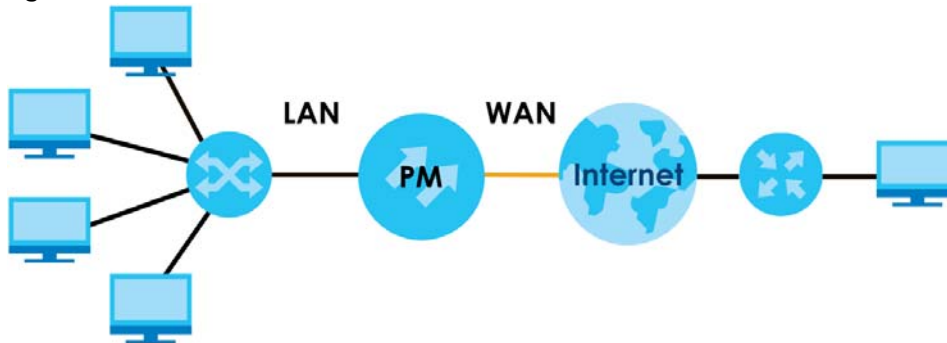
Broadband

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 28 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 10 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 102](#).

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.

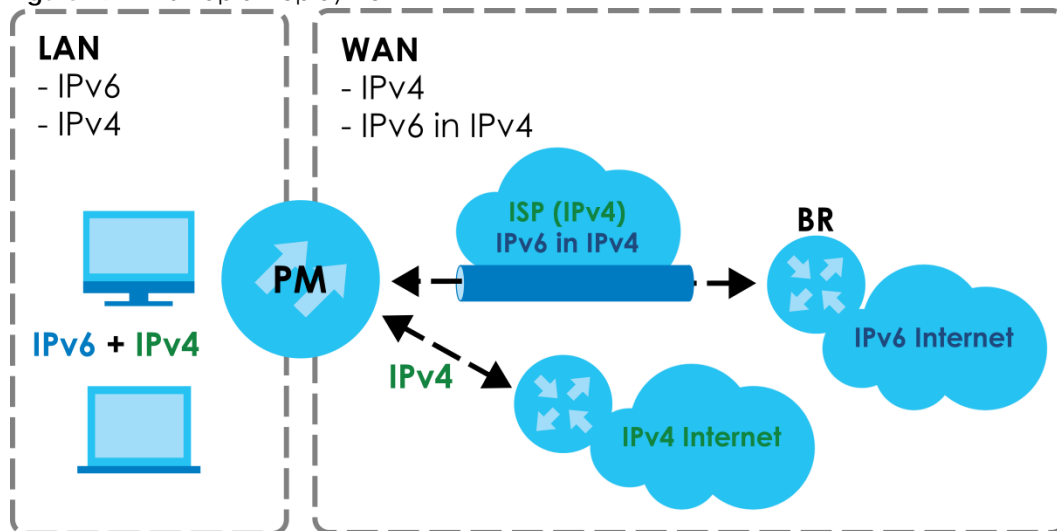
If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP addresses.

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 29 IPv6 Rapid Deployment

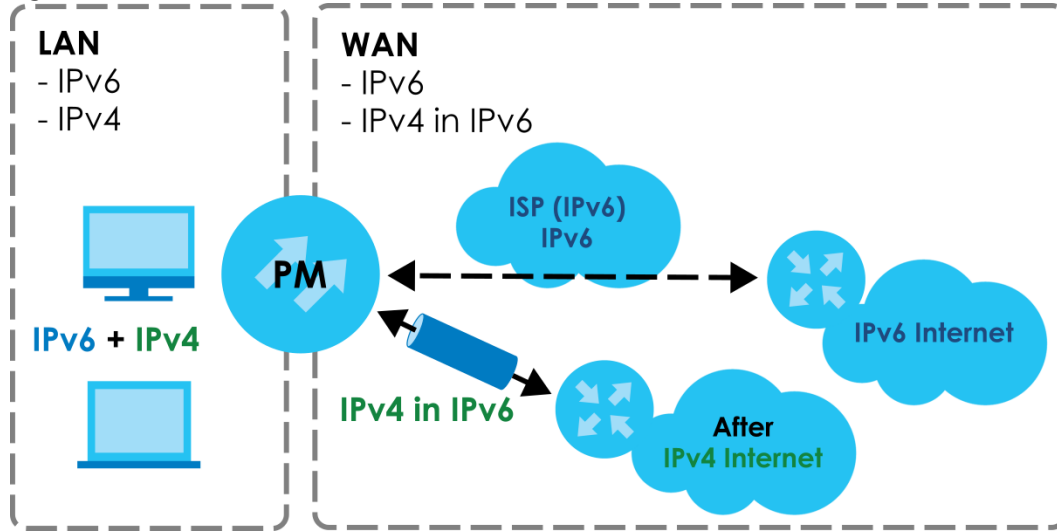


Dual Stack Lite

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 (**AFTR** 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 30 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 31 Network Setting > Broadband

Broadband												
Use this screen to change your Zyxel Device's Internet access settings. The summary table shows you the configured WAN services (connections) on the Zyxel Device. Use information provided by your ISP to configure WAN settings.												
Add New WAN Interface												
#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	GPON	PON	Bridge	Bridge	N/A	N/A	N	N	N	N	N	

The following table describes the labels in this screen.

Table 11 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 32 Network Setting > Broadband > Add New or Edit WAN Interface (Routing Mode).

General

Name

GPON

Type

GPON

Mode

Routing

Encapsulation

PPPoE

IPv4/IPv6 Mode

IPv4 IPv6 DualStack

VLAN

802.1p

4

802.1q

(0~4094)

MTU

1500

PPP Information

PPP User Name

admin

PPP Password

PPP Connection Trigger

Auto Connect

On Demand

Idle Timeout

0

min

PPPoE Passthrough

VLAN

802.1p

4

802.1q

(0~4094)

MTU

1500

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

192.168.0.9

DNS Server

Obtain DNS Info Automatically

Use Following Static DNS Address

Primary DNS Server

Secondary DNS Server

Routing Feature

NAT

IGMP Proxy

Apply as Default Gateway

Fullcone NAT

IPv6 Address

Obtain an IPv6 Address Automatically

Static IPv6 Address

IPv6 Address

Prefix Length

8

IPv6 DNS Server

Obtain IPv6 DNS Info Automatically

Use Following Static IPv6 DNS Address

Primary DNS Server

Secondary DNS Server

IPv6 Routing Feature

MLD Proxy

Apply as Default Gateway

DHCPv6 Option

IPv6 Address From DHCPv6 Server

Other Information From DHCPv6 Server

Cancel

Apply

The following table describes the labels in this screen.

Table 12 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 12 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 41 for more information.	
Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.	
Automatically configured by DHCP	The Automatically configured by DHCP 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 DHCP 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 12 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.
DHCP 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	<p>Select Option 42 to have the PM Device get NTP time server information from DHCP packets sent from the DHCP server.</p> <p>Select Option 43 to have the PM Device get vendor specific information from DHCP packets sent from the DHCP server.</p> <p>Select Option 120 to have the PM Device get static route information from DHCP packets sent from the DHCP server.</p> <p>Select Option 121 to have the PM Device get SIP server information from DHCP packets sent from the DHCP server.</p>
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	<p>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.</p> <p>This is available only when you set the Encapsulation to IPoE.</p>
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 12 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 41 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 33 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)

The screenshot shows the 'Edit WAN Interface' configuration page. The 'General' tab is active, indicated by a blue toggle switch. Under 'General', the 'Name' field is set to 'GPON', 'Type' is 'GPON', and 'Mode' is 'Bridge'. The 'VLAN' tab is inactive, indicated by a grey toggle switch. Under 'VLAN', the '802.1p' field is set to '0', the '802.1q' field is empty with a range of '(0~4094)', and the 'MTU' field is set to '2000'. At the bottom, there are 'Cancel' and 'Apply' buttons.

The following table describes the labels in this screen.

Table 13 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 52](#)).

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, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

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

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 34 Network Setting > Home Networking

Home Networking

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices.

LAN IP Setup

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Cancel Apply

The following table describes the fields on this screen.

Table 14 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 54](#)).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the PM Device ([Section 8.3 on page 58](#)).

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 35 Security > Certificates > Local Certificates

Certificates

Local Certificates Trusted CA

The Zyxel 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.

Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import the signed certificates.

Replace PrivateKey/Certificate file in PEM format

☐ Private Key is protected by password

Current File	Subject	Issuer	Valid From	Valid To	Modify
--------------	---------	--------	------------	----------	--------

The following table describes the labels in this screen.

Table 15 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.
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 36 Create Certificate Request

The following table describes the labels in this screen.

Table 16 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.
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 37 Certificate Request: View

View Certificate

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.

Name: certificate 1

Type: none

Subject: /CN=021018-DX5301-80-S090Y0000000/O=zyxel/ST=taipei/C=TW

Certificate: [Empty text box]

Private Key: -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAo4GibqQ7OYVxf02Z8WXfV8T066wbh
HyZhuW+ly7xLLQ0efT
Y5Xp1UbvvRr2Wg+JVdyC35aLxqYU4AZ4+90GBnDPuYxdY2
k/2u2lNnxv/s0Sxd
1eLu2GiaAhPC9vh6/iAT1WijkMzNP0eHAOUv/3Zr2FWC8C
d7xihMO9VcooUieYn
WDZfRgs4M13p2jyNd1zy2OVuhtNHmx8XeqwPnmO9PJEAH

Signing Request: -----BEGIN CERTIFICATE REQUEST-----
MIICnDCCAYQCAQAwVzEnMCUGA1UEAwweMDIxMDE4LU
RYNTMwMS1CMC1TMDkwWTAw
MDAwMDAwMQ4wDAYDVQQKDAV6eXhibDEPMA0GA1UE
CAwGdGFpcGVpMQswCQYDVQQGQ
EwJUVzCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQo
CggEBAKOBIG6kOzmFcX9N
mQVl3I2PE9OusG4R8mYblvMu85C0NHn9WEI6dVG770a9lo

Back

The following table describes the fields in this screen.

Table 17 Certificate Request: View

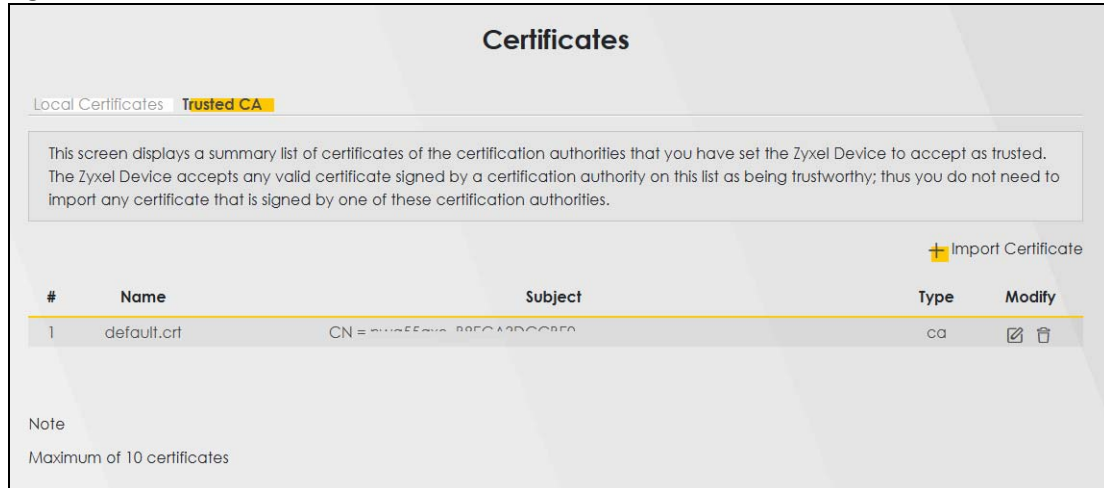
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, 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 38 Security > Certificates > Trusted CA



The following table describes the fields in this screen.

Table 18 Security > Certificates > Trusted CA

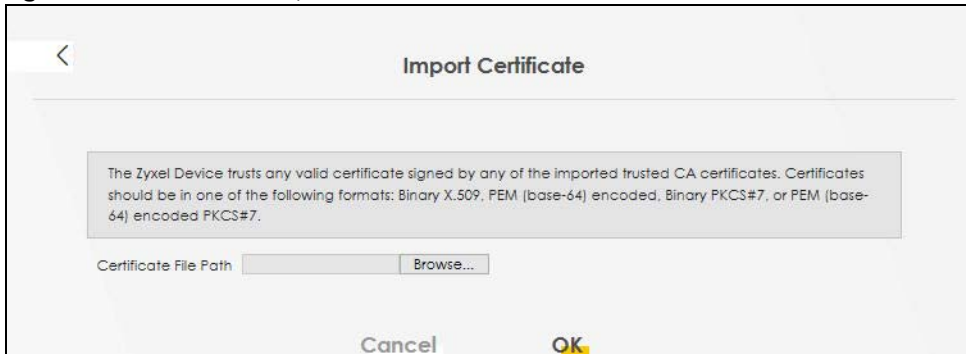
LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the PM Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays 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 39 Trusted CA: Import Certificate



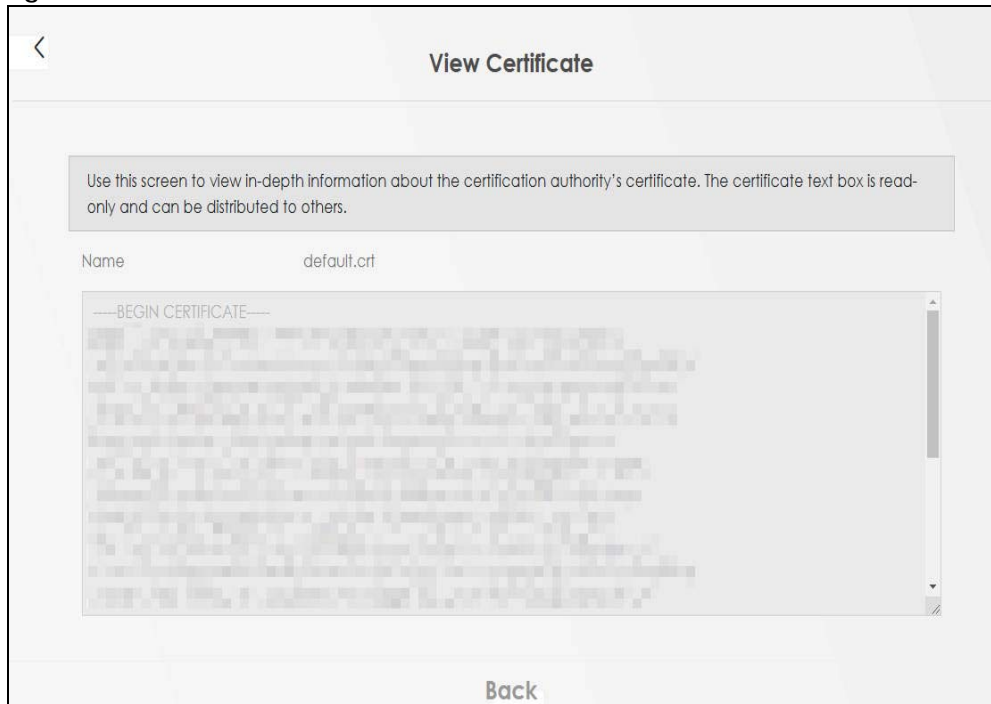
The following table describes the fields in this screen.

Table 19 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 40 Trusted CA: View

The following table describes the fields in this screen.

Table 20 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	<p>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.</p> <p>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 floppy disk for example).</p>
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.

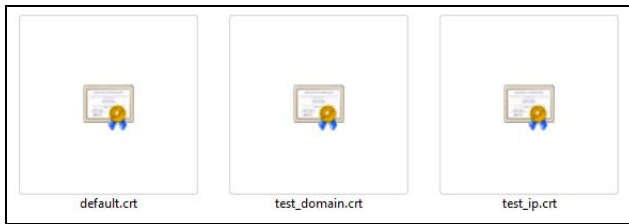
8.4.1 Verify a Certificate

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.

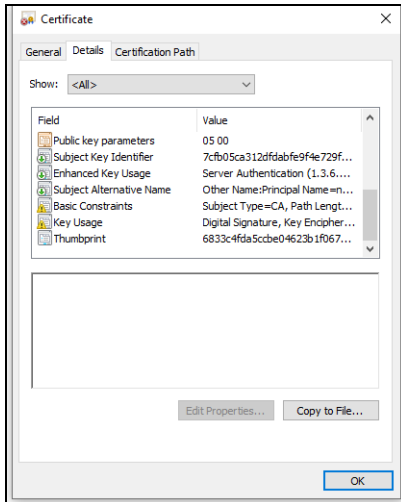
You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

- 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

Log

9.1 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.

9.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 9.2 on page 64](#)).
- Use the **Security Log** screen to see the security-related logs ([Section 9.3 on page 65](#)).

9.1.2 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 21 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 21 Syslog Severity Levels (continued)

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

9.2 System Log

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

Figure 41 System Monitor > Log > System Log

The following table describes the labels in this screen.

Table 22 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.

9.3 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 42 System Monitor > Log > Security Log

System Log **Security Log**

Use the **Security Log** screen to see the security-related logs for the categories that you select. You can filter the entries by selecting a severity level and/or category.

Level Category

Clear Log **Refresh** **Export Log**

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the labels in this screen.

Table 23 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 10

Traffic Status

10.1 Overview

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

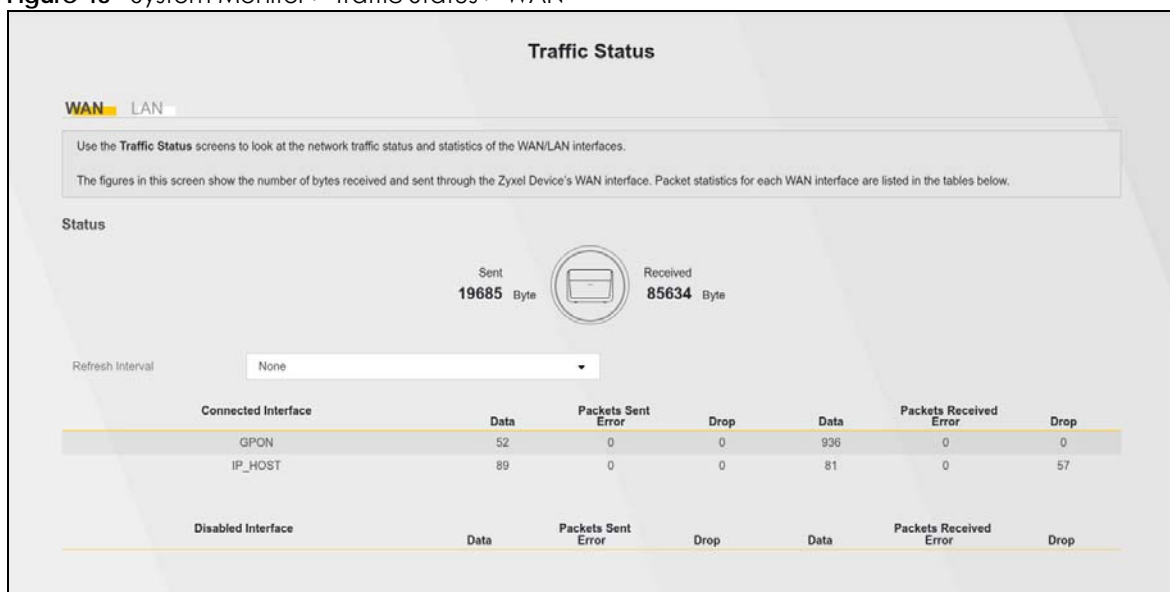
10.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 10.2 on page 66](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 10.3 on page 67](#)).

10.2 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 43 System Monitor > Traffic Status > WAN



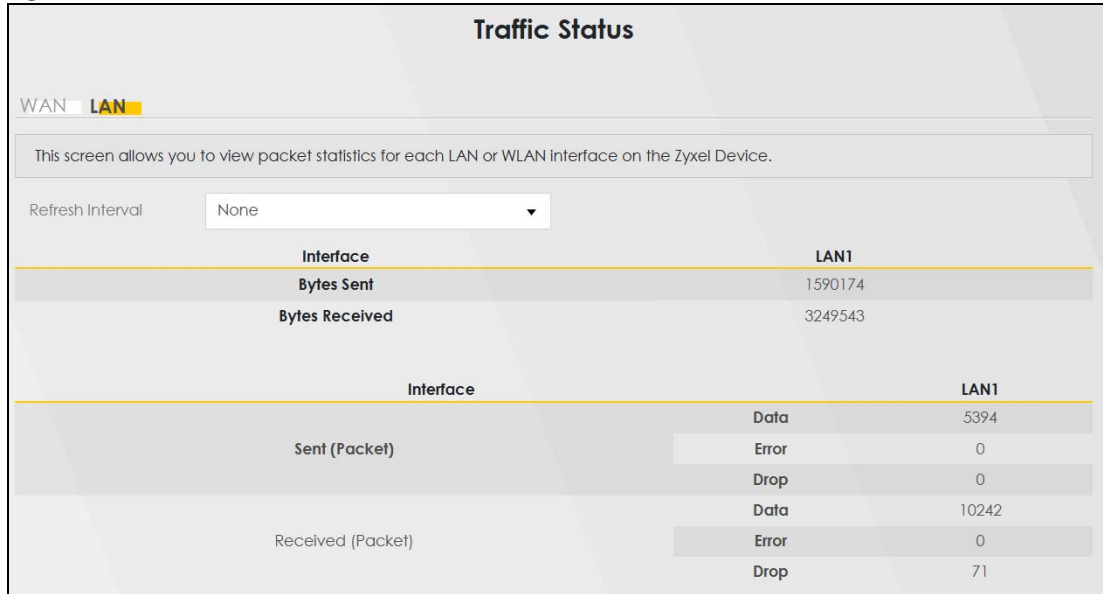
The following table describes the fields in this screen.

Table 24 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.

10.3 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 44 System Monitor > Traffic Status > LAN

The following table describes the fields in this screen.

Table 25 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 11

Optical Signal Status

11.1 Overview

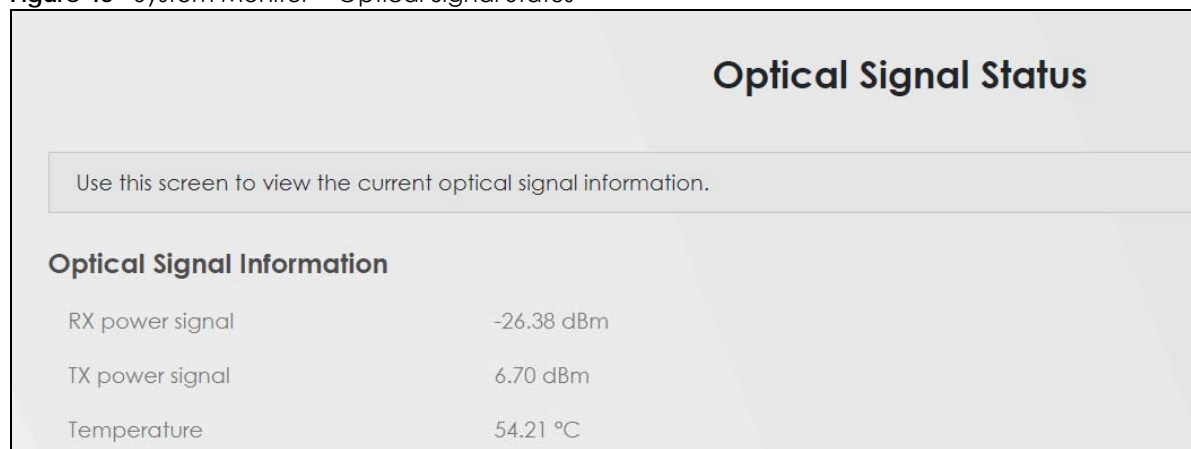
Use this screen to view the PON transceiver's TX power and RX power level and its temperature.

11.2 Optical Signal Status

Click **System Monitor > Optical Signal Status** to open the **Optical Signal Status** screen to see the real-time DDML 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 45 System Monitor > Optical Signal Status



The following table describes the labels in this screen.

Table 26 System Monitor > Optical Signal Status

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

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

Table 27

LABEL	NORMAL RANGE
RX power signal	-8 to -27 dBm
TX power signal	0.5 to 5 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 DDML 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 12

System

12.1 Overview

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

12.2 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 46 Maintenance > System

System

Use this screen to name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Host Name: PM7500-00

Domain Name: home

Cancel **Apply**

The following table describes the labels on this screen.

Table 28 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 13

User Account

13.1 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.

13.2 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 47 Maintenance > User Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Remote Privilege	Modify
1	<input checked="" type="checkbox"/>	admin	5	60	5	Administrator	LAN,WAN	
2	<input checked="" type="checkbox"/>	Zyxel_123	3	5	5	Administrator	LAN	
3	<input checked="" type="checkbox"/>	Zyxel_ABC	3	5	5	User	LAN,WAN	

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 29 Administrator/User privilege differences

LINK	TAB	ADMINISTRATOR	USER
Connection Status			
	Connection Status	Yes	Yes
Network			

Table 29 Administrator/User privilege differences (continued)

LINK	TAB	ADMINISTRATOR	USER
	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 30 Maintenance > User Account

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

13.2.1 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 48 Maintenance > User Account > Add

The following table describes the labels on this screen.

Table 31 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	<p>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.</p> <p>Note that as you enter a password, the screen displays a (*) for each character you enter. Click the eye icon to view the password.</p> <p>After you change the password, use the new password to access the PM Device.</p> <p>If you are changing your existing password, you have to first enter your Old Password then enter your New Password.</p>
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 31 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 72 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 14

Remote Management

14.1 Overview

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

14.2 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 49 Maintenance > Remote Management

Service	LAN	Port	Redirect ⓘ
HTTP	<input checked="" type="checkbox"/> Enable	80	<input checked="" type="checkbox"/> Enable
HTTPS	<input checked="" type="checkbox"/> Enable	443	
SSH	<input checked="" type="checkbox"/> Enable	22	
PING	<input checked="" type="checkbox"/> Enable		

Cancel Apply

The following table describes the labels on this screen.

Table 32 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
Service	<div>This is the service you may use to access the PM Device.</div> <ul style="list-style-type: none">• 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	<div>Select the Enable check box for the corresponding services that you want to allow access to the PM Device from the LAN.</div>

Table 32 Maintenance > Remote Management > MGMT Services (continued)

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

CHAPTER 15

Time

15.1 Overview

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

15.2 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 50 Maintenance > Time

Use this screen to configure the Zyxel Device's time based on your local time zone. You can enter a time server address, select the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings if needed.

Current Date/Time

Current Time 07:18:40
Current Date 2021-08-16

Time and Date Setup

Time Protocol SNTP (RFC-1769)

First Time Server Address Other pool.ntp.org

Second Time Server Address clock.nyc.he.net

Third Time Server Address clock.sjc.he.net

Fourth Time Server Address None

Fifth Time Server Address None

Time Zone

Time Zone (GMT+01:00) Amsterdam, Berlin, Bern, Rome, ▼

Daylight Savings

Active ☒

Start Rule

Day ☐ 1 in

☒ Last Sunday in

Month March

Hour 2 0

End Rule

Day ☐ 1 in

☒ Last Sunday in

Month October

Hour 3 0

Cancel **Apply**

The following table describes the labels on this screen.

Table 33 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 33 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 16

Log Setting

16.1 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.

16.2 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 51 Maintenance > Log Setting

The screenshot shows the 'Log Setting' configuration page. At the top, the title 'Log Setting' is centered. Below it, a grey box contains instructions: 'Use this screen to enable or disable Zyxel log settings, and which type of logs the Zyxel Device records.' and 'Currently only support to store logs on the Zyxel Device.' The main settings are divided into two sections: 'Syslog Setting' and 'Active Log'. In 'Syslog Setting', there is a 'Syslog Logging' toggle switch (currently off), a 'Mode' dropdown menu set to 'Local File', a 'Syslog Server' text input field with '0.0.0.0' and a label '(Server NAME or IPV4/IPV6 Address)', and a 'UDP Port' text input field with '514' and a label '(Server Port)'. The 'Active Log' section is split into 'System Log' and 'Security Log'. Under 'System Log', there are checkboxes for 'TR-069', 'HTTP', 'System' (checked), and 'OMCI'. Under 'Security Log', there are checkboxes for 'Account' and 'Attack' (checked). At the bottom, there are 'Cancel' and 'Apply' buttons.

Log Setting

Use this screen to enable or disable Zyxel log settings, and which type of logs the Zyxel Device records.

Currently only support to store logs on the Zyxel Device.

Syslog Setting

Syslog Logging ☐

Mode Local File

Syslog Server 0.0.0.0 (Server NAME or IPV4/IPV6 Address)

UDP Port 514 (Server Port)

Active Log

System Log

☐ TR-069

☐ HTTP

☒ System

☐ OMCI

Security Log

☐ Account

☒ Attack

Cancel **Apply**

The following table describes the fields on this screen.

Table 34 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Slide the switch to the right to enable syslog logging.
Mode	<p>Select Remote to have the PM Device send it to an external syslog server.</p> <p>Select Local File to have the PM Device save the log file on the PM Device itself.</p> <p>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.</p> <p>Note: A warning appears upon selecting Remote or Local File and Remote. Just click OK to continue.</p>
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.
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 17

Firmware Upgrade

17.1 Overview

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

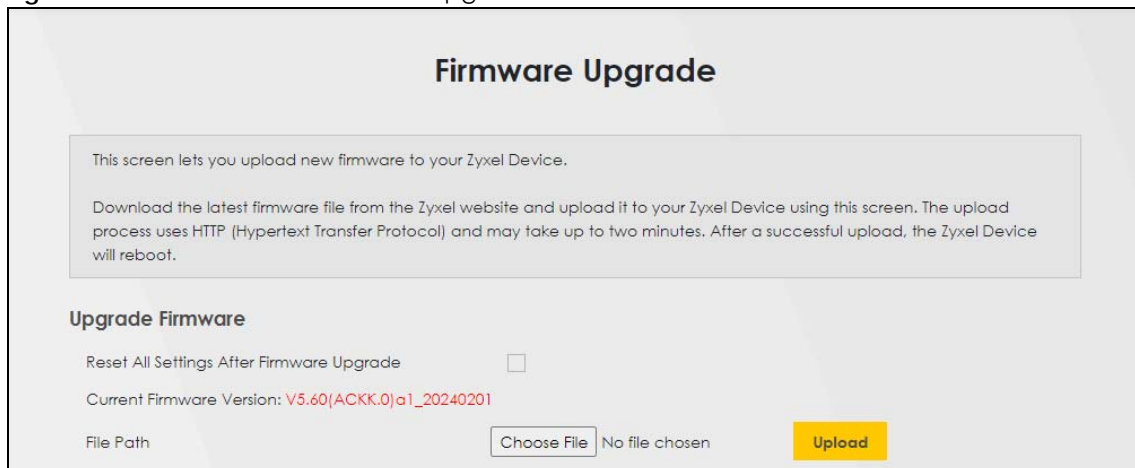
Only use firmware for your device's specific model. Refer to the label on the bottom of your PM Device.

17.2 Firmware

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

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

Figure 52 Maintenance > Firmware Upgrade



The screenshot shows a web interface titled "Firmware Upgrade". It contains a text box explaining the process: "This screen lets you upload new firmware to your Zyxel Device. Download the latest firmware file from the Zyxel website and upload it to your Zyxel Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the Zyxel Device will reboot." Below this, there is a section titled "Upgrade Firmware" with a checkbox for "Reset All Settings After Firmware Upgrade" and a text field showing the "Current Firmware Version: V5.60(ACKK.0)a1_20240201". At the bottom, there is a "File Path" label, a "Choose File" button, a "No file chosen" status, and a yellow "Upload" button.

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.

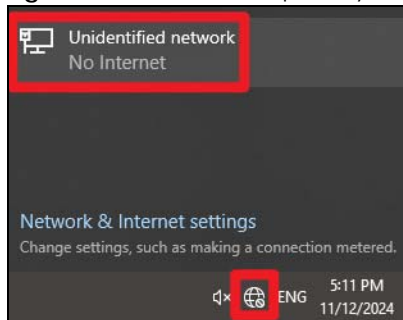
Table 35 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Reset All Settings After Firmware Upgrade	Click the check box to have the PM Device automatically reset itself after the new firmware is uploaded.
Current Firmware Version	This is the present Firmware version and the date created.
File Path	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 two minutes.

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

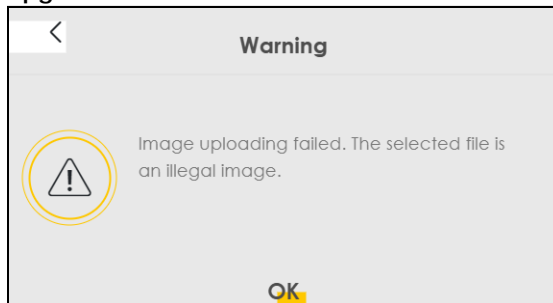
The PM Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 53 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 18

Backup/Restore

18.1 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.

18.2 Backup/Restore

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

Figure 54 Maintenance > Backup/Restore

Backup/Restore

Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes.

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

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Backup

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path

Choose File

No file chosen

Upload

Back to Factory Default Settings

Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.0.1
- DHCP will be reset to default setting

Reset

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 36 Restore Configuration

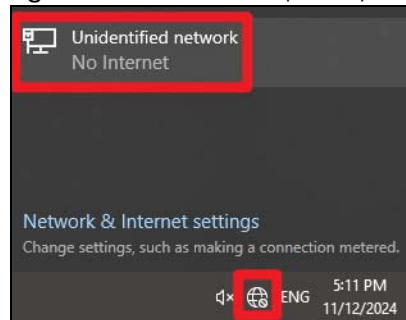
LABEL	DESCRIPTION
File Path	Enter the location of the file you want to upload in this field or click Choose File / Browse to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click 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 55 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 17](#) for more information on the **RESET** button.

18.3 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 56 Maintenance > Reboot



CHAPTER 19

Diagnostic

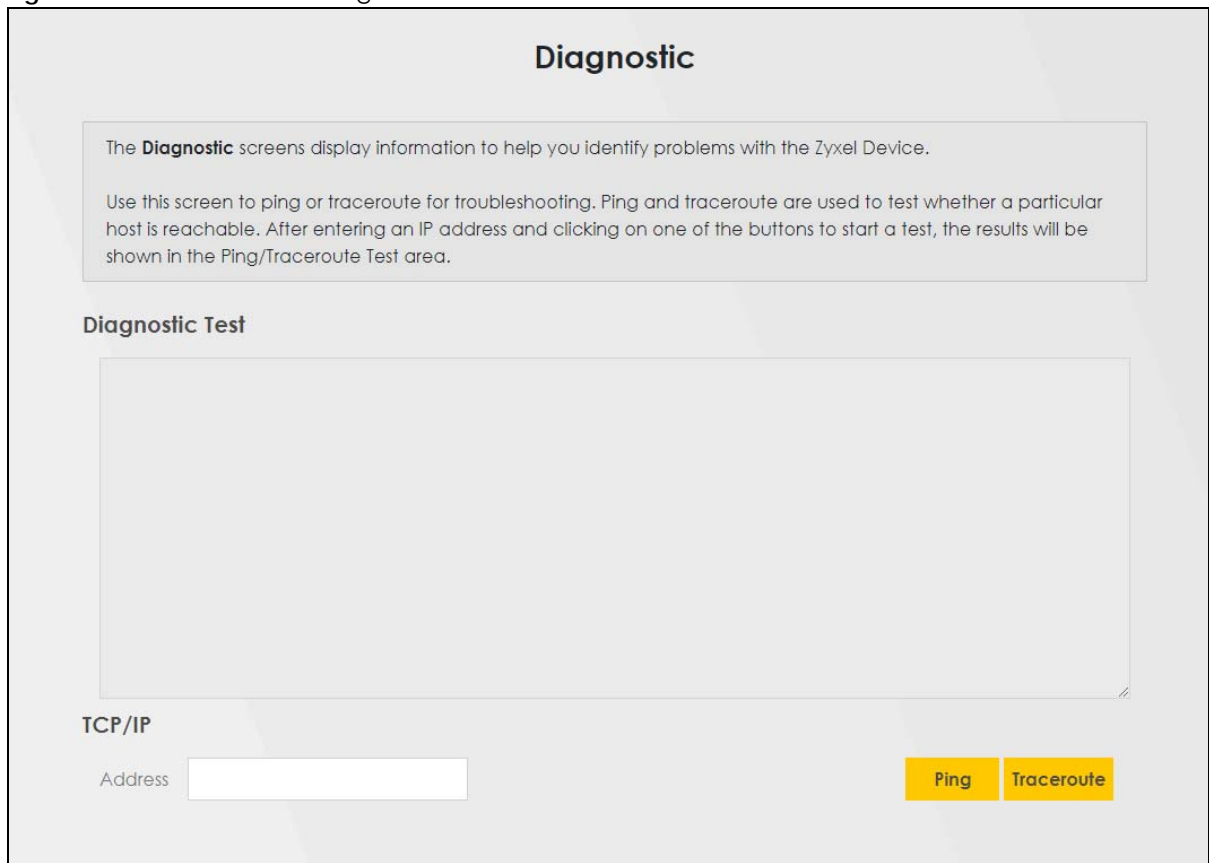
19.1 Overview

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

19.2 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 57 Maintenance > Diagnostic



The screenshot shows the 'Diagnostic' screen. At the top, the title 'Diagnostic' is centered. Below it, a text box contains instructions: 'The **Diagnostic** screens display information to help you identify problems with the Zyxel Device. Use this screen to ping or traceroute for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area.' Below this is a section titled 'Diagnostic Test' with a large empty box for results. At the bottom, there is a 'TCP/IP' section with an 'Address' label and a text input field. To the right of the input field are two yellow buttons labeled 'Ping' and 'Traceroute'.

The following table describes the fields on this screen.

Table 37 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 20

Troubleshooting

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

- [Power, Hardware Connections, and LEDs](#)
- [PM Device Access and Login](#)
- [Internet Access](#)

20.1 Power, Hardware Connections, and LEDs

[The PM Device does not turn on. None of the LEDs turn on.](#)

- 1 Make sure the PM Device is turned on.
- 2 Make sure you are using the power adapter or cord included with the PM Device.
- 3 Make sure the power adapter or cord is connected to the PM Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the PM Device off and on.
- 5 If the problem continues, contact the vendor.

[One of the LEDs does not behave as expected.](#)

- 1 Make sure you understand the normal behavior of the LED. See [Section 2.2 on page 14](#).
- 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.

20.2 PM Device Access and Login

I forgot the IP address for the PM Device.

- 1 The default LAN IP address is 192.168.0.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the PM Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the PM Device (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 2.3.1 on page 17](#).

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 14](#).

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 52](#)), 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 from 192.168.0.2 to 192.168.0.254. See [Section 5.2.1 on page 32](#).
- 3 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 2.2 on page 14](#).
- 4 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 5 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).
- 6 Reset the device to its factory defaults and try to access the PM Device with the default IP address. See [Section 2.3.1 on page 17](#).

- 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 20.1 on page 93](#).

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.

20.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** or [Section 2.2 on page 14](#).

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 14](#) 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 14](#).
- 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 device.

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

For Zyxel Communications Corp. Network offices, see <https://www.zyxel.com/index.shtml> for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

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

Korea

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

Malaysia

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Belarus

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

Belgium (Netherlands)

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

Bulgaria

- Zyxel Communications Corp. Bulgaria

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

Czech Republic

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

Denmark

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Norway

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

Poland

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

Romania

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

Russian Federation

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

Slovakia

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

Spain

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

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

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

South America

Argentina

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

Brazil

- Zyxel Communications Corp. Communications Brasil Ltda.

- <https://www.zyxel.com/br/pt>

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

- Zyxel Communications Corp. Communications Corp.
- <https://il.zyxel.com>

North America

USA

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

APPENDIX B

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 3.4×10^{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 38 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 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 (0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

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

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

Table 39

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 servers on a local site.

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

Table 40

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.

Table 41

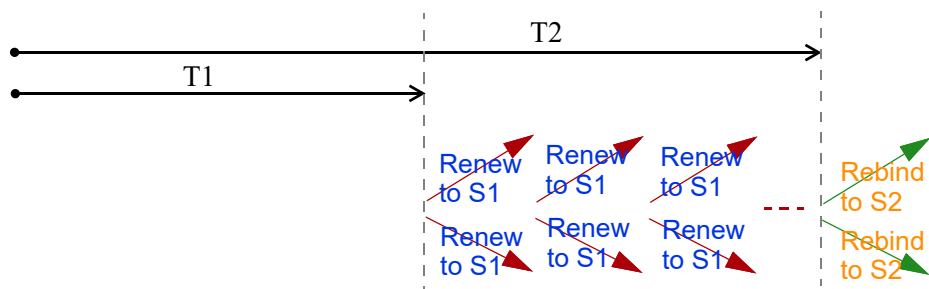
MAC	00	:	13	:	49	:	12	:	34	:	56
-----	----	---	----	---	----	---	----	---	----	---	----

Table 42

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 unreach, 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.

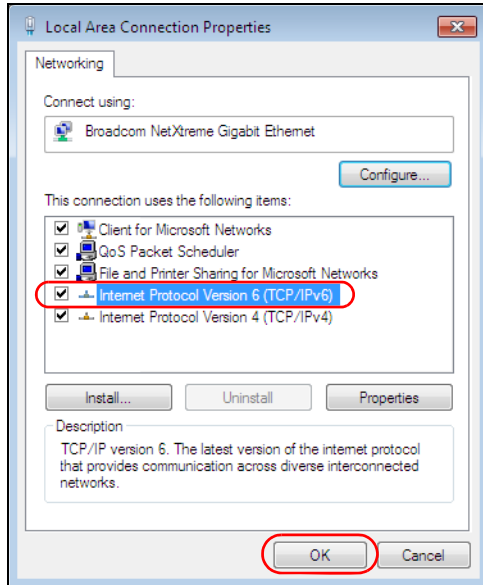
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected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

Copyright © 2024 by Zyxel and/or its affiliates

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

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

Regulatory Notice and Statement

Europe and the United Kingdom



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

Belgium (English)	National Restrictions <ul style="list-style-type: none">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.
België (Flemish)	
Belgique (French)	
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 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 ΕΞΟΠΛΙΣΜΟΣ 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)	<p>Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> 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/ 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/ 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 deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 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 și 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 laitteen 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 съществени изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

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

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- 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 adaptor 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. Wenn 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, llévalo 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

Table 43

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to www.zyxel.com to view this product's documentation and certifications.

Zyxel Limited Warranty

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

Note

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

To obtain the services of this warranty, contact your vendor.

Registration

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

Trademarks

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

Open Source Licenses

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

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

Index

Numbers

6RD [41](#)

A

Access Troubleshooting [95](#)

administrator password [20](#)

Alerts and Logs [63](#)

B

backup

configuration [87](#)

bandwidth capacity

cable type [12](#)

Bridge Mode [48](#)

Broadband

overview [40](#)

broadband [40](#)

C

CA [54](#), [58](#), [60](#)

cable type

Ethernet [12](#)

Canonical Format Indicator See CFI

Certificate [54](#)

authentication [54](#)

CA

creating [56](#)

factory default [55](#)

File Format [61](#)

public key [54](#)

replacing [55](#)

storage space [55](#)

Certification [109](#)

Certification Authority [54](#), [60](#)

Certification Authority. see CA

certifications

viewing [112](#)

CFI [51](#)

CGNAT

Carrier-Grade NAT [42](#)

configuration

backup [87](#)

reset [88](#)

restoring [88](#)

contact information [97](#)

copyright [108](#)

creating certificate [56](#)

customer support [97](#)

D

diagnostic [90](#)

digital IDs [54](#)

disclaimer [108](#)

distance maximum

cable type [12](#)

DNS server address assignment [51](#)

Dual Stack Lite [41](#)

E

Encapsulation [50](#)

PPP over Ethernet [50](#)

encapsulation method

technical reference [50](#)

F

fiber [17](#), [95](#)

firmware [84](#)
version [29](#)

I

IEEE 802.1Q [51](#)
Internet Protocol version 6, see IPv6
IP address [52](#)
ping [90](#)
IP address assignment [50](#)
IP over Ethernet [50](#)
IPoE technical reference [50](#)
IPv6 [102](#)
addressing [102](#)
Enabling IPv6 [106](#)
EUI-64 [104](#)
global address [102](#)
interface ID [104](#)
link-local address [102](#)
Neighbor Discovery Protocol [102](#)
ping [102](#)
prefix [102](#)
prefix length [102](#)
unspecified address [103](#)
ISP [41](#)
Address Family Transition Router [41](#)
Border Relay router [41](#)
DNS server address [30](#)
Internet Service Provider [42](#)
WAN IP address [41](#)

L

LAN [40, 52](#)
IP address [52](#)
status [30, 31](#)
subnet mask [52](#)
LEDs [14](#)
login [19](#)
passwords [20](#)
logs [63, 66, 69, 82](#)
security [65](#)

M

managing the device
good habits [13](#)
MLD [106](#)
MTU (Multi-Tenant Unit) [50](#)
multi-gigabit [12](#)

N

network disconnect
temporary [85](#)
network map [23](#)

O

OMCI [83](#)

P

passwords [20](#)
ping [90](#)
PM Device
managing [13](#)
PON [11, 15, 16, 17, 95](#)
PPPoE [50](#)
Benefits [50](#)
technical reference [50](#)
product registration [112](#)
Public and Private Keys [61](#)

R

registration
product [112](#)
reset [88](#)
RESET Button [17](#)
restart [89](#)
restoring configuration [88](#)
Routing Mode [43](#)

S

- security logs [65](#)
- service access control [76](#)
- status [26](#)
 - firmware version [29](#)
 - LAN [30, 31](#)
 - WAN [30](#)
- subnet mask [52](#)
- Syslog [63](#)
 - overview [63](#)
 - severity levels [63](#)
- system
 - firmware [84](#)
 - version [29](#)
 - passwords [20](#)
 - status [26](#)
 - LAN [30, 31](#)
 - WAN [30](#)

T

- TPID [51](#)
- traceroute [90](#)
- trademarks [112](#)
- transmission speed
 - cable type [12](#)
- troubleshooting [90](#)

U

- upgrading firmware [84](#)

V

- Virtual Local Area Network See VLAN
- VLAN [50](#)
 - Introduction [50](#)
- VLAN ID [51](#)
- VLAN tag [51](#)

W

- WAN
 - settings [40](#)
 - status [30](#)
 - Wide Area Network, see WAN [40](#)
- WAN IP address [41](#)
- warranty
 - note [112](#)
- web configurator
 - login [19](#)
 - passwords [20](#)