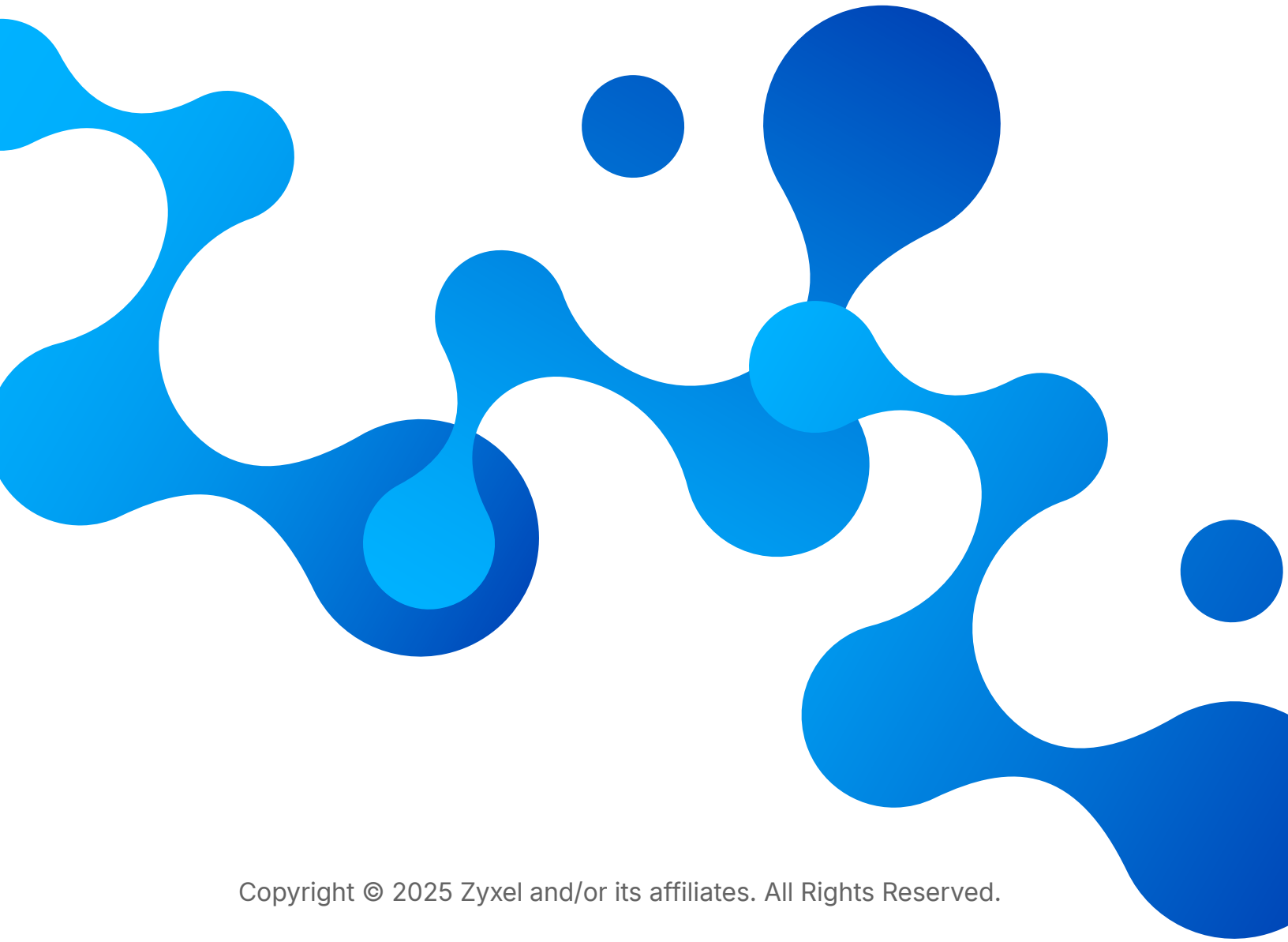
ZYXEL
COMMUNICATIONS

User's Guide

EE/PE Series

Default Login Details	
LAN IP Address	http://192.168.1.1
Login	admin
Password	See the device label

Version 5.19-5.63 Ed 4, 08/2025



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 Zyxel Device.

- Zyxel One app. Download the Zyxel One app from Google Play or Apple Store to manage the Zyxel Device using a smartphone or tablet. To view Zyxel One app tutorials, please go to *https://service-provider.zyxel.com/app-help/ZyxelOne/FLA/LAN*

- More Information

  Go to *https://service-provider.zyxel.com/global/en/tech-support* to find other information on Zyxel 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 Zyxel 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** > **Routing** > **DNS Route** means you first click **Network Setting** in the navigation panel, then the **Routing** submenu, and then finally the **DNS Route** tab to get to that screen.

Icons Used in Figures

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

Zyxel Device 	Generic Router 	Switch 
Server 	Firewall 	USB Storage Device 
Printer 	4G LTE/5G NR Base Station 	Desktop 
Laptop 	Smart TV 	Wireless Device 

Accessibility and Compatibility

Introduction

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

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

Accessibility Feature – Screen Reader Support

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

To use the screen reader, do the following:

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

Accessibility Feature – Keyboard Navigation

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

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

How to Get Support

If you are an Internet Service Provider (ISP), please contact your Zyxel sales or service representative for direct support.

If you obtained your Zyxel Device from an ISP, please contact your ISP's support team directly, as the Zyxel Devices may have custom configurations.

Contents Overview

PART I
User's Guide

CHAPTER 1
Introducing the Zyxel Device

1.1 Overview

The Zyxel Device refers to the models listed in the tables.

EE Series

- EE3301-00
- EE4410-00
- EE5301-00
- EE6510-10
- EE6601-00

PE Series

- PE3301-00
- PE5301-01

1.1.1 EE Series

The EE Series are Ethernet gateways that provide Internet access through the Ethernet WAN port or an SFP port.

The following table describes the feature differences of the EE Series by model. For more details about the ports panel, please refer from EE3301-00 to EE6601-00.

Table 1 EE Series Feature Comparison

	EE3301-00	EE5301-00	EE6601-00
WiFi 7 Wireless Standard	BE7200	BE7200	BE19000
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz 6 GHz
Theoretical Maximum WiFi Speed	7.2 Gbps	7.2 Gbps	19 Gbps
SFP+ Cage	NO	10G XGS-PON 10G AON	10G AON
Ethernet WAN	1 / 2.5 Gbps	1 / 2.5 / 5 / 10 Gbps	1 / 2.5 / 5 / 10 Gbps
USB	3.0	3.0	3.0
Phone Port (VoIP)	1 FXS	2 FXS	2 FXS
Zero-Wait DFS	YES	YES	YES
Wall Mount	YES	YES	YES
App Management	Zyxel One	Zyxel One	Zyxel One

Table 2 EE Series Feature Comparison

	EE6510-10	EE4410-00
Wi-Fi 7 Wireless Standard	BE18000	BE18000
Supported Frequency Bands	2.4 GHz 5 GHz 6 GHz	2.4 GHz 5 GHz 6 GHz
Theoretical Maximum WiFi Speed	18 Gbps	18 Gbps
SFP+ Cage	NO	NO
Ethernet WAN	1 / 2.5 / 10 Gbps	1 / 2.5 Gbps
USB	3.0	NO
Phone Port (VoIP)	NO	NO
Zero-Wait DFS	NO	NO
Wall Mount	YES	YES
App Management	Zyxel One	Zyxel One

1.1.2 PE Series

The PE Series are PON (Passive Optical Network) gateways that connect to the Internet though a fiber cable.

The following table describes the feature differences of the PE Series by model. For more details about the ports panel, please refer to PE3301-00 and PE5301-01.

Table 3 PE Series Feature Comparison

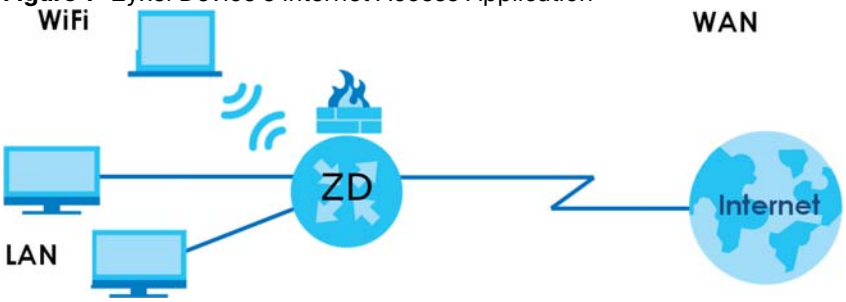
	PE3301-00	PE5301-01
WiFi 7 Wireless Standard	BE7200	BE7200
Supported Frequency Bands	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Theoretical Maximum WiFi Speed	7.2 Gbps	7.2 Gbps
SFP+ Cage	NO	NO
PON WAN	1.25 / 2.5G (GPON)	10G / 10G (XGSPON)
USB	3.0	3.0
Phone Port (VoIP)	2 FXS	2 FXS
Zero-Wait DFS	YES	YES
Wall Mount	YES	YES
App Management	Zyxel One	Zyxel One

1.2 Example Applications

This section shows the few examples of using the Zyxel Device in various network environments.

Connect the WAN port to the Internet. Connect computers to the Zyxel Device’s LAN ports, or wirelessly, and access the Internet simultaneously.

Figure 1 Zyxel Device's Internet Access Application



In the figure above, you can also configure Firewall on the Zyxel Device for secure Internet access. When the Firewall is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

1.2.1 WAN Priority

The WAN connection priority is as follows:

1. PON WAN
2. SFP
3. Ethernet WAN
4. DSL
5. Cellular WAN (3G/4G)
   See Section 1.2.6 on page 26 for more information about Cellular backup.

1.2.2 Dual-Band WiFi

Note: Check Section 1.1 on page 19 to see if your Zyxel Device supports dual-band WiFi.

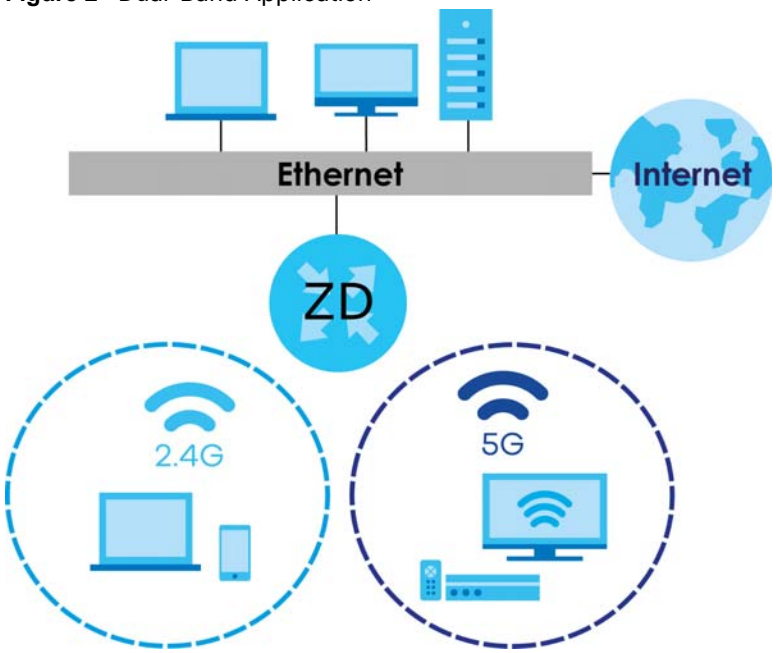
When WiFi is enabled on the Zyxel Device, IEEE 802.11a/b/g/n/ac/ax/be compliant clients, such as notebooks, tablets, and smartphones can wirelessly connect to the Zyxel Device to access network resources.

With dual-band, the Zyxel Device is a gateway that can use both 2.4 GHz and 5 GHz WiFi networks at the same time. IOT devices and other low-bandwidth clients could use the 2.4 GHz band for basic connectivity, while the 5GHz band handles time-sensitive traffic such as high-definition video, music, and gaming.

The Zyxel Device supports WiFi 7 that is most suitable in areas with a high concentration of users. Zyxel Devices support backward compatibility with older WiFi standards, ensuring seamless connectivity with

previous-generation devices.

Figure 2 Dual-Band Application



1.2.3 Triple-Band WiFi

Note: Check Section 1.1 on page 19 to see if your Zyxel Device supports triple-band WiFi.

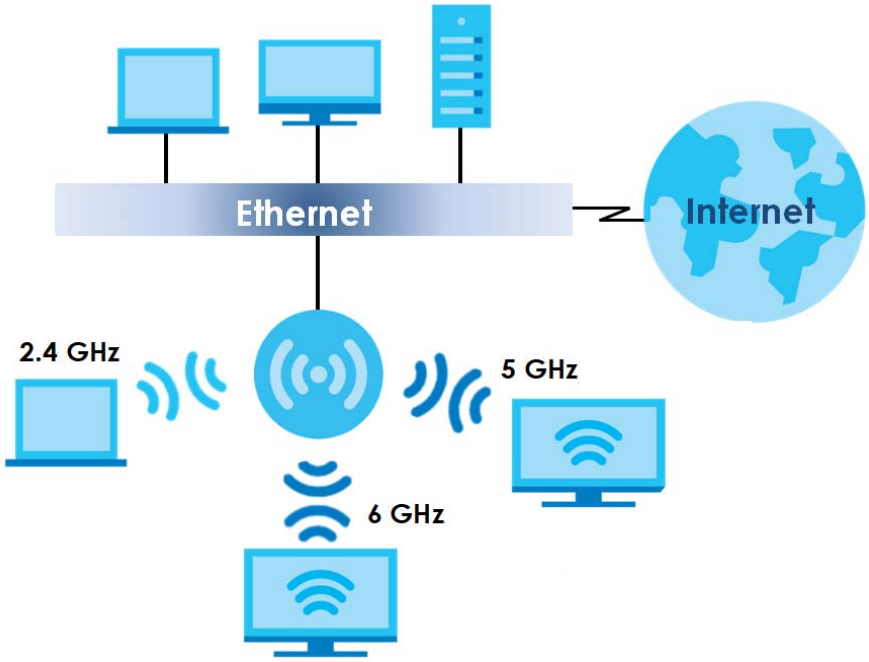
With triple-band, the Zyxel Device can use 2.4 GHz / 5 GHz / 6 GHz bands to operate simultaneously.

The 6 GHz band provides less coverage but has the highest amount of channels among the three frequency bands. Use the 6GHz band for the most congestion-free transmission for tri-band clients.

Note: Due to each country's regulations on frequency band usage, the available bands (2.4 GHz, 5 GHz, and 6 GHz) may differ by countries or markets the Zyxel Device products are sold to.

You can leverage concurrent tri-band connectivity across 2.4 GHz, 5 GHz, and 6 GHz bands. This allows IoT devices and various clients to simultaneously maintain connections for basic tasks with 2.4 GHz. At the same time, 5 GHz and 6 GHz handle time-sensitive traffic, and high-bandwidth applications like high-definition video, music, and gaming.

Figure 3 Triple-Band Application



WiFi 7 (IEEE802.11be)

WiFi 7 (802.11be) is backwards compatible with WiFi 6 and WiFi 6E. WiFi 7 is a WiFi standard that supports 2.4 GHz, 5 GHz and 6 GHz frequency bands with the following improvements over WiFi 6 and WiFi 6E.

Table 4 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES		WiFi 6	WiFi 6E	WiFi 7
Theoretical Maximum Speed (Up-to)		9.6 Gbps		46 Gbps
Supported Frequency Bands		2.4 GHz/5 GHz	2.4 GHz/5 GHz/6 GHz	2.4 GHz/5 GHz/6 GHz
Supported Channel Bandwidth		20/40/80/160 MHz	20/40/80/160 MHz	20/40/80/160/320 MHz
Total Spectrum (Up-to)	2.4 GHz	80 MHz		80 MHz
	5 GHz	500 MHz		500 MHz
	6 GHz	Not supported.	1200 MHz	1200 MHz
Other Features (OFDMA/BSS Coloring/TWT/Two-Way MU-MIMO/ Beamforming/1024-QAM)		WiFi 6E inherits all the features from WiFi 6.		WiFi 7 inherits all the features from WiFi 6 and WiFi 6E, with the addition of multi-link operation and preamble puncturing.

Faster Data Transmission

WiFi 7 allows faster data transmission using:

- 4096 QAM (Quadrature Amplitude Modulation) – enhances the amount of data transmitted over the available bandwidth.
- 320 MHz Channel Bandwidth – enlarges the supported channel bandwidth to 320 MHz, allowing higher data throughput.

- Multiple Resource Units (RUs) – allows an AP to allocate multiple RUs to a WiFi client.

Multi-Link Operation (MLO)

WiFi 7 MLO allows a WiFi client to connect to the Zyxel Device using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Devices without MLO can only transmit data on one band at a time.

Figure 4 Without Multi-Link Operation

The Zyxel Device can support multiple frequency bands (2.4 GHz, 5 GHz and 6 GHz), but a WiFi client can only connect to the Zyxel Device using one of these frequency bands. The other frequency bands are unused. The client's data transmission speed depends on the frequency band they are connected to.

To use MLO, both the Zyxel Device and the WiFi client have to support MLO.

Figure 5 Multi-Link Operation Example

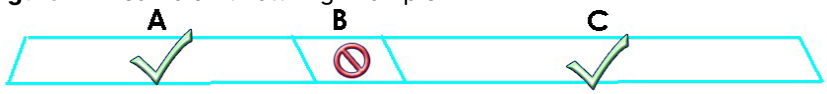
Preamble Puncturing

In WiFi 6 and earlier, any interference would cause the entire WiFi channel to become unavailable. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) becomes unavailable.

Figure 6 Without Preamble Puncturing

WiFi 7 preamble puncturing allows you to block the specific portion of the channel that is experiencing interference while continuing to use the rest of the WiFi channel. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) is still available.

Figure 7 Preamble Puncturing Example



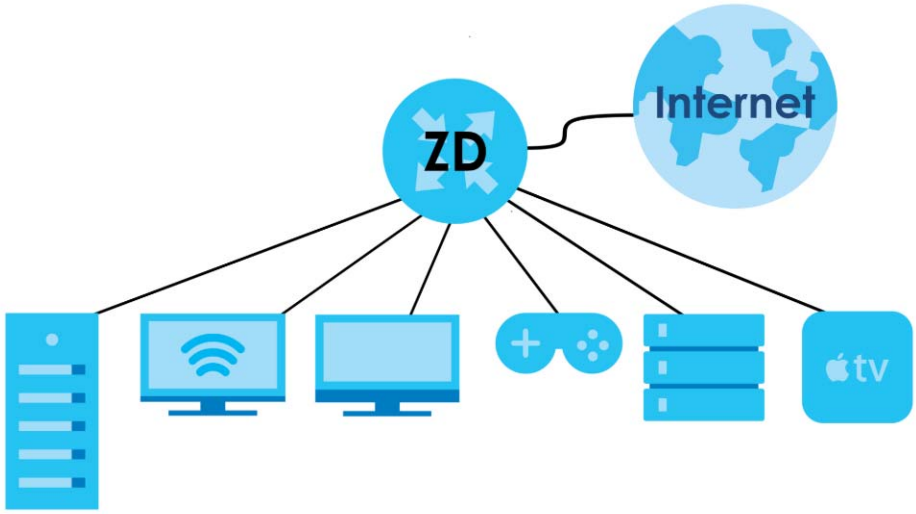
1.2.4 Multi-Gigabit Ethernet

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 Section 2.3 on page 38 for the speeds your Zyxel 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 Zyxel 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 5 on page 25 for the correct Ethernet cable type.

Figure 8 Multi-Gigabit Application



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

Table 5 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
Category 6	5G / 10G	100 m / 55 m	250 MHz

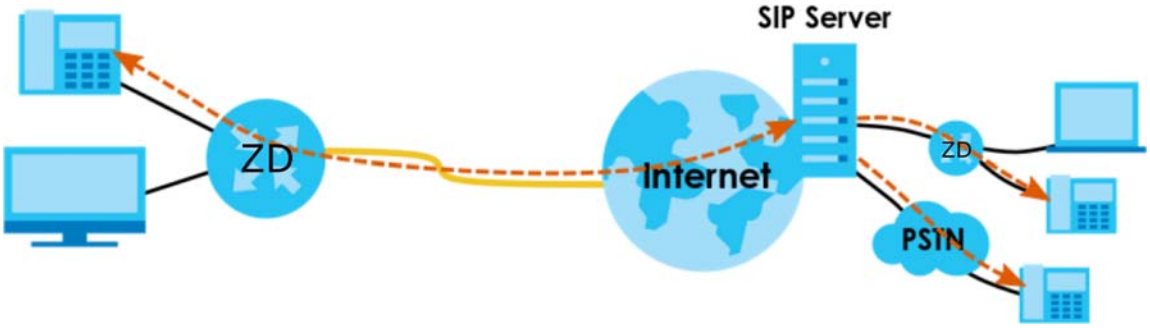
Table 5 Ethernet Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 6a	10G	100 m	500 MHz
Category 7	10G	100 m	600 MHz

1.2.5 VoIP Applications

The Zyxel Device's VoIP function allows you to register up to eight SIP (Session Initiation Protocol) accounts and use the Zyxel Device to make and receive VoIP telephone calls. The Zyxel Device sends your call to a VoIP service provider's SIP server which forwards the calls to either VoIP or PSTN phones.

Figure 9 VoIP Application



1.2.6 Zyxel Device's USB Support

The USB port of the Zyxel Device is used for cellular WAN backup, file-sharing, and media server.

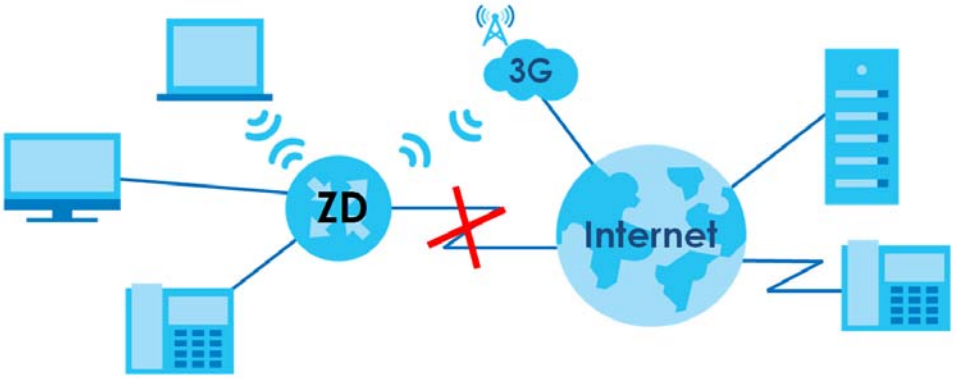
Cellular WAN Backup

Connect a supported cellular USB dongle with an active SIM card to the USB port. This adds a second WAN interface and allows the Zyxel Device to wirelessly access the Internet via a cellular network. The cellular WAN connection is a backup in case the DSL/Ethernet/Fiber connection fails.

To set up a cellular connection, click **Network** > **Broadband** > **Cellular Backup**.

To update the supported cellular USB dongle list, download the latest WWAN package from the Zyxel website and upload it to the Zyxel Device using the **Maintenance** > **Firmware Upgrade** screen.

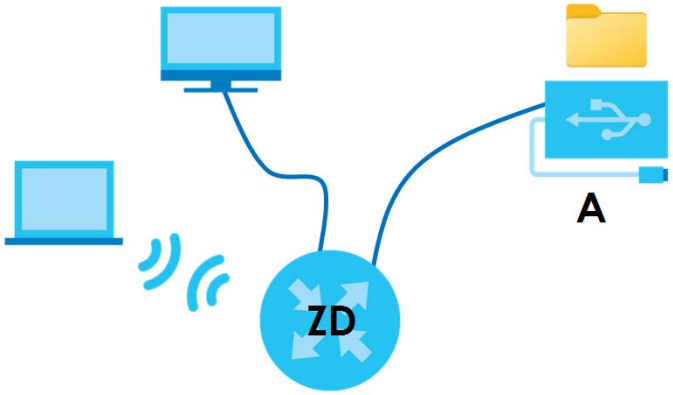
Figure 10 Internet Access Application: Cellular WAN



File Sharing

Use the built-in USB 3.0 port to share files on a USB memory stick or a USB hard drive (**A**).

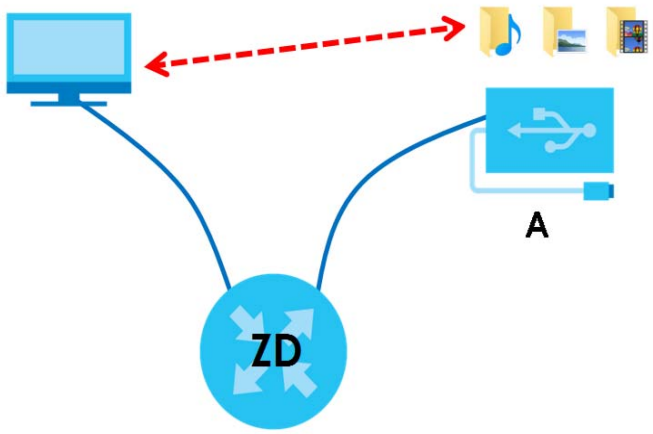
Figure 11 USB File Sharing Application



Media Server

You can also use the Zyxel Device as a media server. This lets anyone on your network play video, music, and photos from a USB device (**A**) connected to the Zyxel Device's USB port (without having to copy them to another computer).

Figure 12 USB Media Server Application



1.3 Ways to Manage the Zyxel Device

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

- Web Configurator. This is recommended for management of the Zyxel Device using a (supported) web browser.

- Secure Shell (SSH), Telnet. Use for troubleshooting the Zyxel Device by qualified personnel.
  - Zyxel One app. Download the Zyxel One app from Google Play or Apple Store to manage the Zyxel Device using a smartphone or tablet. To view Zyxel One app tutorials, please go to *https://service-provider.zyxel.com/app-help/ZyxelOne/FLA/LAN*

1.4 Good Habits for Managing the Zyxel Device

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

- Change the WiFi and Web Configurator passwords. Use a password that is not easy to guess and that consists of different types of characters, such as numbers, letters, and special characters.
- Write down the passwords and put it in a safe place.
- Back up the configuration. 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 Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Zyxel Device. You could simply restore your last configuration.

CHAPTER 2
Hardware

2.1 Overview

This section describes the front and rear panels for each model. Refer to the Zyxel Device's Quick Start Guides to see the product drawings and how to make the hardware connections.

2.2 LED Indicators Panel

The following shows the LED indicator panel and the LED behaviors of the Zyxel Device. None of the LEDs are on if the Zyxel Device is not receiving power. See Section 2.3 on page 38 to check whether your Zyxel Device has ports for multi-gigabit Ethernet, SFP, PON, or phone connections.

Ethernet Gateways

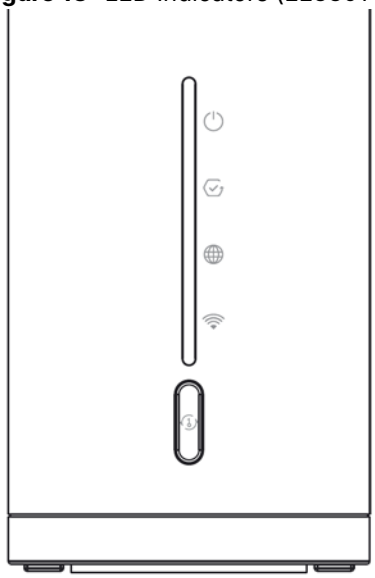
- EE3301-00
- EE4410-00
- EE5301-00
- EE6510-10
- EE6601-00

PON Gateways

- PE3301-00
- PE5301-01

EE3301-00

Figure 13 LED Indicators (EE3301-00)



The following are the LED descriptions for your Zyxel Device.

Table 6 LED Descriptions (EE3301-00)

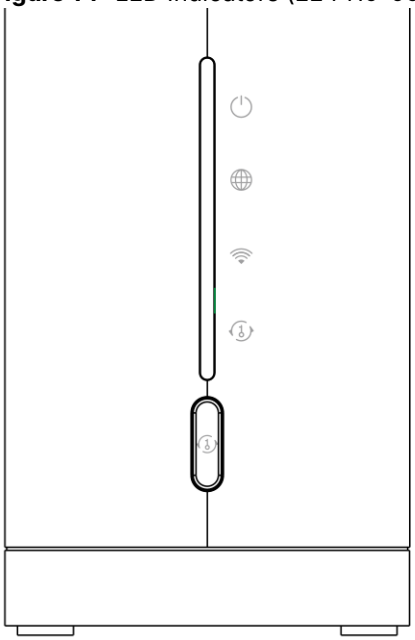
LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use. The Mesh pairing is done.
		Blinking	The Zyxel Device is booting up or under the Mesh pairing process.
	Red	On	The Zyxel Device detects an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware or the Mesh pairing process has failed.
	Off		The Zyxel Device is not receiving power.
STATUS	Green	On	The WAN connection is active and ready for use. All phone ports are on-hook. An VoIP account is registered for at least one phone port, and there is no voice message in the corresponding VoIP account.
		Blinking	At least one telephone connected to one of the phone ports has its receiver off the hook or there is an incoming call. There is no voice message in the corresponding VoIP account.
	Amber	On	The VoIP service is enabled, but the VoIP account registration has failed.
	Off		All phone ports are on-hook. The VoIP function is disabled, or there is no registered VoIP account defined for any of the phone ports.
INTERNET	Green	On	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is active.
		Blinking	The Zyxel Device is sending or receiving traffic.
	Red	On	The Zyxel Device attempted to obtain an WAN IP but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Blinking	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is active.
	Off		There is no Internet connection or the gateway is in bridged mode.

Table 6 LED Descriptions (EE3301-00) (continued)

LED	COLOR	STATUS	DESCRIPTION
WiFi / WPS	Green	On	The WiFi is activated.
		Blinking	The Zyxel Device is communicating with WiFi clients.
	Amber	Blinking	The Zyxel Device is setting up a WPS connection with a WiFi client.
	Off		The WiFi network is not activated.

EE4410-00

Figure 14 LED Indicators (EE4410-00)



The following are the LED descriptions for your Zyxel Device.

Table 7 LED Descriptions (EE4410-00)

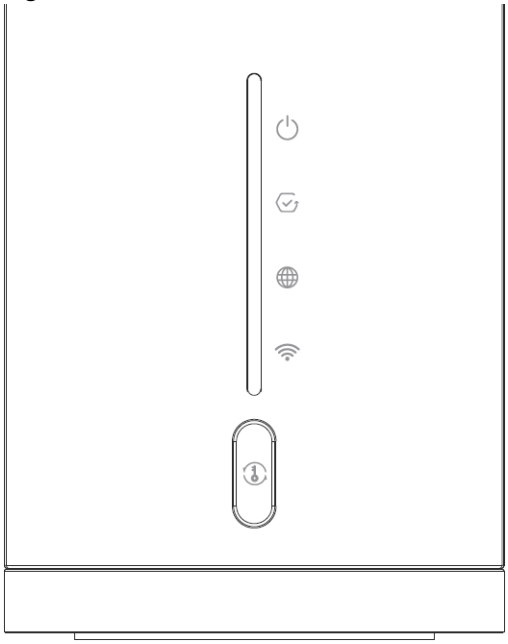
LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use. The Mesh pairing is done.
		Blinking	The Zyxel Device is booting up or under the Mesh pairing process.
	Red	On	The Zyxel Device detects an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware or the Mesh pairing process has failed.
	Off		The Zyxel Device is not receiving power.
INTERNET	Green	On	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is active.
		Blinking	The Zyxel Device is sending or receiving traffic.
	Red	On	The Zyxel Device attempted to obtain an WAN IP but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		There is no Internet connection or the gateway is in bridged mode.

Table 7 LED Descriptions (EE4410-00) (continued)

LED	COLOR	STATUS	DESCRIPTION
WiFi	Green	On	The 2.4 GHz, 5 GHz, and 6 GHz wireless connections are ready.
		Blinking	The Zyxel Device is communicating with WiFi clients.
	Off		Either the 2.4 Ghz, 5 Ghz, or 6 Ghz wireless connection is not ready or has failed.
WPS	Green	On	The Mesh network is ready for use.
		Blinking	The WPS process is in progress.
		Off	The Mesh network is not ready.
	Amber	Blinking	The IPTV Wi-Fi network WPS is in progress.

EE5301-00

Figure 15 LED Indicators (EE5301-00)



The following are the LED descriptions for your Zyxel Device.

Table 8 LED Descriptions (EE5301-00)

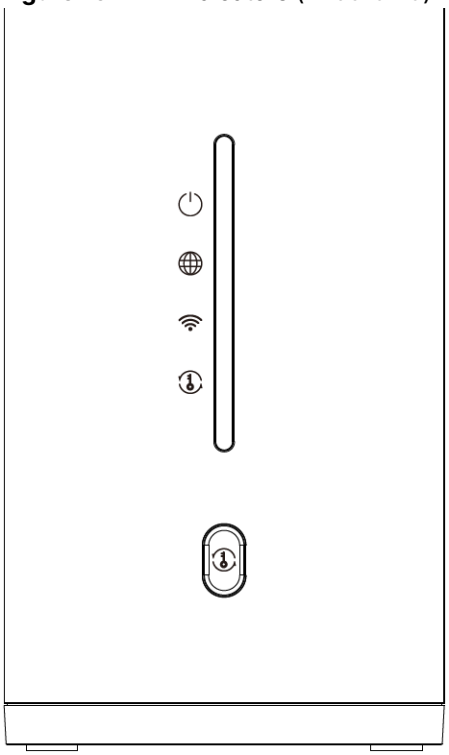
LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use. The Mesh pairing is done.
		Blinking	The Zyxel Device is booting up or under the Mesh pairing process.
	Red	On	The Zyxel Device detects an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware or the Mesh pairing process has failed.
	Off		The Zyxel Device is not receiving power.

Table 8 LED Descriptions (EE5301-00) (continued)

LED	COLOR	STATUS	DESCRIPTION
STATUS	Green	On	The WAN connection is active and ready for use. All phone ports are on-hook. An VoIP account is registered for at least one phone port, and there is no voice message in the corresponding VoIP account.
		Blinking	At least one telephone connected to one of the phone ports has its receiver off the hook or there is an incoming call. There is no voice message in the corresponding VoIP account.
	Amber	On	The VoIP service is enabled, but the VoIP account registration has failed.
		Blinking	The PON registration has failed. (For PON connection only)
	Off		All phone ports are on-hook. The VoIP function is disabled, or there is no registered VoIP account defined for any of the phone ports.
INTERNET	Green	On	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is active.
		Blinking	The Zyxel Device is sending or receiving traffic.
	Red	On	The Zyxel Device attempted to obtain an WAN IP but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		There is no Internet connection or the gateway is in bridged mode.
WiFi	Green	On	The WiFi is activated.
		Blinking	The Zyxel Device is communicating with WiFi clients.
	Amber	Blinking	The Zyxel Device is setting up a WPS connection with a WiFi client.
	Off		The WiFi network is not activated.

EE6510-10

Figure 16 LED Indicators (EE6510-10)



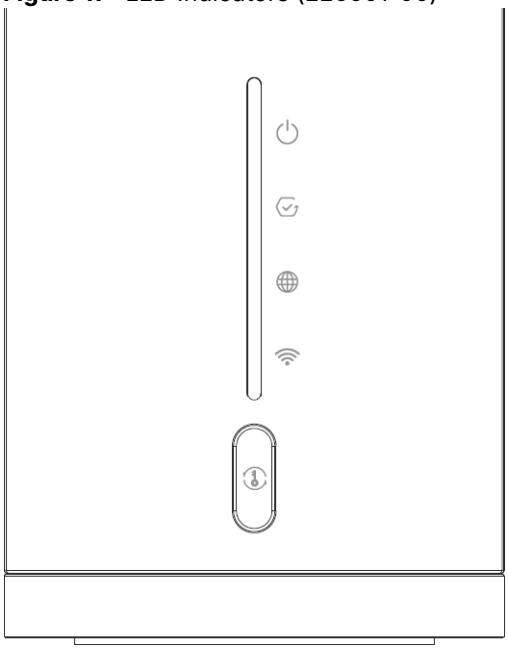
The following are the LED descriptions for your Zyxel Device.

Table 9 LED Descriptions (EE6510-10)

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting up.
	Red	On	The Zyxel Device detects an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware.
		Off	The Zyxel Device is not receiving power.
INTERNET	Green	On	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is up.
		Blinking	The Zyxel Device is sending or receiving Internet data.
		Off	There is no Internet connection or the Zyxel Device is in **Bridge** mode.
	Red	On	The Zyxel Device attempted to obtain an WAN IP address but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
Wi-Fi	Green	On	The 2.4 GHz, 5 GHz or 6 GHz Wi-Fi connection is activated.
		Blinking	The Zyxel Device is sending or receiving data.
		Off	The 2.4 GHz, 5 GHz, and 6 GHz Wi-Fi network is not ready or failed.
WPS	Green	On	The Mesh network is ready for use.
		Blinking	The WPS process is in progress.
		Off	The Mesh network is not ready.
	Amber	Blinking	The IPTV Wi-Fi network WPS is in progress.

EE6601-00

Figure 17 LED Indicators (EE6601-00)



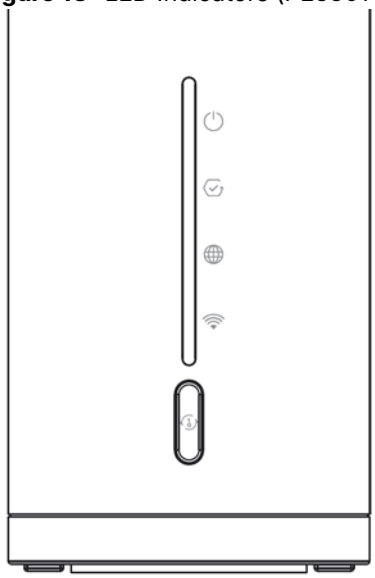
The following are the LED descriptions for your Zyxel Device.

Table 10 LED Descriptions (EE6601-00)

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting up.
	Red	On	The Zyxel Device detects an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware.
	Off		The Zyxel Device is not receiving power.
STATUS 	Green	On	The WAN connection is active and ready for use. All phone ports are on-hook. An VoIP account is registered for at least one phone port, and there is no voice message in the corresponding VoIP account.
		Blinking	At least one telephone connected to one of the phone ports has its receiver off the hook or there is an incoming call. There is no voice message in the corresponding VoIP account.
	Amber	On	The VoIP service is enabled, but the VoIP account registration has failed.
	Off		All phone ports are on-hook. The VoIP function is disabled, or there is no registered VoIP account defined for any of the phone ports.
INTERNET 	Green	On	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is active.
		Blinking	The Zyxel Device is sending or receiving traffic.
	Red	On	The Zyxel Device attempted to obtain an WAN IP but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		There is no Internet connection or the gateway is in bridged mode.
WiFi 	Green	On	The WiFi is activated.
		Blinking	The Zyxel Device is communicating with WiFi clients.
	Amber	Blinking	The Zyxel Device is setting up a WPS connection with a WiFi client.
	Off		The WiFi network is not activated.

PE3301-00

Figure 18 LED Indicators (PE3301-00)



The following are the LED descriptions for your Zyxel Device.

Table 11 LED Descriptions (PE3301-00)

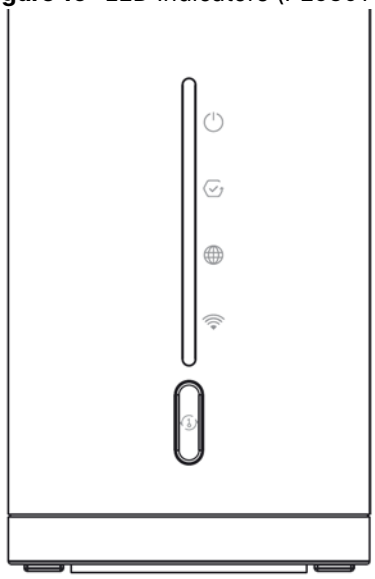
LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use. The Mesh pairing is done.
		Blinking	The Zyxel Device is booting up or under the Mesh pairing process.
	Red	On	The Zyxel Device detects an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware or the Mesh pairing process has failed.
		Off	The Zyxel Device is not receiving power.
STATUS	Green	On	The WAN connection is active and ready for use. All phone ports are on-hook. An VoIP account is registered for at least one phone port, and there is no voice message in the corresponding VoIP account. PON registration is successful.
		Blinking	At least one telephone connected to one of the phone ports has its receiver off the hook or there is an incoming call. There is no voice message in the corresponding VoIP account.
	Amber	On	The VoIP service is enabled, but the VoIP account registration has failed.
		Blinking	PON registration is in progress. (For PON connection only)
	Off		All phone ports are on-hook. The VoIP function is disabled, or there is no registered VoIP account defined for any of the phone ports.

Table 11 LED Descriptions (PE3301-00) (continued)

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is active.
		Blinking	The Zyxel Device is sending or receiving traffic.
	Red	On	The Zyxel Device attempted to obtain an WAN IP but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Blinking	The Zyxel Device is receiving a low optical signal.
	Off		There is no Internet connection or the gateway is in bridged mode.
WiFi / WPS	Green	On	The WiFi is activated.
		Blinking	The Zyxel Device is communicating with WiFi clients.
	Amber	Blinking	The Zyxel Device is setting up a WPS connection with a WiFi client.
	Off		The WiFi network is not activated. The WPS process was expired or successful.

PE5301-01

Figure 19 LED Indicators (PE5301-01)



The following are the LED descriptions for your Zyxel Device.

Table 12 LED Descriptions (PE5301-01)

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use. The Mesh pairing is done.
		Blinking	The Zyxel Device is booting up or under the Mesh pairing process.
	Red	On	The Zyxel Device detects an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware or the Mesh pairing process has failed.
		Off	The Zyxel Device is not receiving power.

Table 12 LED Descriptions (PE5301-01) (continued)

LED	COLOR	STATUS	DESCRIPTION
STATUS	Green	On	The WAN connection is active and ready for use. All phone ports are on-hook. An VoIP account is registered for at least one phone port, and there is no voice message in the corresponding VoIP account. PON registration is successful.
		Blinking	At least one telephone connected to one of the phone ports has its receiver off the hook or there is an incoming call. There is no voice message in the corresponding VoIP account.
	Amber	On	The VoIP service is enabled, but the VoIP account registration has failed.
		Blinking	PON registration is in progress. (For PON connection only)
	Off		All phone ports are on-hook. The VoIP function is disabled, or there is no registered VoIP account defined for any of the phone ports.
INTERNET	Green	On	The Zyxel Device has a WAN IP address (either static or assigned by a DHCP server) and the Internet connection is active.
		Blinking	The Zyxel Device is sending or receiving traffic.
	Red	On	The Zyxel Device attempted to obtain an WAN IP but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Blinking	The Zyxel Device is receiving a low optical signal.
	Off		There is no Internet connection or the gateway is in bridged mode.
WiFi / WPS	Green	On	The WiFi is activated.
		Blinking	The Zyxel Device is communicating with WiFi clients.
	Amber	Blinking	The Zyxel Device is setting up a WPS connection with a WiFi client.
	Off		The WiFi network is not activated. The WPS process was expired or successful.

2.3 Ports Panel

The following shows the Zyxel Device ports panel and connection ports.

Ethernet Gateways

- EE3301-00
- EE4410-00
- EE5301-00
- EE6510-10
- EE6601-00

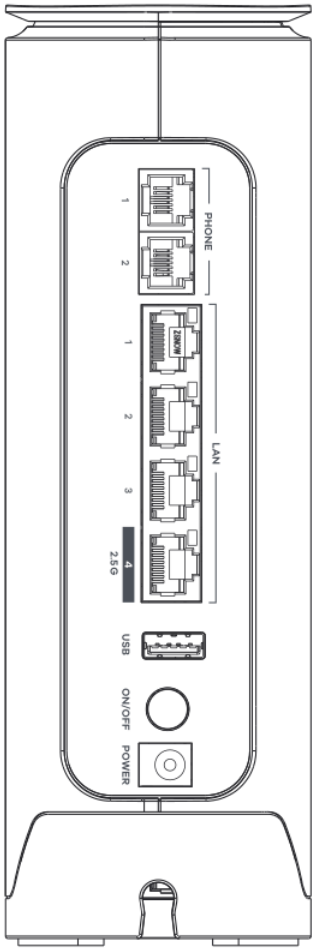
PON Gateways

- PE3301-00
- PE5301-01

EE3301-00

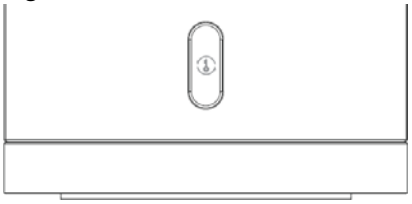
Place the Zyxel Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 20 Rear Panel (EE3301-00)



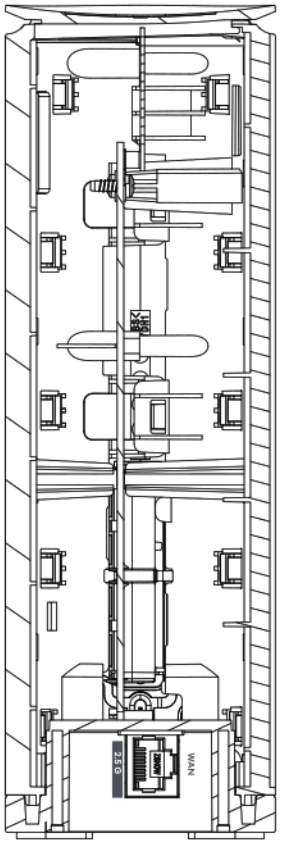
The WPS and WiFi On/Off button is on the front panel, near the bottom of the Zyxel Device.

Figure 21 WPS and WiFi On /Off Button on the Front Side of the Zyxel Device (EE3301-00)



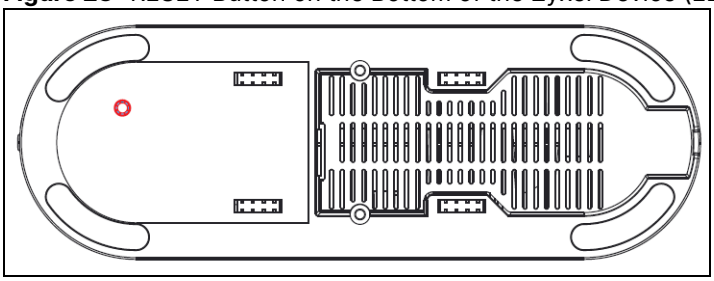
Remove the bottom cover to see the **2.5G WAN** port near the bottom of the Zyxel Device.

Figure 22 WAN Port (EE3301-00)



The **RESET** button is on the bottom of the Zyxel Device.

Figure 23 RESET Button on the Bottom of the Zyxel Device (EE3301-00)



The following table describes the items on the port panels of your Zyxel Device.

Table 13 Panel Ports and Buttons(EE3301-00)

LABEL	DESCRIPTION
PHONE 1, 2	Connect analog phones to the **PHONE** ports with RJ-11 cables for VoIP services.
LAN1 to 3	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
2.5G LAN (LAN 4)	The 2.5G LAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps and 2.5 Gbps. Connect computers or other Ethernet devices to the **2.5G LAN** port for Internet access with speed up to 2.5 Gbps.
USB	The USB port is used for cellular WAN backup, file-sharing, and media server.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device.

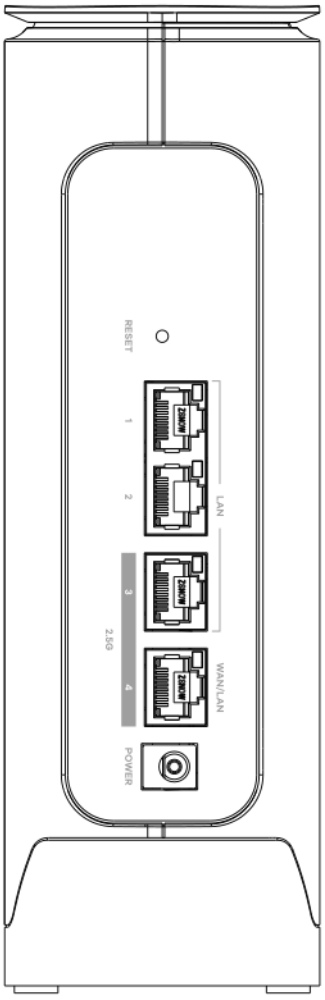
Table 13 Panel Ports and Buttons(EE3301-00) (continued)

LABEL	DESCRIPTION
WPS and WiFi On/Off	WPS: Press the WPS and WiFi On /Off button once within 3 seconds to quickly setup a secure WiFi connection between the device and a WPS-compatible client. WiFi On/Off: Press the WPS and WiFi On /Off button more than 15 seconds to enable the WiFi function.
2.5G WAN	The 2.5G WAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps and 2.5 Gbps. Connect an Ethernet cable to the **2.5G WAN** port for an (up to) 2.5 Gbps Ethernet connection.
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.

EE4410-00

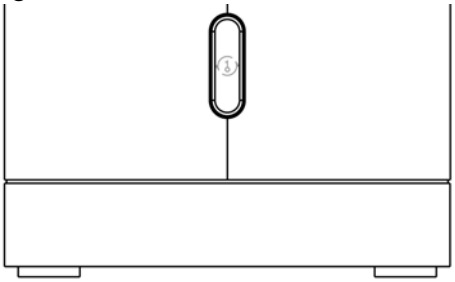
Place the Zyxel Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 24 Rear Panel (EE4410-00)



The WPS button is on the front panel, near the bottom of the Zyxel Device.

Figure 25 WPS Button on the Front Side of the Zyxel Device (EE4410-00)



The following table describes the items on the port panels of your Zyxel Device.

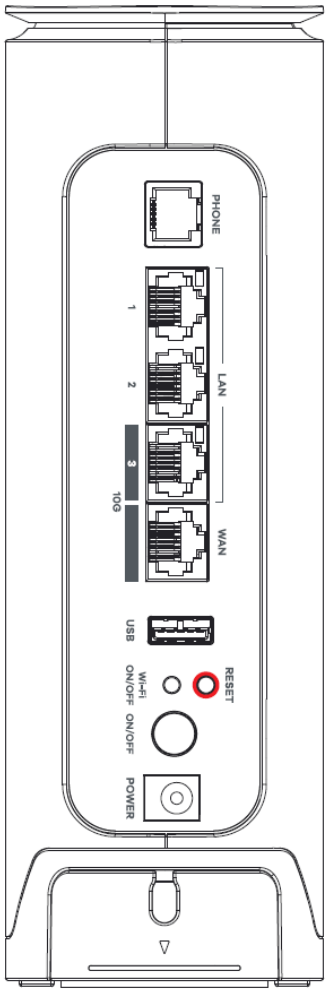
Table 14 Panel Ports and Buttons(EE4410-00)

LABEL	DESCRIPTION
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
LAN1, 2	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
2.5G LAN (LAN 3)	The 2.5G LAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps and 2.5 Gbps. Connect computers or other Ethernet devices to the **2.5G LAN** port for Internet access with speed up to 2.5 Gbps.
2.5G WAN (LAN 4)	The 2.5G WAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps and 2.5 Gbps. Connect an Ethernet cable to the **2.5G WAN** port for an (up to) 2.5 Gbps Ethernet connection.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device.
WPS	Press the WPS button more than 1 second to quickly setup a secure WiFi connection between the device and a WPS-compatible client.

EE5301-00

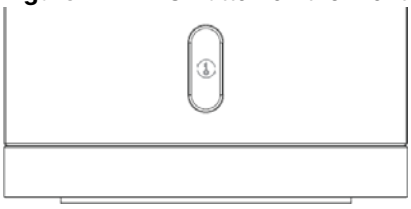
Place the Zyxel Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 26 Rear Panel (EE5301-00)



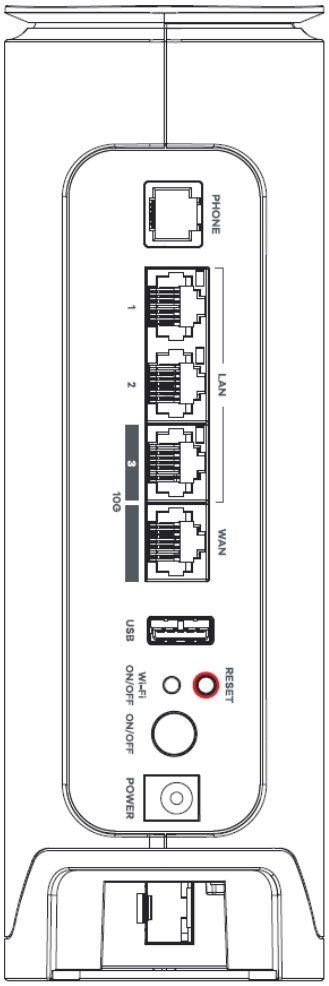
The WPS button is on the front panel, near the bottom of the Zyxel Device.

Figure 27 WPS Button on the Front Side of the Zyxel Device (EE5301-00)



The SFP+ Cage is on the bottom of the Zyxel Device.

Figure 28 SFP+ Cage on the Bottom of the Zyxel Device (EE5301-00)



The following table describes the items on the ports panels of your Zyxel Device.

Table 15 Panel Ports and Buttons(EE5301-00)

LABEL	DESCRIPTION
PHONE	Connect analog phones to the **PHONE** ports with RJ-11 cables for VoIP services.
LAN1, LAN2	LAN1 and LAN2 are 1G ports supporting speeds of 100/1000 Mbps. Connect computers or other Ethernet devices to Ethernet ports for Internet access.
10G LAN (LAN3)	The 10G LAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps. Connect computers or other Ethernet devices to the **10G LAN** port for Internet access with speed up to 10 Gbps.
10G WAN	The 10G WAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps. Connect an Ethernet cable to the **10G WAN** port for an (up to) 10 Gbps Ethernet connection.
USB	The USB port is used for cellular WAN backup, file-sharing, and media server.
Wi-Fi ON/ OFF	Press the **Wi-Fi ON/OFF** button for more than 2 seconds to enable the WiFi function.
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device.

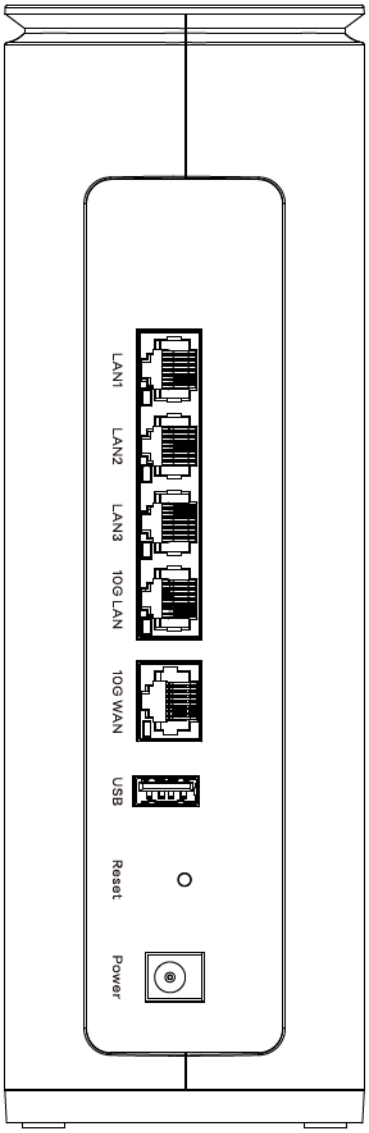
Table 15 Panel Ports and Buttons(EE5301-00) (continued)

LABEL	DESCRIPTION
WPS	Press the **WPS** button once within 3 seconds to quickly setup a secure WiFi connection between the device and a WPS-compatible client.
SFP+	Insert a compatible SFP transceiver to the SFP port and connect a fiber optic or Ethernet cable for an (up to) 10 Gbps Internet connection.

EE6510-10

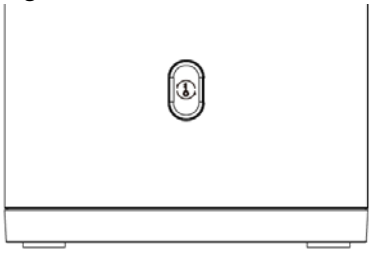
Place the Zyxel Device with the ports and buttons facing you and the Zyxel logo at the top.

Figure 29 Rear Panel (EE6510-10)



The WPS button is on the front panel, near the bottom of the Zyxel Device.

Figure 30 WPS / WLAN Button on the Front Side of the Zyxel Device(EE6510-10)



The following table describes the items on the ports panels of your Zyxel Device.

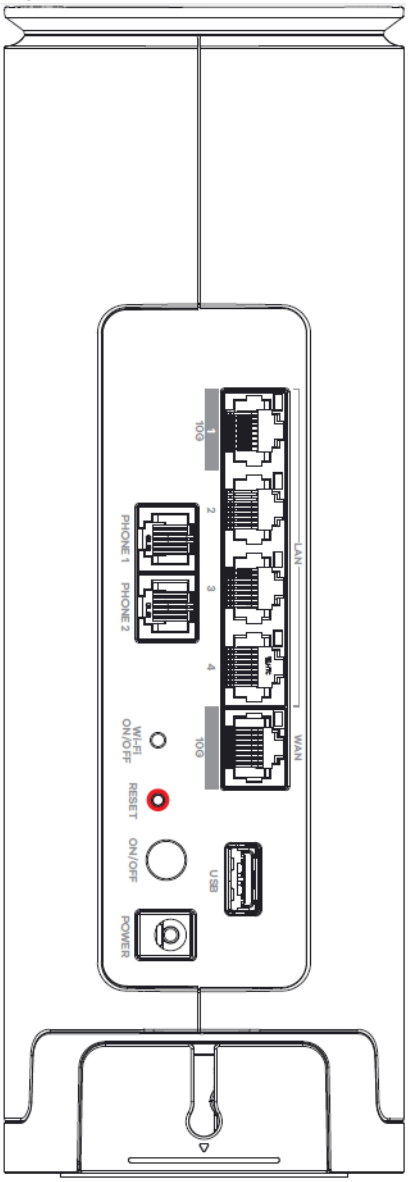
Table 16 Panel Ports and Buttons (EE6510-10)

LABEL	DESCRIPTION
LAN1 to 3	LAN1 to LAN3 are 1G ports supporting speeds of 100/1000 Mbps. Connect computers or other Ethernet devices to Ethernet ports for Internet access.
10G LAN	The 10G LAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps, 2.5 Gbps, and 10 Gbps. Connect computers or other Ethernet devices to the **10G LAN** port for Internet access with speed up to 10 Gbps.
10G WAN	The 10G WAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps, 2.5 Gbps, and 10 Gbps. Connect an Ethernet cable to the **10G WAN** port for an (up to) 10 Gbps Ethernet connection.
USB	The USB port is used for cellular WAN backup, file-sharing, and media server.
Reset	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
Power	Connect the power adapter and press the **ON/OFF** button to start the device.
WPS / WLAN	Press the **WPS** button once more than 1 second to quickly setup a secure Wi-Fi connection between the device and a WPS-compatible client.

EE6601-00

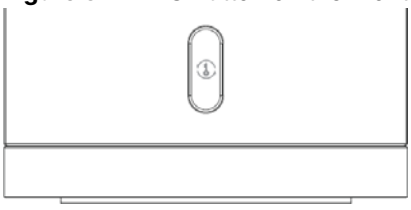
Place the Zyxel Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 31 Rear Panel (EE6601-00)



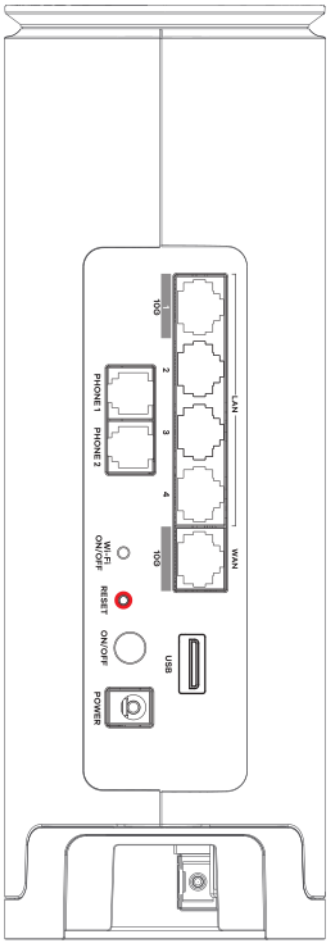
The WPS button is on the front panel, near the bottom of the Zyxel Device.

Figure 32 WPS Button on the Front Side of the Zyxel Device (EE6601-00)



The SFP+ Cage is on the bottom of the Zyxel Device.

Figure 33 SFP+ Cage on the Bottom of the Zyxel Device (EE6601-00)



The following table describes the items on the ports panels of your Zyxel Device.

Table 17 Panel Ports and Buttons (EE6601-00)

LABEL	DESCRIPTION
10G LAN (LAN1)	The 10G LAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps. Connect computers or other Ethernet devices to the **10G LAN** port for Internet access with speed up to 10 Gbps.
LAN2 to LAN4	LAN2 to LAN4 are 1G ports supporting speeds of 100/1000 Mbps. Connect computers or other Ethernet devices to Ethernet ports for Internet access.
10G WAN	The 10G WAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps. Connect an Ethernet cable to the **10G WAN** port for an (up to) 10 Gbps Ethernet connection.
PHONE1/2	Connect analog phones to the **PHONE** ports with RJ-11 cables for VoIP services.
Wi-Fi ON/ OFF	Press the **Wi-Fi ON/OFF** button for more than 2 seconds to enable the WiFi function.
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device.
USB	The USB port is used for cellular WAN backup, file-sharing, and media server.

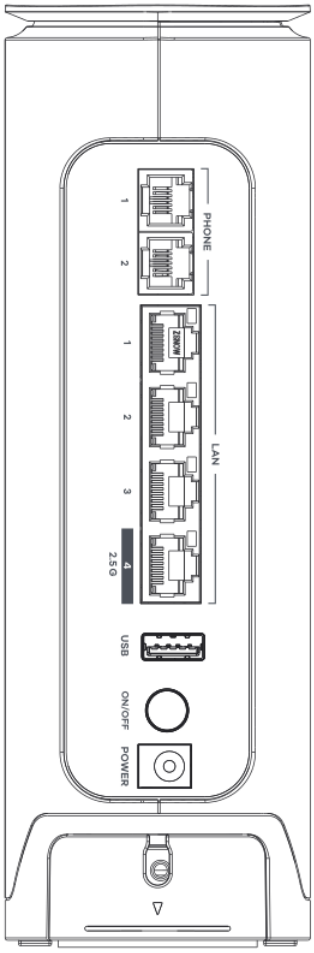
Table 17 Panel Ports and Buttons (EE6601-00) (continued)

LABEL	DESCRIPTION
WPS	Press the **WPS** button once within 3 seconds to quickly setup a secure WiFi connection between the device and a WPS-compatible client.
SFP+ Cage	Insert a compatible SFP transceiver to the SFP port and connect a fiber optic or Ethernet cable for an (up to) 10 Gbps Internet connection.

PE3301-00

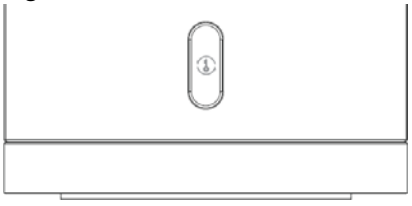
Place the Zyxel Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 34 Rear Panel (PE3301-00)



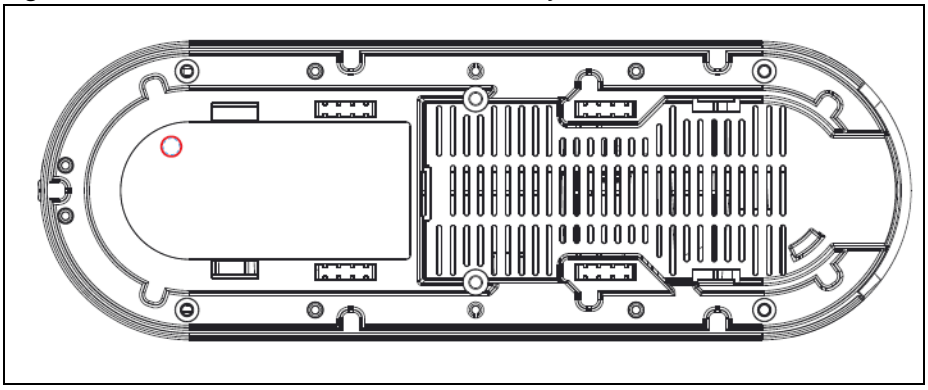
The WPS button is on the front panel, near the bottom of the Zyxel Device.

Figure 35 WPS and WiFi On /Off Button on the Front Side of the Zyxel Device (PE3301-00)



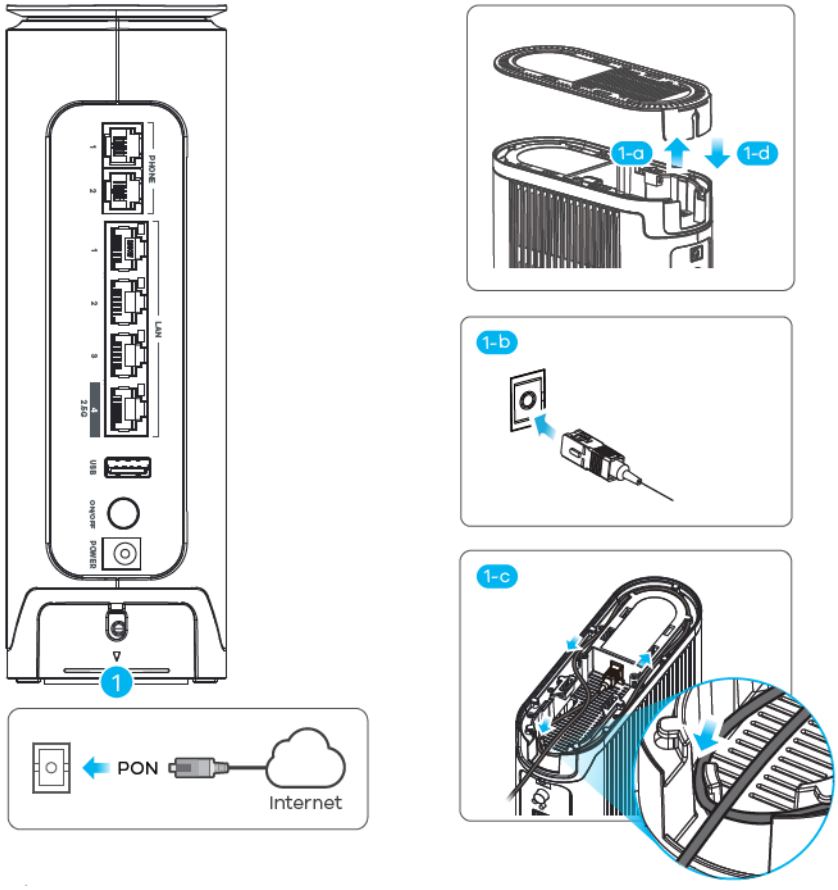
The **RESET** button is on the bottom of the Zyxel Device.

Figure 36 RESET Button on the Bottom of the Zyxel Device (PE3301-00)



The PON port is on the bottom of the Zyxel Device.

Figure 37 PON port on the Bottom of the Zyxel Device (PE3301-00)



The following table describes the items on the port panels of your Zyxel Device.

Table 18 Panel Ports and Buttons (PE3301-00)

LABEL	DESCRIPTION
PHONE 1, 2	Connect analog phones to the **PHONE** ports with RJ-11 cables for VoIP services.
LAN1, 3	Connect computers or other Ethernet devices to Ethernet ports for Internet access.

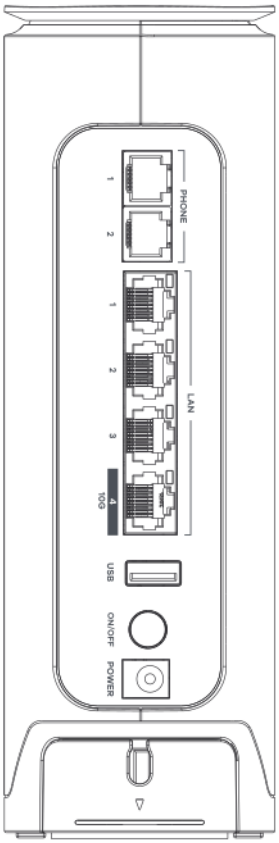
Table 18 Panel Ports and Buttons (PE3301-00) (continued)

LABEL	DESCRIPTION
2.5G LAN (LAN 4)	The 2.5G LAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps and 2.5 Gbps. Connect computers or other Ethernet devices to the **2.5G LAN** port for Internet access with speed up to 2.5 Gbps.
USB	The USB port is used for cellular WAN backup, file-sharing, and media server.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device.
WPS and WiFi On/Off	WPS: Press the **WPS** button once within 3 seconds to quickly setup a secure WiFi connection between the device and a WPS-compatible client. WiFi On/Off: Press the **WPS** button more than 15 seconds to enable the WiFi function.
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
PON	Connect the fiber optic cable to the PON (Passive Optical Network) port for Internet access.

PE5301-01

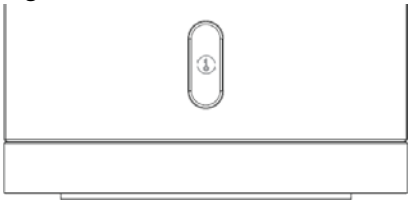
Place the Zyxel Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 38 Rear Panel (PE5301-01)



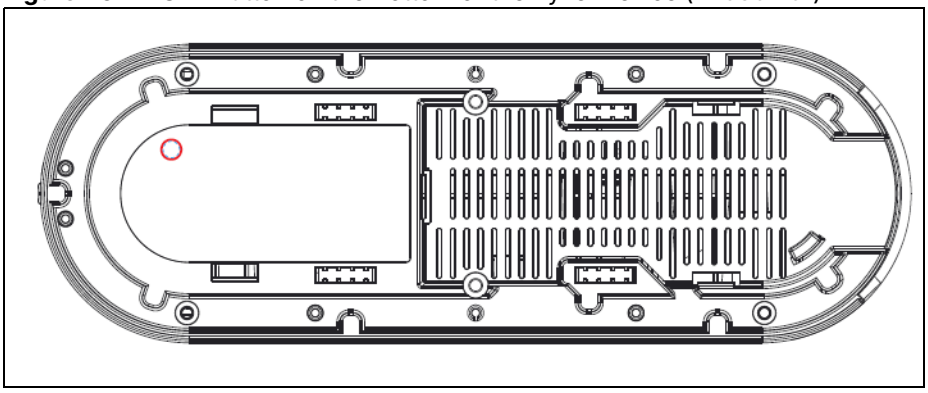
The WPS button is on the front panel, near the bottom of the Zyxel Device.

Figure 39 WPS and WiFi On /Off Button on the Front Side (PE5301-01)



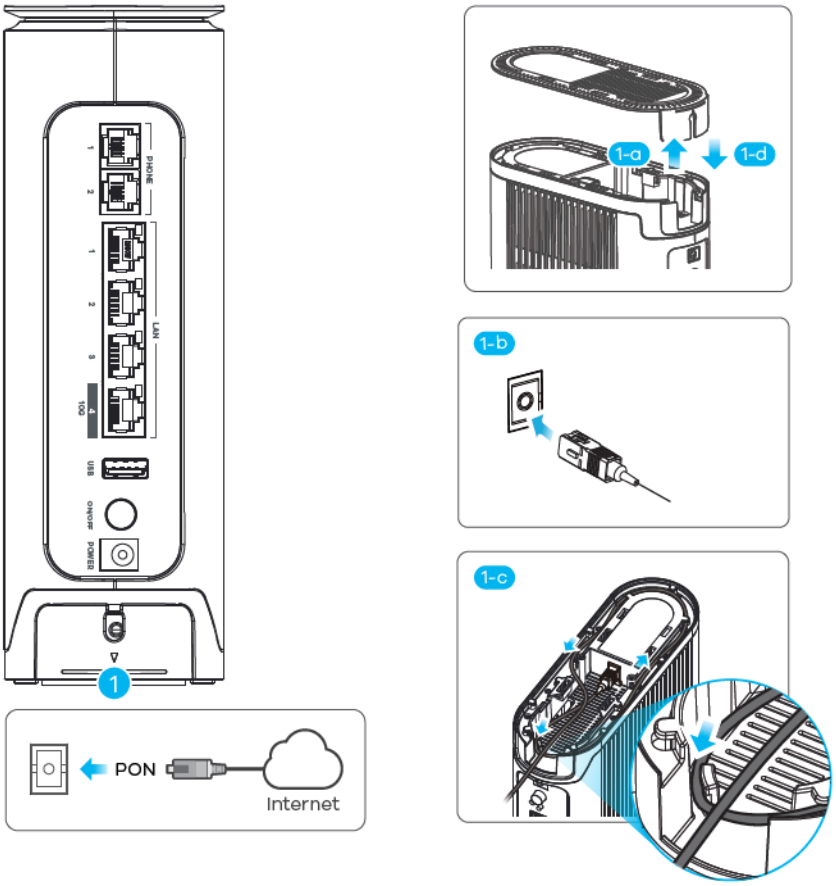
The **RESET** button is on the bottom of the Zyxel Device.

Figure 40 RESET Button on the Bottom of the Zyxel Device (PE5301-01)



The PON port is on the bottom of the Zyxel Device.

Figure 41 PON port on the Bottom of the Zyxel Device (PE5301-01)



The following table describes the items on the port panels of Zyxel Device.

Table 19 Panel Ports and Buttons (PE5301-01)

LABEL	DESCRIPTION
PHONE 1, 2	Connect analog phones to the **PHONE** ports with RJ-11 cables for VoIP services.
LAN 1to 3	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
10G LAN (LAN 4)	The 10G LAN port is a multi-gigabit Ethernet port that supports connection speeds of 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps. Connect computers or other Ethernet devices to the **10G LAN** port for Internet access with speed up to 10 Gbps.
USB	The USB port is used for cellular WAN backup, file-sharing, and media server.
POWER	Connect the power adapter and press the **ON/OFF** button to start the device.
WPS and WiFi On/Off	WPS: Press the **WPS** button once within 3 seconds to quickly setup a secure WiFi connection between the device and a WPS-compatible client. WiFi On/Off: Press the **WPS** button more than 15 seconds to enable the WiFi function.
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
PON	Connect the fiber optic cable to the PON (Passive Optical Network) port for Internet access.

2.3.1 Transceiver Installation/Removal

Transceiver Installation

Use the following steps to install an SFP transceiver.

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

2 Align the transceiver in front of the slot opening.

3 Make sure the latch is in the lock position (latch styles vary), then insert the transceiver into the slot with the exposed section of PCB board facing down.

4 Press the transceiver firmly until it clicks into place.

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

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

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

Figure 42 Latch in the Lock Position

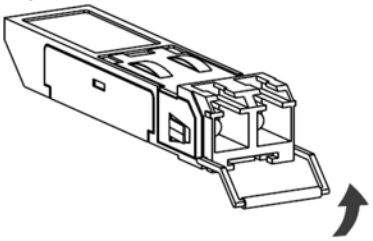


Figure 43 Transceiver Installation Example

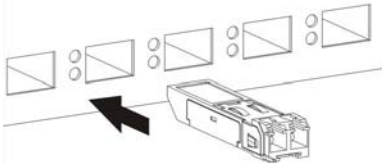
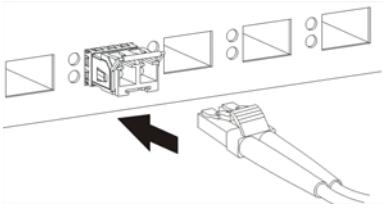


Figure 44 Connecting the Fiber Optic Cables



Transceiver Removal

Use the following steps to remove an SFP transceiver.

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

2 Remove the fiber optic cables from the transceiver.

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

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

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

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

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

Figure 45 Removing the Fiber Optic Cables

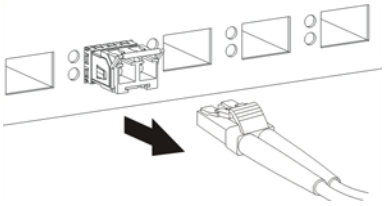


Figure 46 Opening the Transceiver's Latch Example

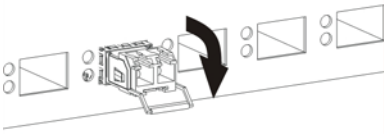
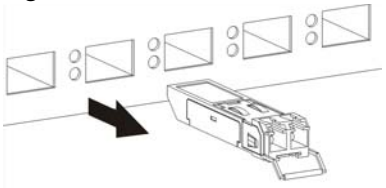


Figure 47 Transceiver Removal Example



2.3.2 WPS Button

You can use the **WPS** button to quickly set up a secure WiFi connection between the Zyxel Device and a WPS-compatible client by adding one device at a time.

To Activate WPS

1 Make sure the **POWER** LED is on and not blinking.

2 Press the **WPS** button once within 3 seconds (see the ports panel table of each Zyxel Device model in Section 2.3 on page 38 for more information) and release it.

3 Press the **WPS** button on another WPS-enabled device within range of the Zyxel Device (within 120 seconds). The **WPS** LED flashes green while the Zyxel Device sets up a WPS connection with the other wireless device.

4 Once the connection is successfully made, the **WPS** LED will light off.

2.3.3 RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to the factory default (see the device label), and the LAN IP address will be “192.168.1.1”.

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for more than 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

CHAPTER 3
Web Configurator

3.1 Overview

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

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

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

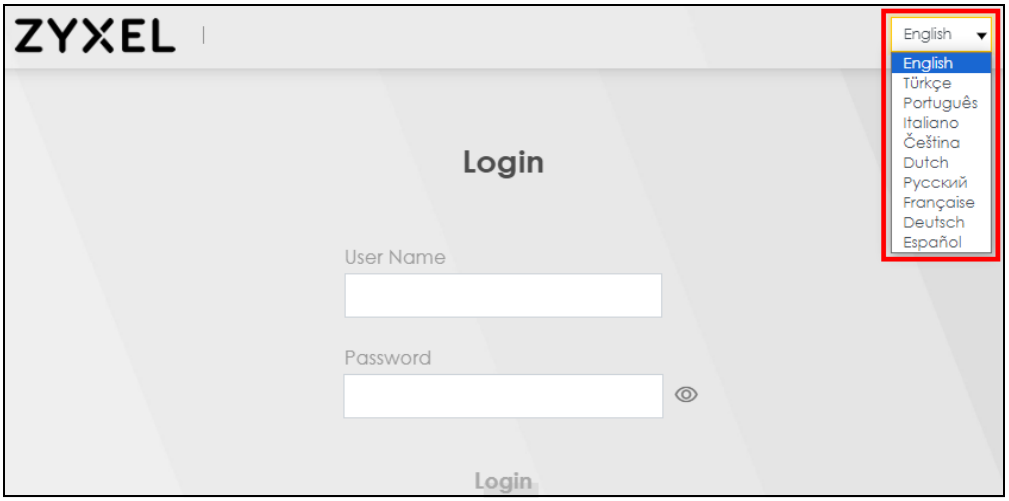
3.1.1 Access the Web Configurator

1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).

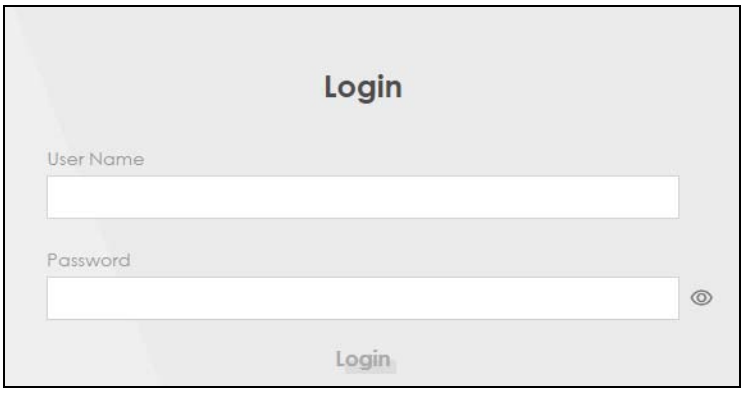
2 Make sure your computer has an IP address in the same subnet as the Zyxel Device.

3 Launch your web browser. Type http://192.168.1.1 in your browser address bar.

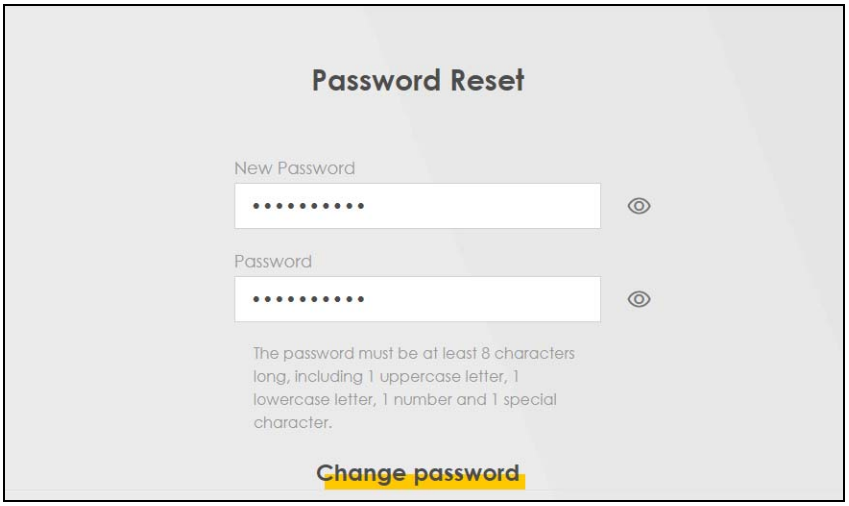
4 A login screen displays. Select the language you prefer (upper right).



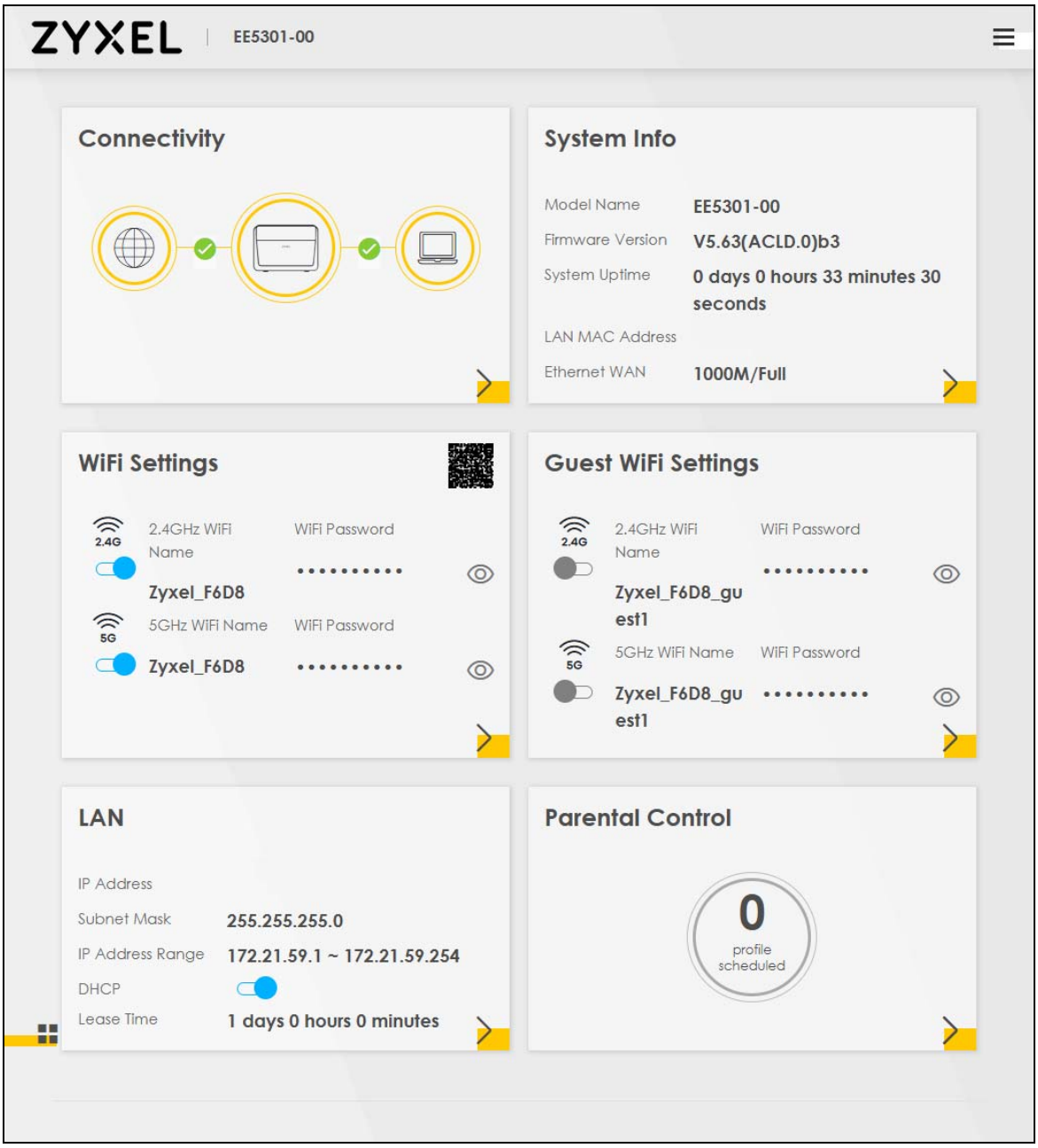
5 To access the administrative Web Configurator and manage the Zyxel Device, enter the default user name **admin** and the randomly assigned default password (see the Zyxel Device label) in the **Login** screen and click **Login**. If you have changed the password, enter your password and click **Login**.



Note: The first time you enter the password, you will be asked to change it. The new password must be at least 8 characters, must contain at least one uppercase letter, one lowercase letter, one number, and one special character. For some models, the password must contain at least one English character and one number. Please see the password requirement displayed on the screen.

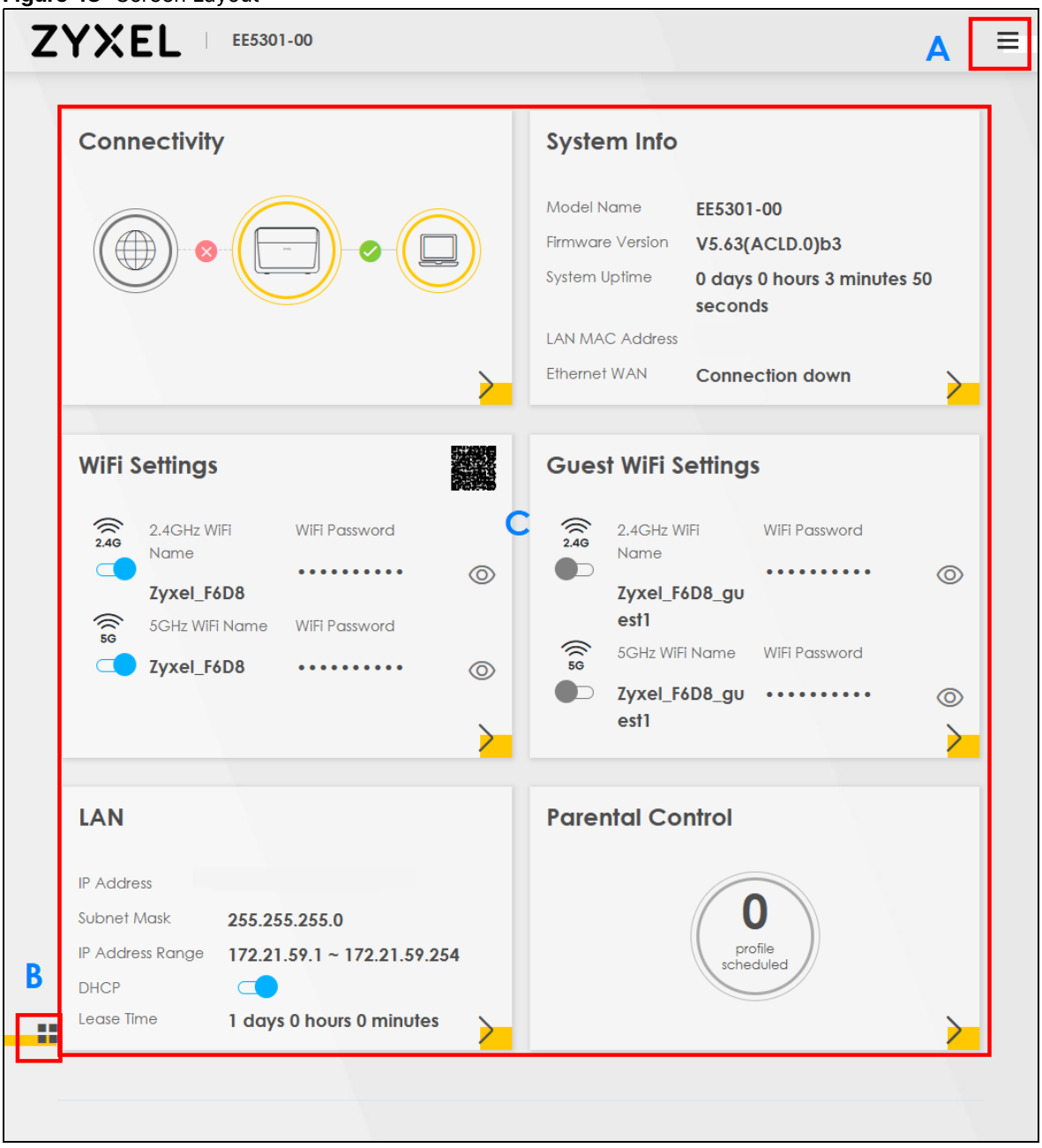


6 The **Connection Status** screen appears. Use this screen to configure basic Internet access and WiFi settings.


ZYXEL
EE5301-00
Connectivity
System Info
Model Name
EE5301-00
Firmware Version
V5.63(ACLD.0)b3
System Uptime
0 days 0 hours 33 minutes 30 seconds
LAN MAC Address
Ethernet WAN
1000M/Full
WiFi Settings
2.4GHz WiFi Name
WiFi Password
Zyxel_F6D8
5GHz WiFi Name
WiFi Password
Zyxel_F6D8
Guest WiFi Settings
2.4GHz WiFi Name
WiFi Password
Zyxel_F6D8_guest1
5GHz WiFi Name
WiFi Password
Zyxel_F6D8_guest1
LAN
IP Address
Subnet Mask
255.255.255.0
IP Address Range
172.21.59.1 ~ 172.21.59.254
DHCP
Lease Time
1 days 0 hours 0 minutes
Parental Control
0
profile scheduled

3.2 Web Configurator Layout

Figure 48 Screen Layout



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

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

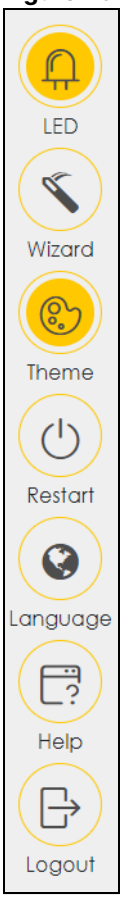
3.2.1 Settings Icon

Click this icon ( ) to see the side bar and navigation panel.

3.2.1.1 Side Bar

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

Figure 49 Side Bar

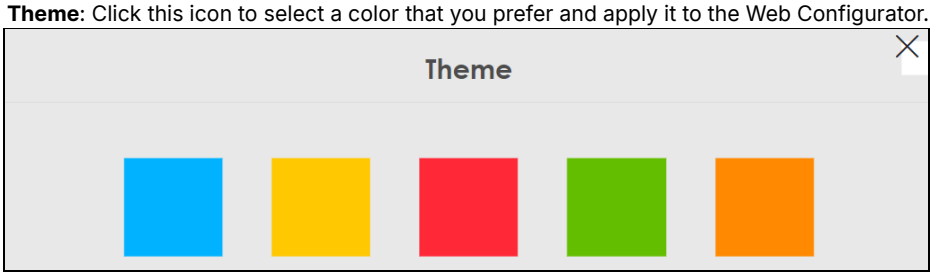


The icons provide the following functions.

Table 20 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	**LED**: Click this icon to turn off/on
	**Wizard**: Click this icon to open scree

Table 20 Web Configurator Icons in the Title Bar (continued)

ICON	DESCRIPTION
	**Theme**: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
	**Language**: Select the language you prefer.
	**Help:** Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.
	**Restart**: Click this icon to reboot the Zyxel Device without turning the power off.
	**Logout**: Click this icon to log out of the Web Configurator.

3.2.1.2 Navigation Panel

Click the menu icon ( ) to display the navigation panel that contains configuration menus and icons (quick links). Click **X** to close the navigation panel.

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

Figure 50 Navigation Panel

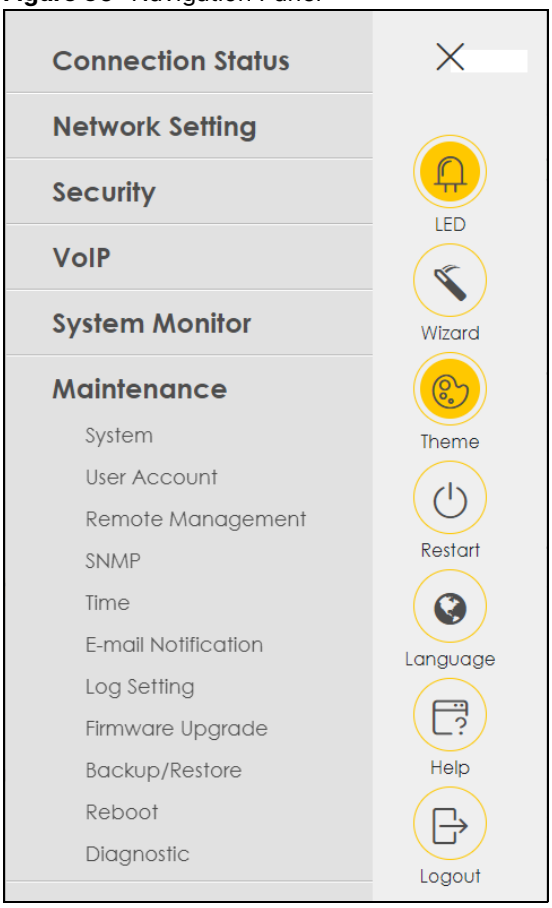


Table 21 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		Use this screen to configure basic Internet access, wireless settings, and parental control settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
	Cellular Backup	Use this screen to configure a cellular WAN connection as a backup to keep you online if the primary WAN connection fails.
Wireless	General	Use this screen to configure the WiFi settings and WiFi authentication or security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the Zyxel Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	Others	Use this screen to configure advanced WiFi settings.
	Channel Status	Use this screen to scan WiFi channel noises and view the results.
	MESH	Use this screen to enable or disable Mesh.

Table 21 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Custom DHCP	Use this screen to configure additional DHCP options.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	STB Vendor ID	Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses.
	Wake on LAN	Use this screen to remotely turn on a device on the local network.
	TFTP Server Name	Use DHCP option 66 to identify a TFTP server name.
	APAS	Use this screen to allow a LAN device to use any available port to access any available service from a remote WAN device.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers.
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device’s port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable the ALGs (Application Layer Gateways) in the Zyxel Device to allow applications to operate through NAT.
	Address Mapping	Use this screen to change your Zyxel Device's IP address mapping settings.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the Zyxel Device.
	PCP	Use this screen to configure PCP (Port Control Protocol) to allow devices such as web or file sharing servers behind the Zyxel Device to receive incoming traffic.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
IGMP/MLD	IGMP/MLD	Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN.
VLAN Group	VLAN Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.

Table 21 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Interface Grouping	Interface Grouping	Use this screen to map a port to create multiple networks on the Zyxel Device.
USB Service	File Sharing	Use this screen to enable file sharing through the Zyxel Device.
	Media Server	Use this screen to use the Zyxel Device as a media server.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Home Security	Connected Home Security	Use this screen to set up a URL filter that blocks users on your network from accessing certain websites.
Parental Control	Parental Control	Use this screen to define time periods and days during which the Zyxel Device performs parental control and/or block web sites with the specific URL.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
VoIP		
SIP	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the Zyxel Device.
	SIP Service Provider	Use this screen to configure the SIP server information, and other SIP settings, such as QoS for VoIP calls, outbound proxy, DTMF mode and SIP timers.
	SIP TLS Common	Use this screen to change the default TLS local port if you need to, and select a local certificate for the SIP server to verify the Zyxel Device.
Phone	Phone Device	Use this screen to control which SIP accounts each phone uses to handle outgoing and incoming calls.
	Region	Use this screen to select your location and call service mode.
Call Rule	Call Rule	Use this screen to configure speed dial for SIP phone numbers that you often call.
Call History	Call History	Use this screen to view detailed information for each outgoing call you made or each incoming call from someone calling you. You can also view a summary list of received, dialed and missed calls.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.

Table 21 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
	Security Log	Use this screen to view all security related events. You can select the level and category of the security events in their proper drop-down list window. Levels include: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: • Account • Attack • Firewall • MAC Filter
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
	NAT	Use this screen to view NAT statistics for connected hosts.
VoIP Status	VoIP Status	Use this screen to view VoIP registration, current call status and phone numbers for the phone ports.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the Zyxel Device.
Multicast Status	IGMP Status	Use this screen to view the status of all IGMP settings on the Zyxel Device.
	MLD Status	Use this screen to view the status of all MLD settings on the Zyxel Device.
WLAN Station Status	WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the Zyxel Device's WiFi.
Cellular Statistics	Cellular Statistics	Use this screen to look at the cellular Internet connection status.
Optical Signal Status	Optical Signal Status	Use this screen to view the optical fiber transceiver's TX power and RX power level and its temperature.
Maintenance		
System	System	Use this screen to set the Zyxel Device name and Domain name.
User Account	User Account	Use this screen to change the user password on the Zyxel Device.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** screen.
Power Monitor	Power Monitor	Use this screen to view the current and past amount of power consumed by the Zyxel Device.
Time	Time	Use this screen to change your Zyxel Device's time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Setting	Log Setting	Use this screen to change your Zyxel Device's log settings.

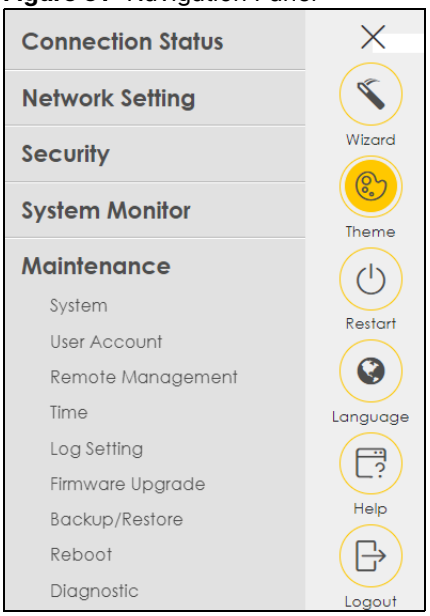
Table 21 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Zyxel Device / Zyxel Mesh system without turning the power off.
	Schedule Reboot	Use this screen to set the time to reboot the Zyxel Device without turning the power off.
Diagnostic	Diagnostic	Use this screen to identify problems with the Internet connection. You can use Ping, Ping 6, TraceRoute, TraceRoute 6, or Nslookup to help you identify problems.

3.2.1.3 Dashboard

Use the menu items in the navigation panel on the right to open screens to configure the Zyxel Device's features.

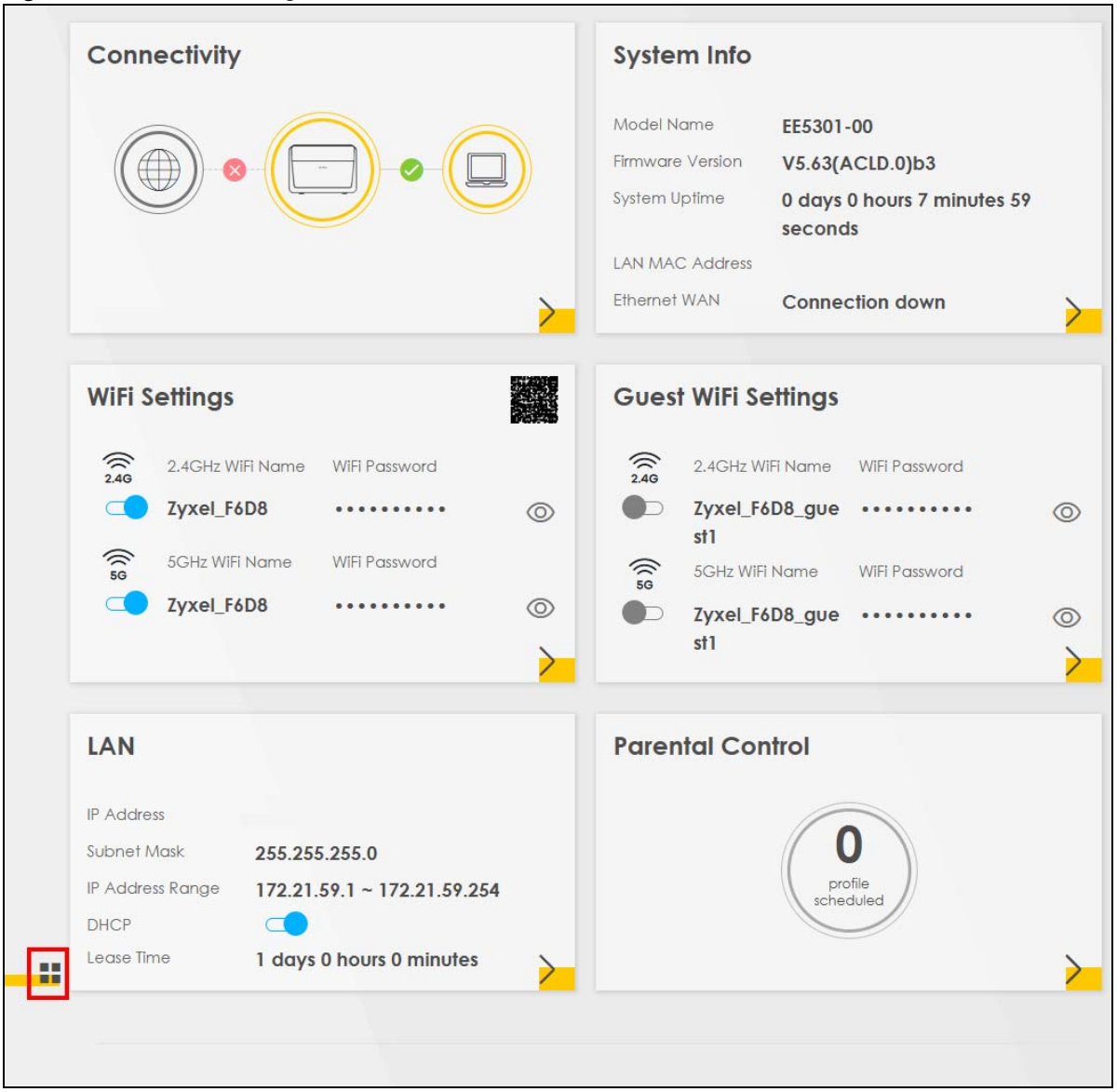
Figure 51 Navigation Panel



3.2.2 Widget Icon

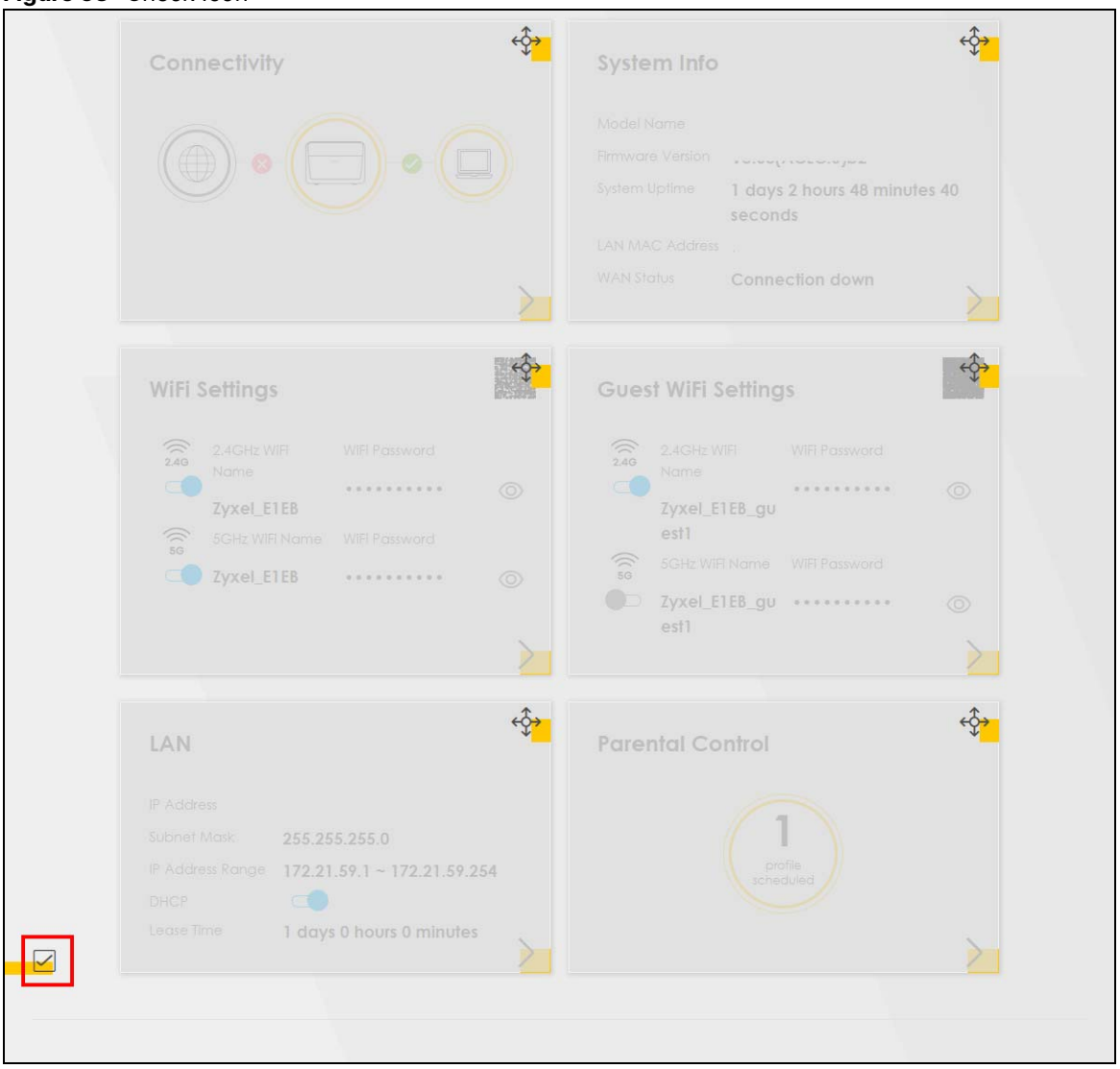
Click the Widget icon ( ) in the lower left corner to arrange the screen order.

Figure 52 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 53 Check Icon



CHAPTER 4
Quick Start

4.1 Quick Start Overview

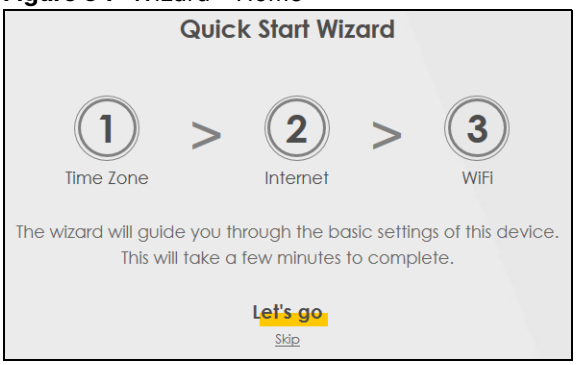
Use the **Wizard** screens to configure the Zyxel Device's time zone and WiFi settings.

Note: See the technical reference chapters for background information on the features in this chapter.

4.2 Quick Start Setup

You can click the **Wizard** icon in the side bar to open the **Wizard** screens. After you click the **Wizard** icon, the following screen appears. Click **Let's go** to proceed with settings on time zone and WiFi networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can click **Skip** to leave the **Wizard** screens.

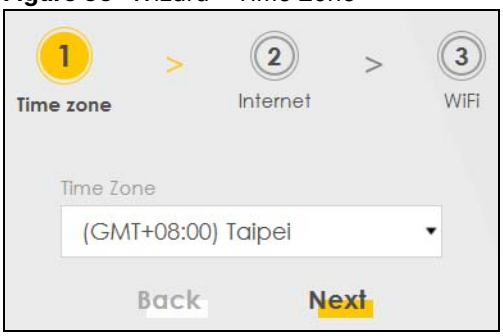
Figure 54 Wizard – Home



4.3 Quick Start Setup – Time Zone

Select the time zone of the Zyxel Device's location. Click **Next**.

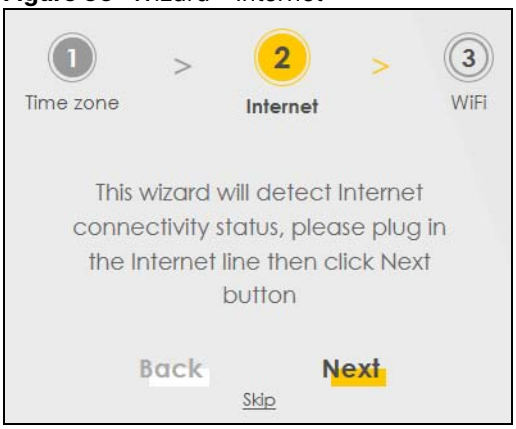
Figure 55 Wizard – Time Zone



4.4 Quick Start Setup – Internet Connection

The Zyxel Device detects your Internet connection status. Click **Next** to continue.

Figure 56 Wizard – Internet



4.4.1 Successful Internet Connection

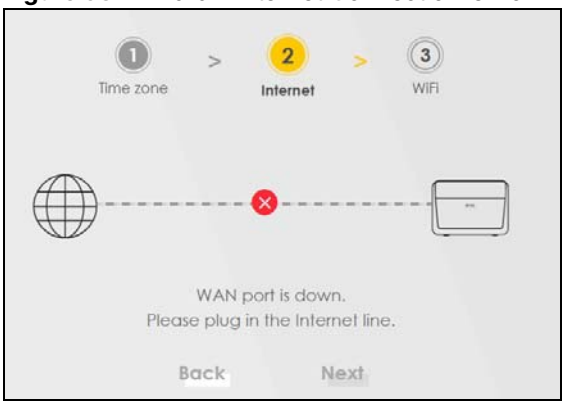
The Zyxel Device has Internet access.

Figure 57 Wizard – Successful Internet Connection

4.4.2 Unsuccessful Internet Connection

The Zyxel Device did not detect a WAN connection. See Section 43.5 on page 433 for troubleshooting the Zyxel Device WAN connection.

Figure 58 Wizard – Internet Connection is Down

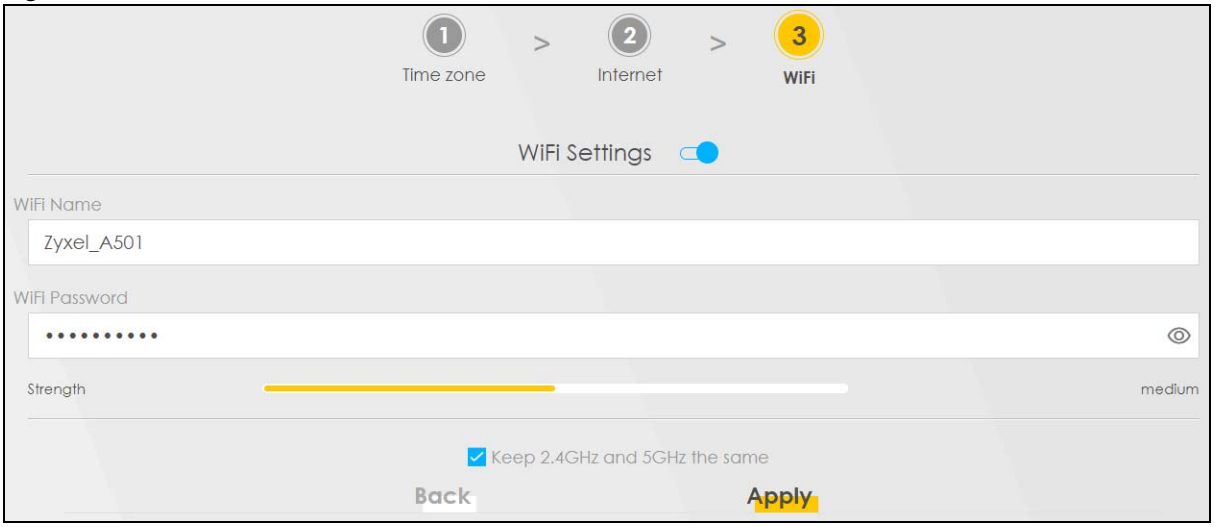


4.5 Quick Start Setup – WiFi

Turn WiFi on or off. If you keep it on, record the **WiFi Name** and **Password** in this screen so you can configure your WiFi clients to connect to the Zyxel Device. If you want to show or hide your WiFi password, click the Eye icon ( ).

Select **Keep 2.4GHz and 5GHz the same** to use the same SSID for 2.4 GHz and 5 GHz WiFi networks. Otherwise, clear the checkbox to have two different SSIDs for 2.4 GHz and 5 GHz WiFi networks. The screen and fields to enter may vary when you select or clear the checkbox.
You have to disable **MPro Mesh** in the **Network** > **Wireless** > **MESH** screen to clear the **Keep 2.4GHz and 5GHz the same** checkbox. Click **Done**.

Figure 59 Wizard – WiFi



4.6 Quick Start Setup – Finish

Your Zyxel Device saves and applies your settings.

CHAPTER 5
Web Interface Tutorials

5.1 Web Interface Overview

This chapter shows you how to use the Zyxel Device's various features.

- Device Settings - Rename your Zyxel Device, change the admin password, and change the management IP address.
- Wired Network Setup - Set up a wired network connection using DSL/GPON/Ethernet.
- WiFi Network Setup - Change the security mode, connect to the WiFi network using the WPS, set up a guest WiFi network with different WiFi bands, and configure the channel and bandwidth for each WiFi band.
- USB Applications - Set up file sharing and play files through Windows Media Player with a USB device.
- Network Security - Configure a firewall rule, set up parental control rule, and configure a MAC Filter rule.
- Internet Calls - Add a SIP service provider or a SIP account, to make phone calls over the Internet.
- Device Maintenance - Upgrade the firmware, back up the firmware, restore the Zyxel Device configuration, and reset the Zyxel Device to factory defaults.
- Remote Access from WAN - Configure remote access to your Zyxel Device and configure the trust domain.

5.2 Device Settings

This section shows you how to:

- Rename Your Zyxel Device
- Change the Admin Password
- Change the Management IP Address

You can rename your device, and change the admin password.

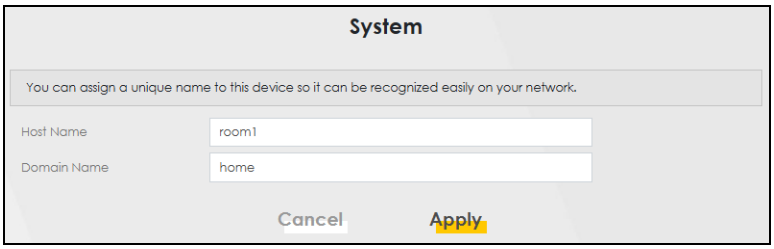
5.2.1 Rename Your Zyxel Device

An FQDN (Fully Qualified Domain Name) is used to identify a specific host on the Internet, consisting of a host name and a domain name.

Proper naming of the host name and domain name makes the Zyxel Device and the network easier to identify, manage, and troubleshoot. The host name is the name of your Zyxel Device, while the domain name is the name of the entire network your Zyxel Device belongs to. If your Zyxel Device's host name is room1, and it belongs to the domain you name with home.com, then your Zyxel Device's FQDN would be room1.home.com.

To change the host name and the domain name, please follow the steps below:

1 Go to the **Maintenance > System** screen. Enter a new host name in the **Host Name** field and a domain name in the **Domain Name** field (special characters and spaces are not allowed). Click **Apply**.

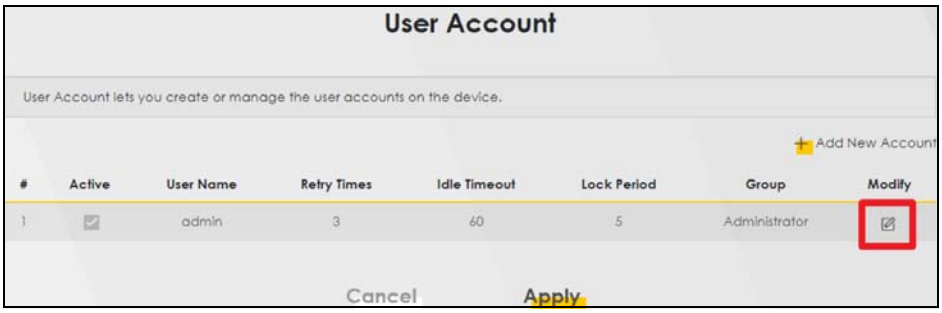


2 Go to the **Connection Status > System Info**. You can see the new host name has been applied successfully.

5.2.2 Change the Admin Password

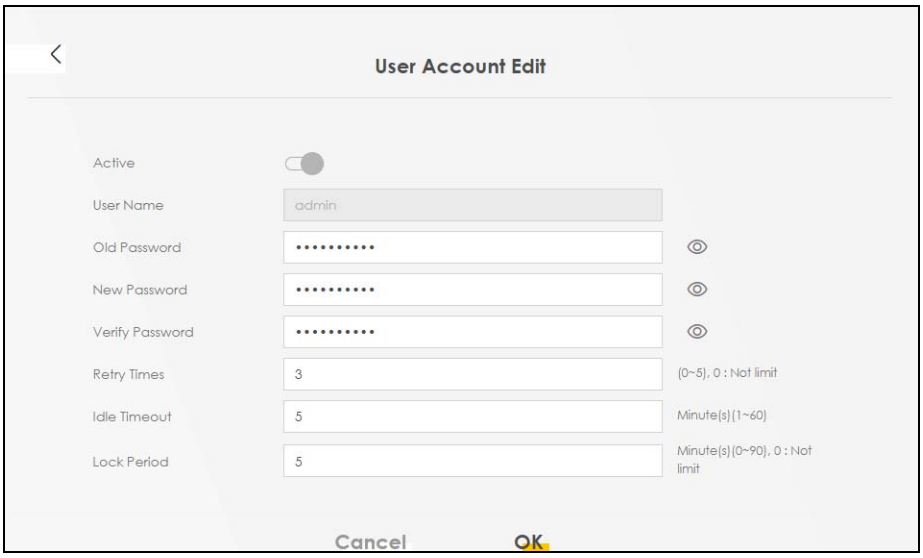
Change the Web Configurator login password regularly to secure access to your Zyxel Device. To change the admin password, follow the steps below:

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



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

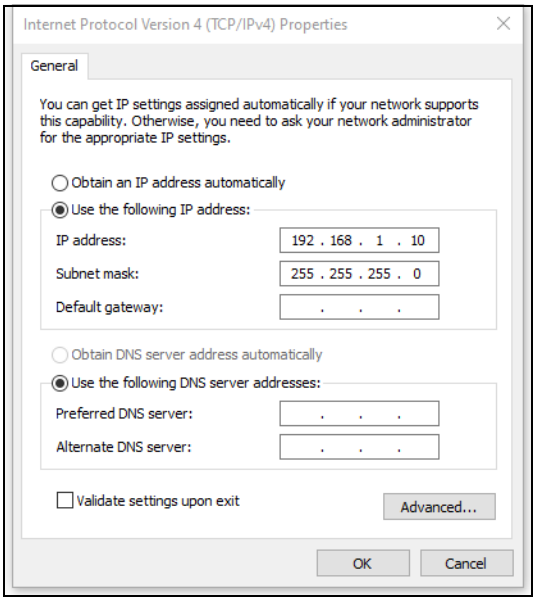
Note: The new password must be at least 8 characters, must contain at least one uppercase letter, one lowercase letter, one number, and one special character. For some models, the password must contain at least one English character and one number. Please see the password requirement displayed on the screen.



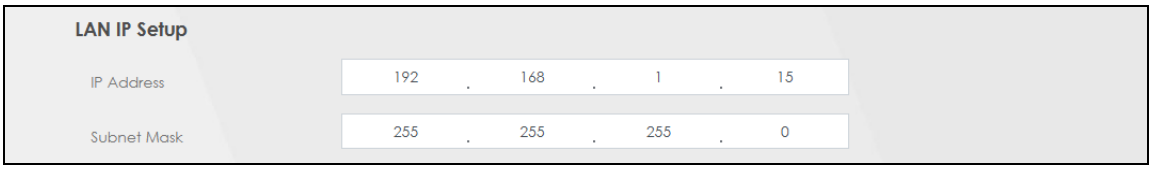
5.2.3 Change the Management IP Address

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

1 Change your computer's IP address to the same subnet as the Zyxel Device. For example, if the default static IP address of the Zyxel Device is 192.168.1.1, set your computer IP address between 192.168.1.2 and 192.168.1.254.

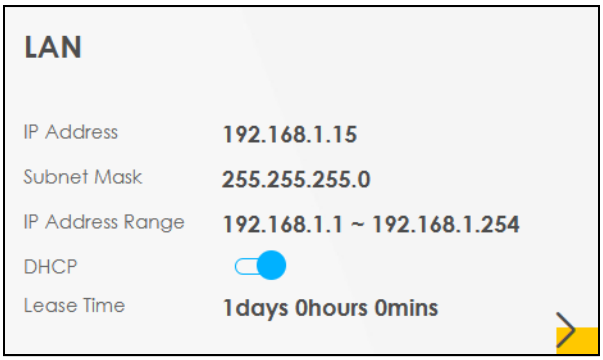


2 Log into the Zyxel Device using the default IP address "192.168.1.1". Go to **Network Setting** > **Home Networking**. Enter your preferred IPv4 address in the **IP Address** field. For example, "192.168.1.15". Click **Apply** and the Zyxel Device will disconnect from your computer due to the IP address change.



3 Enter the new IP address “192.168.1.15” in the address bar to check if you can access the Zyxel Device’s Web Configurator.

4 After logging in, click the menu icon ( ) and go to **Connection Status**. In the **LAN** section, the **IP Address** should now be “192.168.1.15”.



5.3 Wired Network Setup

This section shows you how to:

- Set Up a GPON Connection
- Set Up an Ethernet Connection

You can set up a PON, DSL or Ethernet Internet connection with the **Broadband** screens. The screens vary by the connection mode, encapsulation type and IP mode (IPv6 or IPv4) you select.

Set the Zyxel Device to **Routing** mode or **Bridge** mode on this connection as follows:

- Use **Routing** mode if you want the Zyxel Device to use routing mode functions such as **NAT**, **Firewall**, or **DHCP Server**. You will need to reconfigure your network if you have an existing router.
- Use **Bridge** mode to pass the ISP-assigned IP address(es) to your devices connected to the LAN port. All traffic from the Internet passes through the Zyxel Device directly to devices connected to the LAN port. Use this mode if you already have a router with complete routing functions in your network.

5.3.1 Set Up a GPON Connection

If you connect to the Internet through a GPON connection, you need to connect a broadband modem or router with Internet access to the WAN GPON port on the Zyxel Device. You need to configure the Internet settings from the broadband modem or router on the Zyxel Device. First, make sure you have Internet access through the broadband modem or router by connecting directly to it.

1 Make sure you have the GPON WAN port connect to a modem or router.

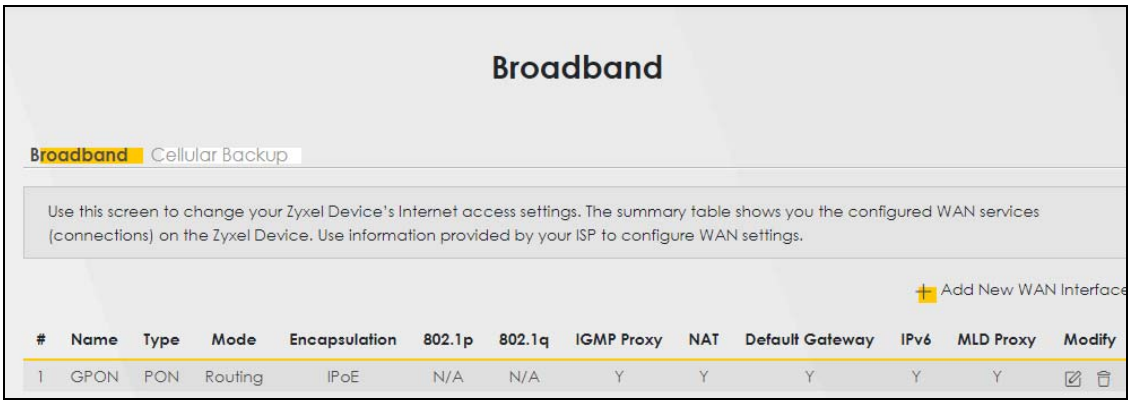
2 Register the GPON serial number on the back label of the Zyxel Device (ONT, Optical Network Terminal) with your Internet service provider (OLT, Optical Line Terminal). The LED indicator will show the status of the registration. The GPON registration process includes the states below for the Zyxel Device:

Table 22 GPON registration process

STATE	DESCRIPTION
O1	Initial State: Check if the GPON port of the Zyxel Device(ONT) is enabled and ready to connect to the Internet service provider (OLT).
O2	Standby State: The Zyxel Device(ONT) is trying to receive signals sent by the Internet service provider (OLT) and is responding.
O3	Serial Number State: The Internet service provider (OLT) is sending a serial number request for the Zyxel Device (ONT). The Zyxel Device (ONT) replies with the GPON serial number found on the back label of the Zyxel Device.
O4	Ranging State: The Internet service provider (OLT) is sending a ranging request to the Zyxel Device (ONT) and is asking for a response.
O5	Operation State: The GPON connection is established between the Zyxel Device (ONT) and the Internet service provider (OLT).

See Table 2.2 on page 29 for more information about the LED of GPON registration.

3 Go to **Network Setting** > **Broadband** and then the following screen appears. Click **Add New WAN Interface**.



4 To set the Zyxel Device to **Routing** mode, see Routing Mode on page 78.
To set the Zyxel Device to **Bridge** mode, see Bridge Mode on page 81.

Routing Mode

1 In this routing mode example, the PON WAN connection has the following information.

General	
Name	GPON-1
Type	GPON
Connection Mode	Routing
Encapsulation	IPoE

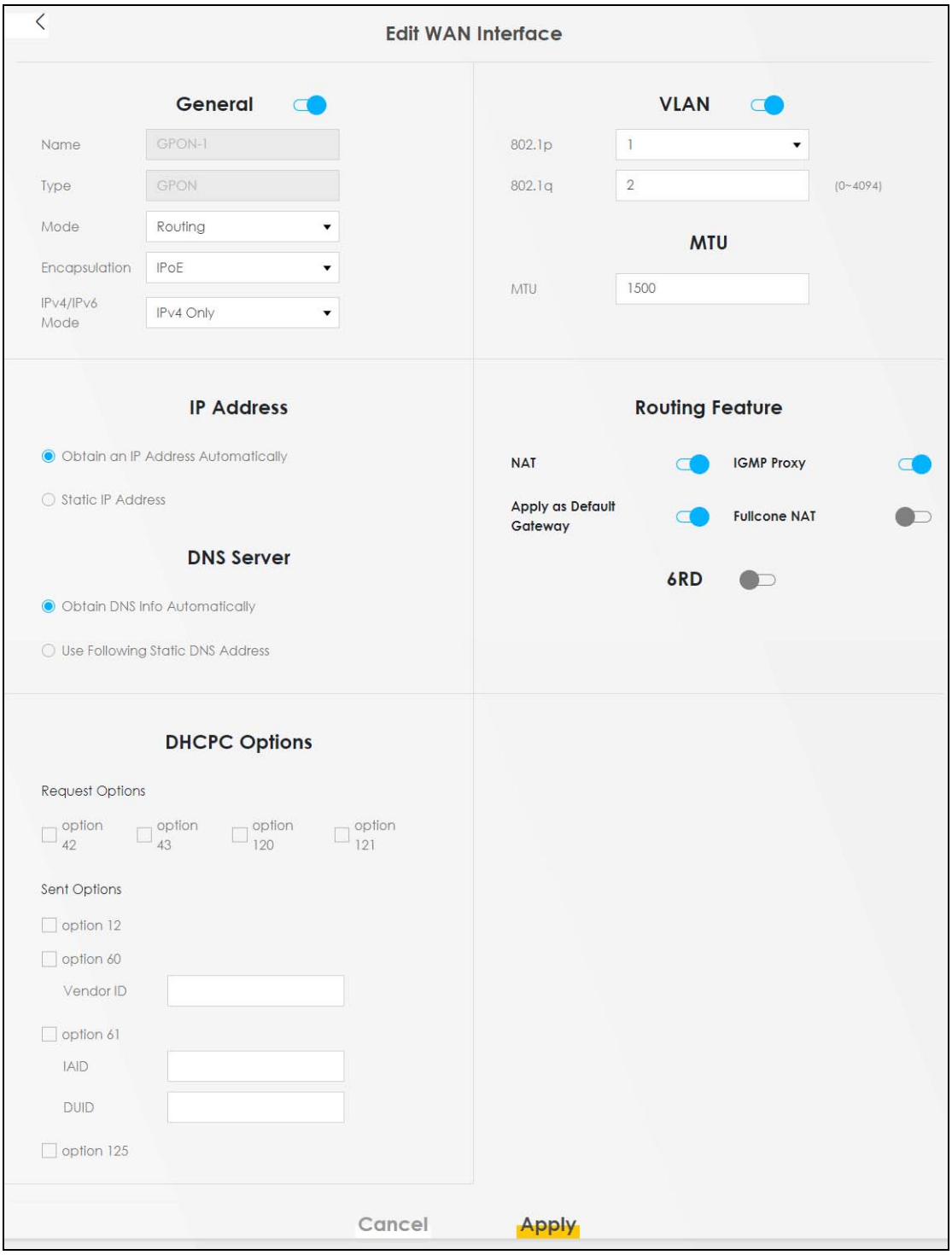
IPv6/IPv4 Mode	IPv4 Only
Others	NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enabled VLAN: Enabled

2 Enter the **General** settings as provided above.
- Enter a **Name** to identify your WAN connection.
- Set the **Type** to **GPON**.
- Set the **Mode** to **Routing**.
- Choose the **Encapsulation** specified by your GPON service provider.
- Set the **IPv4/IPv6 Mode** to **IPv4 Only**.

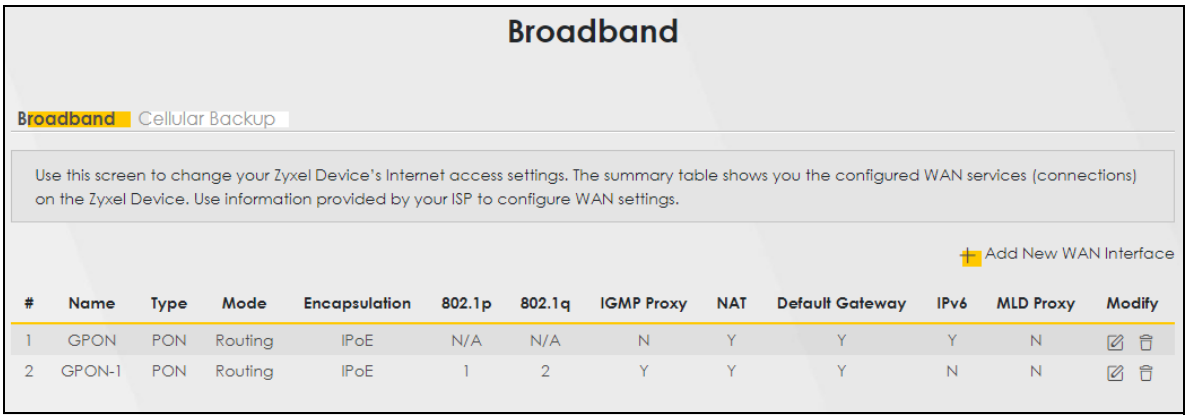
3 Under **Routing Feature**, enable **NAT** and **Apply as Default Gateway.**

4 For the rest of the fields, use the default settings.

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



6 Try to connect to a website to see if you have correctly set up your Internet connection. Go to the **Network Setting > Broadband** screen to view the established Ethernet connection. The new connection is displayed on the **Broadband** screen



The new connection is displayed on the **Broadband** screen.

Bridge Mode

1 In this bridge mode example, the GPON WAN connection has the following information.

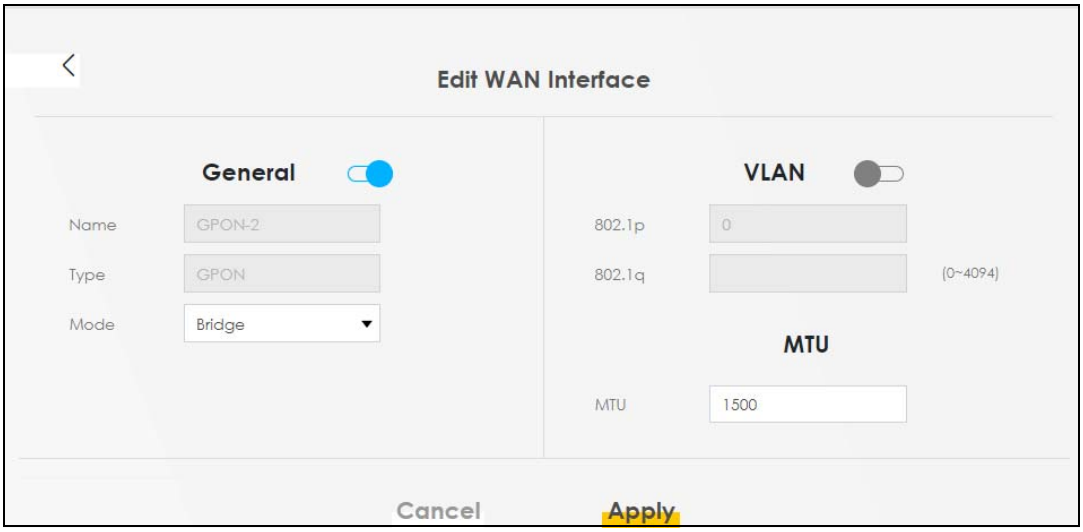
General	
Name	GPON-2
Type	GPON
Connection Mode	Bridge

2 Enter the **General** settings provided by your Internet service provider.

- Enter a **Name** to identify your WAN connection.
- Set the **Type** to **GPON**.
- Set your GPON connection **Mode** to **Bridge**.

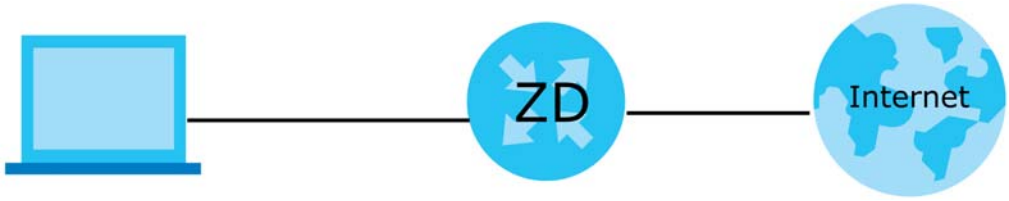
3 For the rest of the fields, use the default settings.

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



5.3.2 Set Up an Ethernet Connection

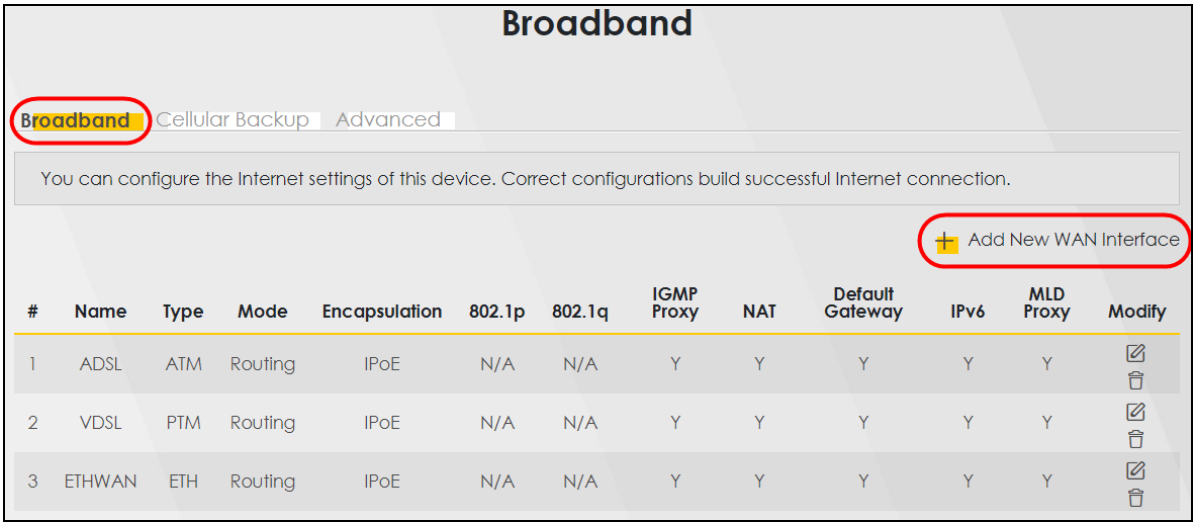
If you connect to the Internet through an Ethernet connection, you need to connect a broadband modem or router with Internet access to the WAN Ethernet port on the Zyxel Device. You need to configure the Internet settings from the broadband modem or router on the Zyxel Device. First, make sure you have Internet access through the broadband modem or router by connecting directly to it.



This example shows you how to configure an Ethernet WAN connection.

1 Make sure you have the Ethernet WAN port connect to a modem or router.

2 Go to **Network Setting** > **Broadband** and then the following screen appears. Click **Add New WAN Interface** to add a WAN connection.



3 To set the Zyxel Device to **Routing** mode, see Routing Mode on page 82.
To set the Zyxel Device to **Bridge** mode, see Bridge Mode on page 85.

Routing Mode

1 In this routing mode example, configure the following information for the Ethernet WAN connection.

General	
Name	My ETH Connection
Type	Ethernet
Connection Mode	Routing

Encapsulation (Internet Type)	IPoE
IPv6/IPv4 Mode	IPv4 Only

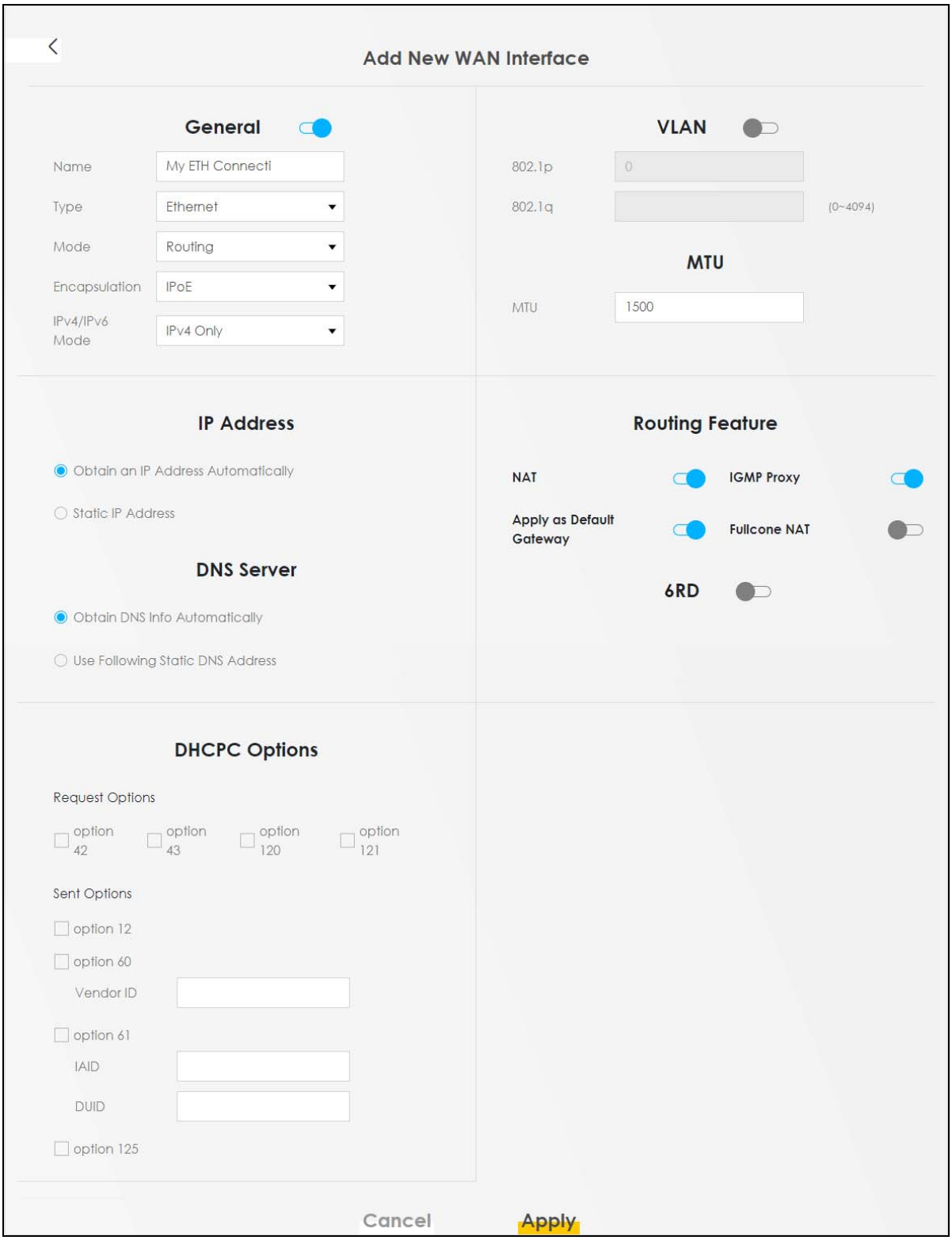
2 Enter the **General** settings provided by your Internet service provider.

- Enter a **Name** to identify your WAN connection.
- Set the **Type** to **Ethernet**.
- Set your Ethernet connection **Mode** to **Routing**.
- Choose the **Encapsulation** specified by your Internet service provider. For this example, select **IPoE** as the WAN encapsulation type.
- Set the **IPv4/IPv6 Mode** to **IPv4 Only**.

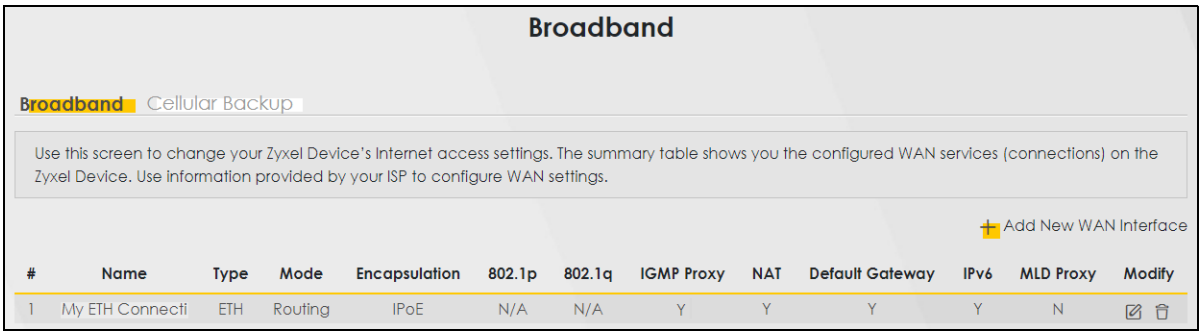
3 Under **Routing Feature**, enable **NAT** and **Apply as Default Gateway**.

4 For the rest of the fields, use the default settings.

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



6 Go to the **Network Setting** > **Broadband** screen to view the established Ethernet connection. The new connection is displayed on the **Broadband** screen.



Bridge Mode

1 In this bridge mode example, configure the following information for the Ethernet WAN connection.

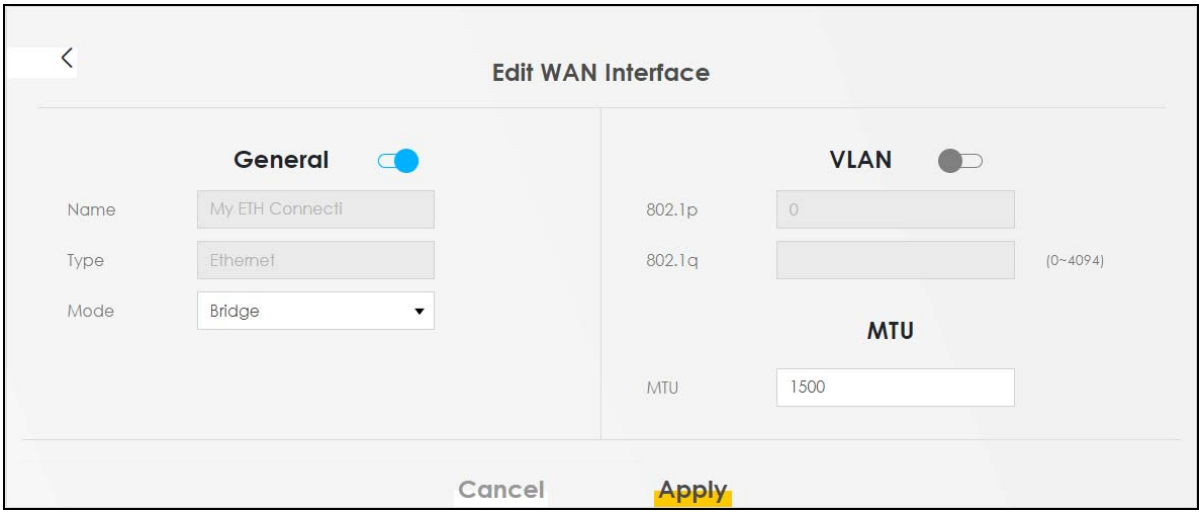
General	
Name	My ETH Connection
Type	Ethernet
Connection Mode	Bridge

2 Enter the **General** settings provided by your Internet service provider.

- Enter a **Name** to identify your WAN connection.
- Set the **Type** to **Ethernet**.
- Set your Ethernet connection **Mode** to **Bridge**.

3 For the rest of the fields, use the default settings.

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



5.4 WiFi Network Setup

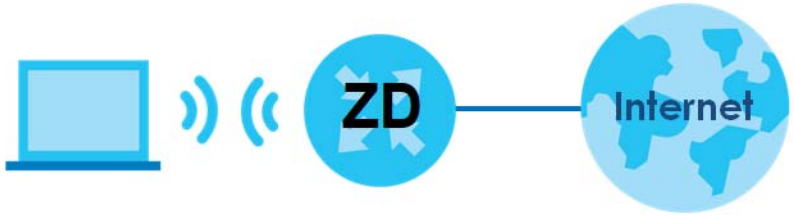
This section shows you how to:

- Change Security Settings on a WiFi Network
- Connect to the Zyxel Device's WiFi Network Using WPS
- Set Up a Guest Network
- Set Up Two Guest WiFi Networks on Different WiFi Bands
- Configure the Channel and Bandwidth for Each WiFi Band

For Zyxel Devices that support MPro Mesh, you can use the app to configure your WiFi network. See Section 1.1 on page 19 for the app you can use to manage the Zyxel Devices.

In this example, you want to set up a WiFi network so that you can use your notebook to access the Internet. In this WiFi network, the Zyxel Device is an access point (AP), and the notebook is a WiFi client. The WiFi client can access the Internet through the AP.

Figure 60 WiFi Network Setup

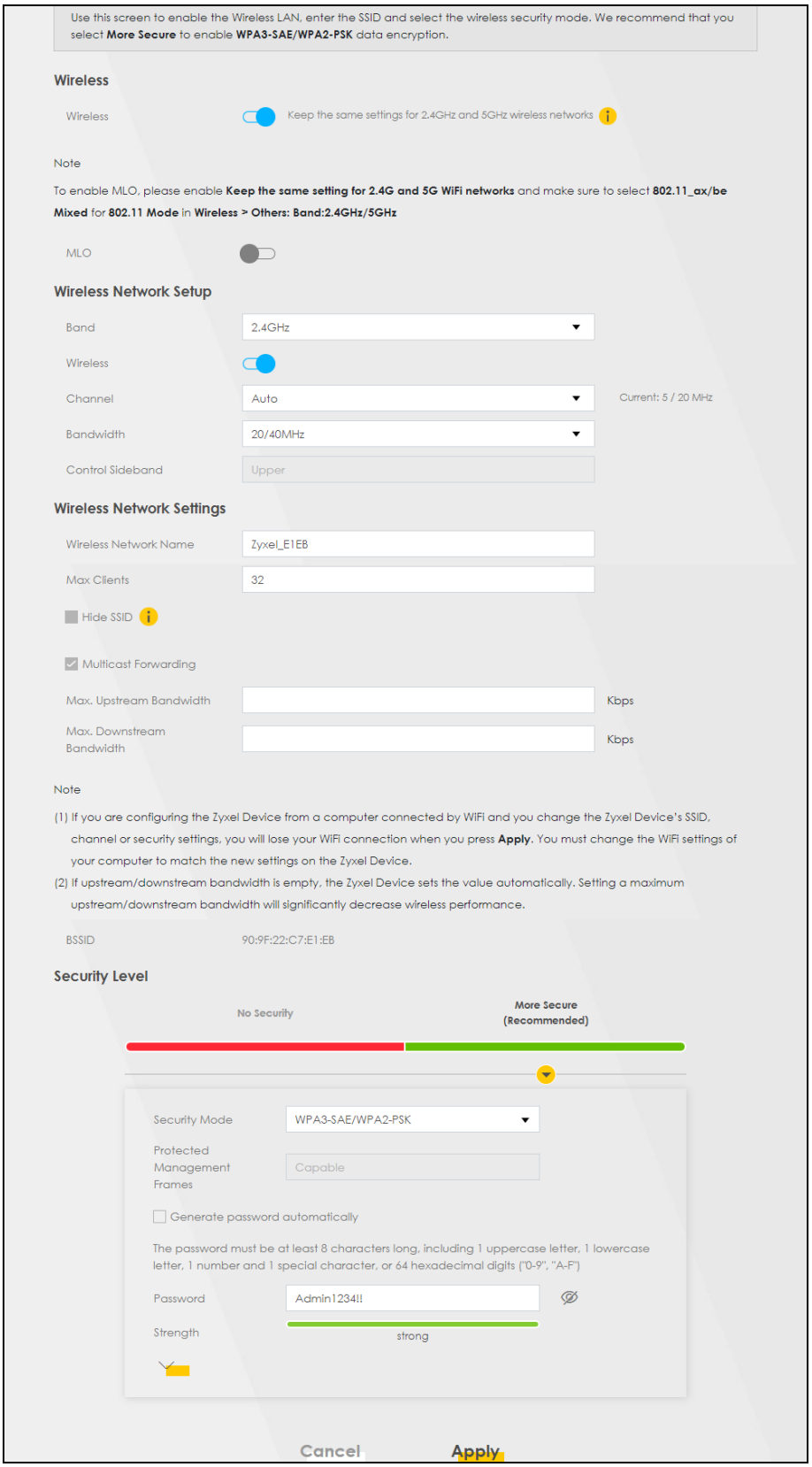


See the label on the Zyxel Device for the WiFi network settings and then connect manually to the Zyxel Device. Alternatively, you can connect to the Zyxel Device WiFi network using WPS.See Section 2.3.3 on page 56.

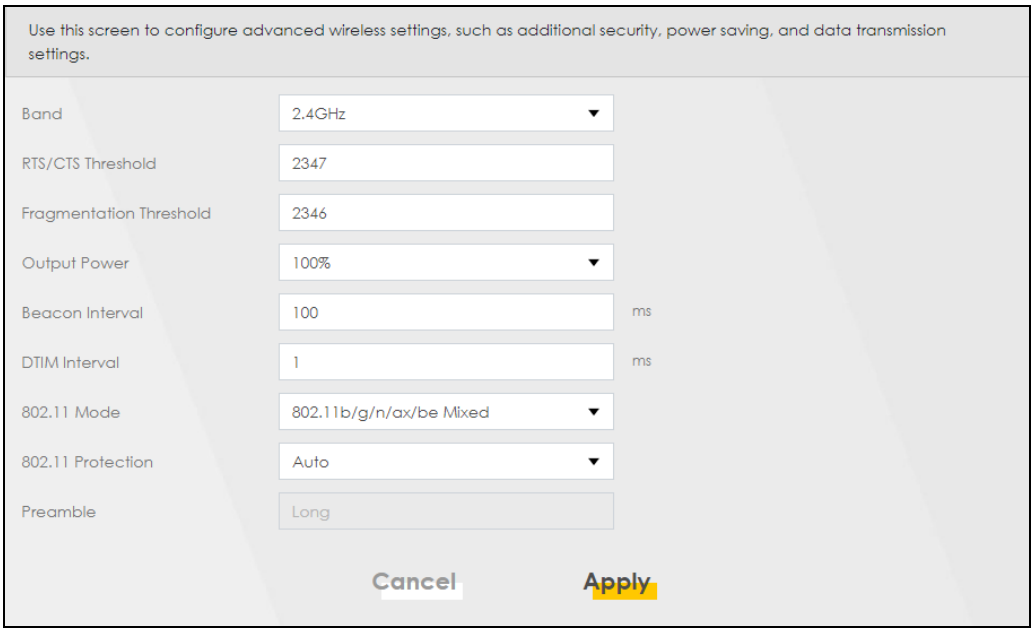
5.4.1 Change Security Settings on a WiFi Network

This example changes the default security settings of a WiFi network to the following:

SSID	Zyxel_E1EB
Pre-Shared Key	Admin1234!!
802.11 Mode	802.11b/g/n/ax/be Mixed



5 Go to the **Wireless** > **Others** screen. Set **802.11 Mode** to **802.11b/g/n /ax/be Mixed**, and then click **Apply**.



You can now use the WPS feature to establish a WiFi connection between your notebook and the Zyxel Device (see Section 8.7 on page 189). Now use the new security settings to connect to the Internet through the Zyxel Device using WiFi.

5.4.2 Connect to the Zyxel Device's WiFi Network Using WPS

This section shows you how to connect a WiFi device to the Zyxel Device's WiFi network using WPS. WPS (WiFi Protected Setup) is a security standard that allows devices to connect to a router securely without you having to enter a password. There is one method:

- **Push Button Configuration (PBC)** – Connect to the WiFi network by pressing a button. This is the simplest method.

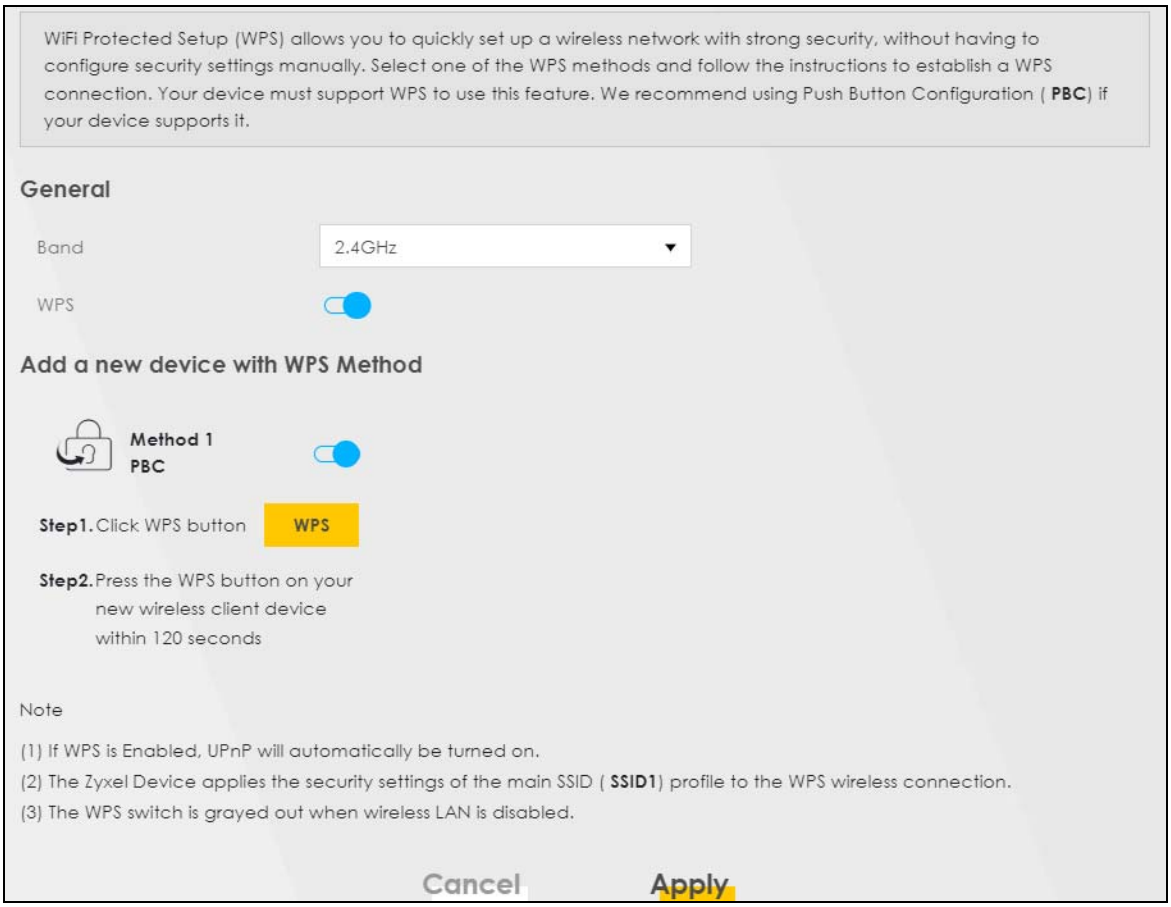
5.4.2.1 WPS Push Button Configuration (PBC)

This example shows how to connect to the Zyxel Device's WiFi network from a notebook computer running Windows 10.

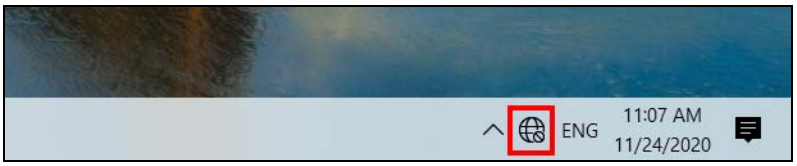
1 Make sure that your Zyxel Device is turned on, and your notebook is within range of the Zyxel Device's WiFi signal.

2 Push and hold the **WPS** button located on the Zyxel Device until the **WiFi** or **WPS** LED starts blinking slowly.
Alternatively, log into the Zyxel Device's Web Configurator, and then go to the **Network Setting** > **Wireless** > **WPS** screen. Enable **WPS** and **Method 1 PBC**, click **Apply**, and then click the **WPS button**.

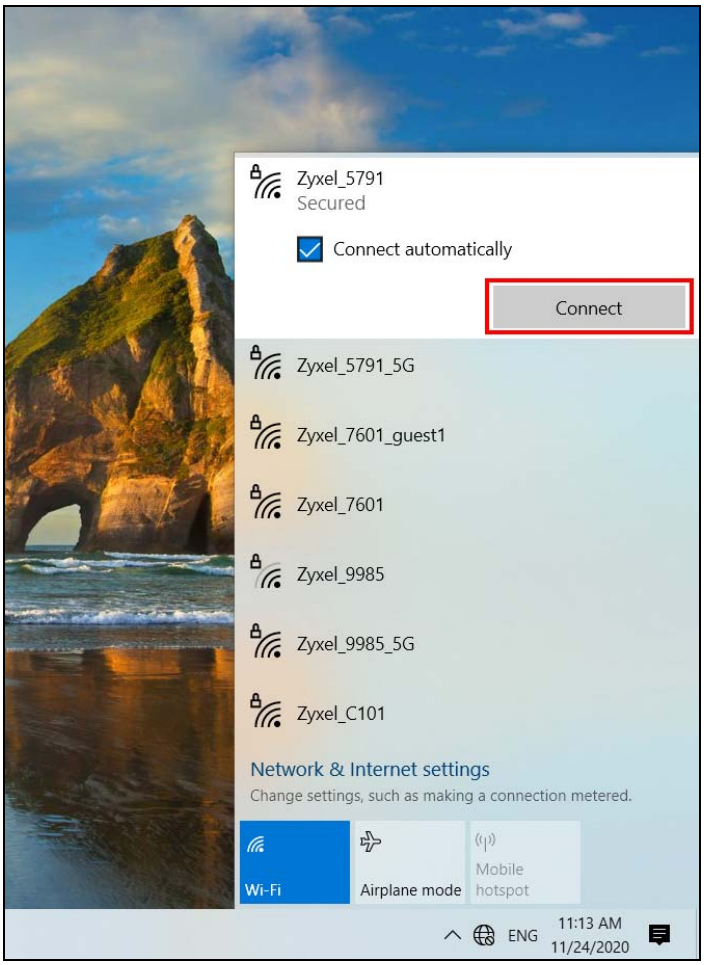
3 Log into the Zyxel Device's Web Configurator, and then go to the **Network Setting** > **Wireless** > **WPS** screen. Enable **WPS** and **Method 1 PBC**, click **Apply**, and then click the **WPS button**.



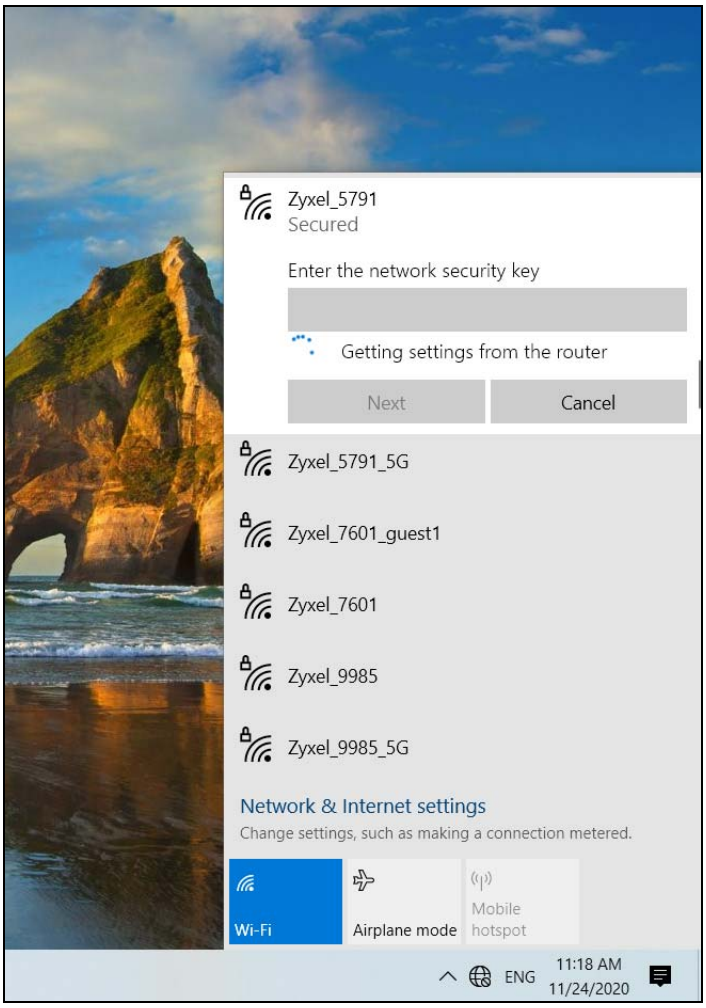
4 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.



5 Locate the WiFi network of the Zyxel Device. The default WiFi network name is “Zyxel_XXXX” (2.4 GHz) or “Zyxel_XXXX_5G” (5 GHz). Then click **Connect**.



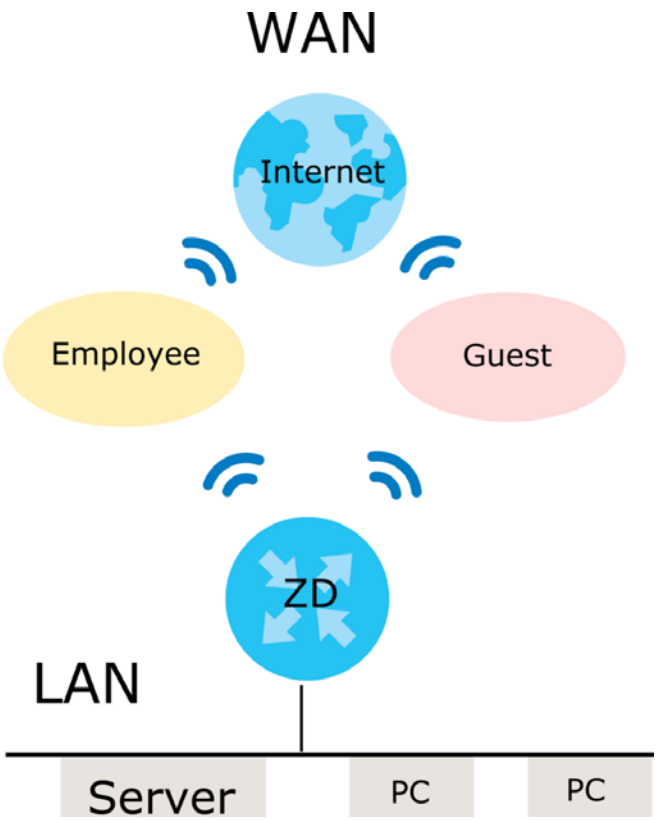
The Zyxel Device sends the WiFi network settings to Windows using WPS. Windows displays “Getting settings from the router”.



The WiFi device is then able to connect to the WiFi network securely.

5.4.3 Set Up a Guest Network

The Zyxel Device authenticates the WiFi device using the PIN, and then sends the WiFi network settings to the device using WPS. This process may take up to 2 minutes. The WiFi device is then able to connect to the WiFi network securely. A company wants to create two WiFi networks for different groups of users as shown in the following figure. Each WiFi network has its own SSID and security mode. Both networks are accessible on both 2.4 GHz and 5 GHz WiFi bands.

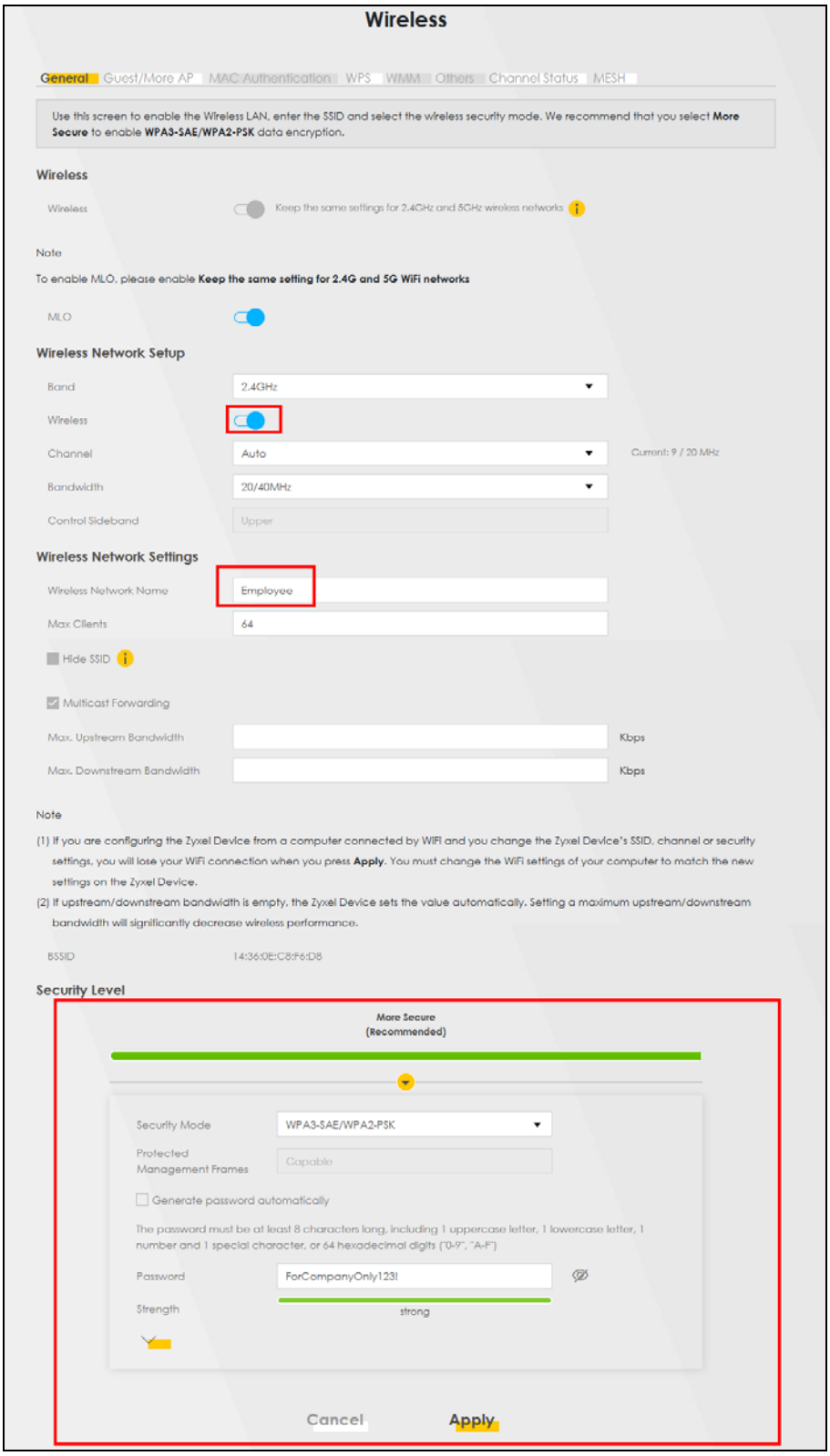


- Employees using the **General** WiFi network group will have access to the local network and the Internet.
- Visitors using the **Guest** WiFi network group with a different SSID and password will have access to the Internet only.

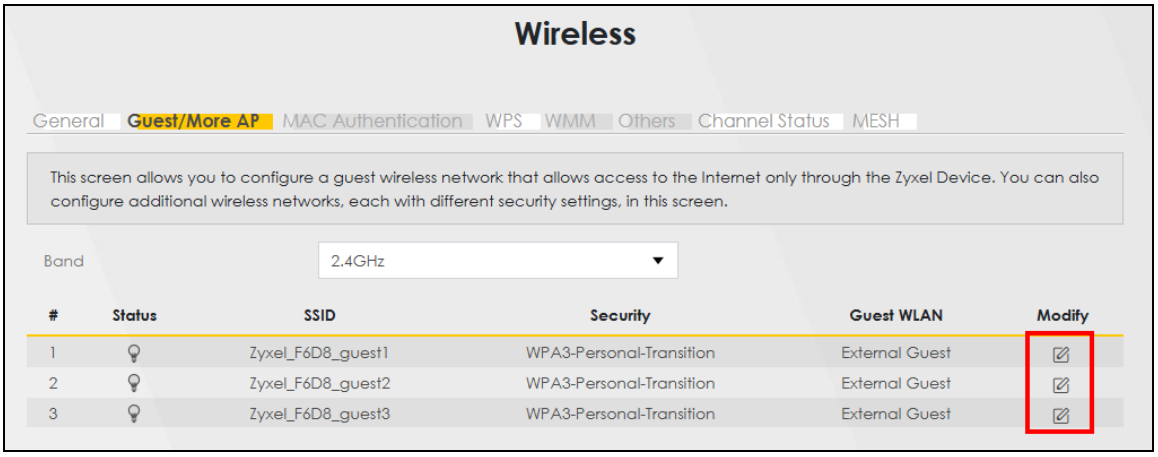
Use the following parameters to set up the WiFi network groups.

	GENERAL	GUEST
2.4/5G SSID	Employee	Guest
Security Level	More Secure	More Secure
Security Mode	WPA3-SAE/WPA2-PSK	WPA3-Personal-Transition
Pre-Shared Key	ForCompanyOnly123!	Guest123456!

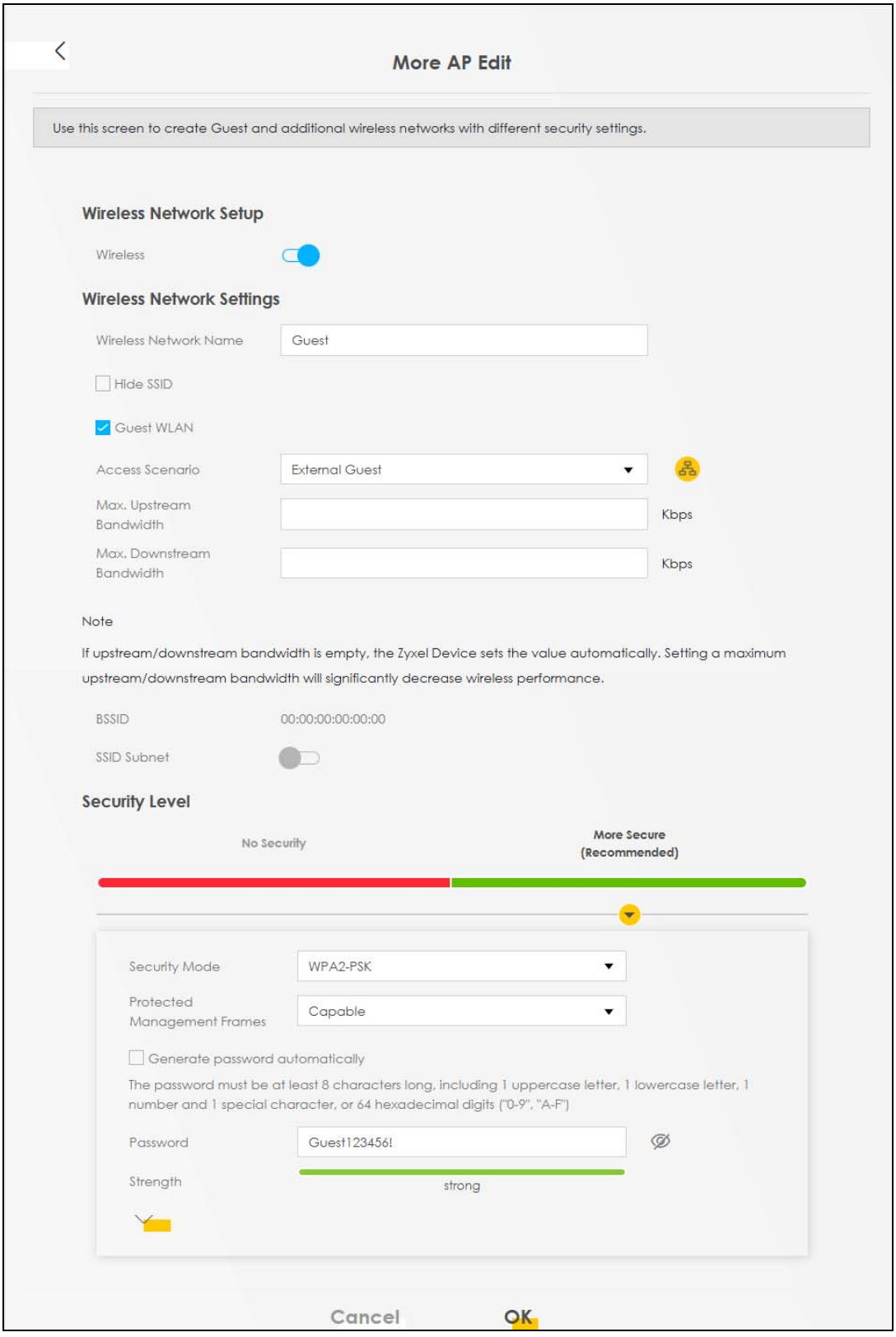
Go to the **Network Setting** > **Wireless** > **General** screen. Use this screen to set up the company's general WiFi network group. Configure the screen using the provided parameters and click **Apply**. Note that if you have employees using 2.4 GHz and 5 GHz devices, enable **Keep the same settings for 2.4GHz and 5GHz wireless networks** to use the same SSID and password. Clear it if you want to configure different SSIDs and passwords for 2.4 GHz and 5 GHz bands.


Wireless
General
Guest/More AP
MAC Authentication
WPS
WMM
Others
Channel Status
MESH
Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select More Secure to enable WPA3-SAE/WPA2-PSK data encryption.
Wireless
Wireless
Keep the same settings for 2.4GHz and 5GHz wireless networks
Note
To enable MLO, please enable Keep the same setting for 2.4G and 5G WiFi networks
MLO
Wireless Network Setup
Band
2.4GHz
Wireless
Channel
Auto
Current: 9 / 20 MHz
Bandwidth
20/40MHz
Control Sideband
Upper
Wireless Network Settings
Wireless Network Name
Employee
Max Clients
64
Hide SSID
Multicast Forwarding
Max. Upstream Bandwidth
Kbps
Max. Downstream Bandwidth
Kbps
Note
(1) If you are configuring the Zyxel Device from a computer connected by WIFI and you change the Zyxel Device's SSID, channel or security settings, you will lose your WiFi connection when you press Apply. You must change the WiFi settings of your computer to match the new settings on the Zyxel Device.
(2) If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.
BSSID
14:36:0E:C8:F6:D8
Security Level
More Secure
(Recommended)
Security Mode
WPA3-SAE/WPA2-PSK
Protected Management Frames
Capable
Generate password automatically
The password must be at least 8 characters long, including 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character, or 64 hexadecimal digits ("0-9", "A-F")
Password
ForCompanyOnly123!
Strength
strong
Cancel
Apply

6 Go to the **Network Setting** > **Wireless** > **Guest/More AP** screen. Click the **Modify** icon to configure the second WiFi network group. A **Home Guest** can access the Internet, LAN wired devices connected to the Zyxel Device, and other Home Guest WiFi clients. An **External Guest** can just access the Internet through the Zyxel Device.



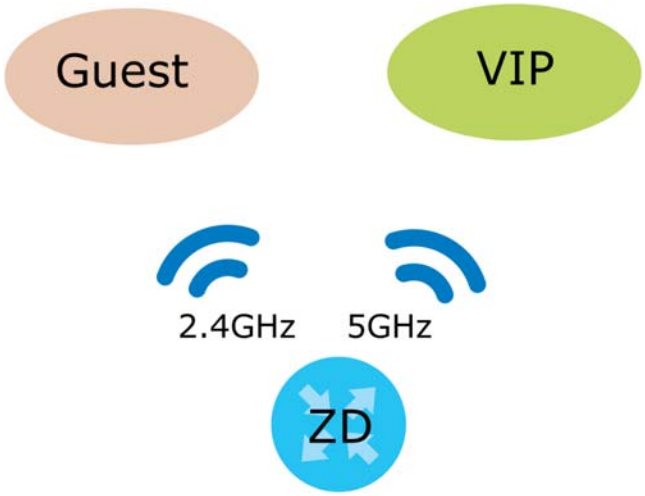
7 On the **Guest**/**More AP** screen, click the **Modify** icon to configure the other Guest WiFi network group. Configure the screen using the provided parameters and click **OK.**



8 Check the status of **Guest** in the **Guest/More AP** screen. A yellow bulb under **Status** means the SSID is active and ready for WiFi access.

5.4.4 Set Up Two Guest WiFi Networks on Different WiFi Bands

In this example, a company wants to create two Guest WiFi networks: one for the **Guest** group and the other for the **VIP** group as shown in the following figure. Each network will have its SSID and security mode to access the internet.



- The **Guest** group will use the 2.4 GHz band.
- The **VIP** group will use the 5 GHz band.

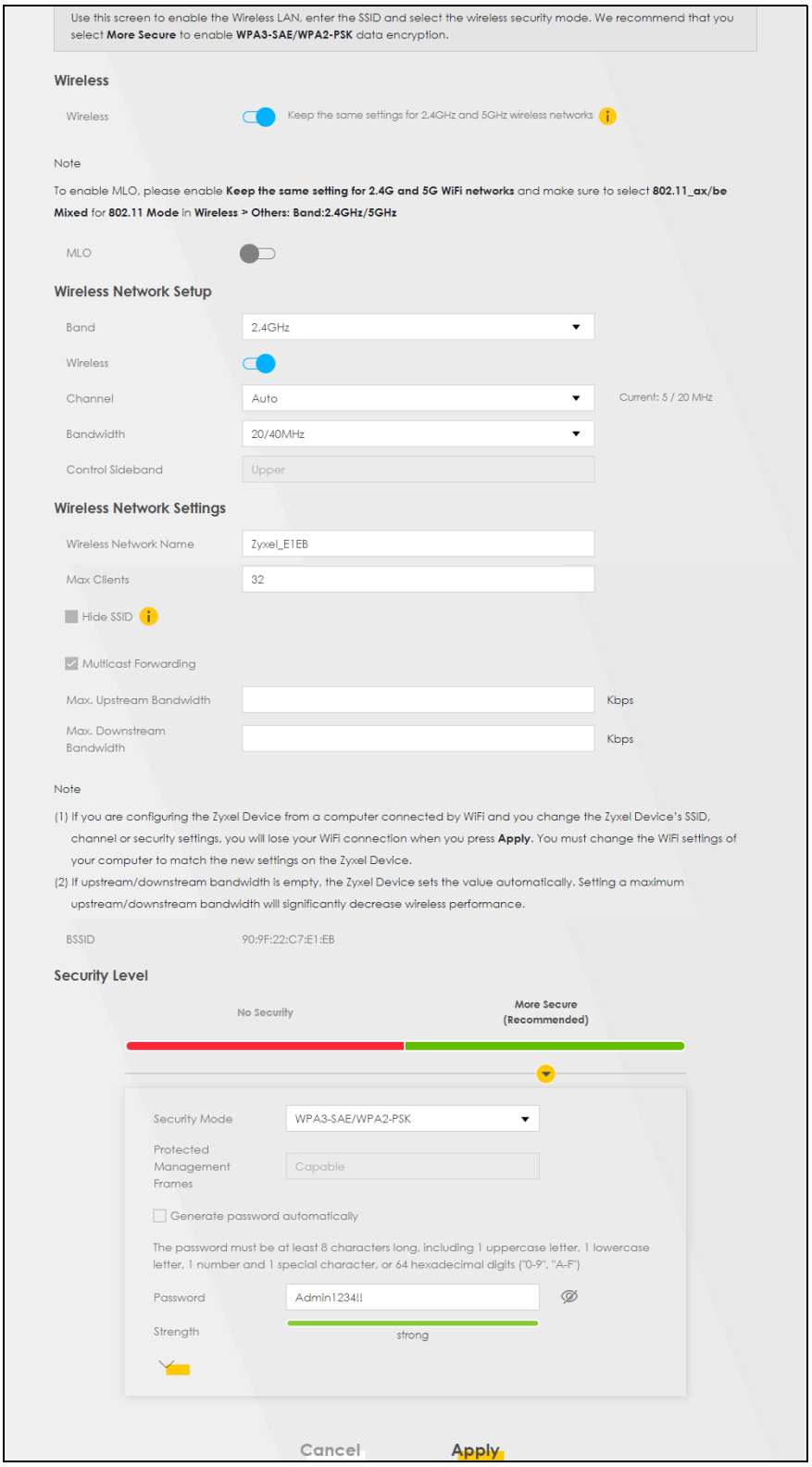
The Company will use the following parameters to set up the WiFi network groups.

Table 23 WiFi Settings Parameters Example

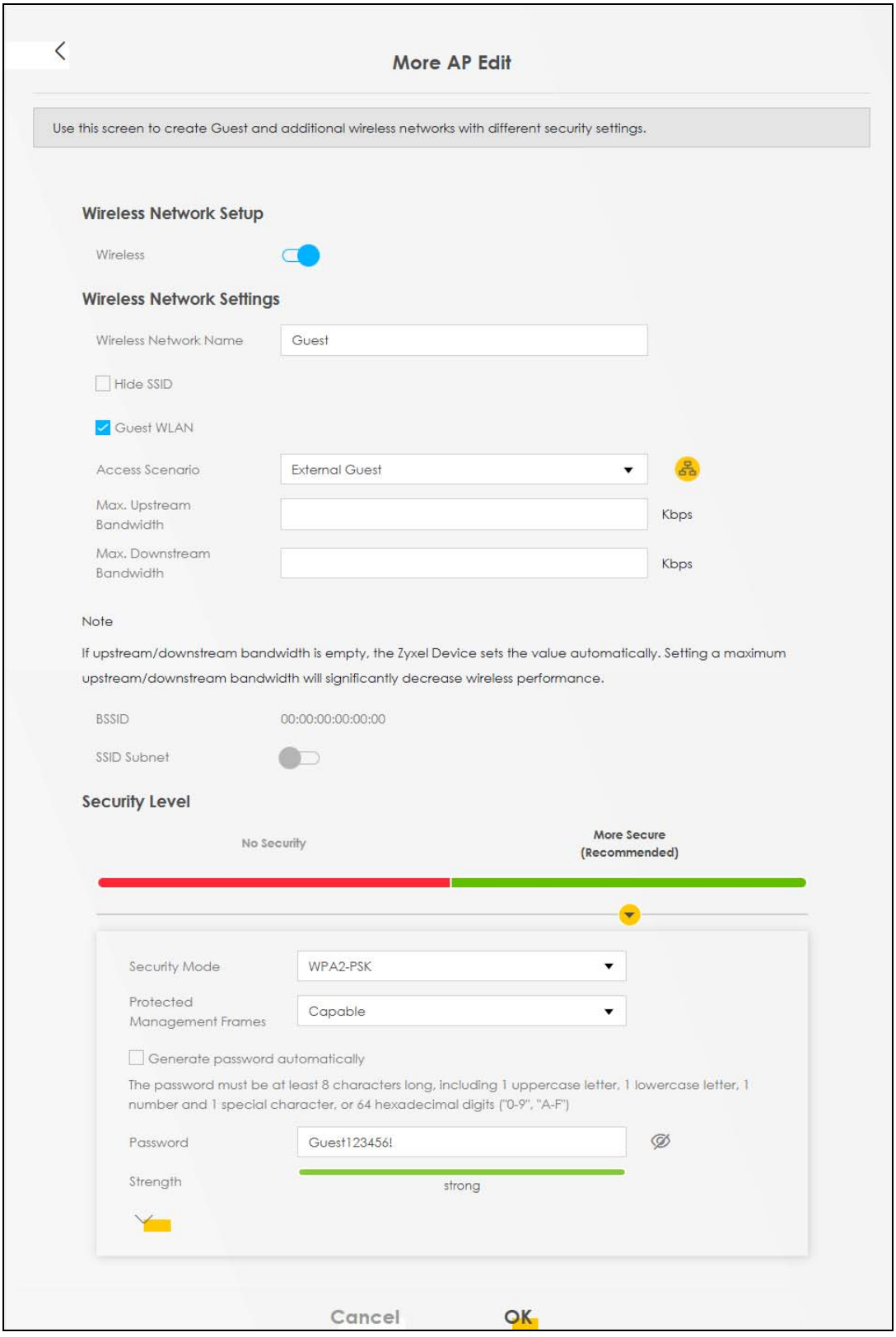
BAND	2.4 GHZ	5 GHZ
SSID	Guest	VIP
Pre-Shared Key	Guest123456!	Zyxel1234@@!

1 Go to the **Wireless** > **General** screen and set **Band** to **2.4GHz** to configure 2.4 GHz Guest WiFi settings for **Guest**. Click **Apply**.

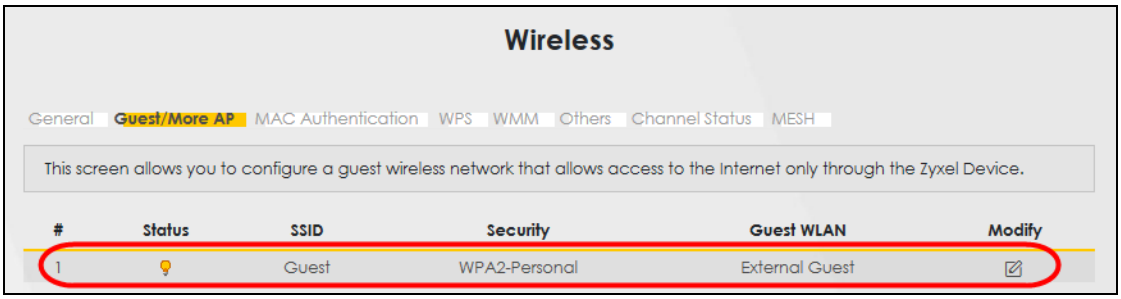
Note: You will not be able to configure the 2.4 GHz and 5 GHz Guest WiFi settings separately if **Keep the same settings for 2.4GHz and 5GHz wireless networks** is enabled.



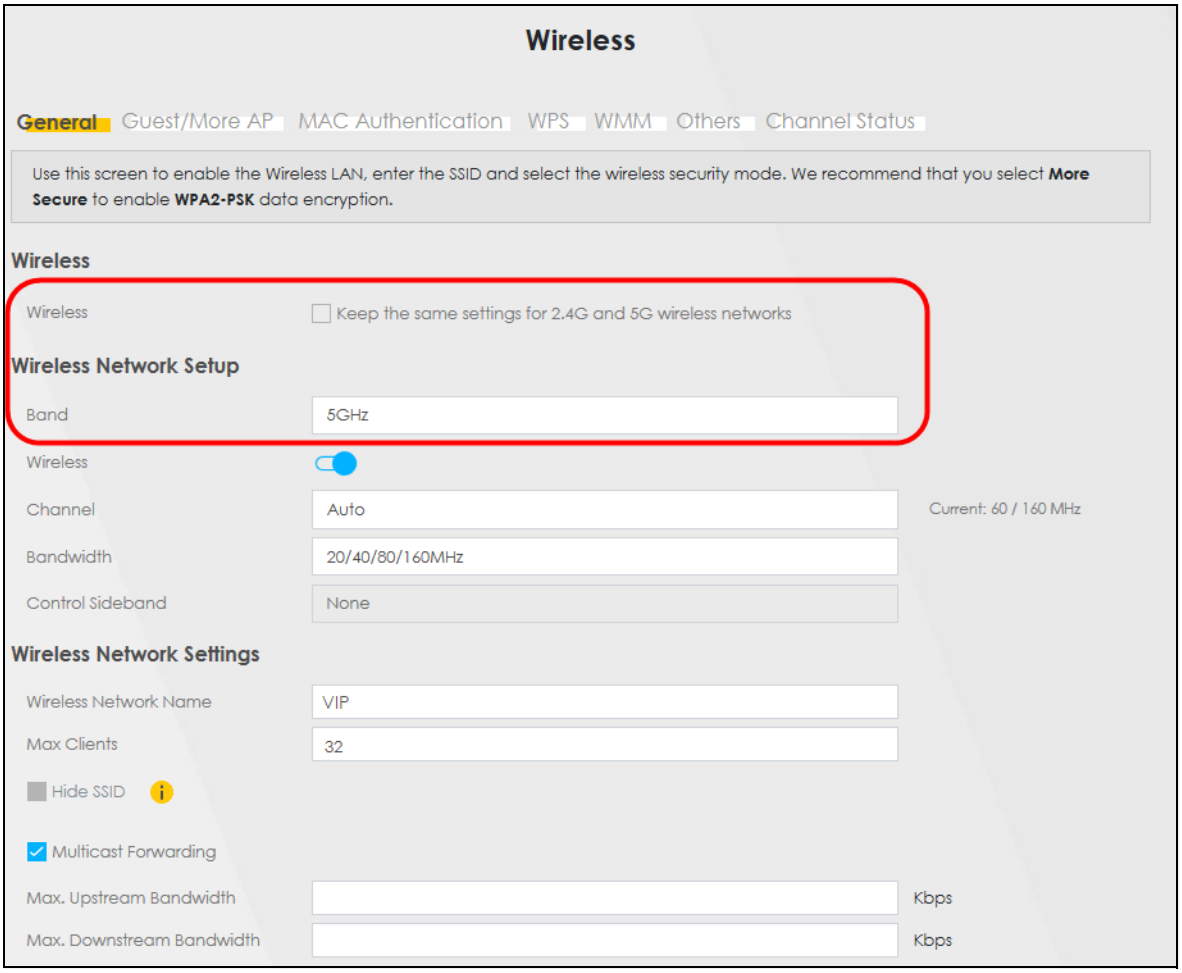
2 Go to the **Wireless** > **Guest/More AP** screen and click the **Modify** icon. The following screen appears. Configure the **Security Mode** and **Password** using the provided parameters and click **OK**.



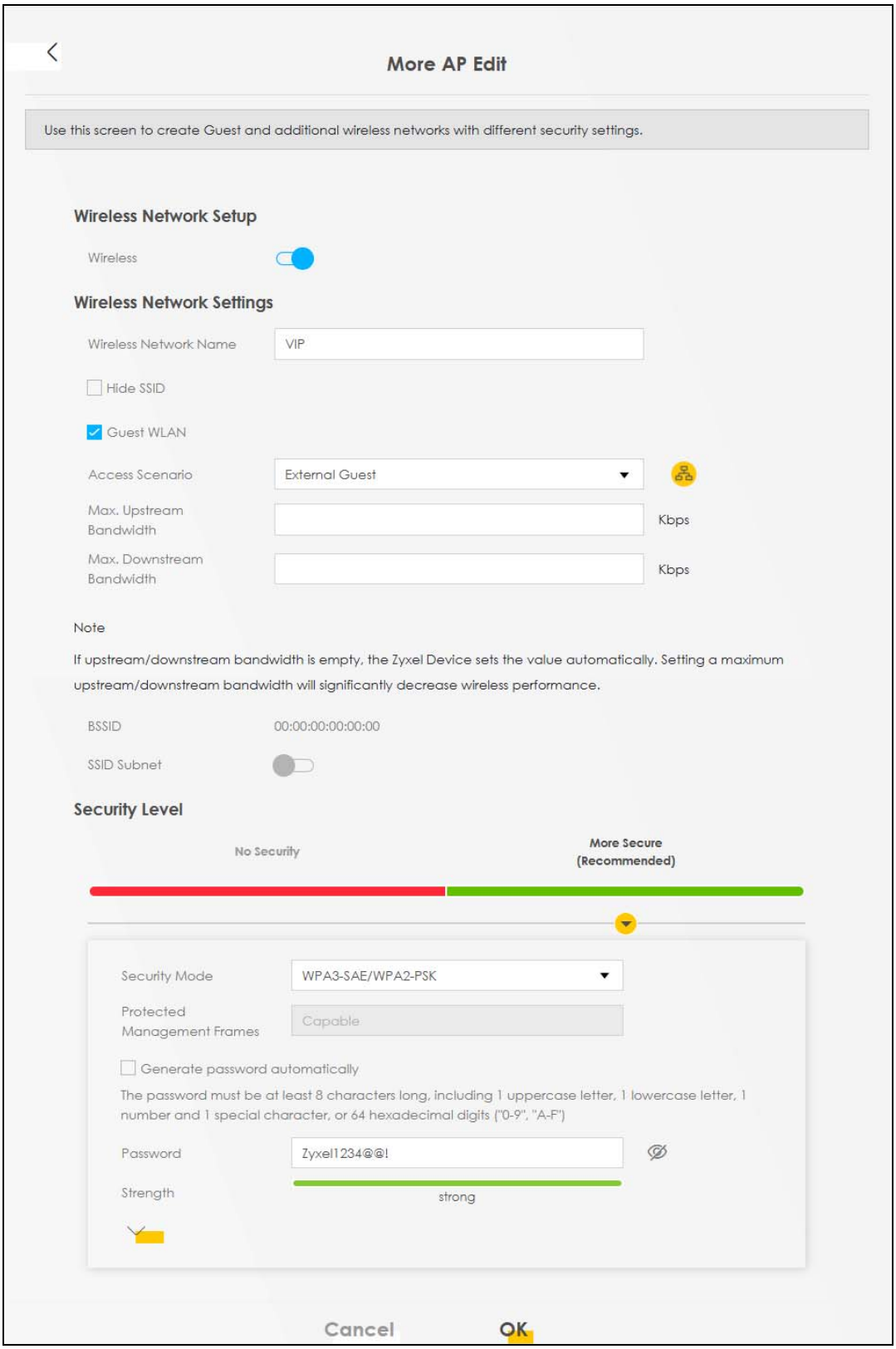
The 2.4 GHz **Guest** WiFi network is now configured.



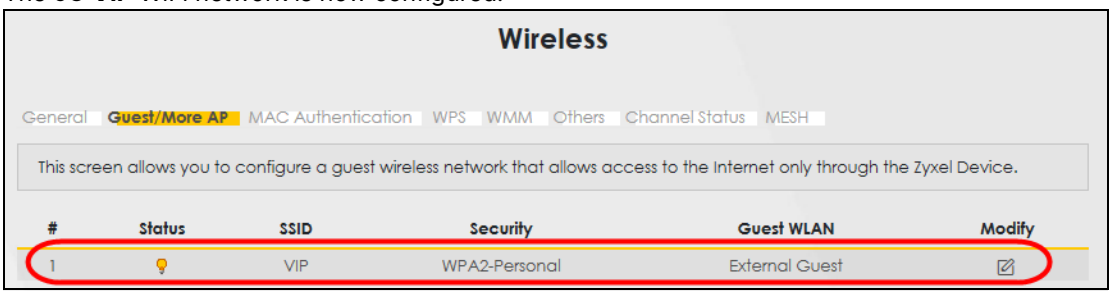
3 Go to the **Wireless** > **General** screen and set **Band** to **5GHz** to configure the 5G Guest WiFi settings for **VIP**. Click **OK**.



4 Go to the **Wireless** > **Guest/More AP** screen and click the **Modify** icon. The following screen appears. Configure the **Security Mode** and **Password** using the provided parameters and click **OK**.


More AP Edit
Use this screen to create Guest and additional wireless networks with different security settings.
Wireless Network Setup
Wireless
Wireless Network Settings
Wireless Network Name
VIP
Hide SSID
Guest WLAN
Access Scenario
External Guest
Max. Upstream Bandwidth
Kbps
Max. Downstream Bandwidth
Kbps
Note
If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease wireless performance.
BSSID
00:00:00:00:00:00
SSID Subnet
Security Level
No Security
More Secure (Recommended)
Security Mode
WPA3-SAE/WPA2-PSK
Protected Management Frames
Capable
Generate password automatically
The password must be at least 8 characters long, including 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character, or 64 hexadecimal digits ("0-9", "A-F")
Password
Zyxel1234@@!
Strength
strong
Cancel
OK

The 5G **VIP** WiFi network is now configured.



5.4.5 Configure the Channel and Bandwidth for Each WiFi Band

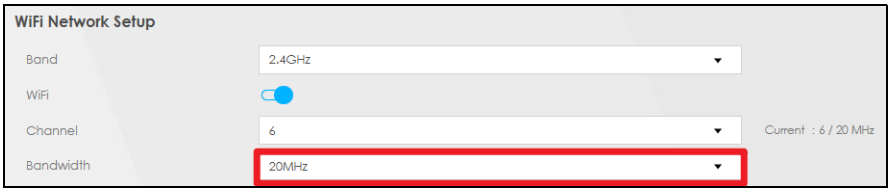
For optimal WiFi network performance, you can change the bandwidth and channel for a specific band to improve the throughput and minimize the interference. You can refer to Table 24 on page 101 for the recommended setup.

In this tutorial, you want to configure the channel to 6 and bandwidth to 20 MHz for 2.4 GHz band.

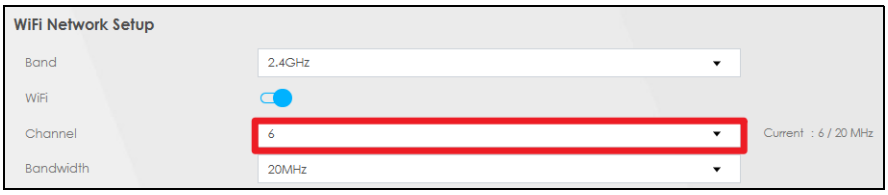
1 Go to **Network Setting** > **Wireless** > **General**.

2 In **Band**, select **2.4GHz** from the drop-down list.

3 In **Bandwidth**, select **20MHz** from the drop-down list.



4 In **Channel**, select **6** from the drop-down list.



The table below shows the recommended application for each band, along with the suggested channel and bandwidth.

Table 24 Recommended Application for Each Band

BAND	BANDWIDTH	CHANNEL	APPLICATION
2.4 GHz	20 MHz	1, 6, 11	Web browsing, email, IoT (Internet of Things)

Table 24 Recommended Application for Each Band (continued)

BAND	BANDWIDTH	CHANNEL	APPLICATION
5 GHz	40 MHz	36, 40, 44, 48	HD streaming, online meetings
	80 MHz	36, 40, 44, 48 or 52-128	4K/8K streaming, multiplayer gaming
6 GHz	80 MHz	1-13 or 37-49	Cloud gaming
	160 MHz	1-13 or 37-49	High-speed gaming, AR/VR, 8K streaming

Note: If you are still unsure about this configuration, you can set the **Channel** to **Auto**, allowing the Zyxel Device to automatically determine the proper channel for the selected band.

5.5 USB Applications

This section shows you how to:

- Set Up File Sharing on Your Zyxel Device
- Access Your Shared Files From a Computer
- Configure the Zyxel Device as a Media server

5.5.1 File Sharing

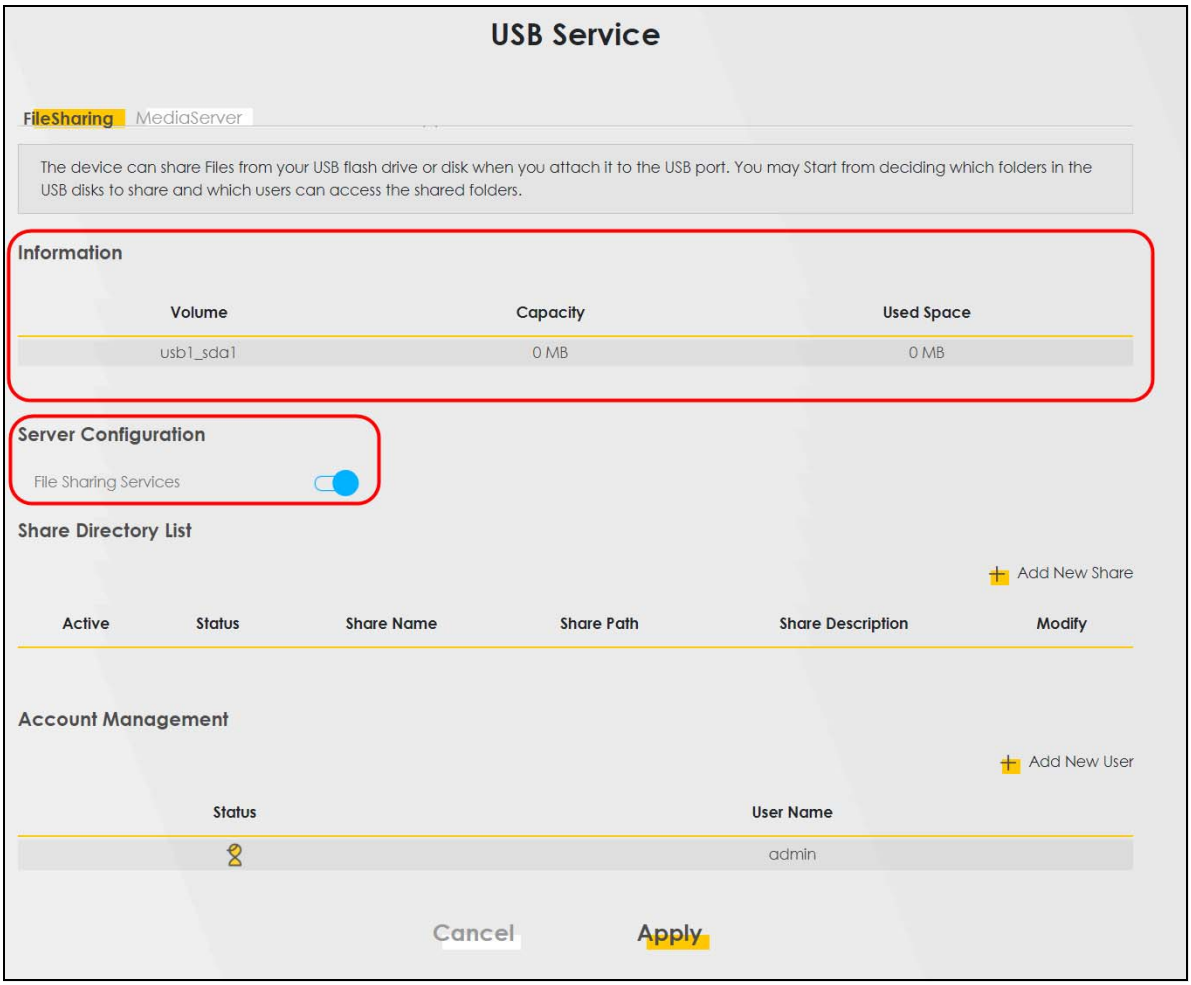
This section shows you how to create a shared folder on your Zyxel Device through a USB device and allow others to access the shared folder with File Sharing services.

5.5.1.1 Set Up File Sharing on Your Zyxel Device

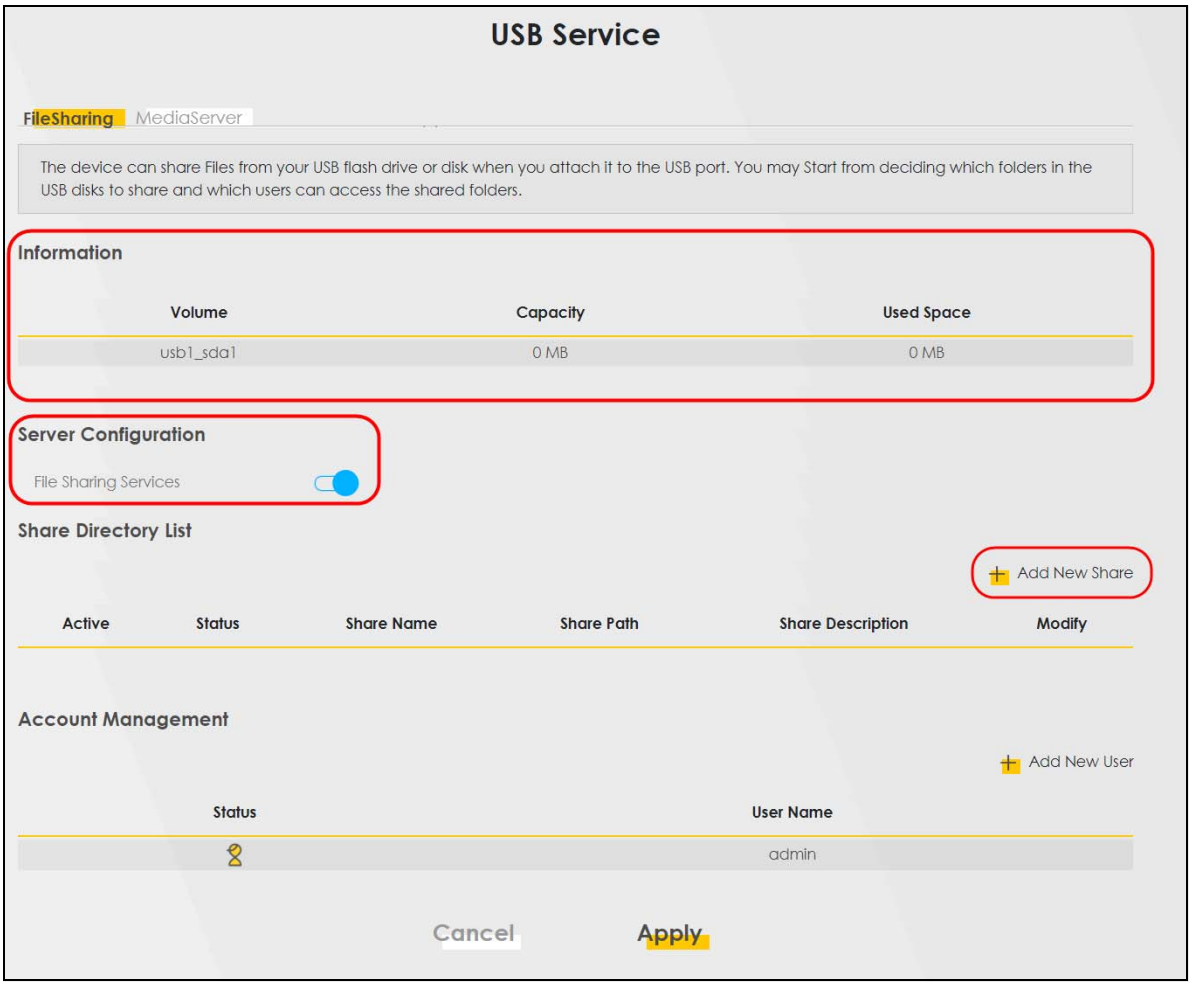
1 Before enabling file sharing in the Zyxel Device, please set up your shared folders beforehand in your USB device.

2 Connect your USB device to the USB port of the Zyxel Device.

3 Go to the **Network Setting** > **USB Service** > **File Sharing** screen. Enable **File Sharing Services** and click **Apply** to activate the file sharing function. The Zyxel Device automatically adds your USB device to the **Information** table.

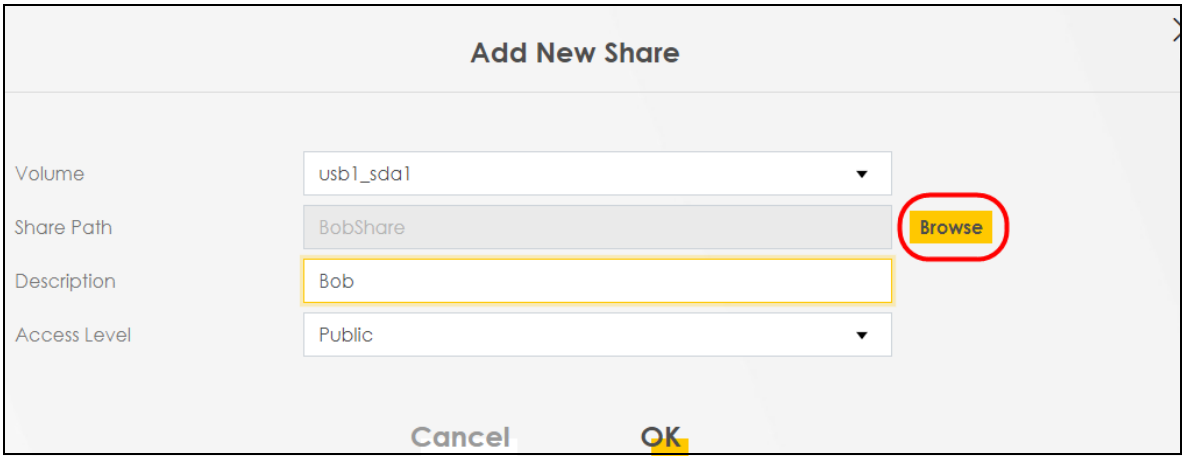


4 Click **+ Add New Share** to add a new share.

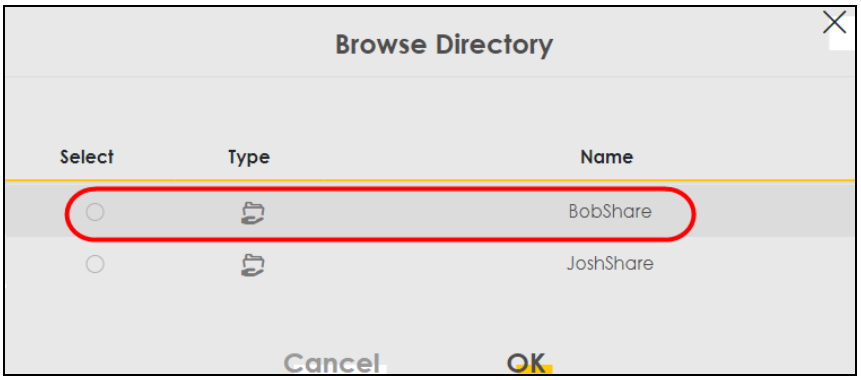


5 The **Add New Share** screen appears.

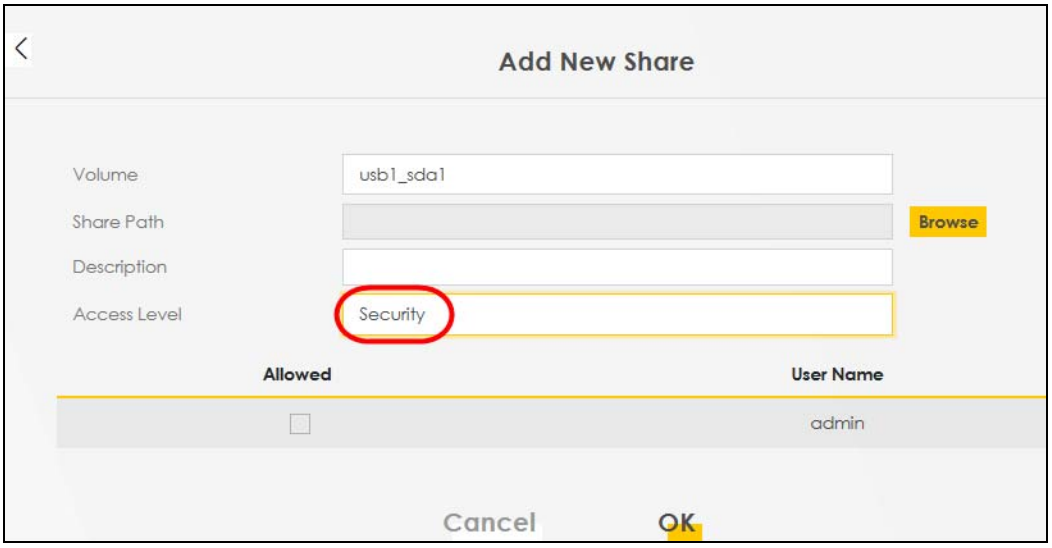
- Select your USB device from the **Volume** drop-down list box.
- Enter a **Description** name for the added share to identify the device.
- Click **Browse** and the **Browse Directory** screen appears.



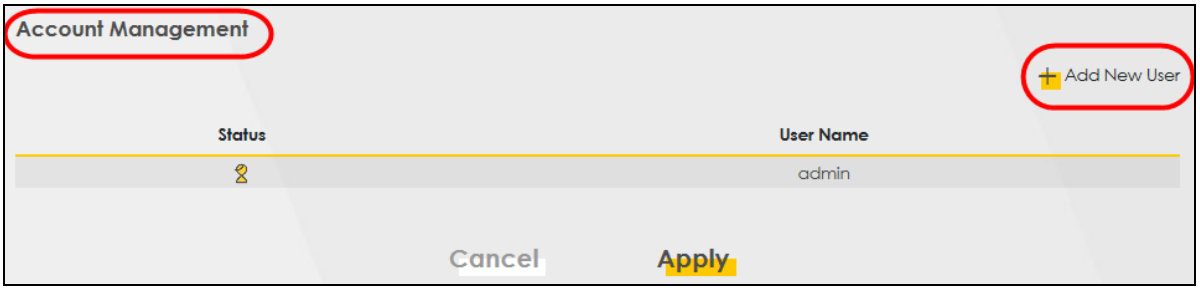
- On the **Browse Directory** screen, select the folder that you want to add as a share. In this example, select **BobShare** and then click **OK**.



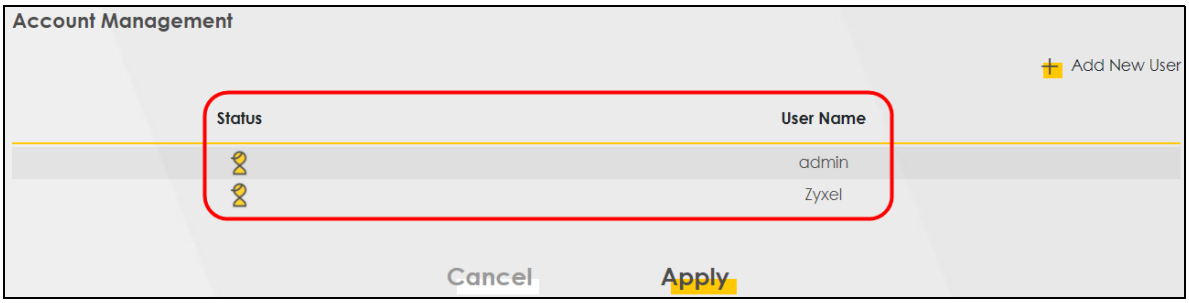
- In **Access Level,** select **Public** to let the share to be accessed by all users connected to the Zyxel Device. Otherwise, select **Security** to let the share to be accessed by specific users to access only. Click **OK** to save the settings.



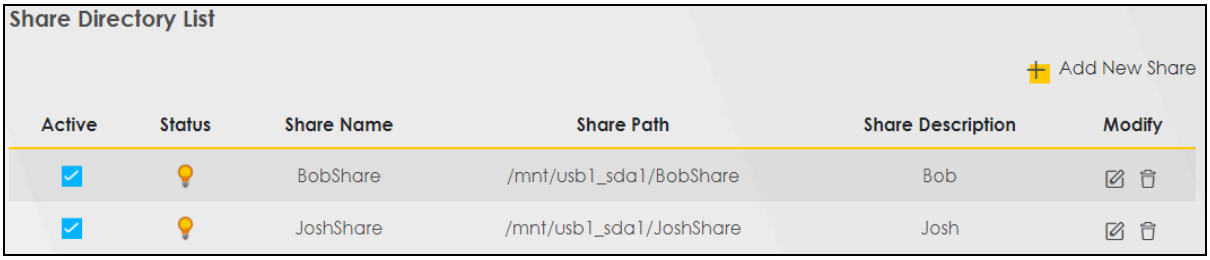
6 To set **Access level** to **Security**, you need to create one or more users accounts. Under **Account Management**, click **+ Add New User** to open the **User Account** screen.



7 After you create a new user account, the screen looks like the following.



8 File sharing is now configured. You can see the USB storage device listed in the table below.



5.5.1.2 Access Your Shared Files From a Computer

You can use Windows Explorer to access the USB storage devices connected to the Zyxel Device.

Note: This example shows you how to use Microsoft Windows 10 to browse shared files in a share called (usb1_sda)Zoeys file. Refer to your operating system's documentation for how to browse your file structure.

1 Open Windows Explorer.

2 In the Windows Explorer's address bar, enter a double backslash "\\" followed by the IP address of the Zyxel Device (the default IP address of the Zyxel Device is 192.168.1.1

3 Double-click on **(usb1_sda)Zoeys file**, and then enter the share's username and password if prompted.

4 After you access **(usb1_sda)Zoeys file** through your Zyxel Device, you do not have to log in again unless you restart your computer.

5.5.2 Media Server

Use the media server feature to play files on a computer or on your television.

This section shows you how the media server feature works using the following:

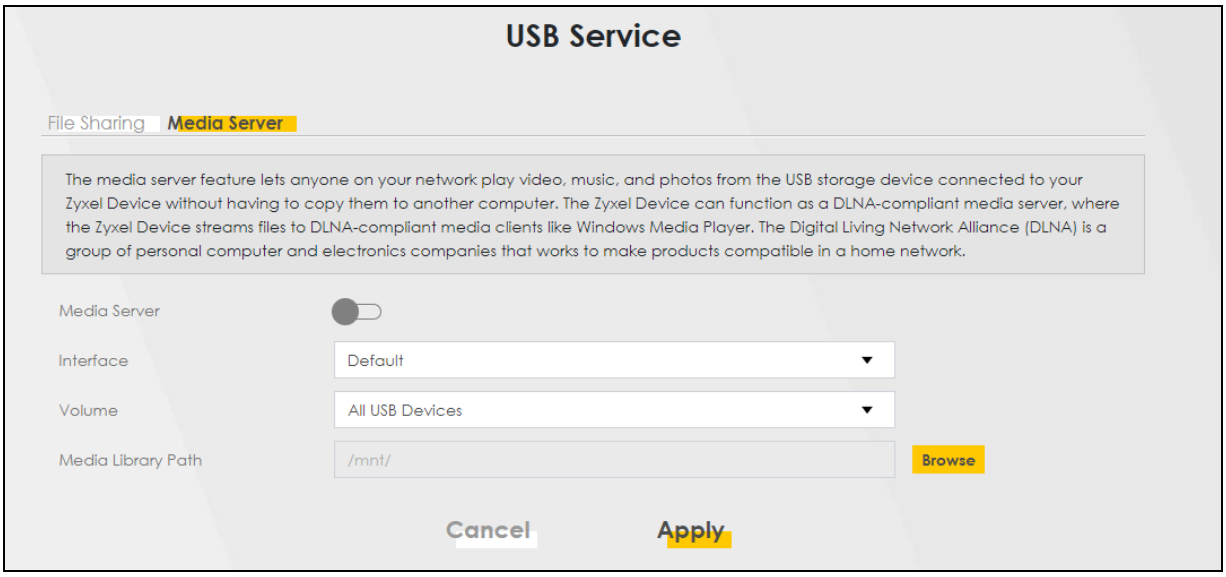
- Microsoft (MS) Windows Media Player
  Media Server works with Windows 10. Make sure your computer is able to play media files (music, videos and pictures).
- A digital media adapter
  You need to set up the media adapter to work with your television (TV).

Before you begin, connect the USB storage device containing the media files you want to play to the USB port of your Zyxel Device.

5.5.2.1 Configure the Zyxel Device as a Media server

To use your Zyxel Device as a media server, follow the steps below.

1 Go to the **Network Setting** > **USB Service** > **Media Server** screen.



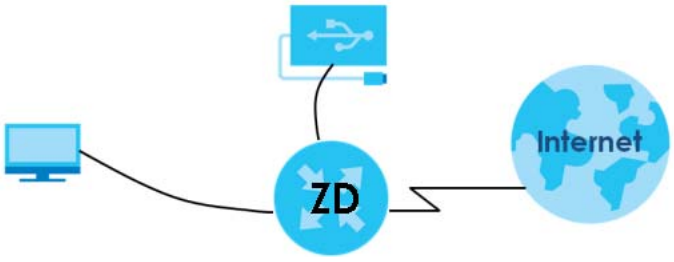
2 Enable **Media Server**, and then select an interface on which you want to enable the media server function.

3 Enter the path clients use to access the media files on a USB storage device connected to the Zyxel Device, and click **Apply**.

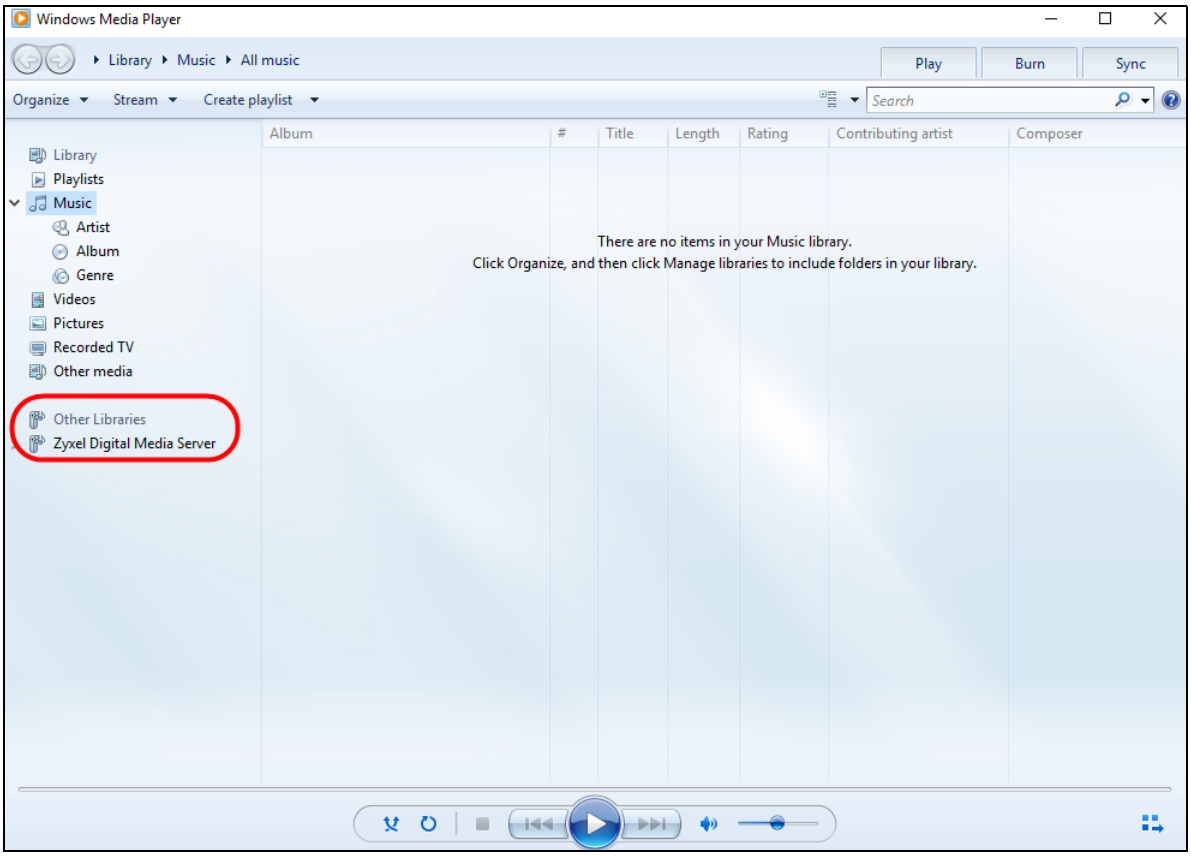
This enables DLNA-compliant media clients to play the video, music and image files in your USB storage device.

5.5.2.2 Playing Media Using Windows Media Player on Windows 10

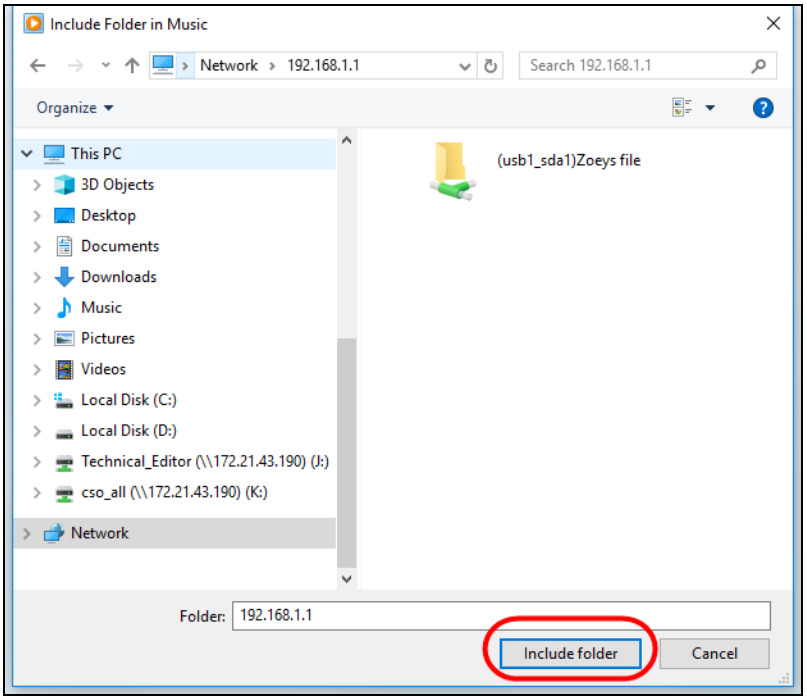
This section shows you how to play the media files on the USB storage device connected to your Zyxel Device using Windows Media Player.



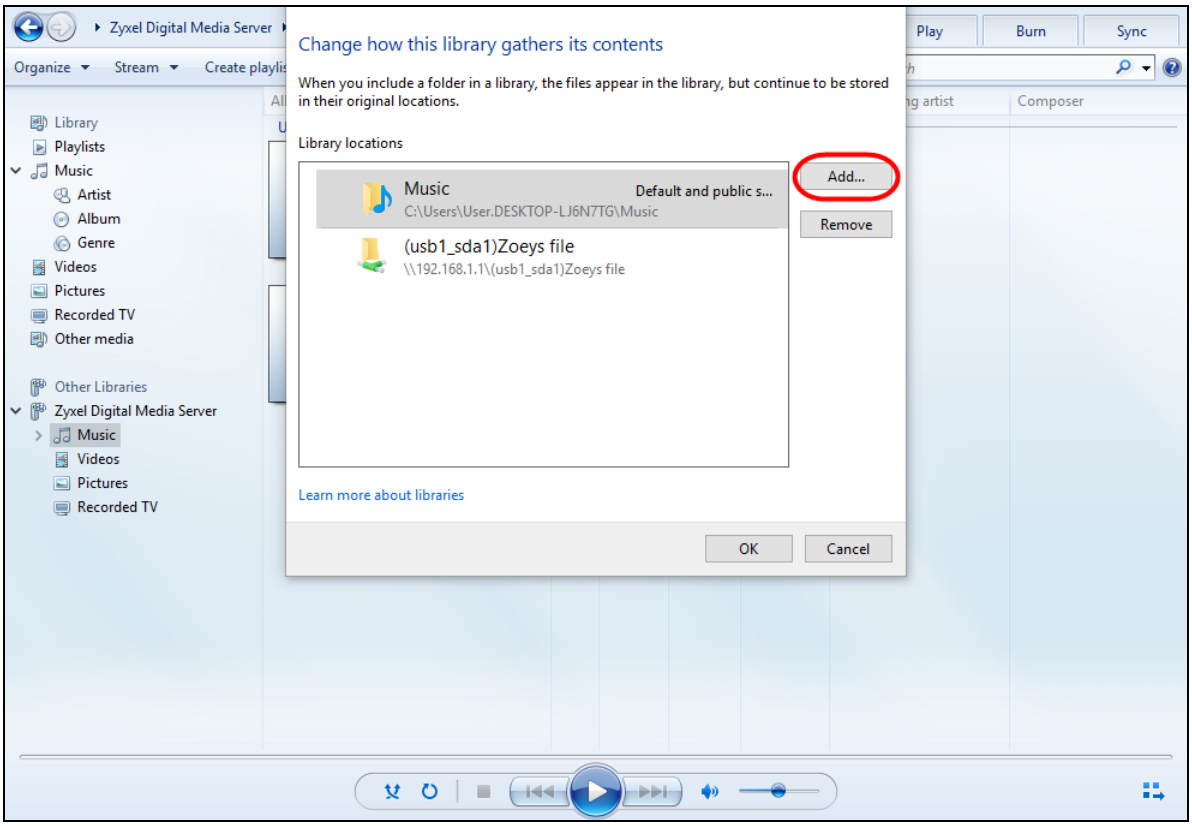
1 Open Windows Media Player. It automatically detects the Zyxel Device.



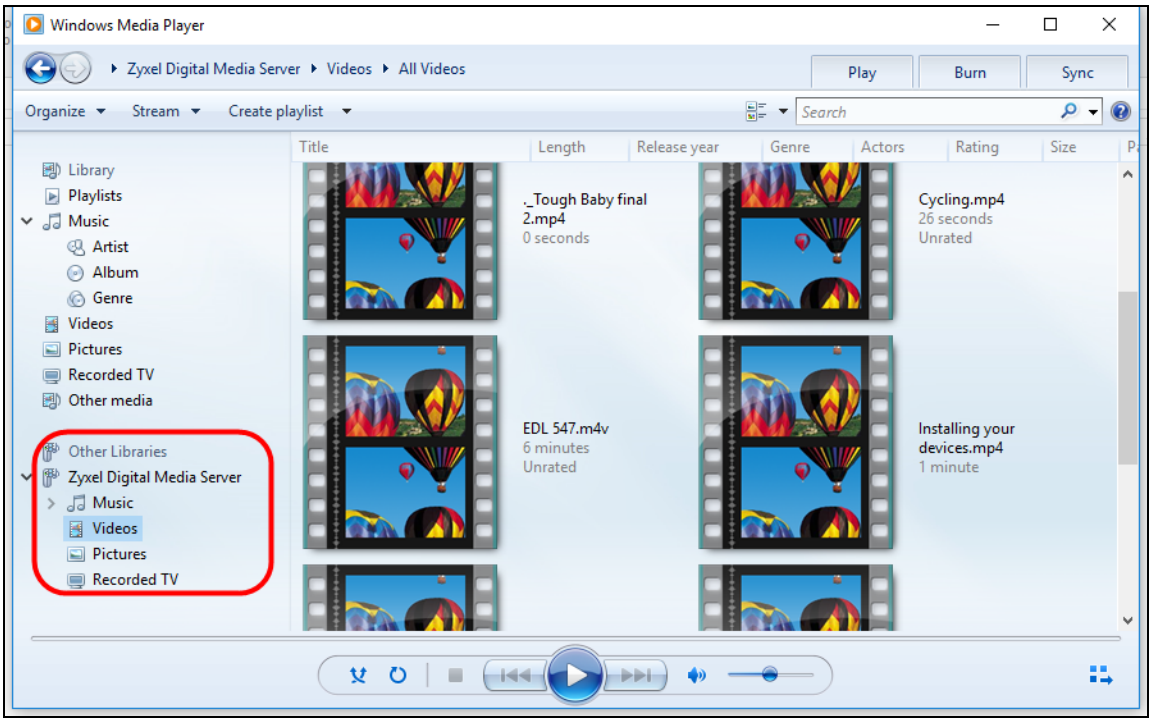
2 If you cannot see the Zyxel Device in the left panel as shown above, go to **Organize** > **Manage Libraries** > **Music** > **Add** on the Windows Media Player Home screen. In the Windows Explorer's address bar, enter **\\192.168.1.1**. The following screen appears. Select the folder containing the media you wish to upload to Windows Media Player, and then click **Include Folder**.



3 Select the shared folder, and then click **Add** to add it to your Media Library. Click **OK** to save the settings.



4 In the right panel, you can browse and play the files available in the USB storage device based on the category (**Music**, **Video**, **Pictures**, **Recorded TV**) you selected.

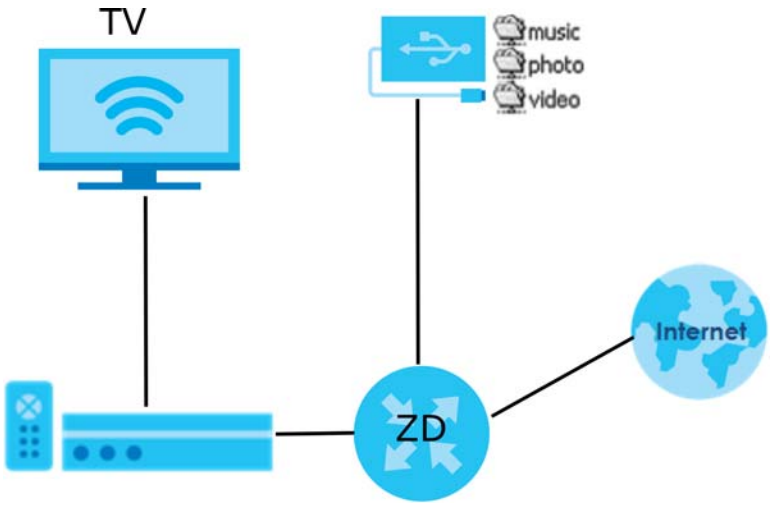


5.5.2.3 Using a Digital Media Player

This section shows you how you can use the Zyxel Device with a hardware digital media player to play media files stored in the USB storage device on your TV screen.

Note: For this tutorial, your digital media player is already connected to the TV.

1 Connect the digital media player to an available LAN port on your Zyxel Device.



2 Turn on the TV and wait for the digital media player **Home** screen to appear. Select the Zyxel Device as your media server.

3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button on the remote control.

5.6 Network Security

This section shows you how to:

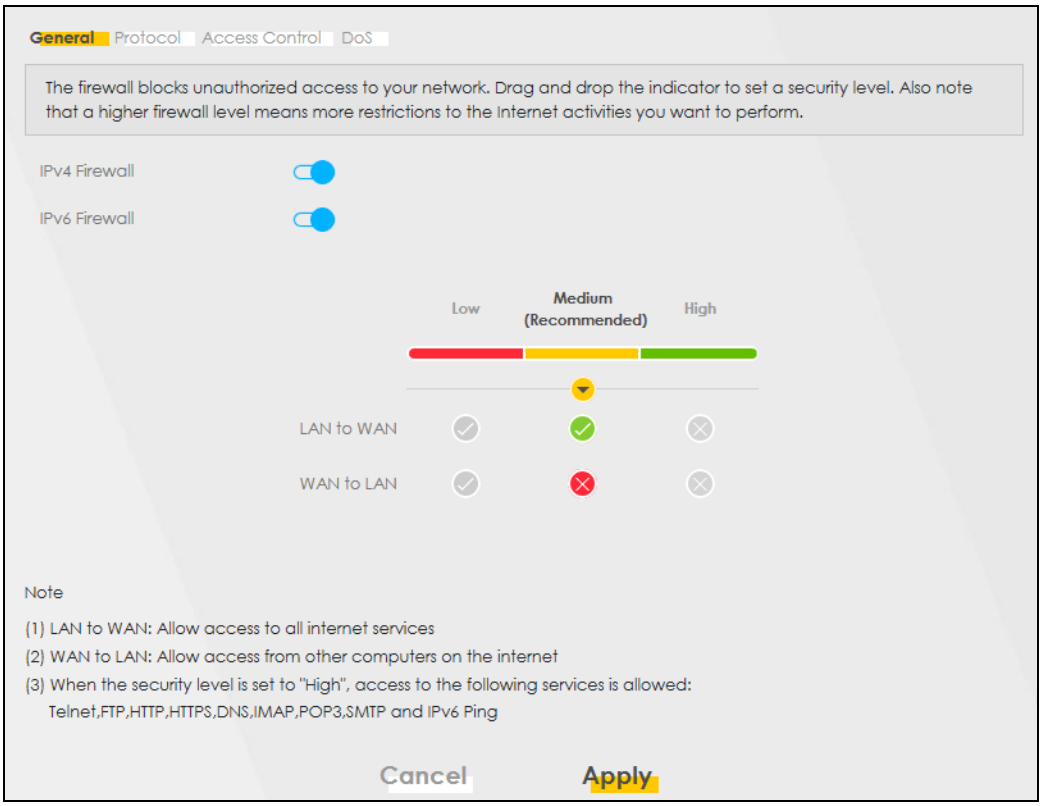
- Configure a Firewall Rule
- Set Up Parental Control
- Configure a MAC Address Filter for Wired LAN Connections

5.6.1 Configure a Firewall Rule

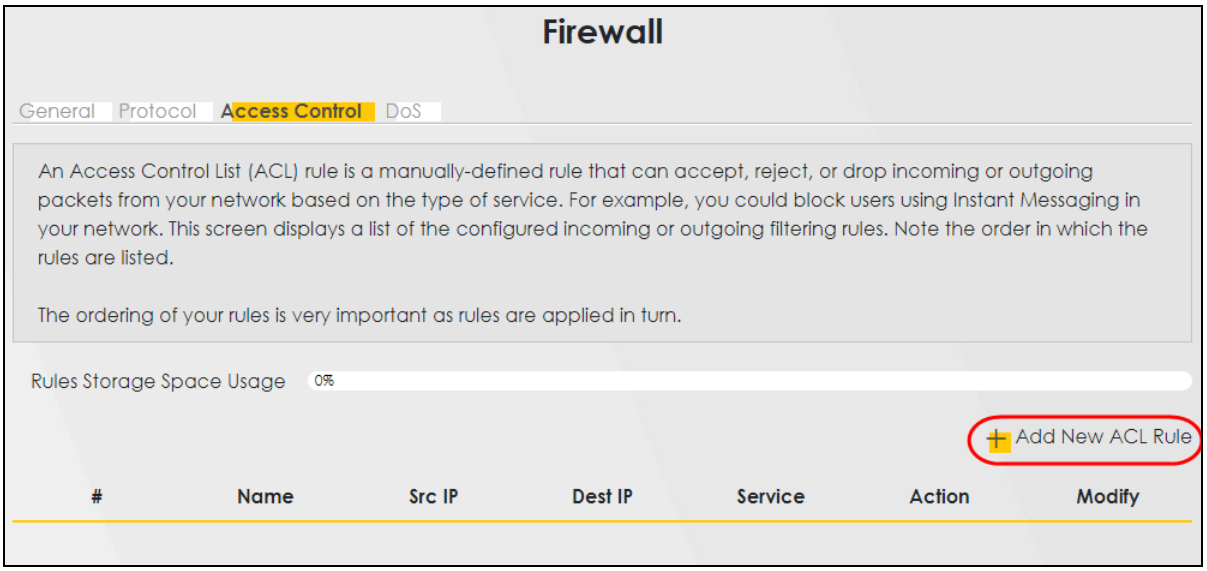
You can enable the firewall to protect your LAN computers from malicious attacks from the Internet.

1 Go to the **Security** > **Firewall** > **General** screen.

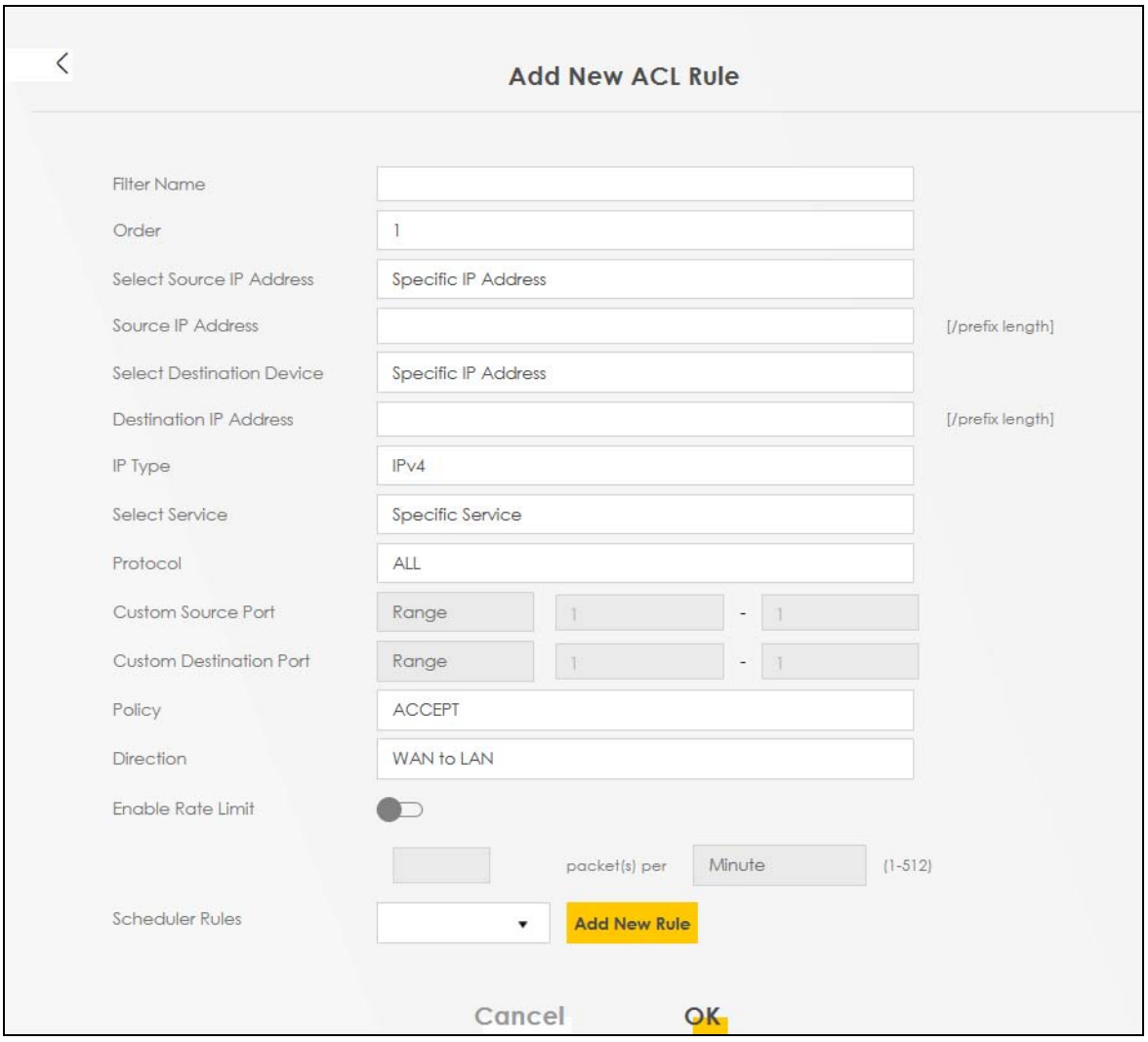
2 Select **IPv4 Firewall**/**IPv6 Firewall** to enable the firewall, and then click **Apply**.



3 Open the **Access Control** screen, click **+ Add New ACL Rule** to create a rule.



4 Use the following fields to configure and apply a new ACL (Access Control List) rule.



- **Filter Name**: Enter a name to identify the firewall rule.:
- **Source IP Address**: Enter the IP address of the computer that initializes traffic for the application or service.
- **Destination IP Address**: Enter the IP address of the computer to which traffic for the application or service is entering.
- **Protocol**: Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP** or **ICMPv6**) used to transport the packets.
- **Policy**: Select whether to (**ACCEPT**, **DROP**, or **REJECT**) the packets.
- **Direction**: Select the direction (**WAN to LAN**, **LAN to WAN**, **WAN to ROUTER**, or **LAN to ROUTER**) of the traffic to which this rule applies.

5 Select **Enable Rate Limit** to activate the rules you created. Click **OK**.

5.6.2 Set Up Parental Control

This section shows you how to configure rules for accessing the Internet using parental control.

Note: The style and features of your parental control vary depending on the Zyxel Device you are using.

5.6.2.1 Configure Parental Control Schedule and Filter

Parental Control Profile (**PCP**) allows you to set up a rule for:

- Internet usage scheduling.
- Websites and URL keyword blocking.

Use this feature to:

- Limit the days and times a user can access the Internet.
- Limit the websites a user can access on the Internet.

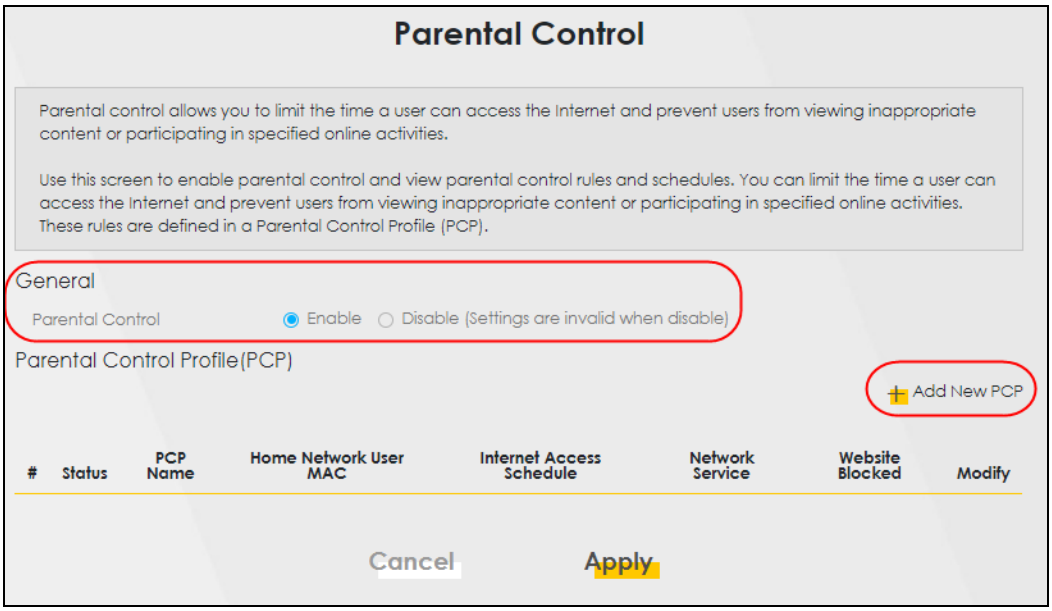
This example shows you how to block a user from accessing the Internet during time for studying. It also shows you how to stop a user from accessing specific websites.

Use the parameters below to configure a schedule rule and a URL keyword blocking rule.

PROFILE NAME	INTERNET ACCESS SCHEDULE	NETWORK SERVICE	SITE/URL KEYWORD
Study	**Day**: Monday to Friday **Time**: 8:00 to 11:00 13:00 to 17:00	**Network Service Setting**: Block **Service Name**: HTTP **Protocol**: TCP **Port**: 80	**Block or Allow the Web Site**: Block the web URLs **Website**: gambling

Parental Control Screen

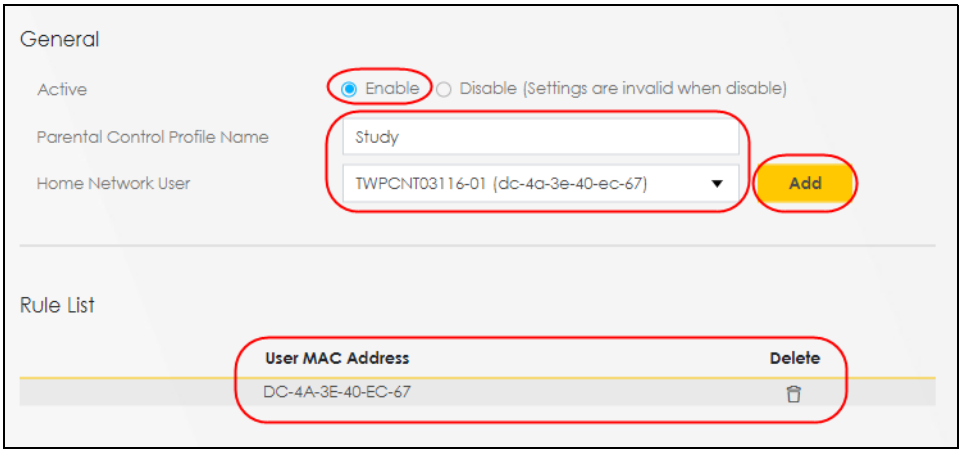
Open the **Parental Control** screen. Select **Enable** under **General** to enable parental control. Then click **+ Add New PCP** to add a rule.



Add New PCP Screen

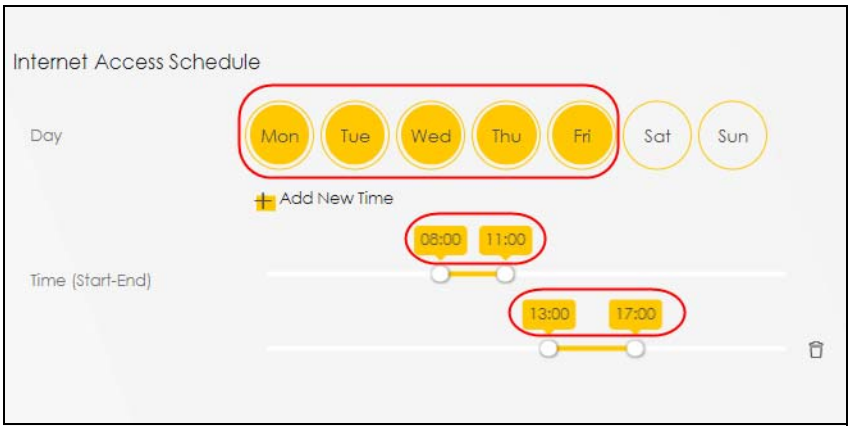
1 Go to **Parental Control** > **Add New PCP**. Under **General**:

- Select **Enable** to enable the rule you are configuring.
- Enter the **Parental Control Profile Name** given in the above parameter.
- Select an user this rule applies to in **Home Network User**, then click **Add**. You will see the MAC address of the user you just select in **Rule List**.



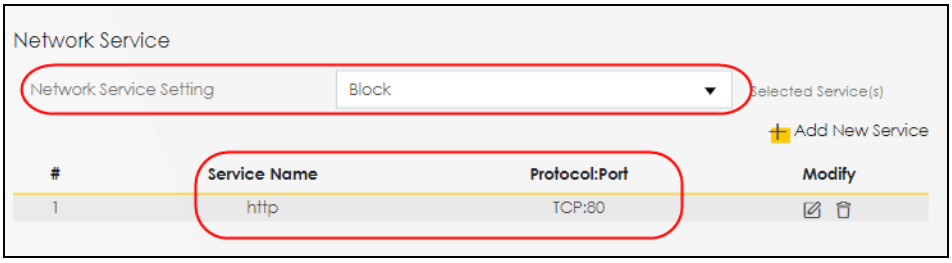
2 Under **Internet Access Schedule**:

- Click **+ Add New Time** to add a second schedule.
- Use the parameter given above to configure the time settings of your schedule.



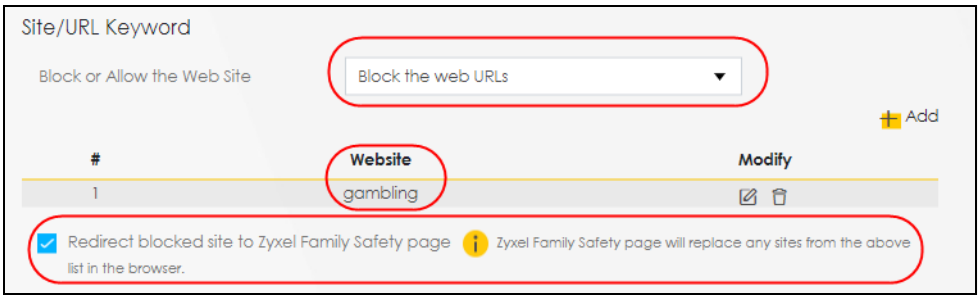
3 Under **Network Service**:

- In **Network Service Setting,** select **Block**.
- Click **+ Add New Service**, then use the parameter given above to configure settings for the Internet service you are blocking.



4 Under **Site / URL Keyword**:

- Select **Block the web URLs** in **Block or Allow the Web Site**.
- Click **Add**, then use the parameter given above to configure settings for the URL keyword you are blocking.
- Select **Redirect blocked site to Zyxel Family Safety page** to redirect the web browser to the Zyxel Family Safety page if he or she tries to access a website with the blocked URL keyword.



5 Click **OK** to save your settings.

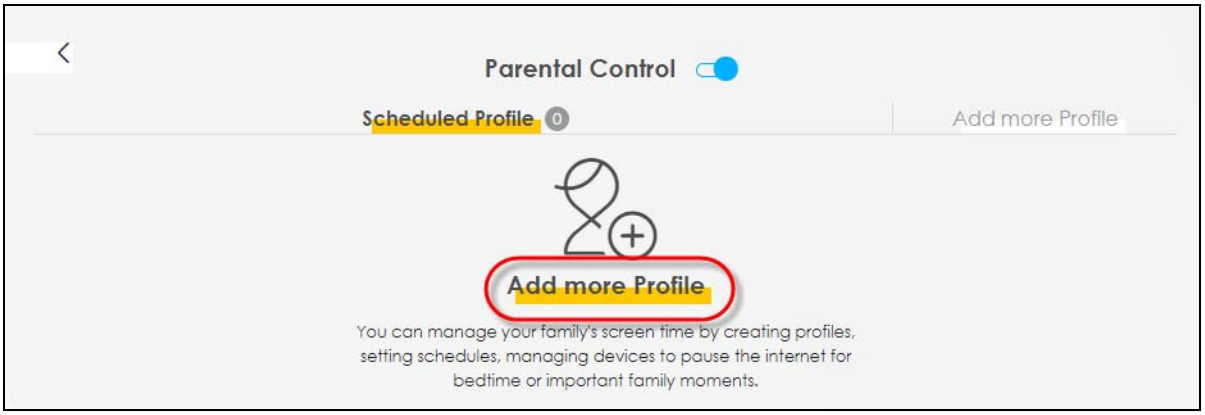
5.6.2.2 Configuring a Parental Control Schedule

Parental Control Profile allows you to set up a schedule rule for Internet usage. Use this feature to limit the days and times a user can access the Internet.

This example shows you how to block an user from accessing the Internet during time for studying. Use the parameter below to configure a schedule rule.

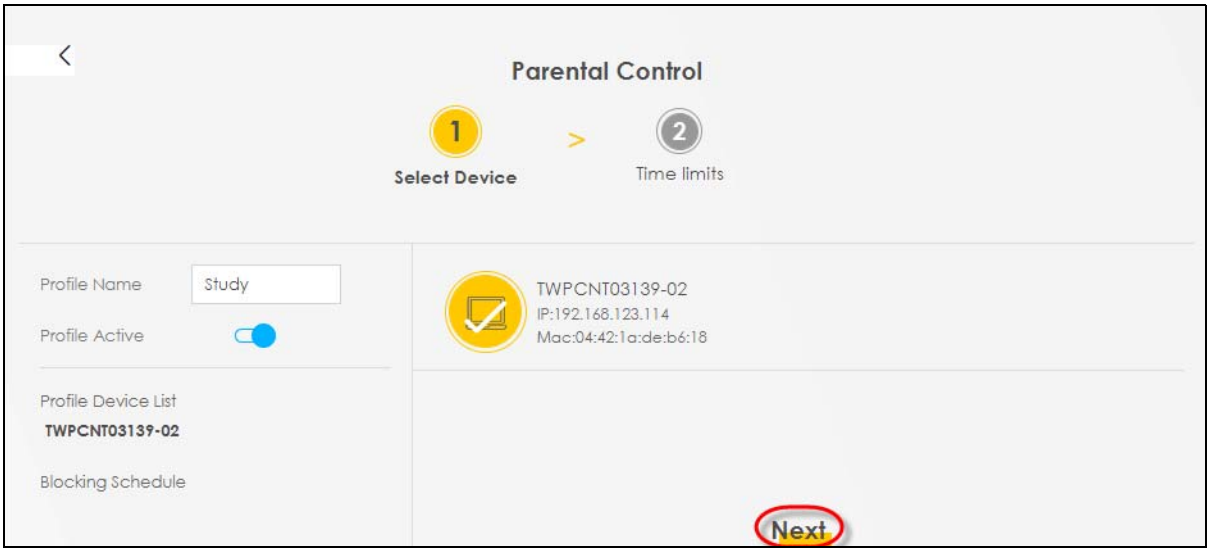
PROFILE NAME	START BLOCKING	END BLOCKING	REPEAT ON
Study	8:00 am	11:00 am	from Monday to Friday
	1:00 pm	5:00 pm	from Monday to Friday

1 Click **Add more Profile** to open the **Parental Control** screen.



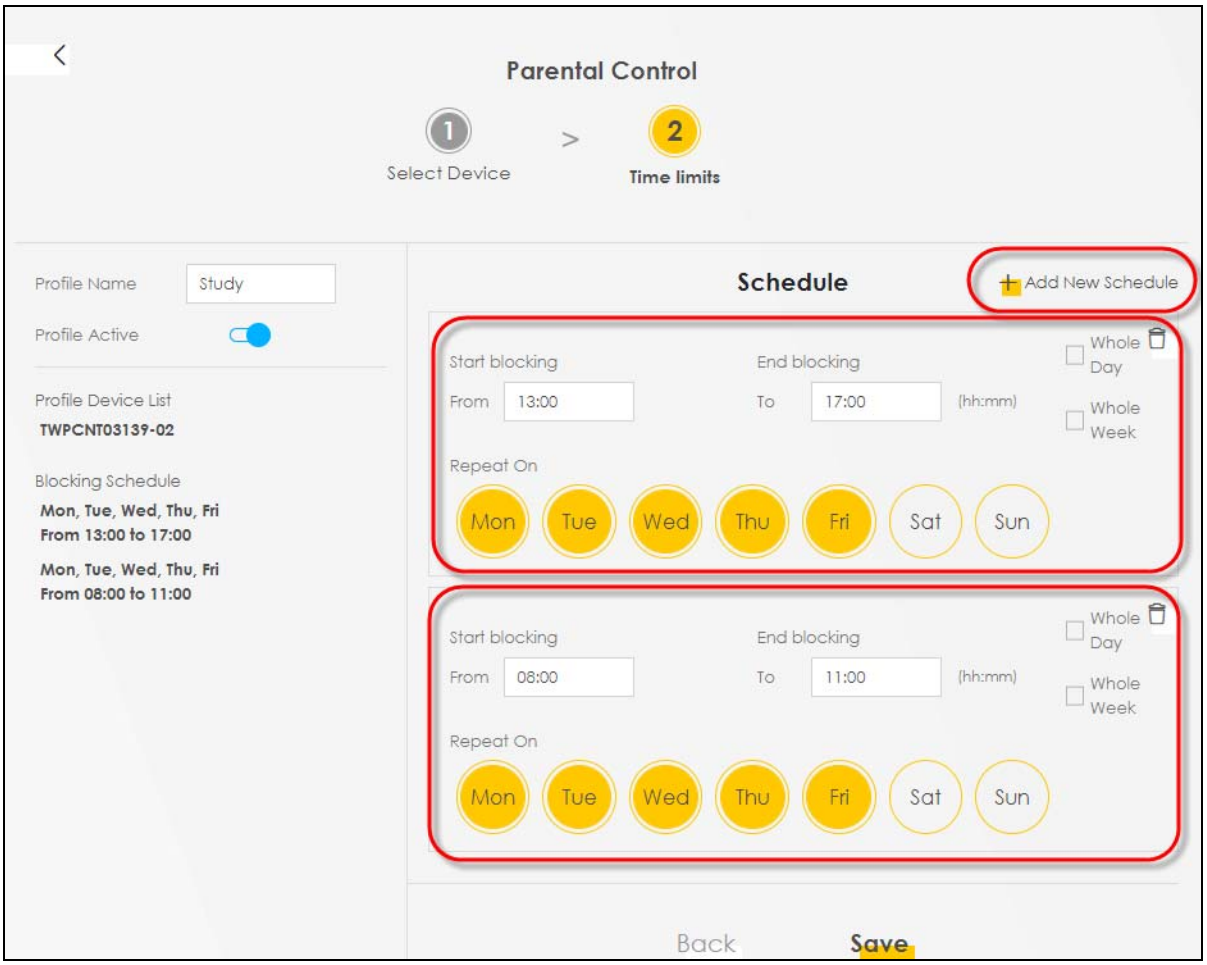
2 Use this screen to add a Parental Control rule.

- Enter the **Profile Name** given in the above parameter.
- Click on the switch to enable **Profile Active**.
- Select a device, and then click **Next** to proceed.



3 Use this screen to edit the Parental Control schedule.

- Click **Add New Schedule** to add a second schedule.
- Use the parameter given above to configure the time settings of your schedules.
- Click **Save** to save the settings.

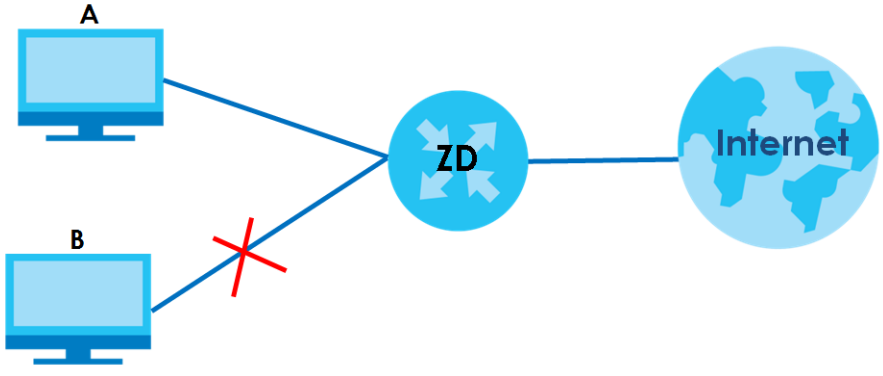


5.6.3 Configure a MAC Address Filter for Wired LAN Connections

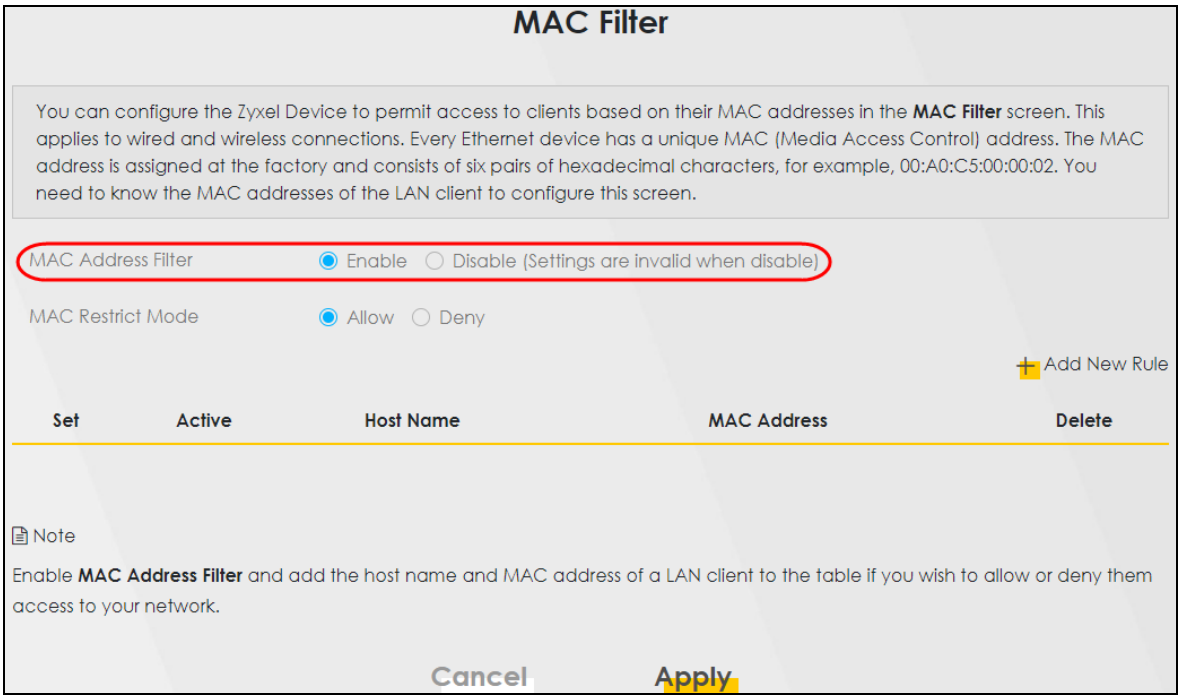
You can use a MAC address filter to exclusively allow or permanently block someone from the wired LAN network.

This example shows that computer B is not allowed access to the wired LAN network.

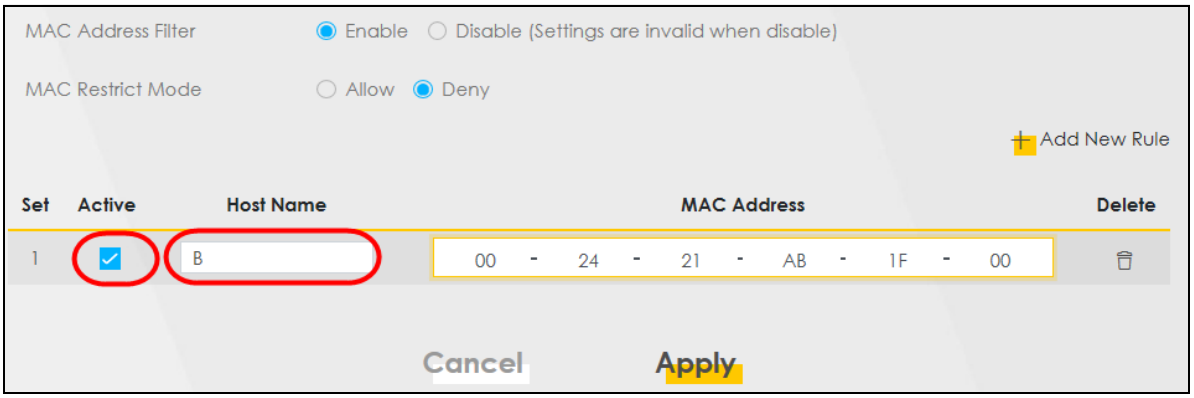
Figure 61 Configure a MAC Address Filter Example



1 Go to the **Security** > **MAC Filter** > **MAC Filter** screen. Under **MAC Address Filter**, select **Enable**.



2 Click **Add New Rule** to add a new entry. Select **Active,** and then enter the **Host Name** and **MAC Address** of computer B. Click **Apply**.



5.7 Internet Calls

This section shows you how to:

- Add a SIP Service Provider
- Add a SIP Account
- Configure a Phone
- Make a VoIP Call

5.7.1 Configure VoIP

To make voice calls over the Internet, you must set up a Session Initiation Protocol (SIP) provider and SIP account on the Zyxel Device. You should have an account with a SIP service provider already set up.

5.7.2 Add a SIP Service Provider

Follow the steps below to add a SIP service provider.

1 Make sure your Zyxel Device is connected to the Internet.

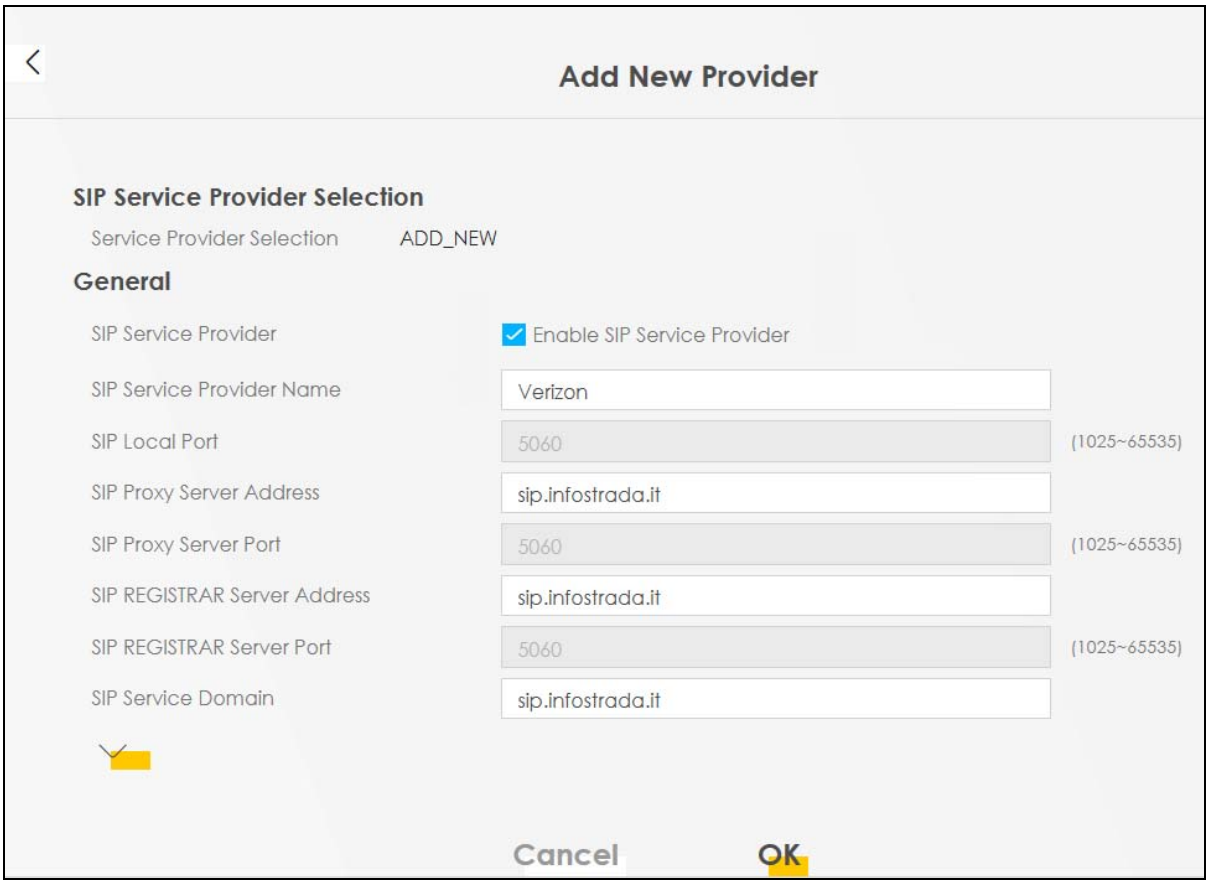
2 Open the Web Configurator.

3 Go to the **VoIP** > **SIP** > **SIP Service Provider** screen. Click the **Add New Provider** button to add the SIP Service Provider.

4 On the **Add New Provider** screen, select **Enable SIP Service Provider**.

5 Enter the **SIP Service Provider Name** of up to 64 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].

6 Enter **SIP Proxy Server Address**, **SIP REGISTRAR Server Address**, and **SIP Service Domain** provided by your SIP service provider. Click **OK** to save your settings.



5.7.3 Add a SIP Account

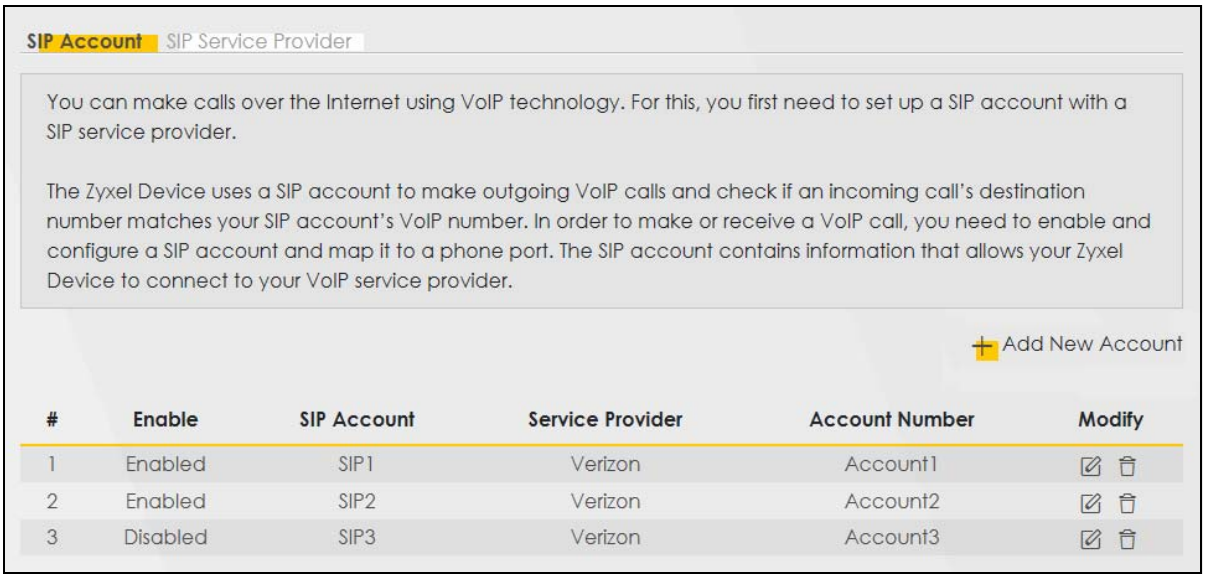
The SIP account must be associated with the SIP service provider configured above. You may configure several SIP accounts for the same service provider. Follow the steps below to set up your SIP account:

1 Make sure your Zyxel Device is connected to the Internet.

2 Open the Web Configurator.

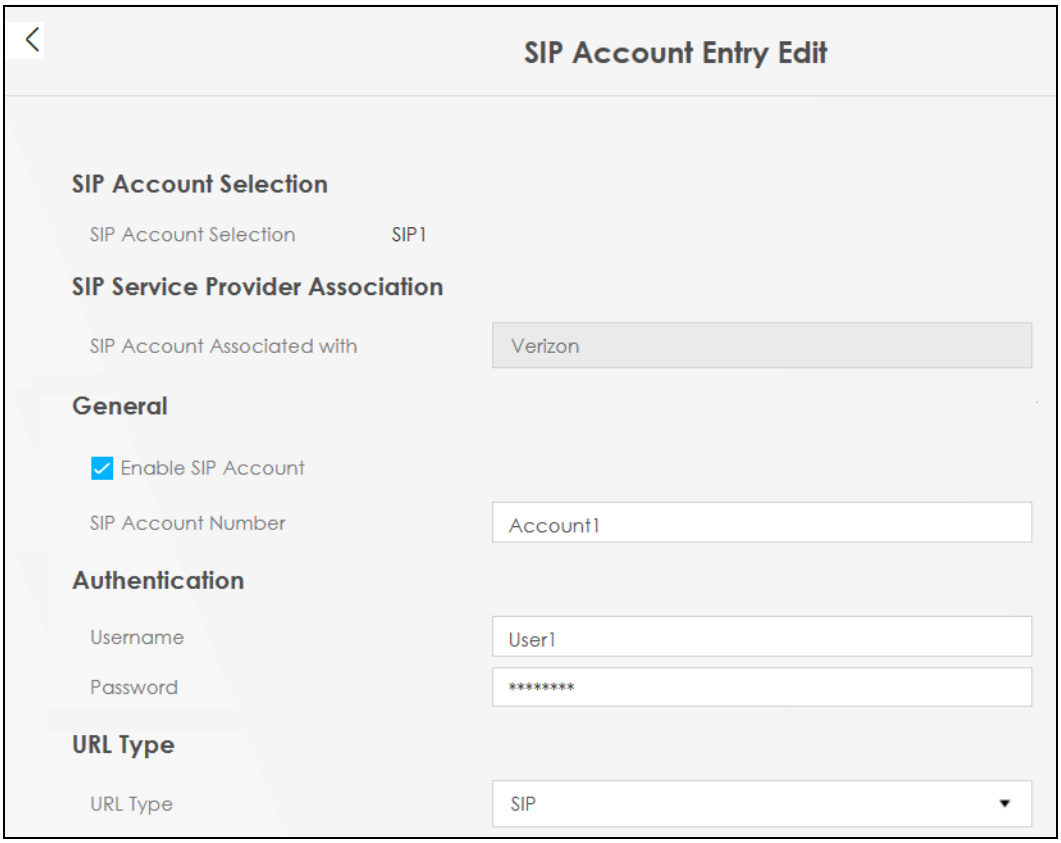
3 Go to the **VoIP** > **SIP** > **SIP Account** screen.

4 Click the **Add New Account** button on the **SIP Account** screen to add a SIP account and map it to a phone port.



5 Under **General,** select **Enable SIP Account**, and then enter the **SIP Account Number**.

6 Under **Authentication,** enter **Username** and **Password**. Leave the other settings as default. Click **OK** to save your settings.

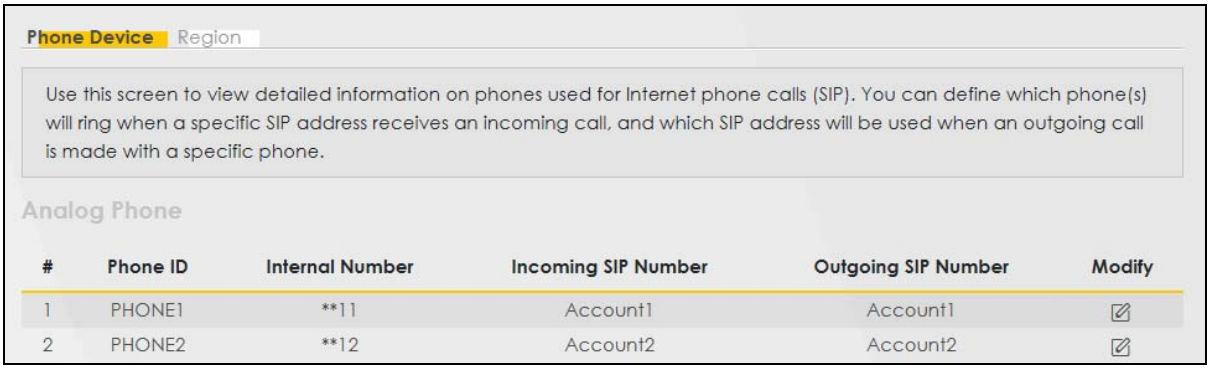


5.7.4 Configure a Phone

You must now configure the phone port to use the SIP account you just configured.

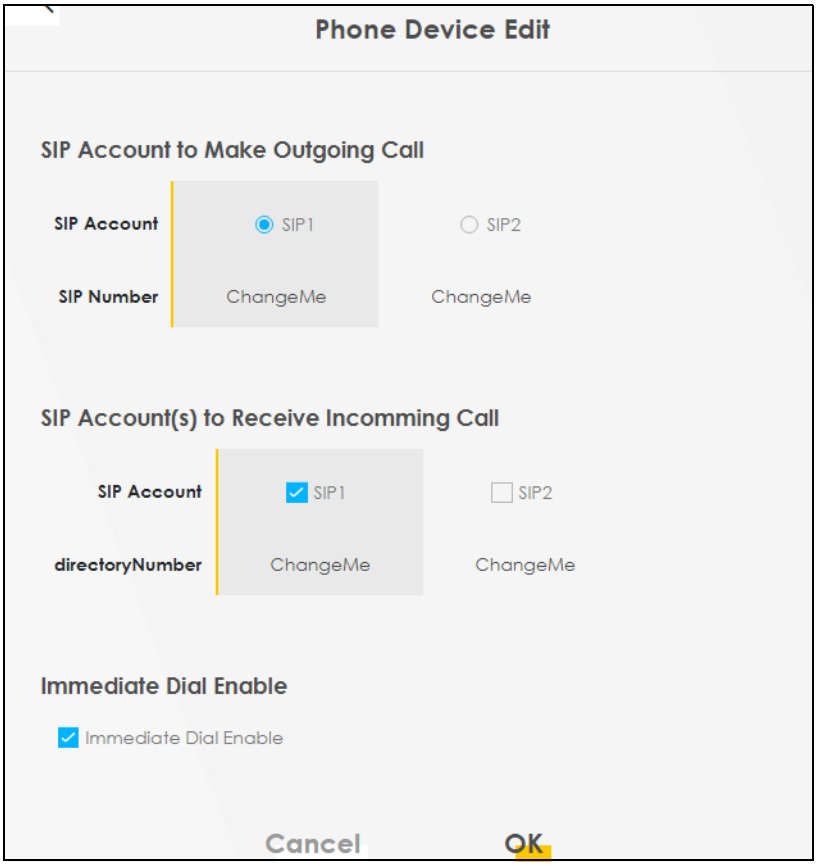
1 Go to the **VoIP** > **Phone** > **Phone Device** screen.

2 Click the **Modify** icon of **PHONE1** to configure PHONE1 on your Zyxel Device. The following screen appears.



3 Under **SIP1 SIP Account to Make Outgoing Call,** select **SIP1** to have the phone connected to the first phone port use the registered SIP1 account to make outgoing calls.

4 Under **SIP Account(s) to Receive Incoming Call,** select **SIP1** to have the phone connected to the first phone port receive phone calls for the SIP1 account. Click **OK** to save your changes.



5.7.5 Make a VoIP Call

Follow these steps to make a phone call using Voice over IP (VoIP).

1. Make sure you connect a telephone to phone port 1 on the Zyxel Device.
2. Make sure the Zyxel Device is turned on and connected to the Internet.
3. Pick up the phone receiver.
4. Dial the VoIP phone number you want to call.

5.8 Device Maintenance

This section shows you how to:

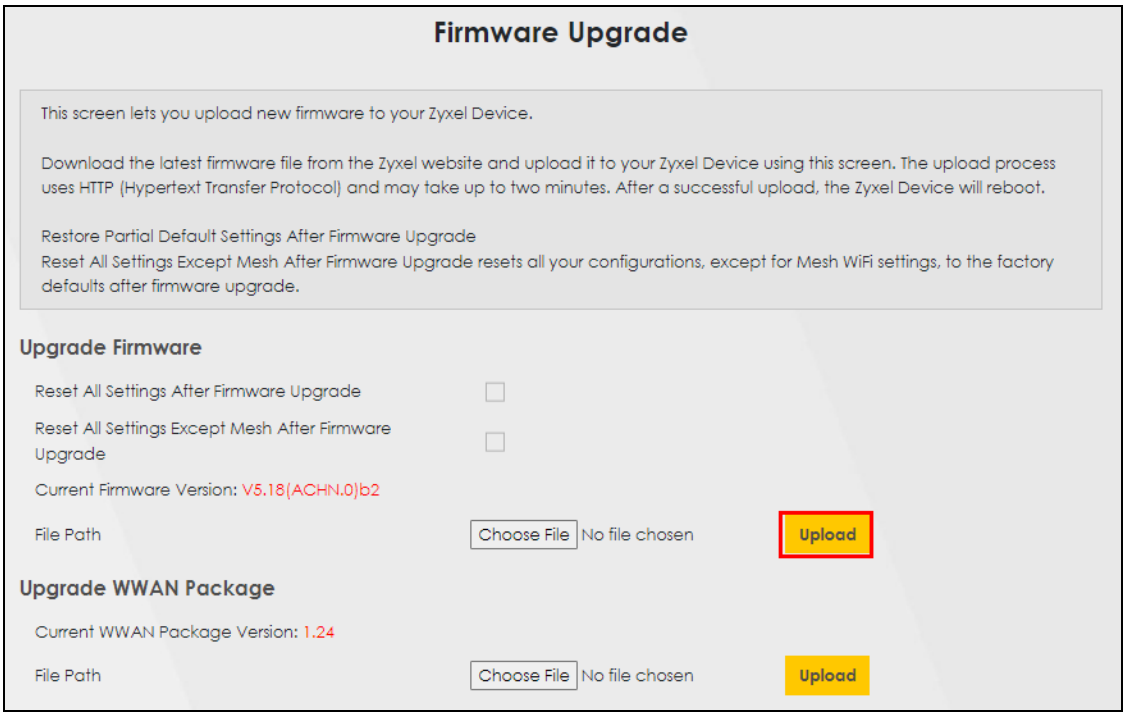
- Upgrade the Firmware
- Back up the Device Configuration
- How to Reset the Zyxel Device to the Factory Defaults

You can upgrade the Zyxel Device firmware, back up the configuration and restore the Zyxel Device to its previous or default settings.

5.8.1 Upgrade the Firmware

Upload the latest firmware to the Zyxel Device for feature enhancements.

1. To download the latest firmware of your Zyxel Device, go to *https://www.zyxel.com/service-provider* and search for your model. The latest firmware will be available under the **Downloads & resources** tab. The model code for the Zyxel Device in this example is v5.13(ABLZ.1). Note the model code for your Zyxel Device.
2. Unzip the file.
3. Go to the **Maintenance** > **Firmware Upgrade** screen.
4. Click **Browse**/**Choose File** and select the file with a ".bin" extension to upload. Click **Upload**.



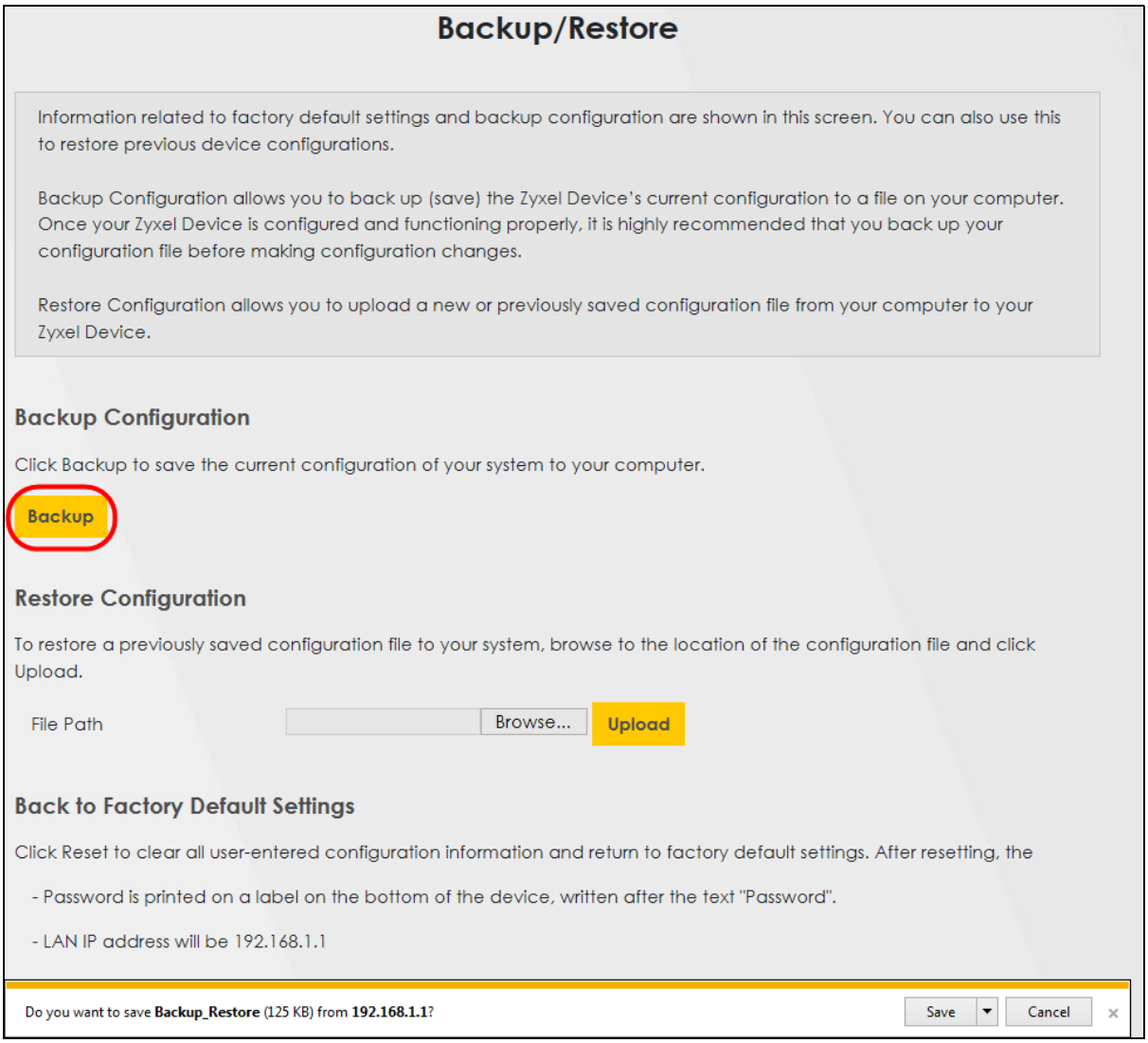
5 This process may take up to 2 minutes to finish. After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

5.8.2 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 Under **Backup Configuration,** click **Backup.** A configuration file is saved to your computer. In this case, the **Backup**/**Restore** file is saved.

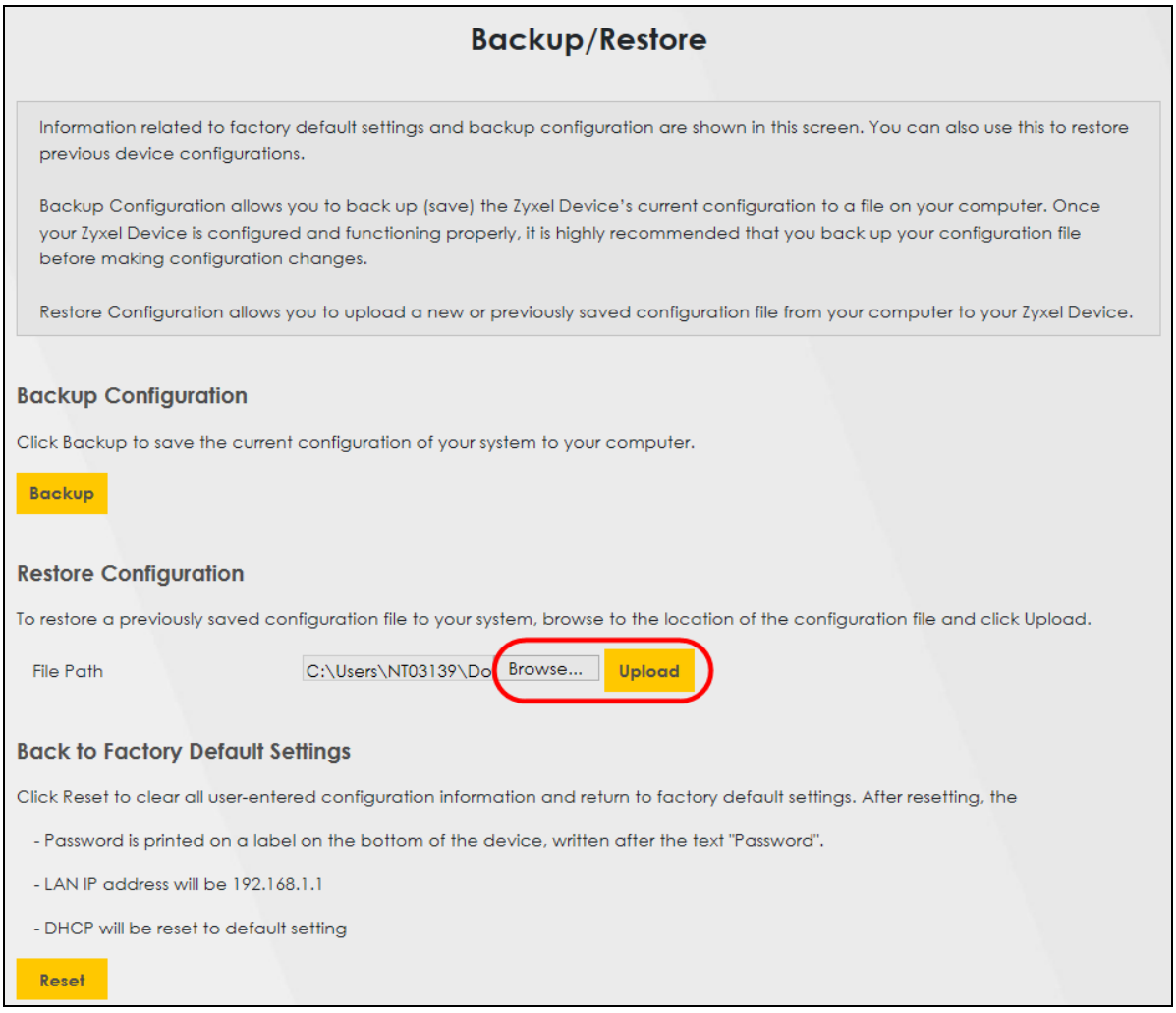


5.8.3 Restore the Device Configuration

This section shows you how to restore a previously-saved configuration file from your computer to your Zyxel Device.

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

2 Under **Restore Configuration**, click **Browse**/**Choose File**, and then select the configuration file that you want to upload. Click **Upload**.

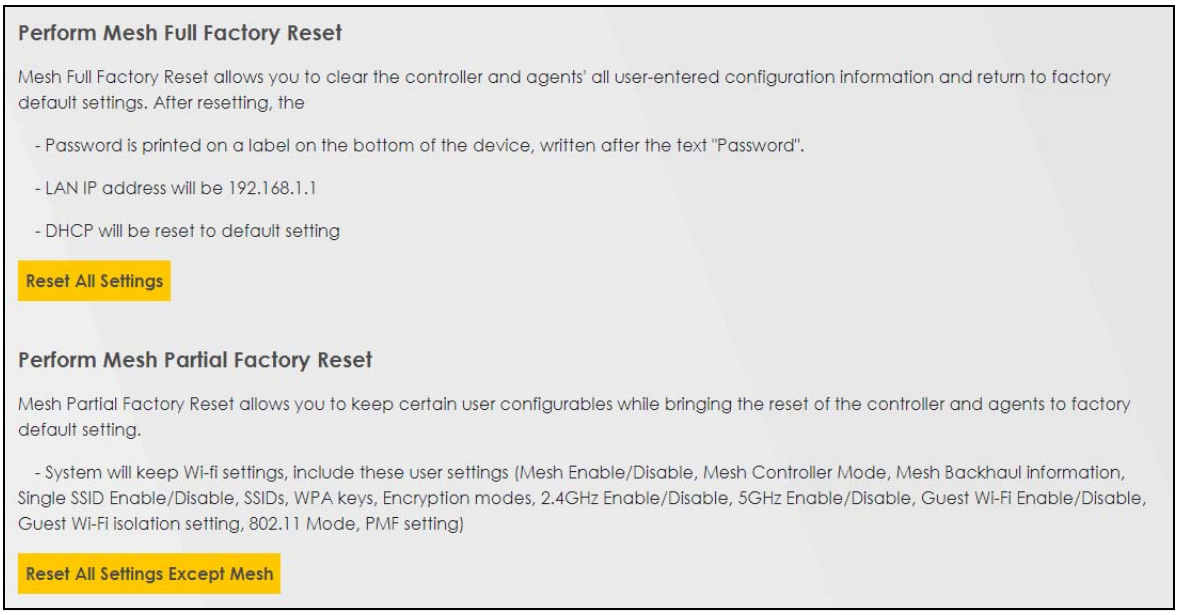


3 The Zyxel Device automatically restarts after the configuration file is successfully uploaded. Wait for one minute before logging into the Zyxel Device again. Go to the **Connection Status** page to check the firmware version after the reboot.

5.8.4 How to Reset the Zyxel Device to the Factory Defaults

To reset the Zyxel 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 Zyxel Device.

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



If you want to reset the Zyxel Device while keeping the Mesh WiFi Settings, click the **Reset All Settings Except Mesh** button. See Chapter 41 on page 418 for more details.

5.9 Remote Access from WAN

This section shows you how to:

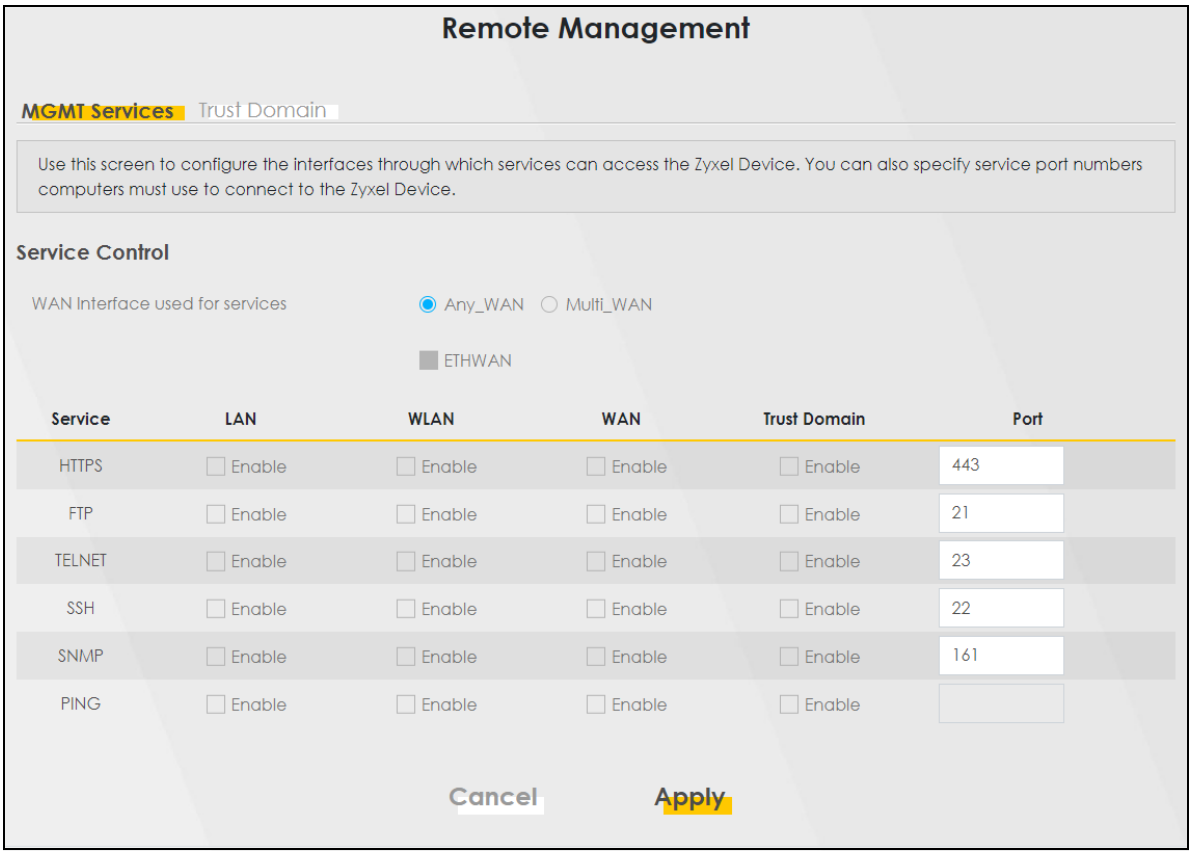
- Configure Access to Your Zyxel Device
- Configure the Trust Domain

You can configure WAN access for a specific trusted computer through HTTPS, SSH to the Zyxel Device. Remote management determines which interface and web services are allowed to access the Zyxel Device.

5.9.1 Configure Access to Your Zyxel Device

Perform the following to configure access to your Zyxel Device:

1 Go to the **Maintenance** > **Remote Management** > **MGMT Services** screen. Select the WAN interface and services allowed to access the Zyxel Device remotely.



These are the different ways to access the Zyxel Device remotely.

ACCESS TYPE	LABEL	DESCRIPTION
LAN / WLAN (WiFi)	LAN / WLAN	This allows access of the selected **Service** from the local LAN.
WAN	WAN	This allows access of the selected **Service** from the WAN connections.
Trust Domain	Trust Domain	This allows access of the selected **Service** only from the trusted IPv4 / IPv6 addresses configured under **Trust Domain**.

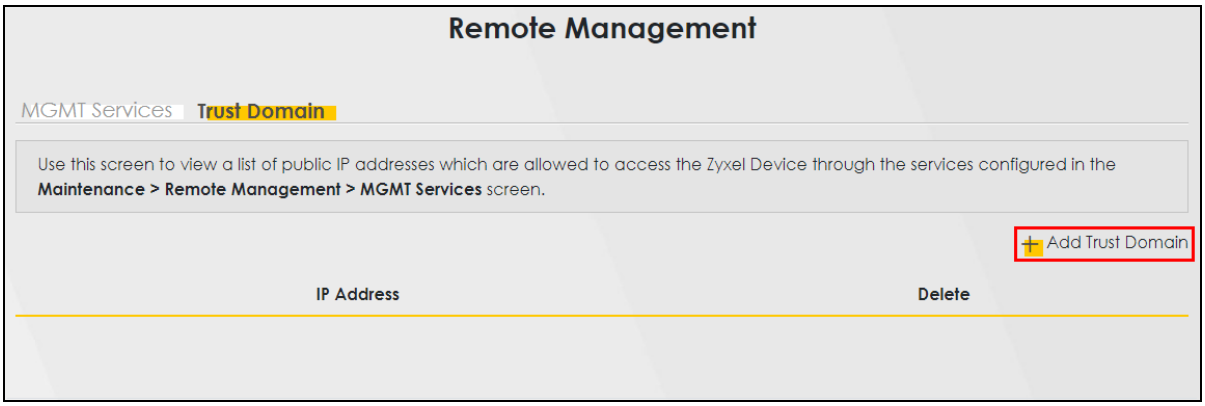
2 Select how you want to access the Zyxel Device remotely.

3 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.

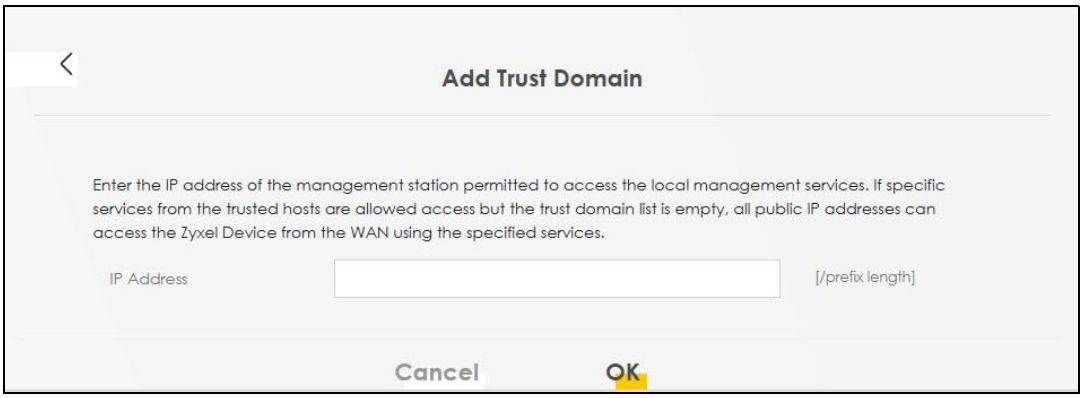
5.9.2 Configure the Trust Domain

Perform the following to configure the Trust Domain on your Zyxel Device:

1 Go to the **Maintenance** > **Remote Management** > **Trust Domain** screen. Click **+ Add Trust Domain** to go to the **Add Trust Domain** screen to add a trusted host IPv4 / IPv6 address.



2 Enter a public IPv4 / IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN. Then click **OK**.



PART II
Technical Reference

CHAPTER 6
Connection Status

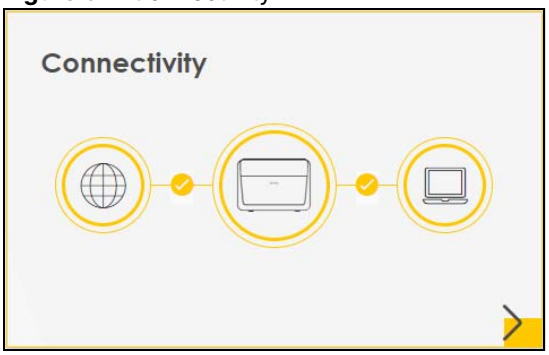
6.1 Connection Status Overview

After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access and WiFi settings in this screen. It also shows the network status of the Zyxel Device and computers or devices connected to it.

6.1.1 Connectivity

Use this screen to view the network connection status of the Zyxel Device and its clients.

Figure 62 Connectivity



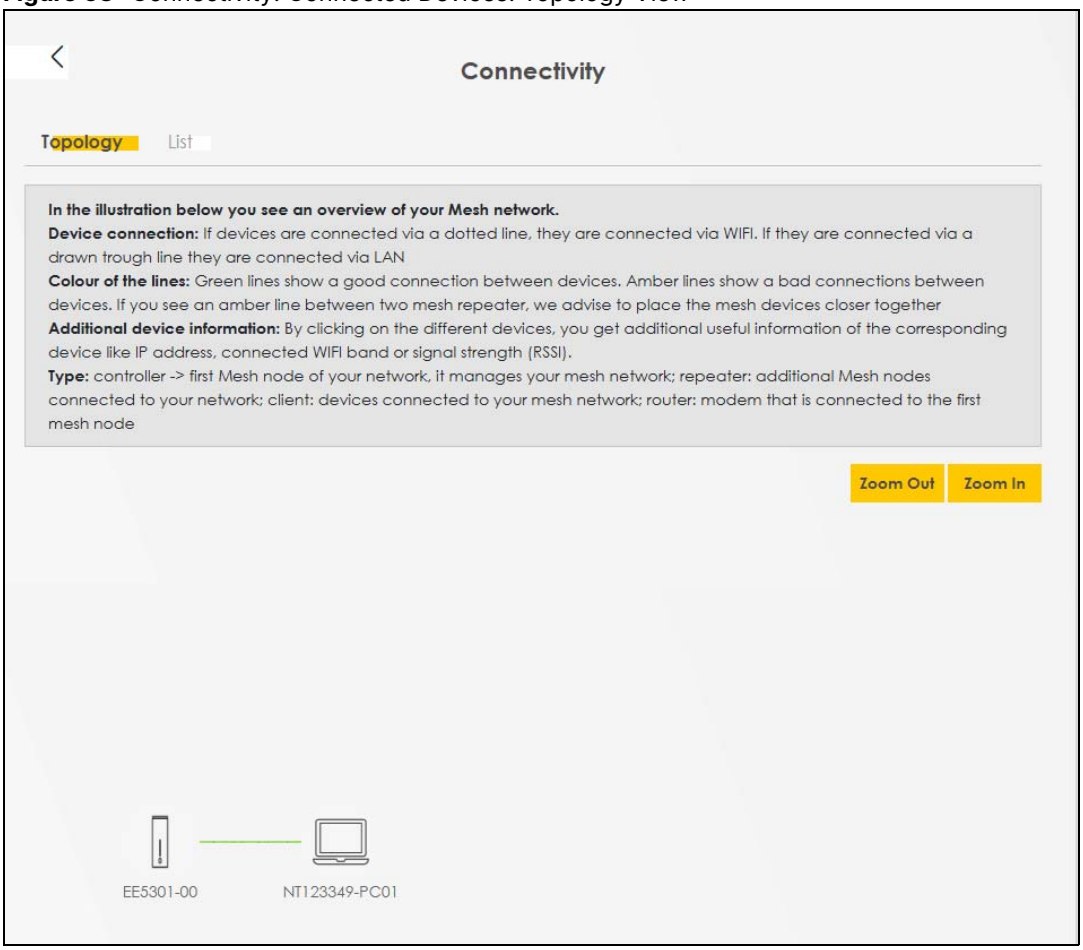
Click the Arrow icon ( ) to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

You can change the icon and name of a connected device. Place your mouse within the device block, and an Edit icon ( ) will appear. Click the Edit icon, and you will see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Click to enable ( ) **Internet Blocking** for a connected WiFi client.

The following screen appears when you enable **MPro Mesh** in the **Network Setting** > **Wireless** > **MESH** screen. Check Section 1.1 on page 19 to see if your Zyxel Device supports Mesh.

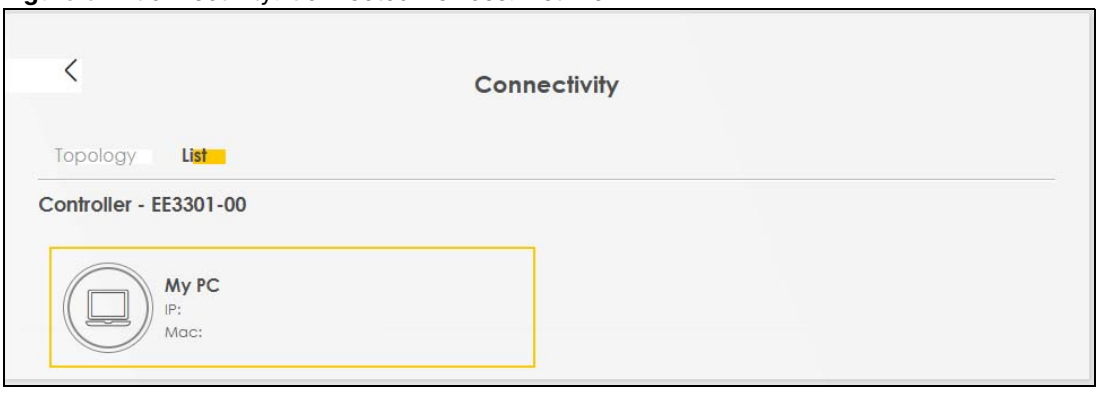
Use the **Topology** view screen to display an overview of your Mesh network.

Figure 63 Connectivity: Connected Devices: Topology View



Use the **List** view screen to view IP addresses and MAC addresses of the WiFi and wired devices connected to the Zyxel Device. Place your mouse within the device block, and an **Edit** icon ( ) will appear. Click the **Edit** icon to change the icon and name of a connected device.

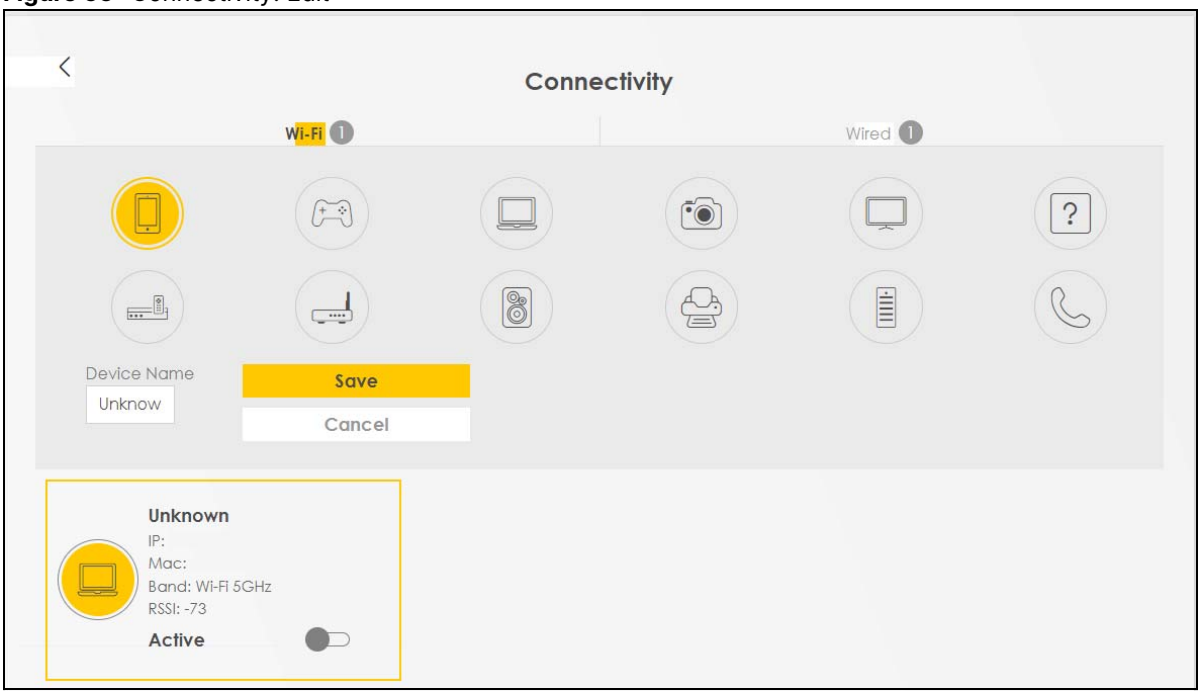
Figure 64 Connectivity: Connected Devices: List View



6.1.2 Icon and Device Name

Select an icon and/or enter a name in the **Device Name** field for a connected device. Click to enable ( ) **Internet Blocking** (or **Active**) for a connected WiFi client. Click **Save** to save your changes.

Figure 65 Connectivity: Edit



6.1.3 System Info

Use this screen to view the basic system information of the Zyxel Device.

Figure 66 System Info

Click the Arrow icon ( ) to view more information on the status of your firewall and interfaces (WAN, LAN, and WLAN).

Figure 67 System Info: Detailed Information

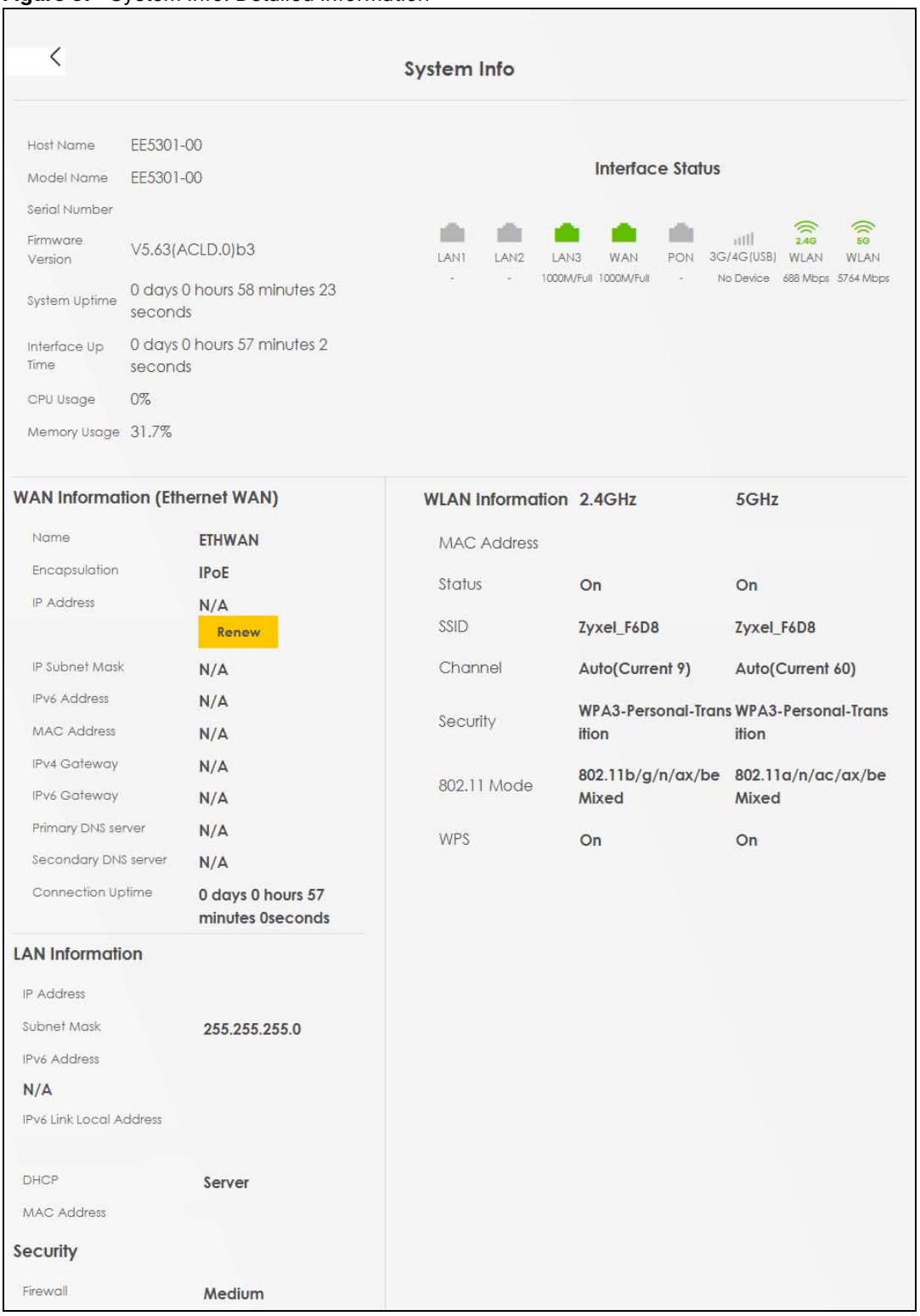
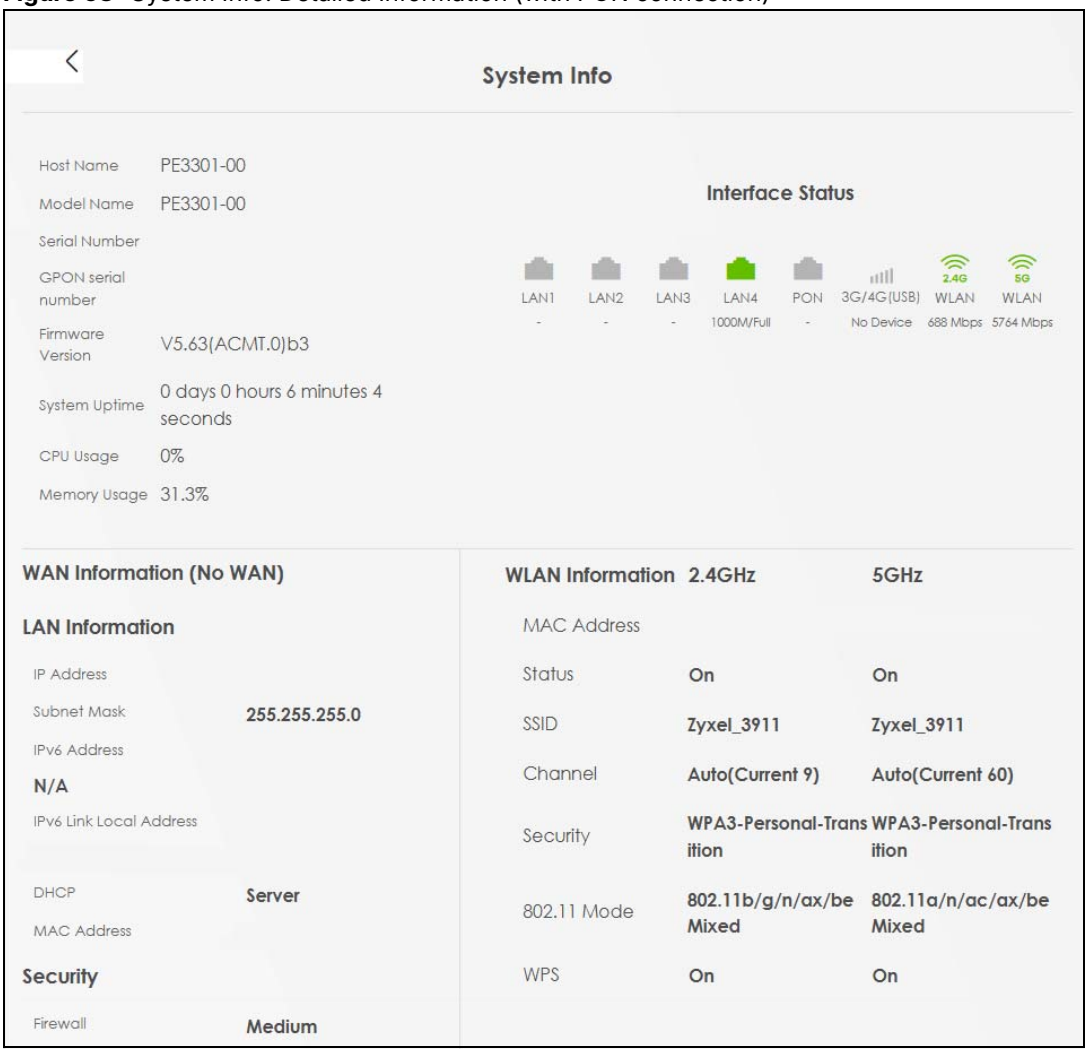


Figure 68 System Info: Detailed Information (with PON connection)



Each field is described in the following table.

Table 25 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the Zyxel Device system name. It is used for identification.
Model Name	This shows the model number of your Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This is the current version of the firmware inside the Zyxel Device.
System Uptime	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (**Maintenance** > **Reboot**), or when you reset it.
WAN Information (These fields display when you have a WAN connection.)	
Name	This field displays the name given to the Internet connection.
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IP address of the Zyxel Device in the WAN. Click the **Release**/ **Renew** button if you want to release/renew your WAN IP address.
IP Subnet Mask	This field displays the current IPv4 subnet mask of the Zyxel Device in the WAN.

Table 25 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device in the WAN.
MAC Address	This field displays the WAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
IPv4 Gateway	This field displays the IPv4 address of the default gateway. The default gateway is a router or switch on the same segment as your Zyxel Device's interface. The gateway helps forward packets to destinations outside the local network.
IPv6 Gateway	This field displays the IPv6 address of the default gateway. The default gateway is a router or switch on the same segment as your Zyxel Device's interface. The gateway helps forward packets to destinations outside the local network.
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.
Primary DNSv6 server	This field displays the first DNS server IPv6 address assigned by the ISP.
Secondary DNSv6 server	This field displays the second DNS server IPv6 address assigned by the ISP.
LAN Information	
IP Address	This is the current IP address of the Zyxel Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the Zyxel Device in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the Zyxel Device for the LAN interface. A link-local address is a special type of the IP address that is only valid for communication within the local network segment or broadcast domain of the device. Typically, link-local addresses are used for automatic address configuration and neighbor discovery protocols.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: **Server** – The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** – The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **Disable** – The Zyxel Device is not providing any DHCP services to the LAN.
Security	
Firewall	This displays the firewall's current security level (**High**, **Medium**, **Low**, or **Disabled**).
WLAN Information	
MAC Address	This shows the WiFi adapter MAC (Media Access Control) Address of the WiFi interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a WLAN.
Channel	This is the channel number currently used by the WiFi interface.
Security	This displays the type of security mode the WiFi interface is using in the WLAN.
802.11 Mode	This displays the type of 802.11 mode the WiFi interface is using in the WLAN.
WPS	This displays whether WPS is activated on the WiFi interface.

6.1.4 WiFi Settings

The following compares the main WiFi network and the guest WiFi network.

Table 26 Main/Guest WiFi Networks key Differences

FEATURE	MAIN WI-FI	GUEST WI-FI
Purpose	For primary household or business users.	For visitors.
Network Access	For access to internal devices, such as printers or file servers.	Internet access only; no access to internal devices.

Use this screen to enable or disable the main WiFi network. When the switch turns blue, the function is enabled. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the main WiFi networks. If you want to show or hide your WiFi passwords, click the Eye icon ( ).

Figure 69 WiFi Settings (for 2.4 GHz and 5 GHz models)

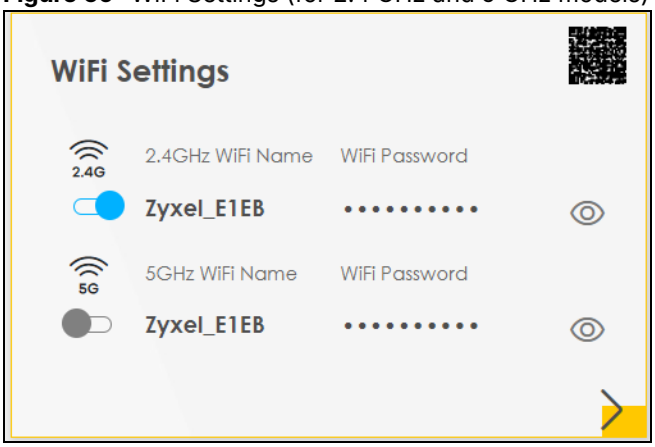
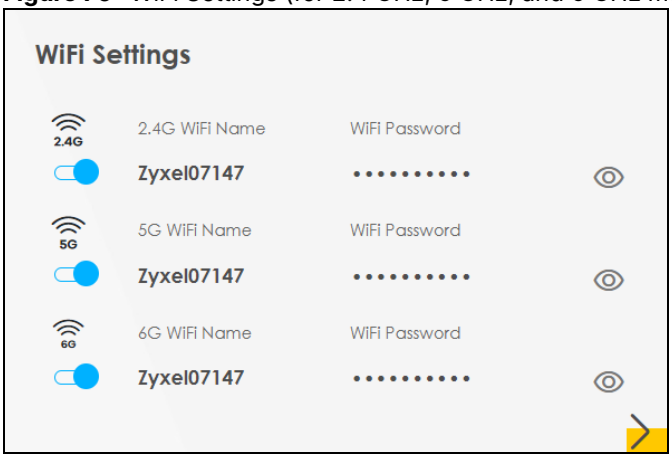


Figure 70 WiFi Settings (for 2.4 GHz, 5 GHz, and 6 GHz models)



Click the Arrow icon ( ) to configure the SSIDs and/or passwords for your main WiFi networks. Click the Eye icon ( ) to display the characters as you enter the WiFi Password.

Scanning the QR code is an alternative way to connect your WiFi client to the WiFi network.

Note: When you enable Mesh in the **Network** > **Wireless** > **MESH** screen, **Keep 2.4G, 5G and 6G the same** will be enabled and cannot be disabled.

Figure 71 WiFi Settings: Configuration (for 2.4 GHz and 5 GHz models)

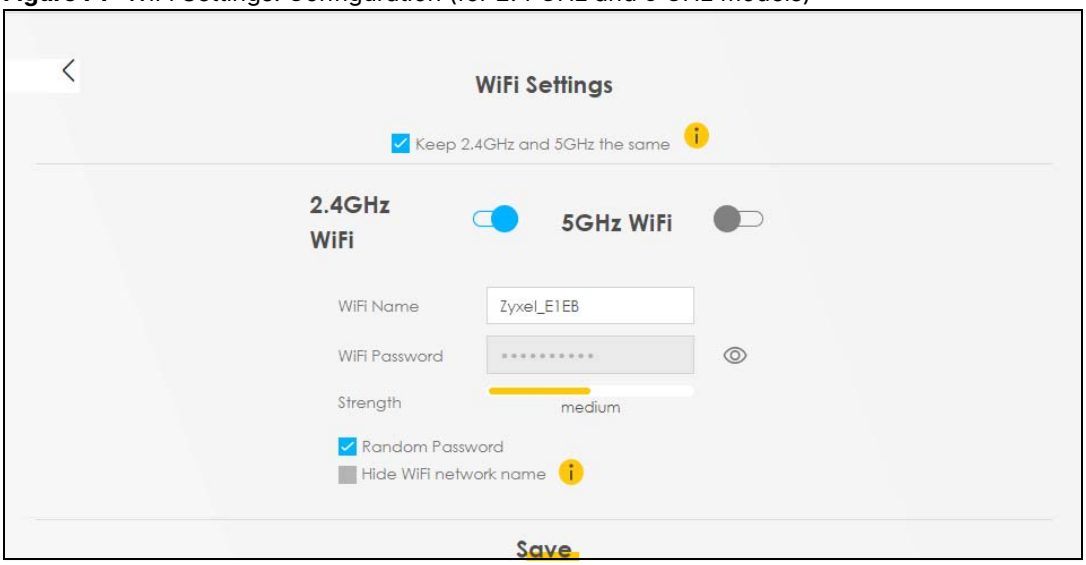
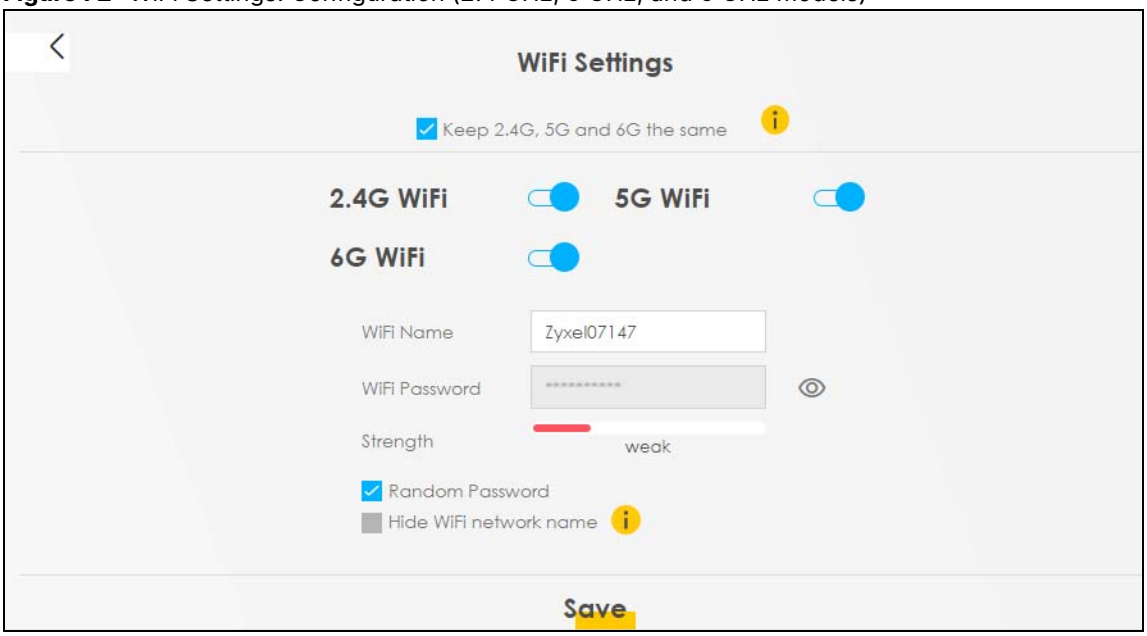


Figure 72 WiFi Settings: Configuration (2.4 GHz, 5 GHz, and 6 GHz models)



Each field is described in the following table.

Table 27 WiFi Settings: Configuration

LABEL	DESCRIPTION
Keep 2.4G, 5G and 6G the same	Select this and the 2.4 GHz, 5 GHz and 6 GHz wireless networks will use the same SSID. If you deselect this, the screen will change. You need to assign different SSIDs for the 2.4 GHz and 5 GHz wireless networks. Note: To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.
2.4G / 5G / 6G WiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz / 6 GHz WiFi network. When the switch turns blue, the function is enabled. Note: To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.
WiFi Name	The SSID (Service Set Identifier) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for the WiFi. You can use up to 32 printable characters, including spaces.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually enter a pre-shared key from 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces. Click the Eye icon to show or hide the password for your WiFi network. When the Eye icon is slashed, you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

6.2 Guest WiFi Settings

Use this screen to enable or disable the guest 2.4 GHz / 5 GHz /6 GHz WiFi networks. When the switch goes to the right (), the function is enabled. Otherwise, it is not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the Eye icon.

Note: To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.

Note: To see the difference of the main WiFi network and the guest WiFi network, please refer to Table 26 on page 138.

Figure 73 Guest WiFi Settings (for 2.4 GHz and 5 GHz models)

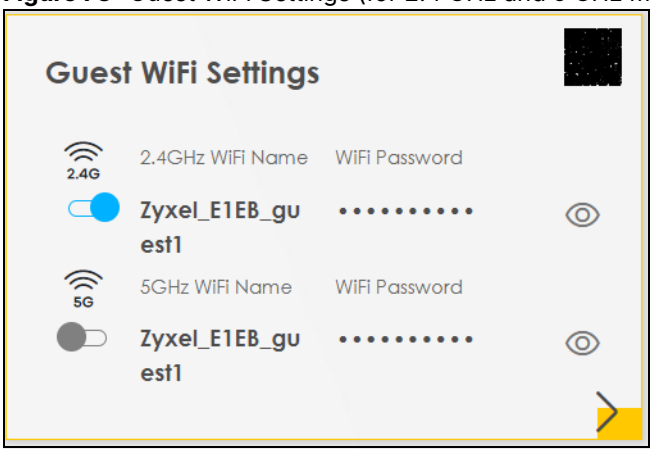
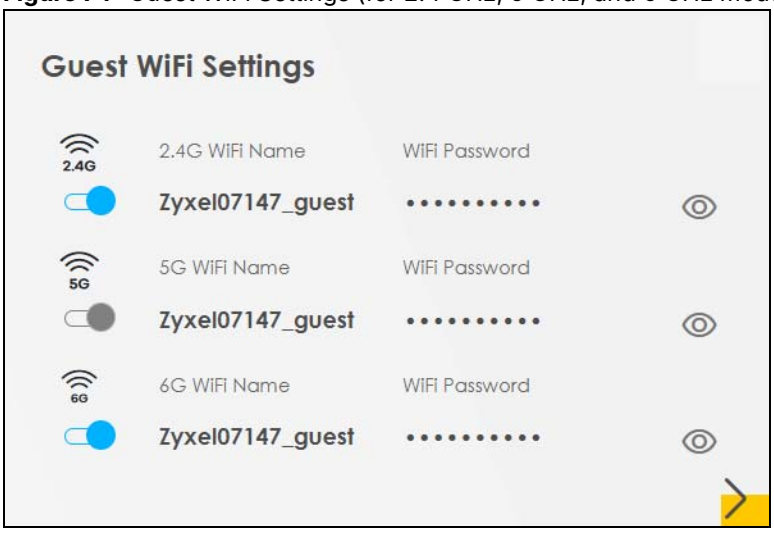


Figure 74 Guest WiFi Settings (for 2.4 GHz, 5 GHz, and 6 GHz models)



Click the Arrow icon ( ) to open the following screen. Use this screen configure the SSIDs and/or passwords for your guest WiFi networks.

To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.

To assign different SSIDs to the 2.4 GHz and 5 GHz guest wireless networks, clear the **Keep 2.4G, 5G and 6G the same** checkbox in the **WiFi Settings** screen, and the **Guest WiFi Settings** screen will change.

Figure 75 Guest WiFi Settings: Different SSIDs (for 2.4 GHz and 5 GHz models)

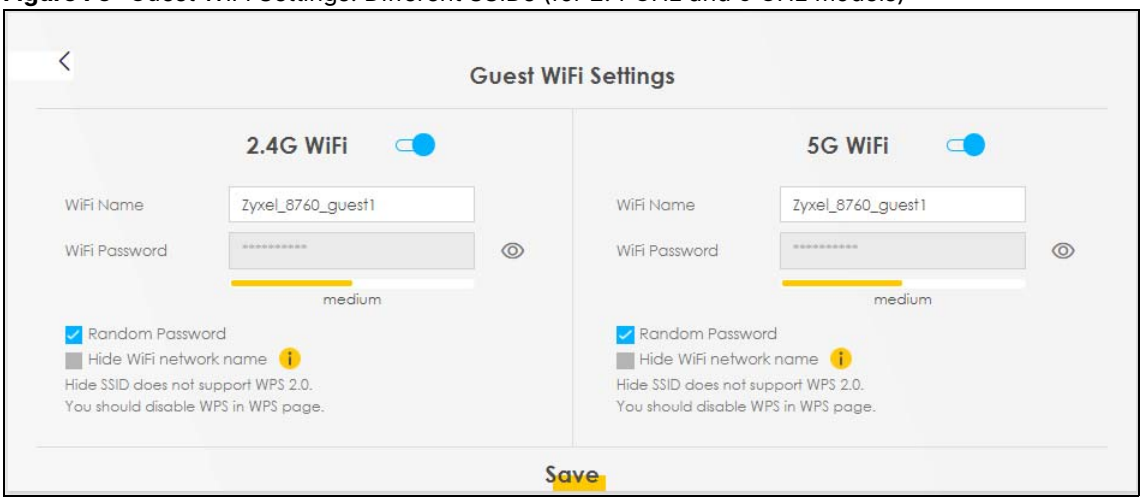
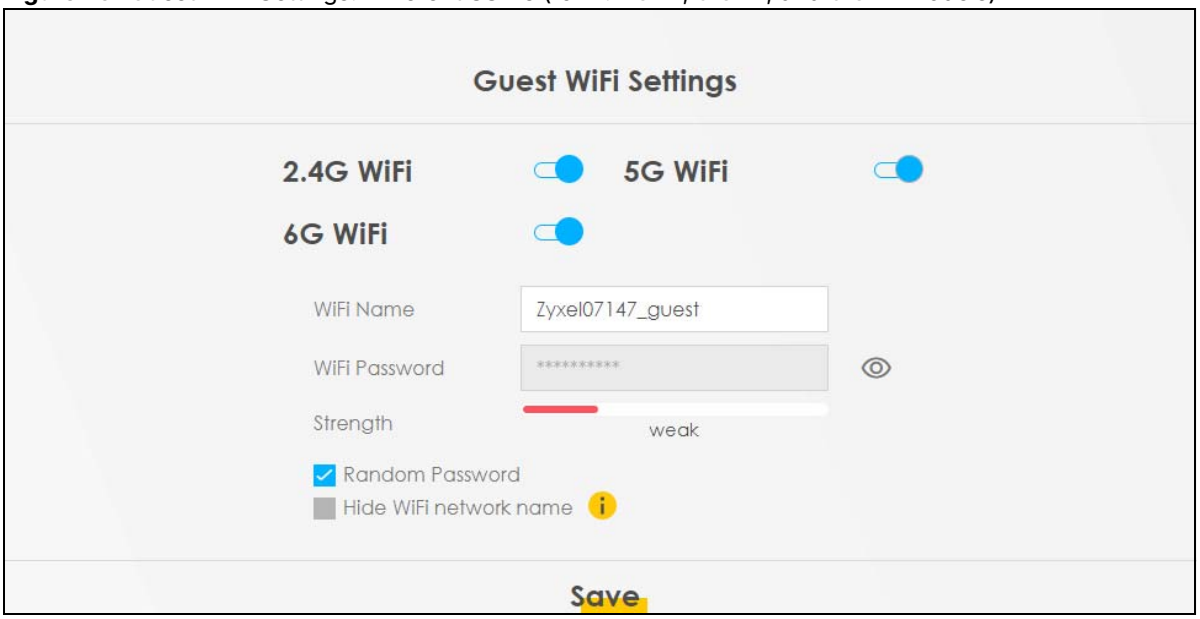


Figure 76 Guest WiFi Settings: Different SSIDs (for 2.4 GHz, 5 GHz, and 6 GHz models)



Each field is described in the following table.

Table 28 WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4G/5G/6G WiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz / 6 GHz WiFi networks. When the switch goes to the right, the function is enabled. Otherwise, it is not. Note: To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable characters, including spaces) for the WiFi.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually enter a pre-shared key from 8 to 64 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.

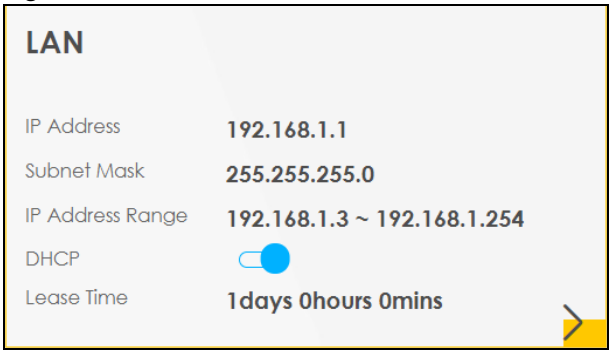
Table 28 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
	Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

6.2.1 LAN

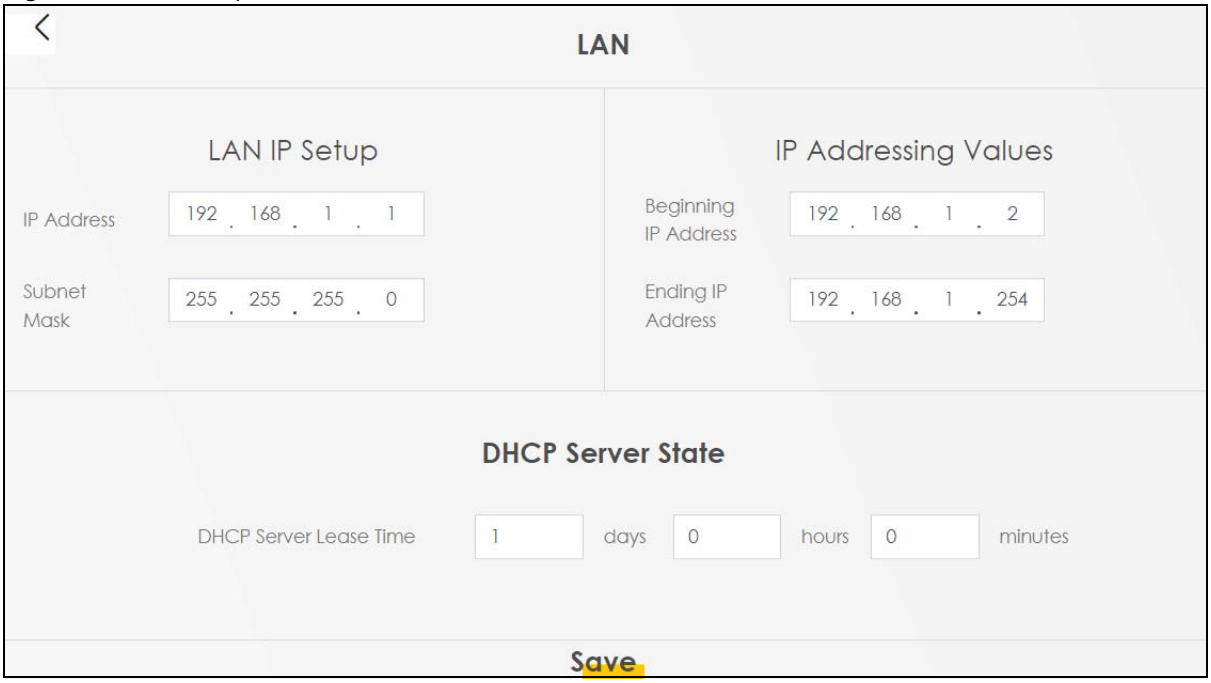
Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device. Click the switch button to turn on/off the DHCP server.

Figure 77 LAN



Click the Arrow icon ( ) to configure the LAN IP settings and DHCP setting for your Zyxel Device.

Figure 78 LAN Setup



Each field is described in the following table.

Table 29 LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel 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.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.

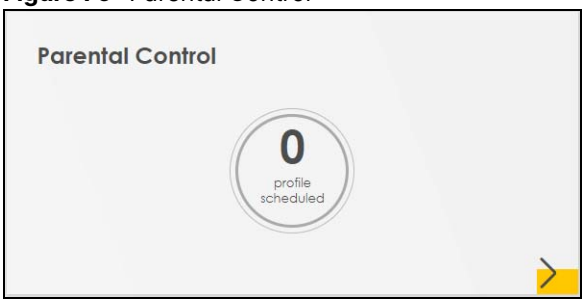
6.3 The Parental Control Screen

Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

Your parental control screens may be different depending on the model you are using. Some Zyxel Devices support scheduling, some support scheduling and URL filtering.

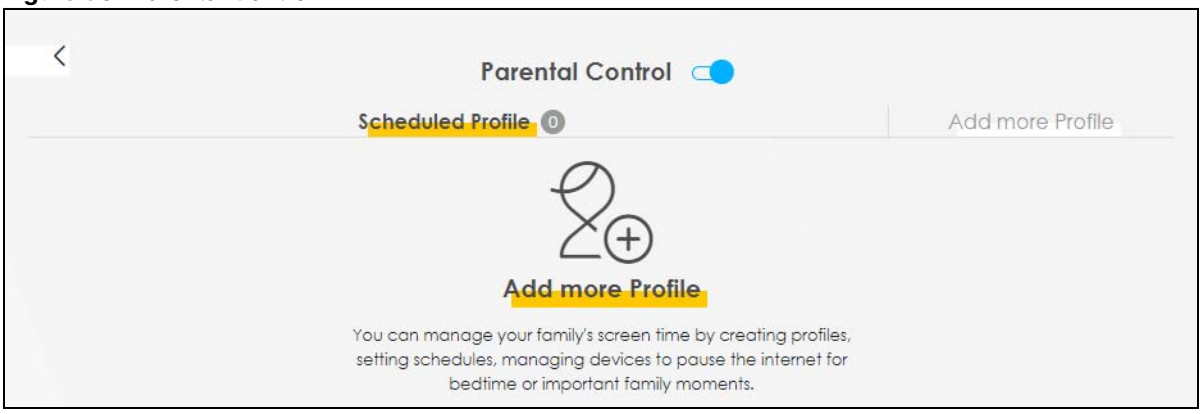
Use this screen to view the number of profiles that were created for parental control.

Figure 79 Parental Control



Click the yellow Arrow icon to open the following screen. Use this screen to enable parental control and add more profiles. Add a profile to create restricted access schedules. Go to the **Security** > **Parental Control** > **Add New PCP**/**Edit** screen to configure URL filtering settings to block the users on your network from accessing certain web sites.

Figure 80 Parental Control



Each field is described in the following table.

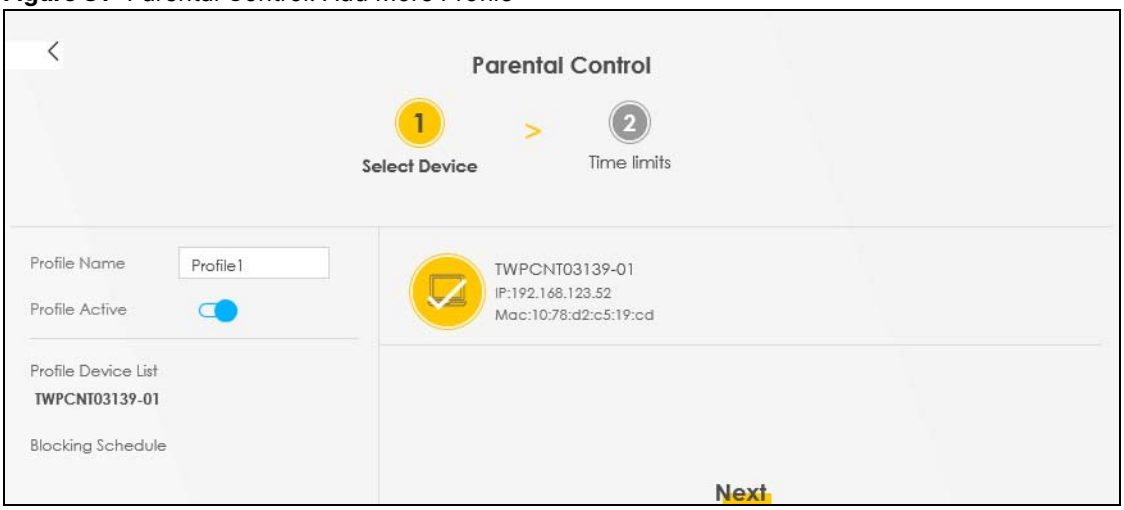
Table 30 Parental Control: Schedule

LABEL	DESCRIPTION
Parental Control	Click this switch to enable parental control.
Scheduled Profile	This screen shows all the created profiles.
Add More Profile	Click this to create a new profile.

6.3.1 Create a Parental Control Profile

Click **Add more Profile** to create a profile. Use this screen to add a devices in a profile and block Internet access on the profile devices.

Figure 81 Parental Control: Add More Profile

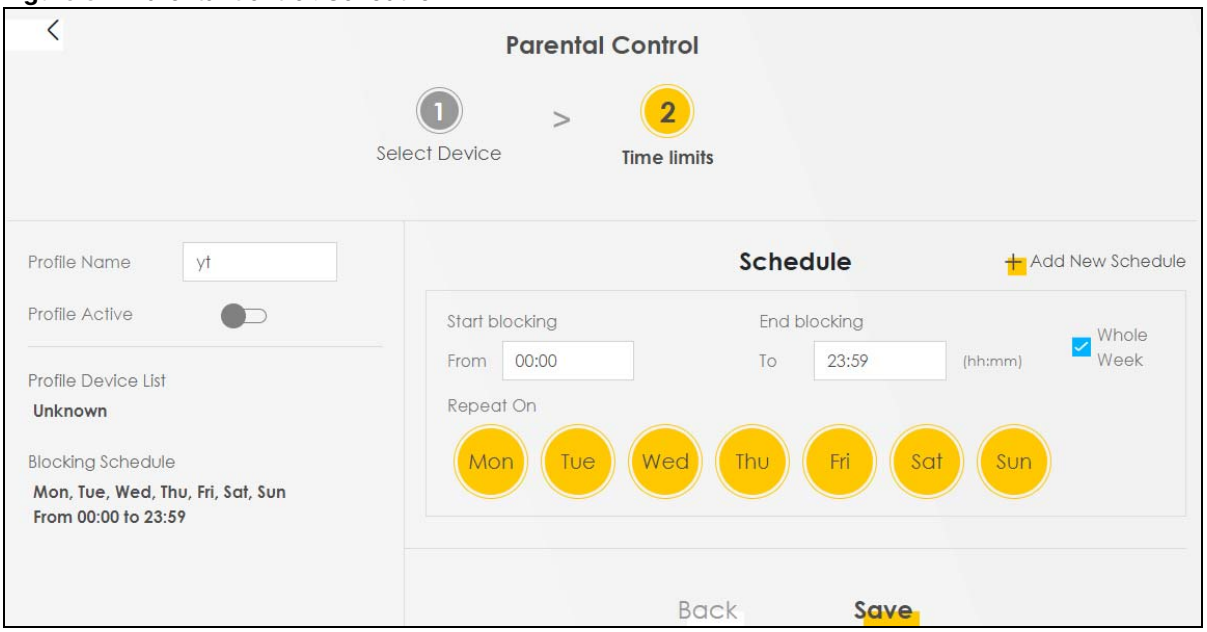


Each field is described in the following table.

Table 31 Parental Control: Add More Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable Internet access. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
	Select a device(s) on your network for this profile.

Figure 82 Parental Control: Schedule



Each field is described in the following table.

Table 32 Parental Control: Schedule

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Profile Active	Click this switch to enable this profile.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile devices.
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save your changes.

Once a profile is created, it will show in the following screen. Click this to **Delete** or **Edit** a profile.

Figure 83 Parental Control: Edit/Delete

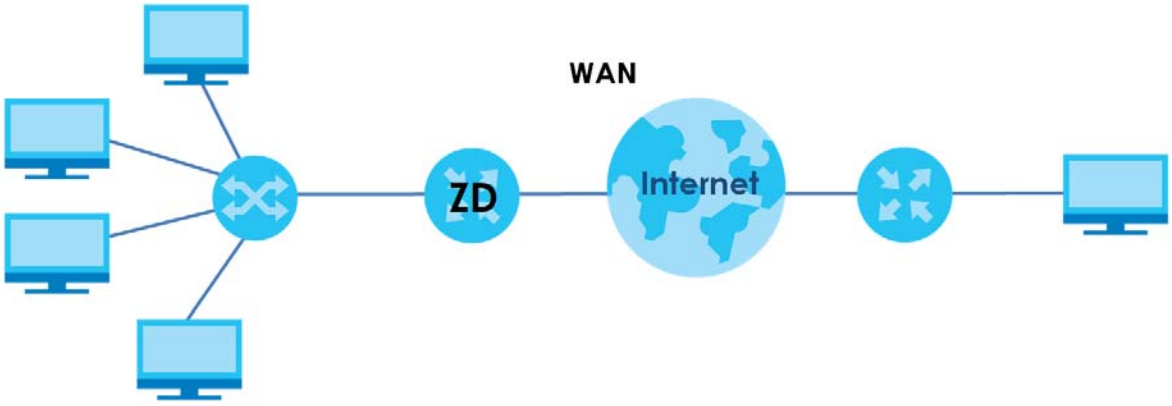
CHAPTER 7
Broadband

7.1 Broadband Overview

This chapter discusses the Zyxel Device's **Broadband** screens. Use these screens to configure your Zyxel Device for Internet access.

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

Figure 84 LAN and WAN



7.1.1 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 Zyxel Device for Internet access.
- Use the **Cellular Backup** screen to configure cellular WAN connection (Section 7.3 on page 160).

Table 33 WAN Setup Overview (Ethernet and PON Gateways)

LAYER-2 INTERFACE	INTERNET CONNECTION		
CONNECTION	MODE	ENCAPSULATION	CONNECTION SETTINGS
Ethernet	Routing	PPPoE	PPP user name and password, WAN IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		IPoE	WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature
	Bridge	N/A	VLAN

Table 33 WAN Setup Overview (Ethernet and PON Gateways)

LAYER-2 INTERFACE	INTERNET CONNECTION		
CONNECTION	**MODE**	**ENCAPSULATION**	**CONNECTION SETTINGS**
GPON	Routing	PPPoE	PPP user name and password, WAN IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		IPoE	WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature
	Bridge	N/A	
Note: This table is for the Ethernet and PON gateways. See Section 1.1 on page 19 for more information.			

7.1.2 What You Need to Know

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

WAN IP Address

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

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC).

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

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`.

IPv6 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.

IPv6 Subnet Masking

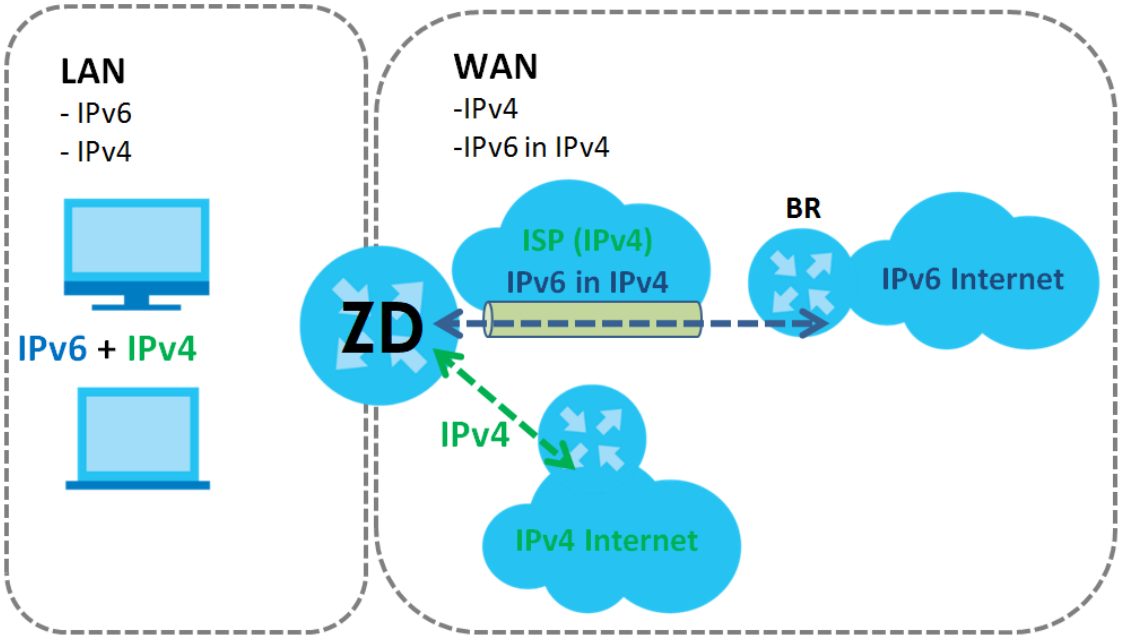
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example,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

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the Zyxel 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 Zyxel 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 Zyxel Device uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 85 IPv6 Rapid Deployment

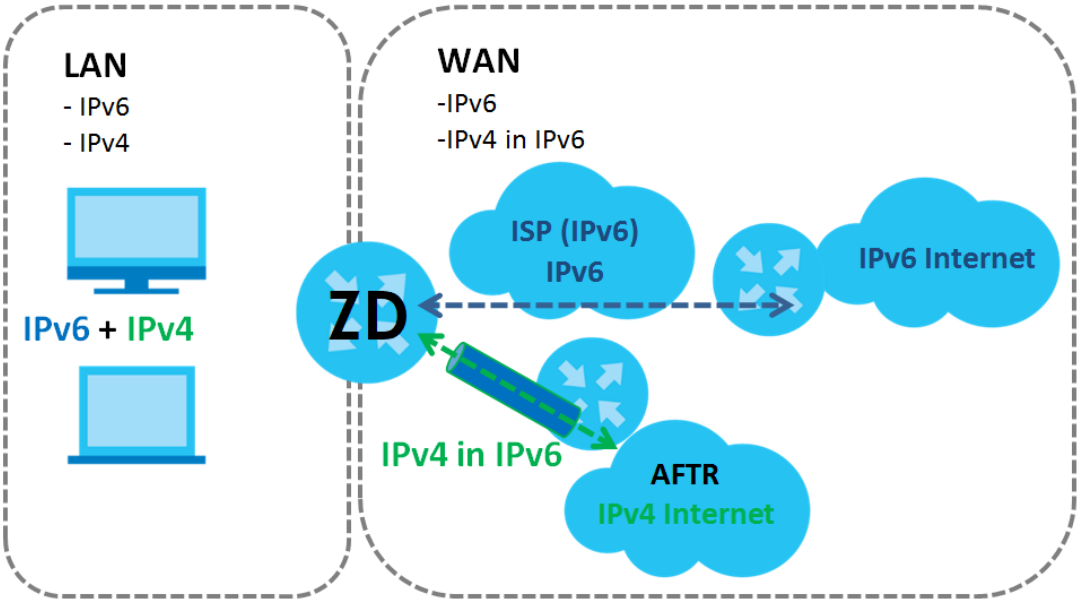


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the Zyxel 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 Zyxel 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 Zyxel Device uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 86 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.

7.1.3 Before You Begin

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

7.2 Broadband Settings for Ethernet, AON and PON Routers

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.

Note: The differences of the broadband screens between Ethernet, AON and PON routers are the type of connections available.

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

Figure 87 Network Setting > Broadband (Ethernet Routers)

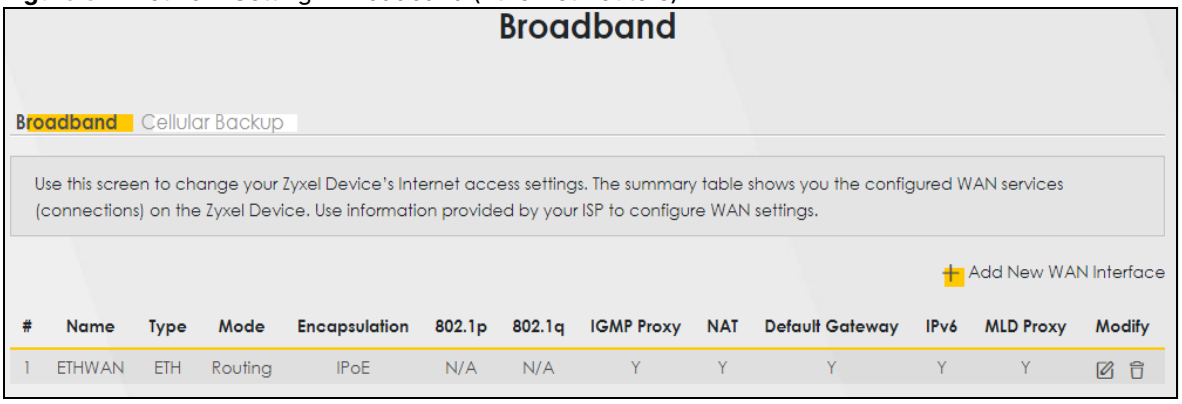
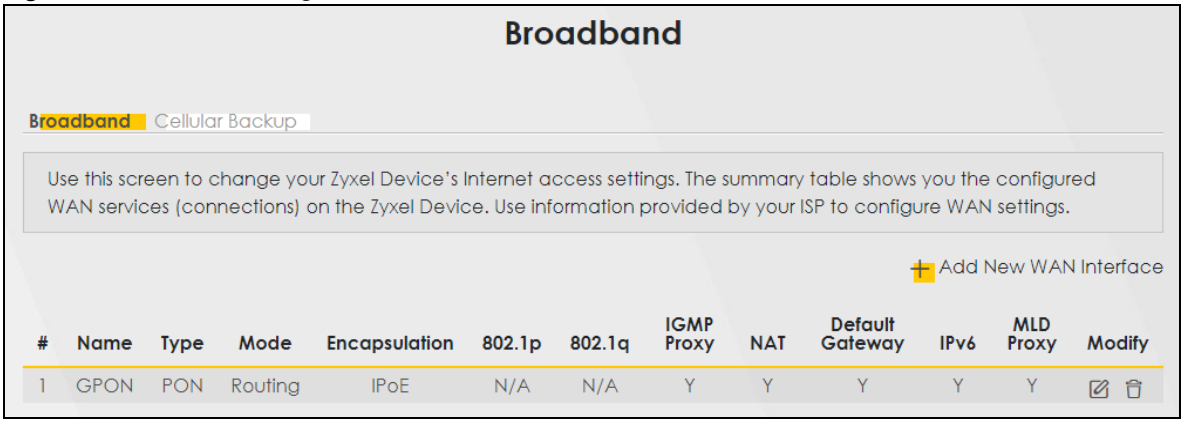


Figure 88 Network Setting > Broadband (AON and PON Routers)



The following table describes the labels in this screen.

Table 34 Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This displays the type of connections available.
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 Zyxel 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 Zyxel 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.

7.2.1 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 or IPv4 mode.

Figure 89 Network Setting > Broadband > Add or Edit New WAN Interface (Ethernet Routers Routing Mode)

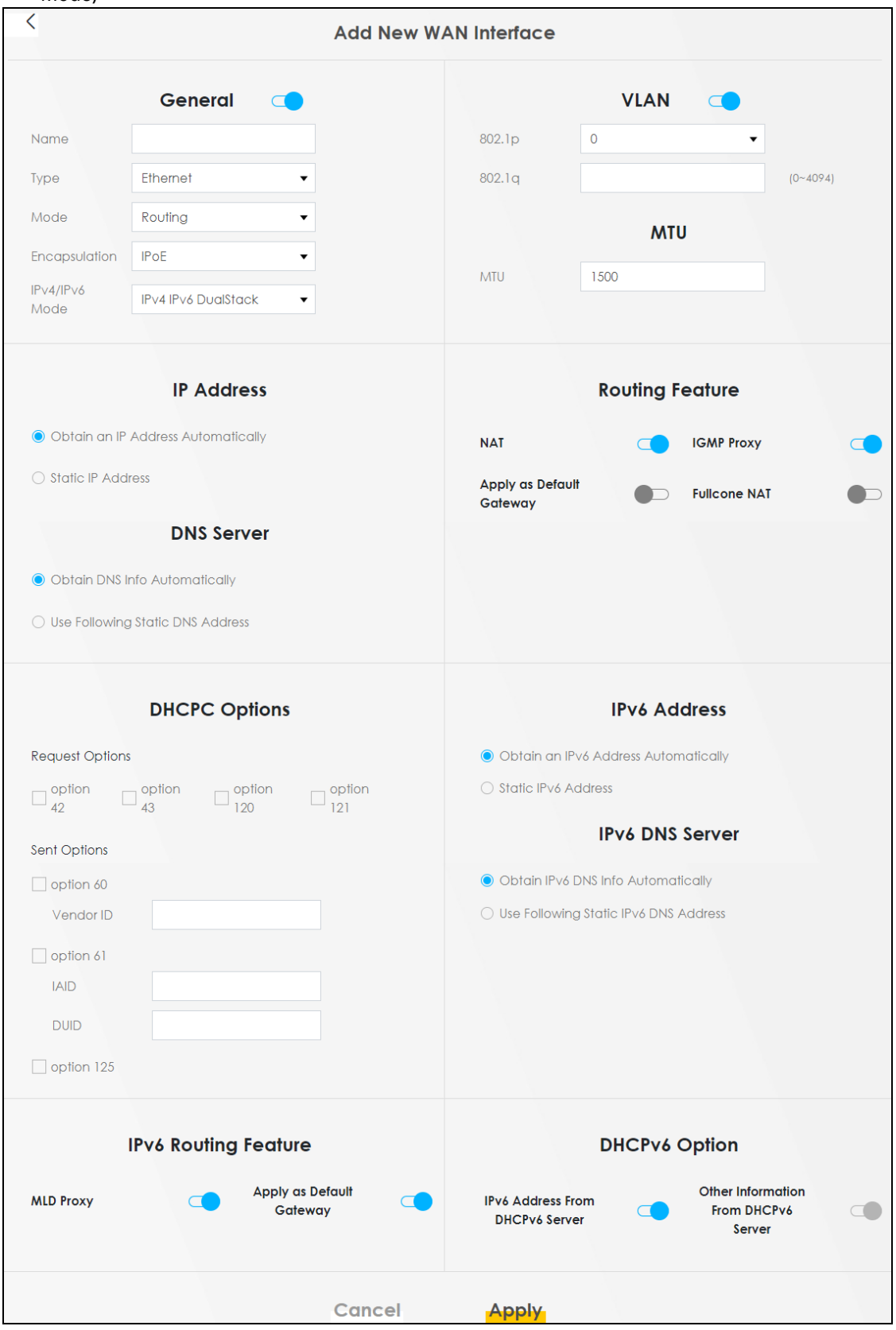
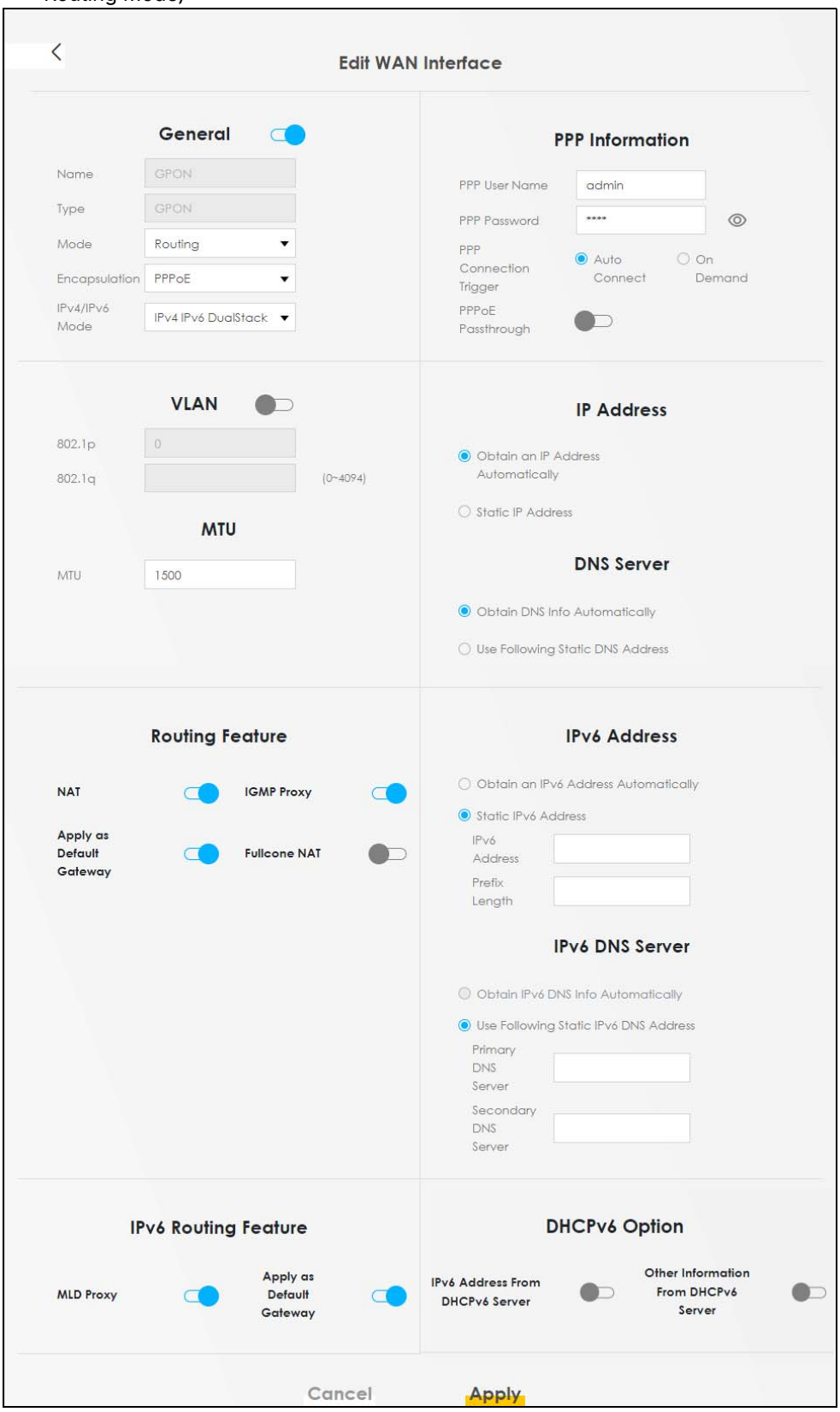


Figure 90 Network Setting > Broadband > Add or Edit New WAN Interface (AON and PON Routers Routing Mode)



The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
General	Click this switch to enable the 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 is you are editing the WAN interface.
Type	This field shows **Ethernet** and indicates an Ethernet connection. This field is read-only is 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 Zyxel Device to run IPv4 only. Select **IPv4 IPv6 DualStack** to allow the Zyxel Device to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the Zyxel Device to run IPv6 only.
PPP Information (This is available only when you select **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. Select **password unmask** to show your entered password in plain text.
PPP Connection Trigger	Select when to have the Zyxel 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 Zyxel 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 only available if you select **On Demand** in the **PPP Connection Trigger** field.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the Zyxel Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP through the Zyxel Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through 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 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	Type 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 35 Network Setting > Broadband > Add or New 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.)	
	Select **Obtain DNS Info Automically** if you want the Zyxel Device to use the DNS server addresses assigned by your ISP. Select **Use Following Static DNS Address** if you want the Zyxel 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 or deactivate NAT on this connection. When the switch goes to the right, the function is enabled. Otherwise, it is not.
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 Zyxel Device act as an IGMP proxy on this connection. When the switch goes to the right, the function is enabled. Otherwise, it is not. This allows the Zyxel 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 Zyxel Device use the WAN interface of this connection as the system default gateway. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Fullcone NAT Enable	Click this switch to enable or disable full cone NAT on this connection. When the switch goes to the right, the function is enabled. Otherwise, it is not. This field is available only when you activate **NAT**. In full cone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.
DHCPC Options (This is available only when you set the **Encapsulation** to **IPoE** and select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.) Note: The available DHCP options may differ by model.	

Table 35 Network Setting > Broadband > Add or New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Request Options	Select **Option 42** to have the Zyxel Device get NTP time server information from DHCP packets sent from the DHCP server. Select **Option 43** to have the Zyxel Device get vendor specific information from DHCP packets sent from the DHCP server. Select **Option 120** to have the Zyxel Device get static route information from DHCP packets sent from the DHCP server. Select **Option 121** to have the Zyxel Device get SIP server information from DHCP packets sent from the DHCP server.
Sent Options	
option 60	Select this and enter the device identity you want the Zyxel 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 Zyxel 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 Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select **Static IPv6 Address** if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interfaces. The gateway helps forward packets to their destinations.
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 Zyxel Device get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select **Use Following Static IPv6 DNS Address** to have the Zyxel 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 Zyxel Device act as an MLD proxy on this connection. This allows the Zyxel Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.

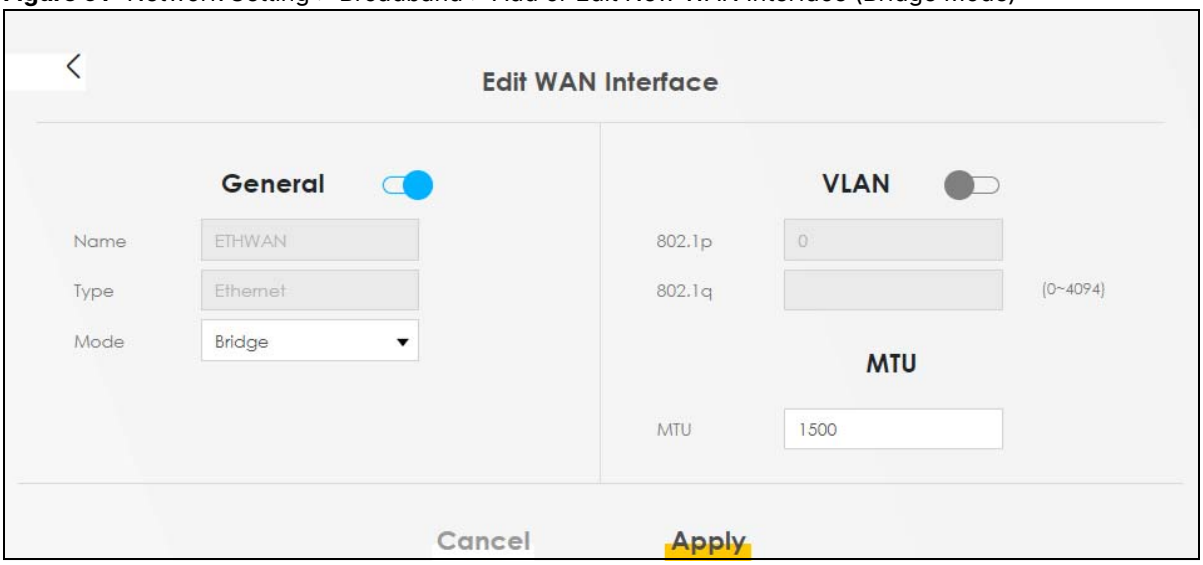
Table 35 Network Setting > Broadband > Add or New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Apply as Default Gateway	Select this option to have the Zyxel 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 151 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.
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 150 for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.	
	Select **Manually Configured** if you have the IPv4 address of the relay server. Otherwise, select **Automatically configured by DHCPC** to have the Zyxel Device detect it automatically through DHCP. The **Automatically configured by DHCPC** option is configurable only when you set the method of encapsulation to **IPoE**.
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.
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.
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 the right) to let the Zyxel Device send DHCP requests to the DHCPv6 server to obtain an IPv6 address.
Other Information From DHCPv6 Server	Click the switch (to the right) to have the Zyxel 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 91 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)



The following table describes the fields in this screen.

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

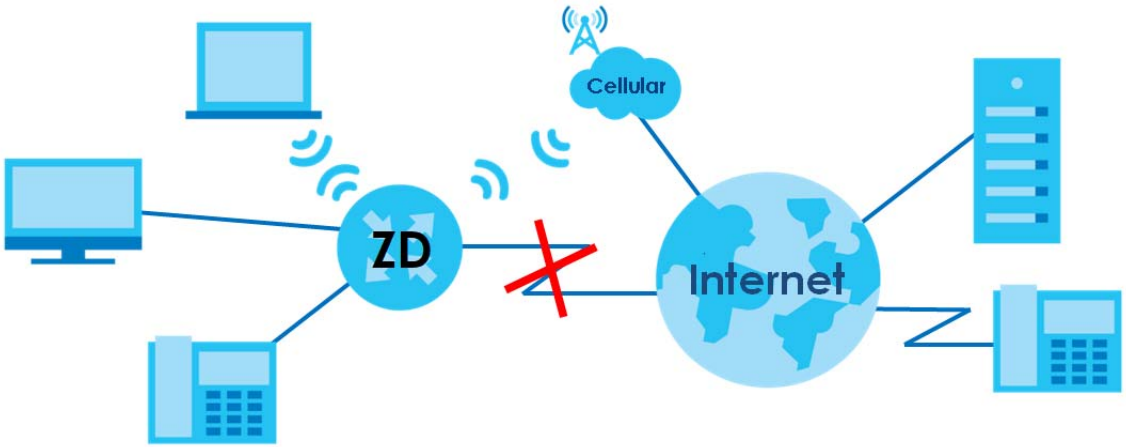
LABEL	DESCRIPTION
General	Click this switch to enable the interface.
Name	Enter a service name of the connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. This field is read-only is you are editing the WAN interface.
Type	This field shows **Ethernet** and indicates an Ethernet connection. This field is read-only is you are editing the WAN interface.
Mode	Select **Bridge** when 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 QoS, Firewall, DHCP server and NAT on traffic from the selected LAN ports.
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	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

7.3 Cellular Backup

The USB port of the Zyxel Device allows you to attach a cellular dongle to wirelessly connect to a cellular network for Internet access. You can have the Zyxel Device use the cellular WAN connection as a backup to keep you online if the primary WAN connection fails for **Consecutive Fail** times. Consult your cellular service provider to configure the settings in this screen. Disconnect the Fiber port to use the cellular

dongle as your primary WAN connection, as the Zyxel Device automatically uses a wired WAN connection when available.

Figure 92 Internet Access Application: Cellular WAN



Use this screen to configure your cellular settings. Click **Network Setting** > **Broadband** > **Cellular Backup**.

The actual data rate you obtain varies depending on the cellular card you use, the signal strength to the service provider's base station, and so on.

Note: Entering a wrong PIN code three times will lock the SIM card in your cellular dongle.

Note: If you select **Drop** in the **Current Cellular Connection** field, the Zyxel Device will drop the cellular WAN connection when the **Time Budget** or **Data Budget** is reached. It may take some time for the cellular WAN connection to be disconnected when the **Time Budget** or **Data Budget** is reached.

Figure 93 Network Setting **>** Broadband > Cellular Backup

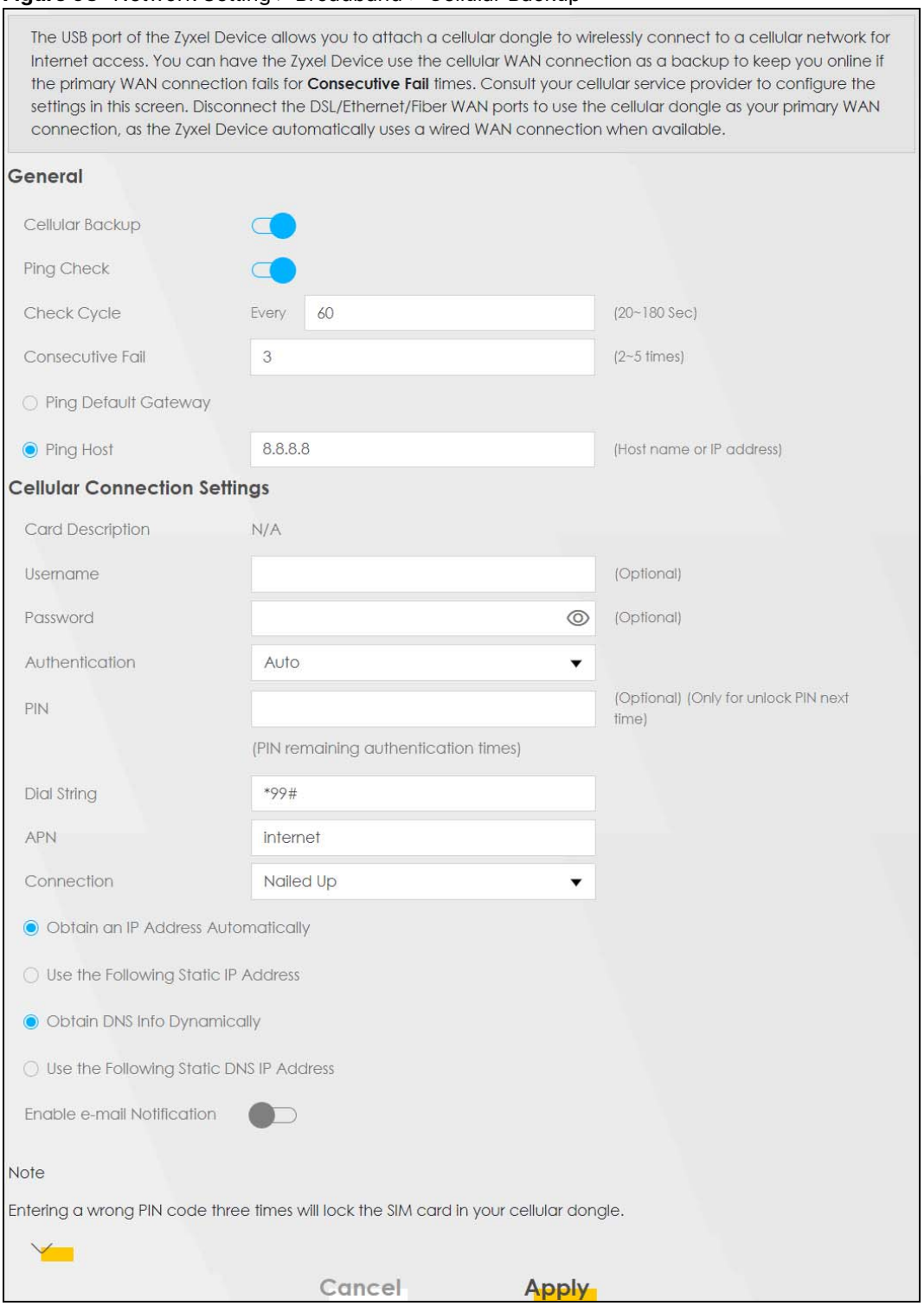
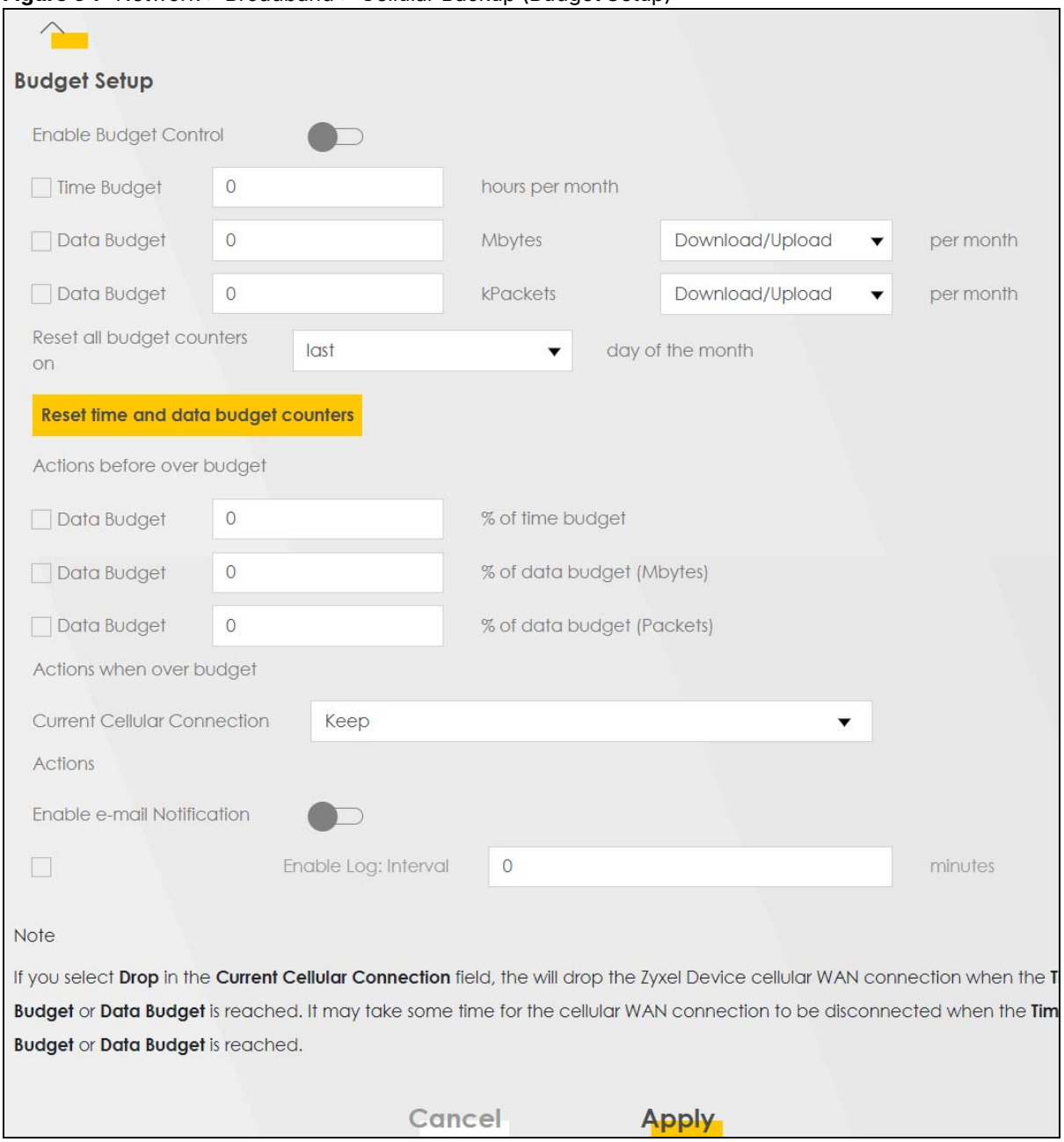


Figure 94 Network > Broadband > Cellular Backup (Budget Setup)



The following table describes the labels in this screen.

Table 37 Network Setting > Broadband > Cellular Backup

LABEL	DESCRIPTION
General	
Cellular Backup	Click this switch to have the Zyxel Device use the cellular connection as your WAN or a backup when the wired WAN connection fails.
Ping Check	Click this switch to ping check the connection status of your WAN. You can configure the frequency of the ping check and number of consecutive failures before triggering cellular backup.
Check Cycle	Enter the frequency of the ping check in this field.

Table 37 Network Setting > Broadband > Cellular Backup (continued)

LABEL	DESCRIPTION
Consecutive Fail	Enter how many consecutive failures are required before cellular backup is triggered.
Ping Default Gateway	Select this to have the Zyxel Device ping the WAN interface's default gateway IP address.
Ping Host	Select this to have the Zyxel Device ping the particular host name or IP address you typed in this field.
Cellular Connection Settings	
Card Description	This field displays the manufacturer and model name of your cellular card if you inserted one in the Zyxel Device. Otherwise, it displays **N/A**.
Username	Enter the user name (of up to 64 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces) given to you by your service provider.
Password	Enter the password (of up to 64 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces) associated with the user name above.
Authentication	The Zyxel Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Type Handshake Authentication Protocol). In PAP, peers identify themselves with a user name and password. In CHAP, additionally to user name and password the Zyxel Device sends regular challenges to make sure an intruder has not replaced a peer. CHAP is more secure than PAP; however, PAP is available on more platforms. Select an authentication protocol (Auto, CHAP or PAP). Contact your service provider for the correct authentication type.
PIN	A PIN (Personal Identification Number) code is a key to a cellular card. Without the PIN code, you cannot use the cellular card. If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the cellular card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Dial String	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or cellular connection in Taiwan.
APN	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Connection	Select **Nailed UP** if you do not want the connection to time out. Select **On Demand** if you do not want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the Zyxel Device automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option if your ISP did not assign you a fixed IP address.
Use the Following Static IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use the following static IP address**.
Subnet Mask	Enter the subnet mask of the IP address.
Obtain DNS Info Dynamically	Select this to have the Zyxel Device get the DNS server addresses from the ISP automatically.

Table 37 Network Setting > Broadband > Cellular Backup (continued)

LABEL	DESCRIPTION
Use the Following Static DNS IP Address	Select this to have the Zyxel Device 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.
Enable e-mail Notification	Select this to enable the email notification function. The Zyxel Device will email you a notification when the cellular connection is up.
Mail Account	Select an email address you have configured in **Maintenance** > **E-mail Notification**. The Zyxel Device uses the corresponding mail server to send notifications. You must have configured a mail server already in the **Maintenance** > **E-mail Notification** screen.
Cellular Backup e-mail Title	Enter a title that you want to be in the subject line of the email notifications that the Zyxel Device sends.
Send Notification to E-mail	Notifications are sent to the email address specified in this field. If this field is left blank, notifications cannot be sent through email.
Click this to show the advanced cellular backup settings.	
Budget Setup	
Enable Budget Control	Click this switch to set a monthly limit for the user account of the installed cellular card. You can set a limit on the total traffic and/or call time. The Zyxel Device takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the cellular connection can be used within one month. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Data Budget (Mbytes)	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted through the cellular connection within one month. Select **Download/Upload** to set a limit on the total traffic in both directions. Select **Download** to set a limit on the downstream traffic (from the ISP to the Zyxel Device). Select **Upload** to set a limit on the upstream traffic (from the Zyxel Device to the ISP). If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Data Budget (kPackets)	Select this and specify how much downstream and/or upstream data (in k Packets) can be transmitted through the cellular connection within one month. Select **Download/Upload** to set a limit on the total traffic in both directions. Select **Download** to set a limit on the downstream traffic (from the ISP to the Zyxel Device). Select **Upload** to set a limit on the upstream traffic (from the Zyxel Device to the ISP). If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Reset all budget counters on	Select the date on which the Zyxel Device resets the budget every month. Select **last** if you want the Zyxel Device to reset the budget on the last day of the month. Select **specific** and enter the number of the date you want the Zyxel Device to reset the budget.
Reset time and data budget counters	Click this button to reset the time and data budgets immediately. The count starts over with the cellular connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.

Table 37 Network Setting > Broadband > Cellular Backup (continued)

LABEL	DESCRIPTION
Actions before over budget	Specify the actions the Zyxel Device takes before the time or data limit exceeds.
Data Budget % of time budget/data budget (Mbytes)/data budget (kPackets)	Select the checkboxes and enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Actions when over budget	Specify the actions the Zyxel Device takes when the time or data limit is exceeded.
Current Cellular Connection	Select **Keep** to maintain an existing cellular connection or **Drop** to disconnect it.
Actions	
Enable e-mail Notification	Click this switch to enable the email notification function. The Zyxel Device will email you a notification whenever over budget occurs.
Mail Account	Select an email address you have configured in **Maintenance** > **E-mail Notification**. The Zyxel Device uses the corresponding mail server to send notifications. You must have configured a mail server already in the **Maintenance** > **E-mail Notification** screen.
Cellular Backup e-mail Title	Enter a title that you want to be in the subject line of the email notifications that the Zyxel Device sends.
Send Notification to E-mail	Notifications are sent to the email address specified in this field. If this field is left blank, notifications cannot be sent through email.
Enable Log: Interval	Select this to and enter the **Interval** of how many minutes (1 – 9999) you want the Zyxel Device to email you.
Cancel	Click **Cancel** to discard any changes to the settings.
Apply	Click **Apply** to save your changes.

7.4 Technical Reference

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

Encapsulation

Be sure to use the encapsulation method required by your ISP. The Zyxel Device can work in bridge mode or routing mode. When the Zyxel 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 ATM (PPPoA)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The Zyxel Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

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

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

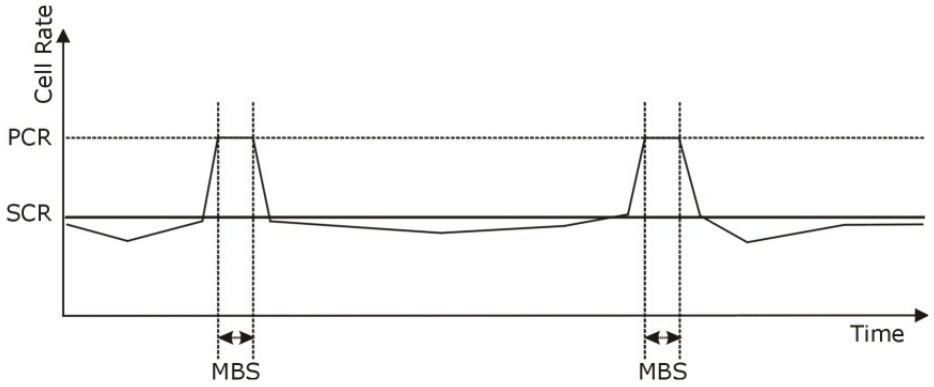
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 95 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (does not tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR does not guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

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

Multicast

IP packets are transmitted in either one of two ways – Unicast (1 sender – 1 recipient) or Broadcast (1 sender – everybody on the network). Multicast delivers IP packets to a group of hosts on the network – not everybody and not just 1.

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. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the Zyxel Device queries all directly connected networks to gather group membership. After that, the Zyxel Device periodically updates this information.

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 Zyxel 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 Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

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`.

IPv6 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.

CHAPTER 8
Wireless

8.1 Wireless Overview

This chapter describes the Zyxel Device's **Network Setting** > **Wireless** screens. Use these screens to set up your Zyxel Device's WiFi network and security settings.

8.1.1 What You Can Do in this Chapter

This section describes the Zyxel Device's **Wireless** screens. Use these screens to set up your Zyxel Device's WiFi connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the WiFi security mode (Section 8.2 on page 174)
- Use the **Guest/More AP** screen to set up multiple WiFi networks on your Zyxel Device (Section 8.3 on page 181).
- Use the **MAC Authentication** screen to allow or deny WiFi clients based on their MAC addresses from connecting to the Zyxel Device (Section 8.4 on page 185).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 8.5 on page 186).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 8.6 on page 188).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 8.7 on page 189).
- Use the **Channel Status** screen to scan the number of accessing points and view the results (Section 8.8 on page 190).
- Use the **MESH** screen to enable or disable Mesh on your Zyxel Device (Section 8.9 on page 192).

8.1.2 What You Need to Know

WiFi Standard / IEEE 802.11

IEEE 802.11 is a set of standards developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networks (WLANs). These standards define how devices like laptops, smartphones, and routers communicate wirelessly using radio waves.

WiFi 6 / IEEE 802.11ax

WiFi 6 is backwards compatible with IEEE 802.11a/b/g/n/ac and is most suitable in areas with a high concentration of users. WiFi 6 devices support Target Wakeup Time (TWT) allowing them to automatically power down when they are inactive.

WiFi 6E (IEEE802.11ax – Extended Standard)

WiFi 6E is an extended standard of WiFi 6 (IEEE 802.11ax). WiFi 6E inherits all the WiFi 6 features and brings with an additional 6 GHz band. The 6 GHz band allows you to avoid possible congested traffic in the lower 2.4 GHz and 5 GHz bands. WiFi clients must support WiFi 6E to connect to the device using the 6 GHz band.

Note: Check your client device's product specification to see if your client device supports the 6 GHz band (WiFi 6E). If not, you should still use the 2.4/5 GHz bands for connection.

WiFi 7 (IEEE802.11be)

WiFi 7 (802.11be) is backwards compatible with WiFi 6 and WiFi 6E. WiFi 7 is a WiFi standard that supports 2.4 GHz, 5 GHz and 6 GHz frequency bands with the following improvements over WiFi 6 and WiFi 6E.

Table 38 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES		WiFi 6	WiFi 6E	WiFi 7
Theoretical Maximum Speed (Up-to)		9.6 Gbps		46 Gbps
Supported Frequency Bands		2.4 GHz/5 GHz	2.4 GHz/5 GHz/6 GHz	2.4 GHz/5 GHz/6 GHz
Supported Channel Bandwidth		20/40/80/160 MHz	20/40/80/160 MHz	20/40/80/160/320 MHz
Total Spectrum (Up-to)	2.4 GHz	80 MHz		80 MHz
	5 GHz	500 MHz		500 MHz
	6 GHz	Not supported.	1200 MHz	1200 MHz
Other Features (OFDMA/BSS Coloring/TWT/Two-Way MU-MIMO/ Beamforming/1024-QAM)		The same (WiFi 6E inherits all the features from WiFi 6).		WiFi 7 inherits all the features from WiFi 6 and WiFi 6E, with the addition of multi-link operation and preamble puncturing.

Faster Data Transmission

WiFi 7 allows faster data transmission using:

- 4096 QAM (Quadrature Amplitude Modulation) – enhances the amount of data transmitted over the available bandwidth.
- 320 MHz Channel Bandwidth – enlarges the supported channel bandwidth to 320 MHz, allowing higher data throughput.
- Multiple Resource Units (RUs) – allows an AP to allocate multiple RUs to a WiFi client.

Multi-Link Operation (MLO)

WiFi 7 MLO allows a WiFi client to connect to the Zyxel Device using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Devices without MLO can only transmit data on one band at a time.

Figure 96 Without Multi-Link Operation

The Zyxel Device can support multiple frequency bands (2.4 GHz, 5 GHz and 6 GHz), but a WiFi client can only connect to the Zyxel Device using one of these frequency bands. The other frequency bands are unused. The client's data transmission speed depends on the frequency band they are connected to.

To use MLO, both the Zyxel Device and the WiFi client have to support MLO.

Figure 97 Multi-Link Operation Example

Finding Out More

See Section 8.10 on page 192 for advanced technical information on WiFi networks.

8.2 Wireless General Settings

Use this screen to enable the WiFi, enter the SSID and select the WiFi security mode. We recommend that you select **More Secure** to enable **WPA3-SAE** data encryption.

Note: If you are configuring the Zyxel Device from a computer connected by WiFi and you change the Zyxel Device's SSID, channel or security settings, you will lose your WiFi connection when you press **Apply**. You must change the WiFi settings of your computer to match the new settings on the Zyxel Device.

Note: If upstream or downstream bandwidth is empty, the Zyxel Device sets the value automatically.

Note: Setting a maximum upstream or downstream bandwidth will significantly decrease wireless performance.

Note: **Keep the same settings for 2.4 GHz, 5 GHz, 6 GHz wireless networks** is enabled and cannot be disabled when you enable **Mesh** in the **Network** > **Wireless** > **MESH** screen. To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.

Click **Network Setting** > **Wireless** to open the **General** screen.

Figure 98 Network Setting > Wireless > General (for 2.4 GHz and 5 GHz models)

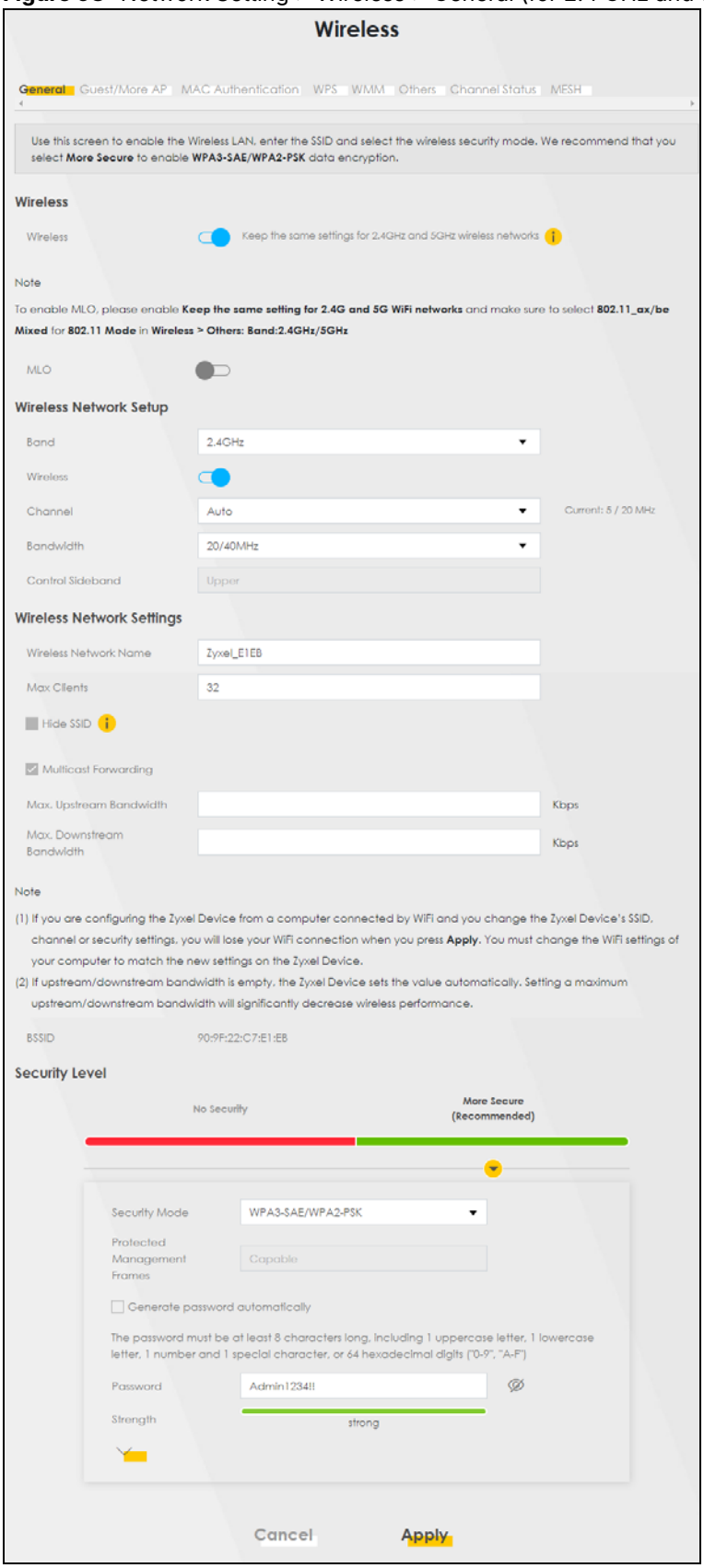
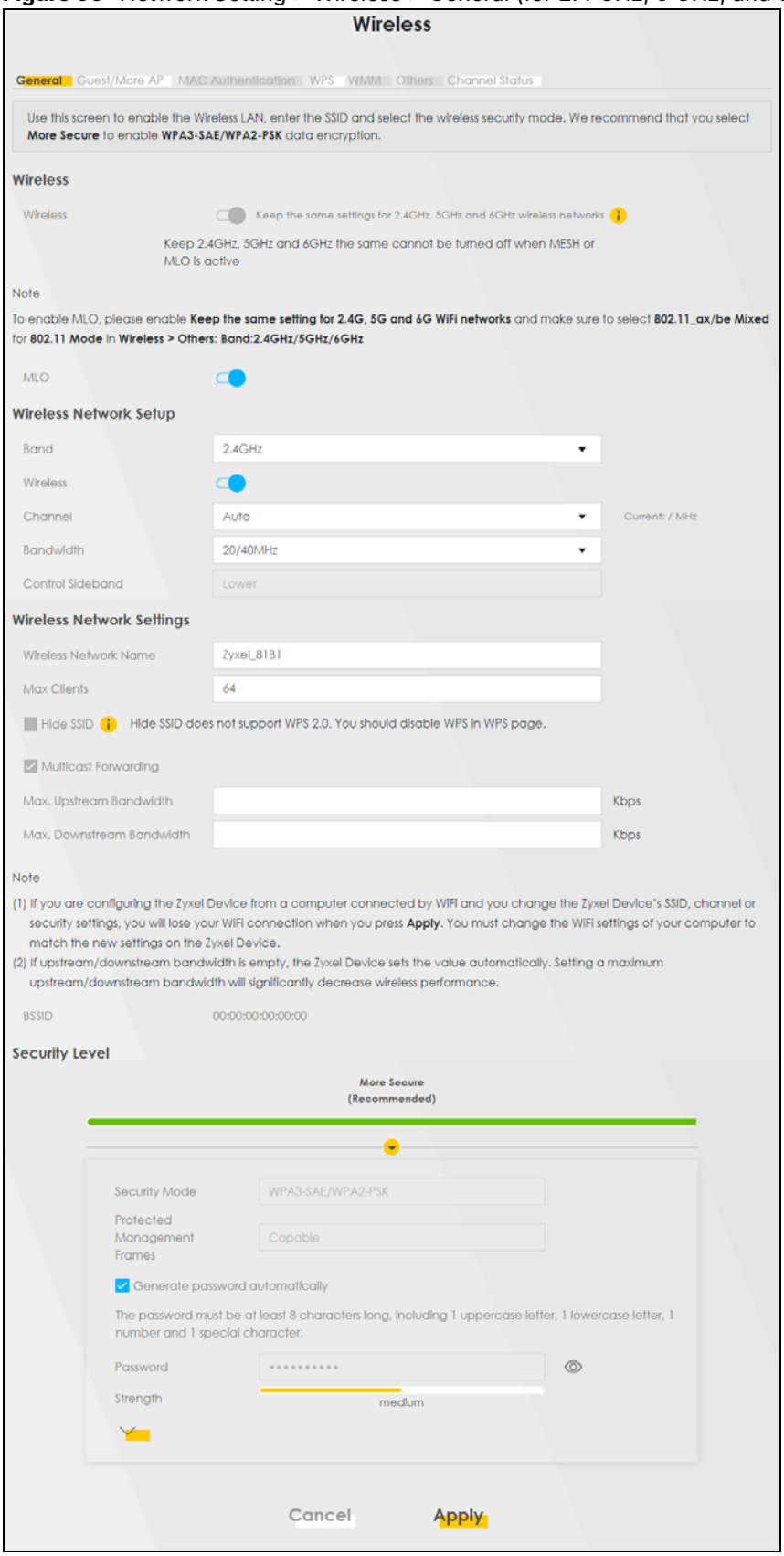


Figure 99 Network Setting > Wireless > General (for 2.4 GHz, 5 GHz, and 6 GHz models)



The following table describes the general WiFi labels in this screen.

Table 39 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	Select **Keep the same settings for 2.4GHz, 5GHz and 6GHz wireless networks** and the 2.4 GHz, 5 GHz and 6 GHz WiFi networks will use the same SSID and wireless security settings. Note: To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.
MLO	Select **MLO** to allow a WiFi 7 client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Note: To enable MLO, select **Keep the same settings for 2.4GHz, 5GHz and 6GHz wireless networks**. Note: To use MLO, both the AP and the WiFi client have to support MLO. Note: To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.
Wireless/WiFi Network Setup	
Band	This shows the WiFi band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax WiFi clients, **5GHz** is used by IEEE 802.11a/n/ac/ax WiFi clients. Note: To see if your model supports 6 GHz, please see Section 1.1 on page 19 for more information.
Wireless/WiFi	Click this switch to enable or disable WiFi in this field. When the switch turns blue, the function is enabled. Otherwise, it is not.
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use **Auto** to have the Zyxel Device automatically determine a channel to use.
Bandwidth	A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the WiFi clients do not support channel bonding. Not all Zyxel Devices support all channels. The Zyxel Device will choose the best bandwidth available automatically depending on the radio you chose and network conditions.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz** or **20/40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless/WiFi Network Settings	
Wireless/WiFi Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for this WiFi network. You can use up to 32 printable characters, including spaces.

Table 39 Network Setting > Wireless > General (continued)

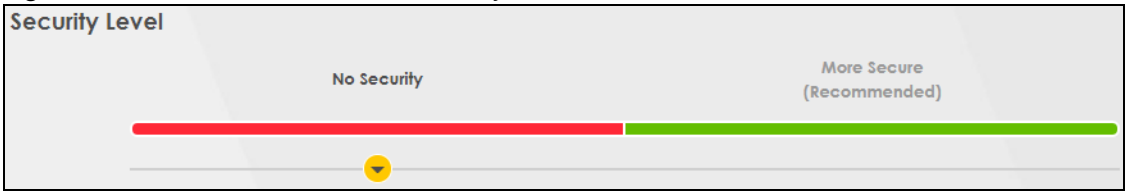
LABEL	DESCRIPTION
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This checkbox is grayed out if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen.
Multicast Forwarding	Select this checkbox to allow the Zyxel Device to convert wireless Multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any WiFi security on your Zyxel Device, your network is accessible to any wireless networking device that is within range.

Figure 100 Wireless > General: No Security



The following table describes the labels in this screen.

Table 40 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all connections without data encryption or authentication.

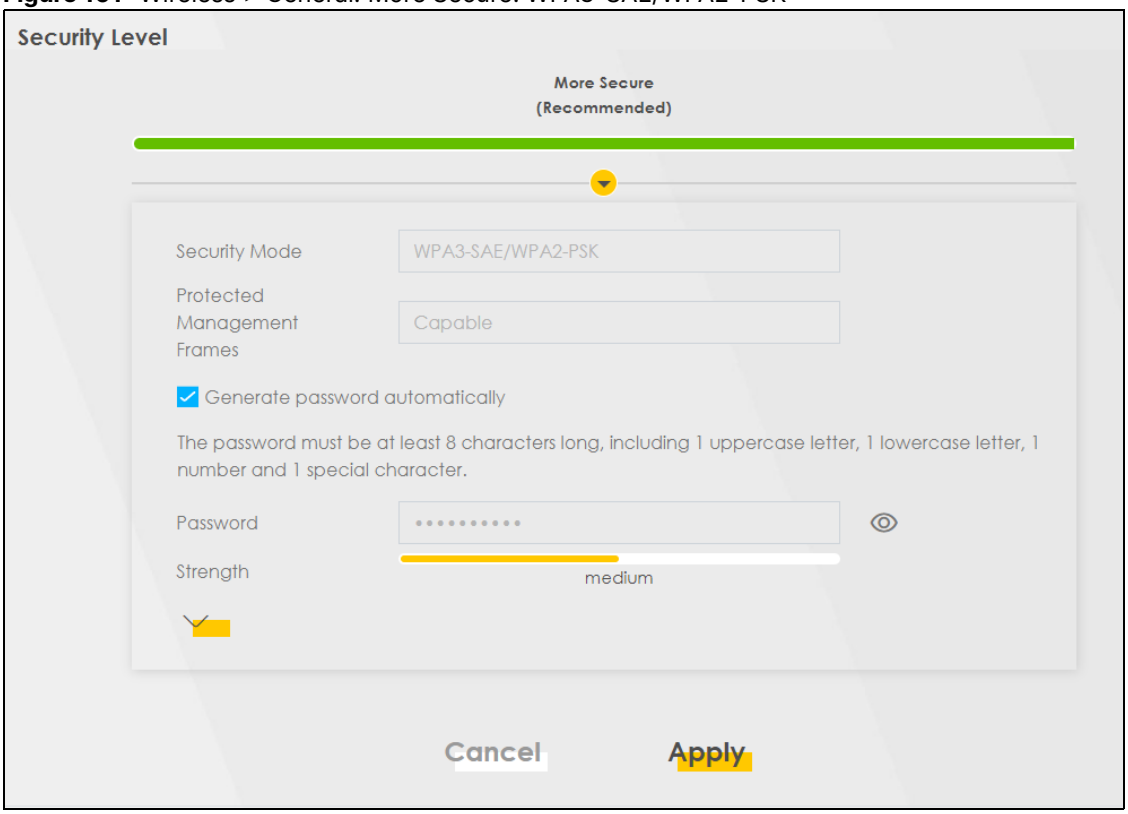
8.2.2 More Secure (Recommended)

The WPA-PSK (WiFi Protected Access-Pre-Shared Key) security mode provides both improved data encryption and user authentication over WEP. Using a pre-shared key, both the Zyxel Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a more robust version of the WPA encryption standard. It offers better security, although the use of PSK makes it less robust than it could be.

The WPA3-SAE (Simultaneous Authentication of Equals handshake) security mode protects against dictionary attacks (password guessing attempts). It improves security by requiring a new encryption key every time a WPA3 connection is made. A handshake is the communication between the Zyxel Device and a connecting client at the beginning of a WiFi session.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA3-SAE** from the **Security Mode** list if your WiFi client supports it. If you are not sure, select **WPA3-SAE/WPA2-PSK** or **WPA2-PSK**.

Figure 101 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK



The following table describes the labels in this screen.

Table 41 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.

Table 41 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK (continued)

LABEL	DESCRIPTION
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	Select **Generate password automatically** or enter a **Password**. The password has two uses. 1. Manual. Manually enter the same password on the Zyxel Device and the client. The password must be at least 8 characters long, including one uppercase letter, one lowercase letter, one number, and one special character. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: More than 63 hexadecimal characters are not accepted for WPS. Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed, you will see the password in plain text. Otherwise, it is hidden.
Strength	This displays the current password strength – **weak**, **medium**, **strong**.
Click this to show more fields in this section. Click this to hide them.	
Encryption	**AES** is the default data encryption type, which uses a 128-bit key. Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your WiFi clients can all use AES. Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. Note: Not all models support **TKIP+AES** encryption.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

8.3 Guest/More AP Screen

Use this screen to configure a guest WiFi network that allows access to the Internet through the Zyxel Device. You can use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. WiFi clients can use different SSIDs to associate with the same access point.

Click **Network Setting** > **Wireless** > **Guest/More AP**.

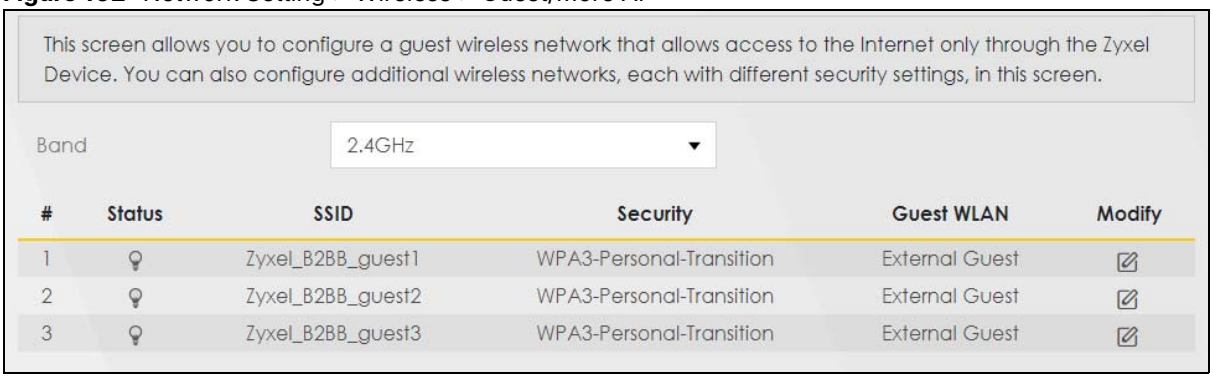
The following table introduces the supported WiFi networks.

Table 42 Supported WiFi Networks

WIFI NETWORKS	WHERE TO CONFIGURE
Main/1	Network Setting > Wireless > General screen
Guest/3	Network Setting > Wireless > Guest/More AP screen

The following screen displays.

Figure 102 Network Setting > Wireless > Guest/More AP



The following table describes the labels in this screen.

Table 43 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active, while a gray bulb signifies that this SSID is not active.
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	This displays if the guest WLAN function has been enabled for this WLAN. A **Home Guest** can access the Internet, LAN wired devices connected to the Zyxel Device, and other Home Guest WiFi clients. An **External Guest** can just access the Internet through the Zyxel Device. **N/A** displays if guest WLAN is disabled.
Modify	Click the **Edit** icon of an SSID profile to configure the SSID profile.

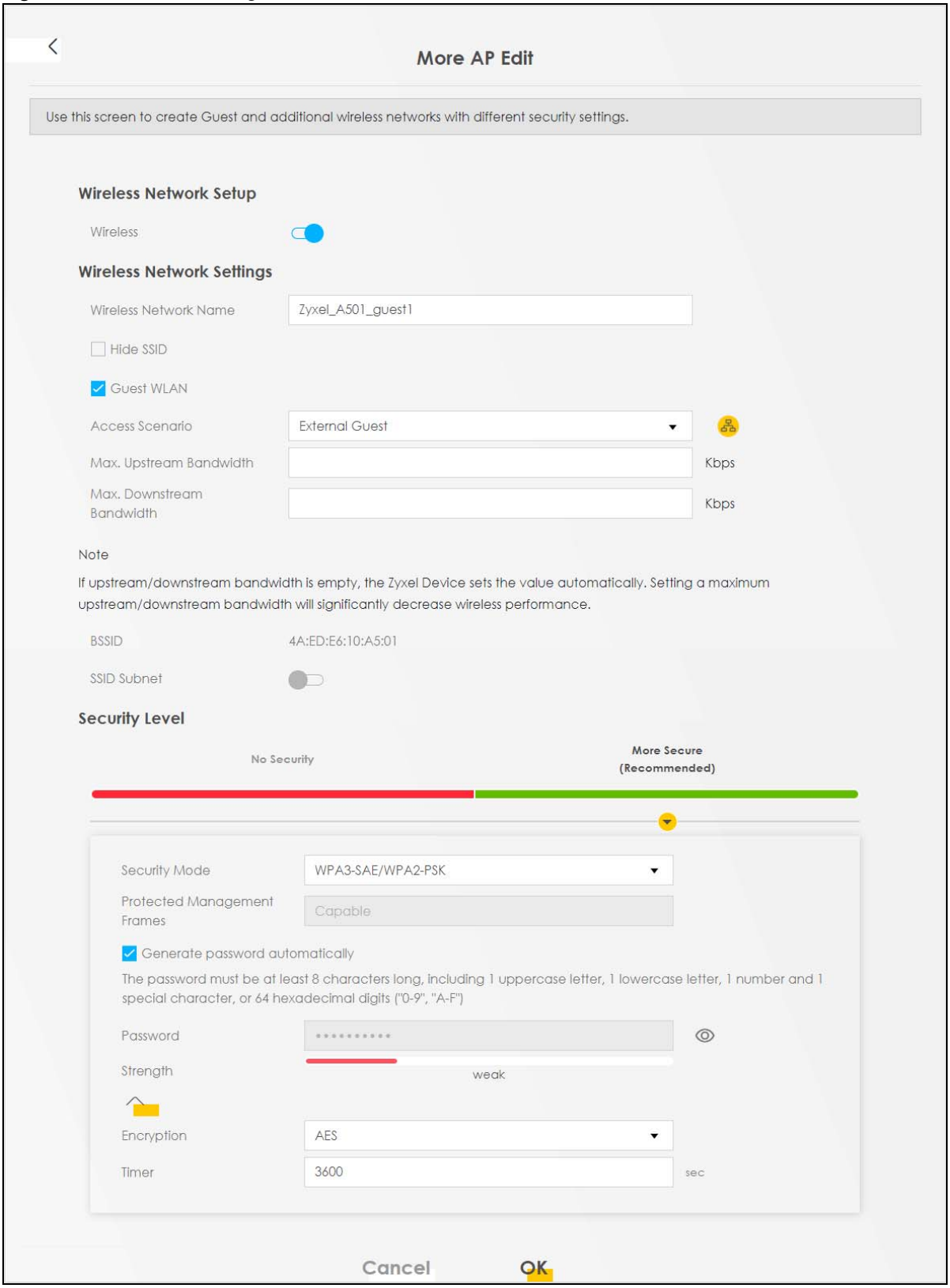
8.3.1 The Edit Guest/More AP Screen

Use this screen to create Guest and additional WiFi networks with different security settings.

Note: If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease WiFi performance.

Click the **Edit** icon next to an SSID in the **Guest/More AP** screen. The following screen displays.

Figure 103 Network Setting > Wireless > Guest/More AP > Edit



The following table describes the fields in this screen.

Table 44 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
WiFi/Wireless Network Setup	
WiFi/Wireless	Click this switch to enable or disable the WiFi in this field. When the switch turns blue, the function is enabled; otherwise, it is not.
WiFi/Wireless Network Settings	
WiFi/Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for the WiFi. You can use up to 32 printable characters, including spaces.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the **Access Scenario** field.
Access Scenario	Select **Home Guest** or **External Guest** to provide different levels of access to the Zyxel Device and the other WiFi clients. A **Home Guest** can access the Internet, LAN wired devices connected to the Zyxel Device, and other Home Guest WiFi clients. An **External Guest** can just access the Internet through the Zyxel Device.
BSSID	This shows the MAC address of the WiFi interface on the Zyxel Device when WiFi is enabled.
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool. The Zyxel Device assigns IP addresses from this DHCP pool to WiFi clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 8.2.1 on page 179 for more details about this field.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. 1. If you did not select **Generate password automatically**, you can manually enter a pre-shared key at least 8 characters long, including one uppercase letter, one lowercase letter, one number, and one special character. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed, you will see the password in plain text. Otherwise, it is hidden.
Strength	This displays the current password strength – **weak**, **medium**, **strong**.
Click this to show more fields in this section. Click again to hide them.	

Table 44 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your WiFi clients can all use AES. Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. Not all models support the **TKIP+AES** option.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.4 MAC Authentication

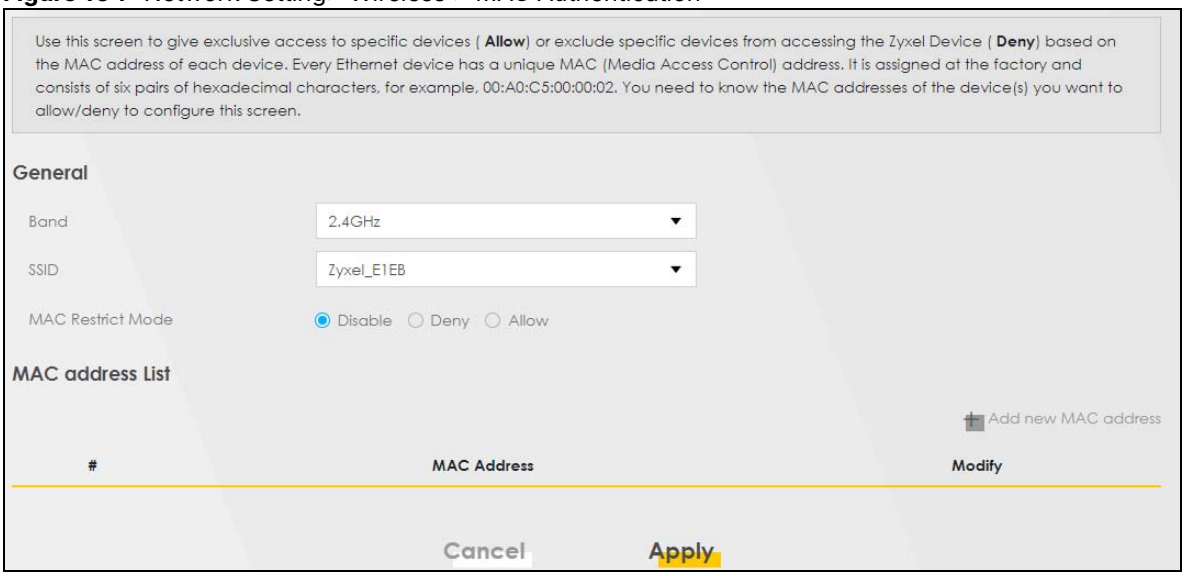
Use this screen to give exclusive access to specific connected devices **(Allow)** or exclude specific devices from accessing the Zyxel Device **(Deny)**, based on the MAC address of each connected device. Every Ethernet device has a unique factory-assigned MAC (Media Access Control) address, which consists of six pairs of hexadecimal characters, for example: 00:A0:C5:00:00:02. You need to know the MAC addresses of the connected device you want to allow/deny to configure this screen.

Note: You can have up to 25 MAC authentication rules.

Note: This screen is not available when Mesh is enabled in the **Network Setting** > **Wireless** > **MESH** screen.

Use this screen to view your Zyxel Device's MAC filter settings and add new MAC filter rules. Click **Network Setting** > **Wireless** > **MAC Authentication**. The screen appears as shown.

Figure 104 Network Setting> Wireless > MAC Authentication



The following table describes the labels in this screen.

Table 45 Network Setting > Wireless > MAC Authentication

LABEL	DESCRIPTION
General	
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device. Select **Allow** to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device.
MAC address List	
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the devices that are allowed or denied access to the Zyxel Device.
Modify	Click the **Edit** icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the **Delete** icon to delete the entry.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

8.5 WPS

Use this screen to configure WiFi Protected Setup (WPS) on your Zyxel Device.

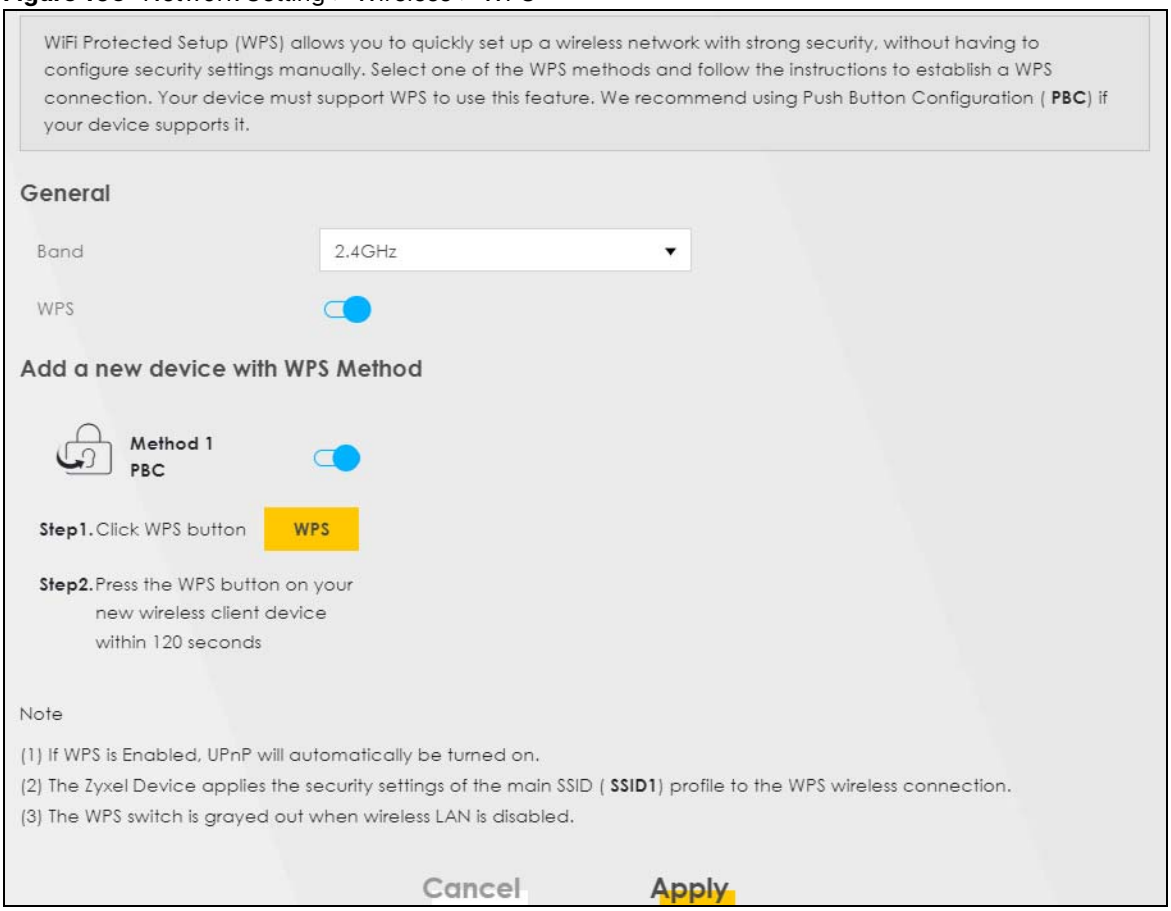
WiFi Protected Setup (WPS) allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection.Your WiFi devices must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your WiFi device supports it.

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection (see Section 8.2.2 on page 180). Some models support more than one SSID profile, check the supported number on the **Network Setting** > **Wireless** > **General** screen.

Note: The WPS switch is unavailable if the WiFi is disabled.
If WPS is enabled, UPnP will automatically be turned on.

Click **Network Setting** > **Wireless** > **WPS**. The following screen displays. Click this switch and it will turn blue. Click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 105 Network Setting > Wireless > WPS



The following table describes the labels in this screen.

Table 46 Network Setting > Wireless > WPS

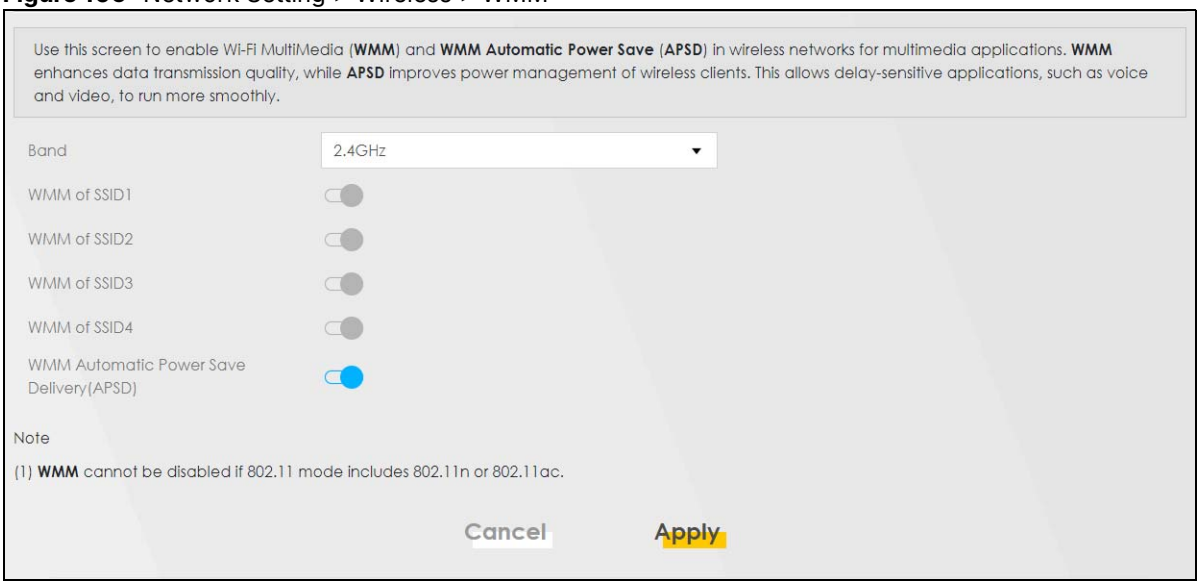
LABEL	DESCRIPTION
General	
WPS	Slide this to the right to enable and have the Zyxel Device activate WPS. Otherwise, it is disabled.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click **Apply** to activate WPS method 1 on the Zyxel Device.
WPS	Click this button to add another WPS-enabled device (within range of the Zyxel Device) to your network. This button may either be a physical button on the outside of a WiFi device, or a menu button similar to the **WPS button** on this screen. Note: You must press the other device's WPS button within 2 minutes of pressing this button.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.6 WMM

Use this screen to enable WiFi MultiMedia (**WMM**) and **WMM Automatic Power Save Delivery** (**APSD**) in WiFi networks for multimedia applications. **WMM** enhances data transmission quality, while **APSD** improves power management of WiFi clients. This allows time-sensitive applications, such as voice and videos, to run more smoothly.

Click **Network Setting** > **Wireless** > **WMM** to display the following screen.

Figure 106 Network Setting > Wireless > WMM



Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

Note: APSD only affects SSID1. For SSID2-SSID4, APSD is always enabled.

Note: This screen is not available when Mesh is enabled in the **Network Setting** > **Wireless** > **MESH** screen.

The following table describes the labels in this screen.

Table 47 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM Automatic Power Save Delivery (APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Zyxel Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Zyxel Device until the Zyxel Device "wakes up." The Zyxel Device wakes up periodically to check for incoming data. Note: This works only if the device to which the Zyxel Device is connected also supports this feature.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

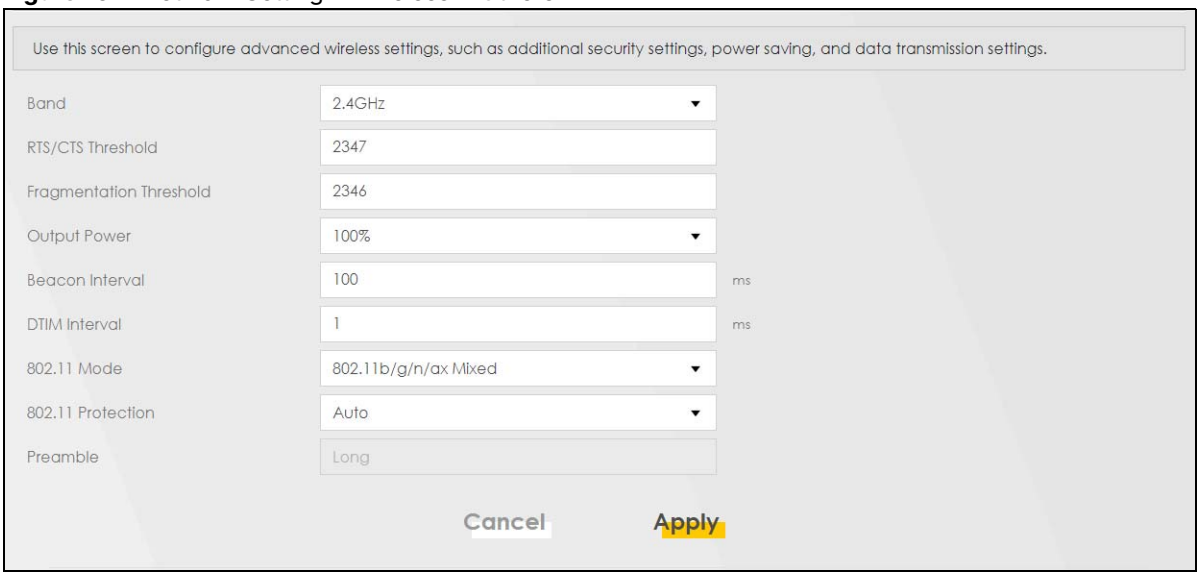
8.7 Others

Use this screen to configure advanced WiFi settings, such as additional security settings, power saving, and data transmission settings. Click **Network Setting** > **Wireless** > **Others**. The screen appears as shown.

Note: This screen is not available when Mesh is enabled in the **Network Setting** > **Wireless** > **MESH** screen.

See Section 8.10.2 on page 194 for detailed definitions of the terms listed here.

Figure 107 Network Setting > Wireless > Others



The following table describes the labels in this screen.

Table 48 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50 ms to 1000 ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and Multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.

Table 48 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 8.10.7 on page 197 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

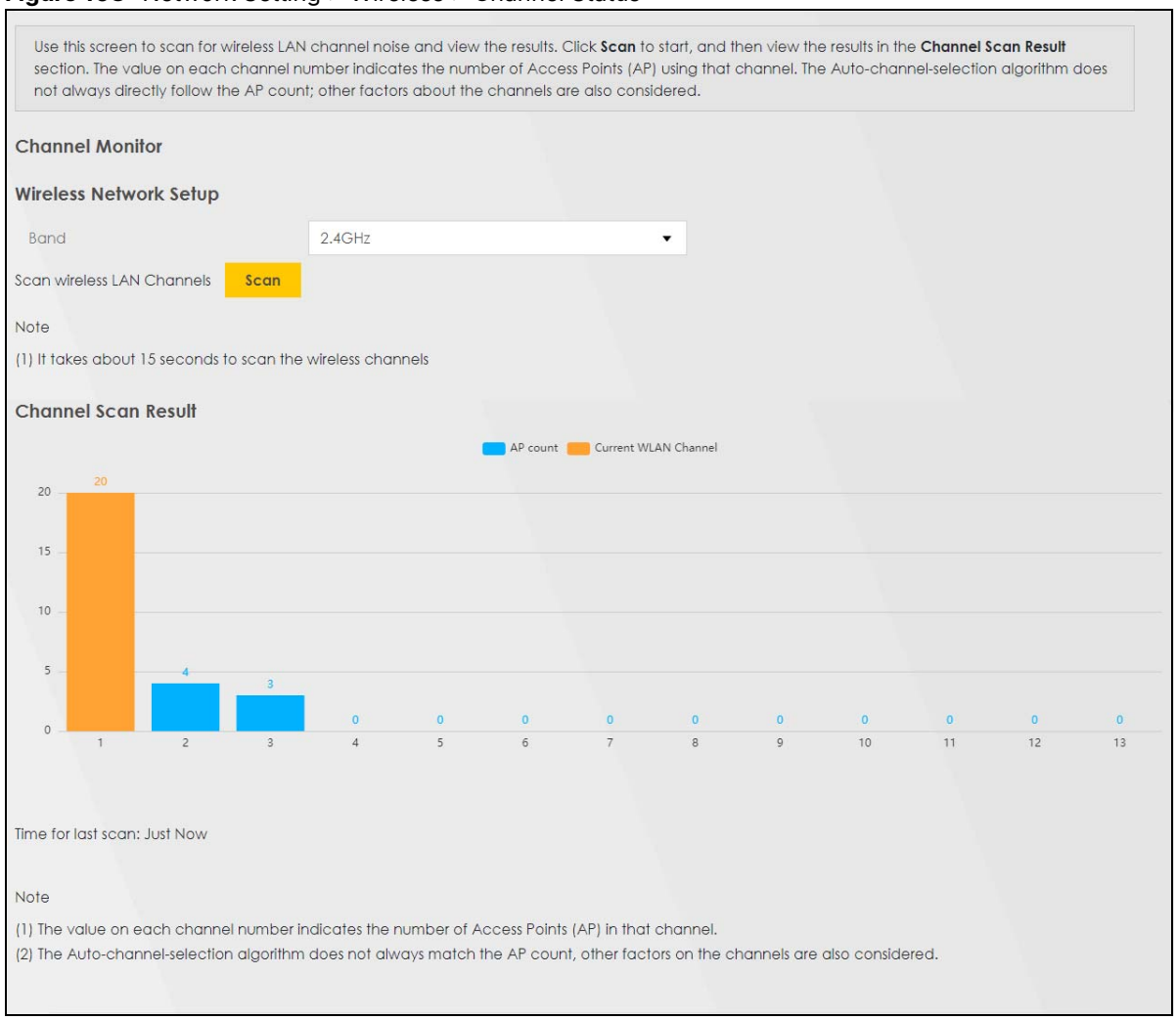
8.8 Channel Status

Use this screen to scan for WiFi channel noise and view the results. Click **Scan** to start, and then view the results in the **Channel Scan Result** section. The value on each channel number indicates the number of Access Points (AP) using that channel. The Auto-channel-selection algorithm does not always directly follow the AP count; other factors about the channels are also considered. Click **Network Setting** > **Wireless** > **Channel Status**. The screen appears as shown.

Note: If the current channel is a DFS channel, the warning 'Channel scan process is denied because current channel is a DFS channel (Channel: 52 – 140). If you want to run channel scan, please select a non-DFS channel and try again.' appears.

Note: The AP count may not be a real-time value.

Figure 108 Network Setting > Wireless > Channel Status



The following table describes the labels in this screen.

Table 49 Network Setting > Wireless > Channel Status

LABEL	DESCRIPTION
Channel Monitor	
Wireless Network Setup	
Band	Select a **2.4 GHz**, **5 GHz or 6 GHz** frequency band on which you want to conduct a channel scan.
Scan wireless LAN Channels	Click the **Scan** button to scan WiFi channels.
Channel Scan Result	This displays the results of the channel scan. The blue bar displays the number of access points (**AP count**) in the WiFi channel. The orange bar displays the WiFi channel that the Zyxel Device is now using.

8.9 MESH

The Zyxel Device supports Mesh to manage your WiFi network. Mesh is the Zyxel implantation of WiFi-Alliance Easy Mesh. It supports AP steering, band steering, auto-configuration and other advances for your WiFi network.

The Zyxel Device can function as a controller to automatically configure WiFi settings on extenders in the network as well as optimize bandwidth usage.

The Zyxel Device optimizes bandwidth usage by directing WiFi clients to an extender (AP steering) or a 2.4 GHz / 5 GHz band (band steering) that is less busy.

See Section 1.3 on page 27 for the complete tutorials with the MPro Mesh app or Zyxel One app.

- Setting up your Mesh network with the Zyxel Device and an Mesh extender,
- setting up your general/guest WiFi,
- basic configurations.

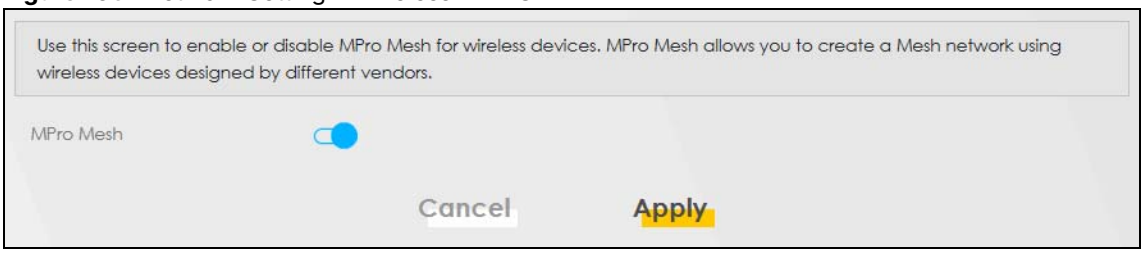
8.9.1 MPro Mesh

Use this screen to enable or disable the Mesh on the Zyxel Device.

Click **Network Setting** > **Wireless** > **MESH**. The following screen displays.

Note: When MPro Mesh is enabled, the SSID and WiFi password of the main 2.4 GHz WiFi network will be copied to the main 5 GHz WiFi network.

Figure 109 Network Setting > Wireless > MESH



The following table describes the labels in this screen.

Table 50 Network Setting > Wireless > MESH

LABEL	DESCRIPTION
MPro Mesh	Click the button (to the right) to enable the Mesh feature on the Zyxel Device and set up your Mesh network.

8.10 Technical Reference

This section discusses WiFi in depth.

8.10.1 WiFi Network Overview

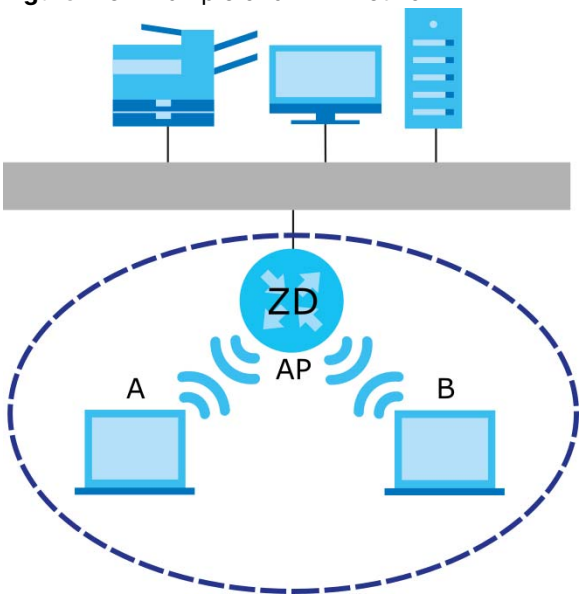
WiFi networks consist of WiFi clients, access points and bridges.

- A WiFi client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous WiFi clients and let them access the network.
- A bridge is a radio that relays communications between access points and WiFi clients, extending a network's range.

Normally, a WiFi network operates in an "infrastructure" type of network. An "infrastructure" type of network has one or more access points and one or more WiFi clients. The WiFi clients connect to the access points.

The following figure provides an example of a WiFi network.

Figure 110 Example of a WiFi Network



The WiFi network is the part in the blue circle. In this WiFi network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

Every WiFi network must follow these basic guidelines.

- Every WiFi device in the same WiFi network must use the same SSID.

  The SSID is the name of the WiFi network. It stands for Service Set IDentifier.
- If two WiFi networks overlap, they should use a different channel.

  Like radio stations or television channels, each WiFi network uses a specific channel, or frequency, to send and receive information.
- Every WiFi device in the same WiFi network must use security compatible with the AP.

  Security stops unauthorized devices from using the WiFi network. It can also protect the information that is sent in the WiFi network.

8.10.2 Additional WiFi Terms

The following table describes some WiFi network terms and acronyms used in the Zyxel Device's Web Configurator.

Table 51 Additional Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a network which covers a large area, devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the devices must sometimes get permission to send information to the Zyxel Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then devices never have to get permission to send information to the Zyxel Device.
Preamble	A preamble affects the timing in your network. There are two preamble modes: long and short. If a WiFi device uses a different preamble mode than the Zyxel Device does, it cannot communicate with the Zyxel Device.
Authentication	The process of verifying whether a device is allowed to use the network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

8.10.3 WiFi Security Overview

By their nature, radio communications are simple to intercept. For WiFi data networks, this means that anyone within range of a WiFi network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a WiFi data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess – for example, a twenty-letter long string of apparently random numbers and letters – but it is not very secure if you use a short key which is very easy to guess – for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it is not just people who have sensitive information on their network who should use security. Everybody who uses any WiFi network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of WiFi security you can set up in the WiFi network.

8.10.3.1 SSID

Normally, the Zyxel Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the Zyxel Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized WiFi devices to get the SSID. In addition, unauthorized WiFi devices can still see the information that is sent in the WiFi network.

8.10.3.2 MAC Address Filter

Every device that can use a WiFi network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each WiFi device in the WiFi network, see the WiFi device's User's Guide or other documentation.

You can use the MAC address filter to tell the Zyxel Device which devices are allowed or not allowed to use the WiFi network. If a WiFi device is allowed to use the WiFi network, it still has to have the correct information (SSID, channel, and security). If a WiFi device is not allowed to use the WiFi network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the WiFi network. Furthermore, there are ways for unauthorized WiFi devices to get the MAC address of an authorized WiFi device. Then, they can use that MAC address to use the WiFi network.

8.10.3.3 Encryption

WiFi networks can use encryption to protect the information that is sent in the WiFi network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 8.10.3.3 on page 195 for information about this.)

Table 52 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	WPA-PSK	
	WPA2	WPA2
Strongest	WPA3-SAE	WPA3 (server certificate validation)

For example, if the WiFi network has a RADIUS server, you can choose **WPA**, **WPA2**, or **WPA3**. If users do not log in to the WiFi network, you can choose no encryption, **WPA2-PSK**, or **WPA3-SAE**.

1. Some devices, such as scanners, can detect networks but cannot use networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

Note: It is recommended that WiFi networks use **WPA3-SAE**, **WPA2-PSK**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized WiFi devices to figure out the original information pretty quickly.

Many types of encryption use a key to protect the information in the WiFi network. The longer the key, the stronger the encryption. Every device in the WiFi network must have the same key.

8.10.4 Signal Problems

Because WiFi networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

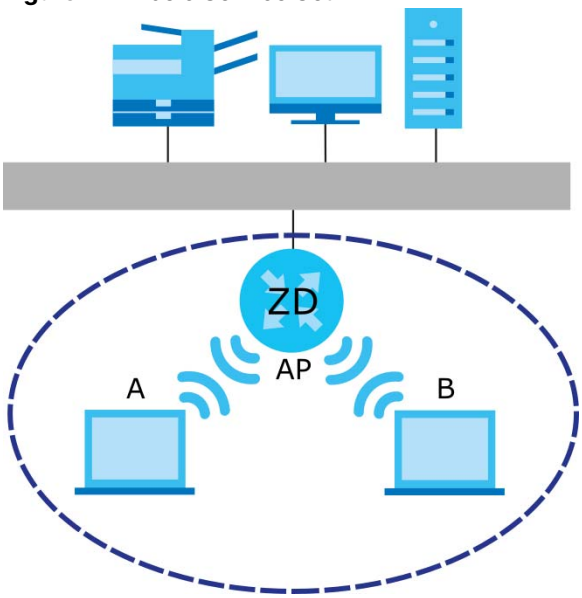
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

8.10.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 111 Basic Service Set



8.10.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Zyxel Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

8.10.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

8.10.7 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant WiFi adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other WiFi devices on the network support, and to provide more reliable communications in busy WiFi networks.

Use short preamble if you are sure all WiFi devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all WiFi devices on the network support it, otherwise the Zyxel Device uses long preamble.

Note: The WiFi devices MUST use the same preamble mode in order to communicate.

8.10.8 WiFi Protected Setup (WPS)

Your Zyxel Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure WiFi network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has 2 minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

8.10.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within WiFi range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the Zyxel Device).
3. Press the button on one of the devices (it does not matter which). For the Zyxel Device you must press the **WiFi** button for more than 5 seconds.
4. Within 2 minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

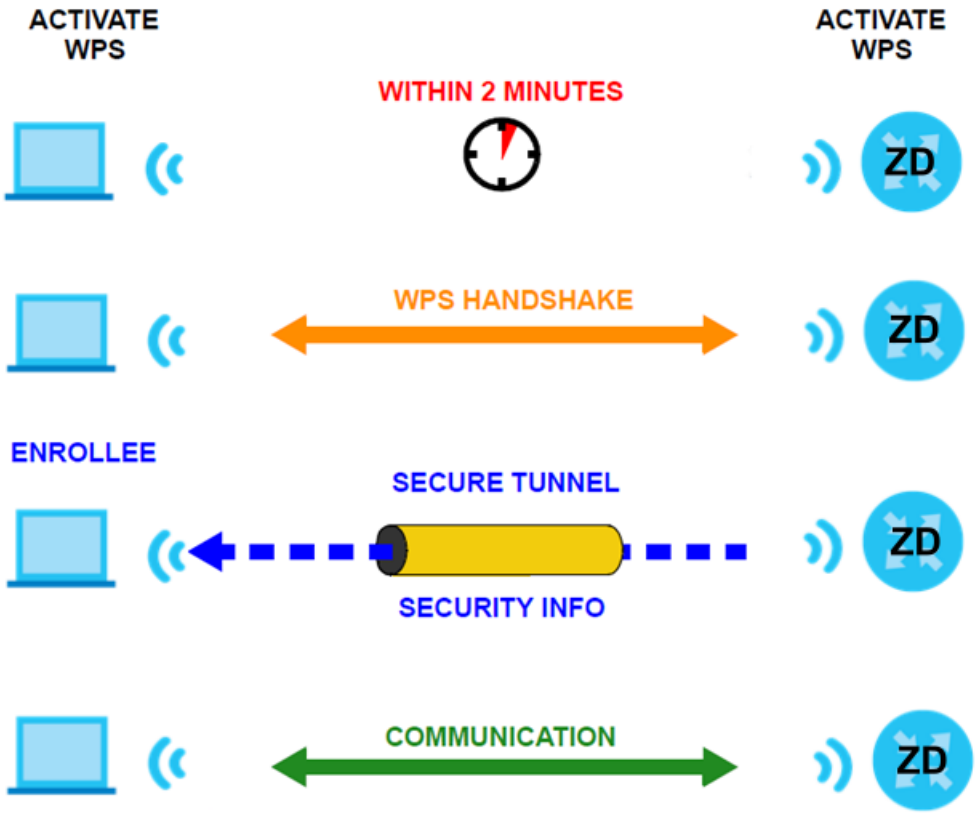
   If you need to make sure that WPS worked, check the list of associated WiFi clients in the AP's configuration utility. If you see the WiFi client in the list, WPS was successful.

8.10.8.2 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA2-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 112 How WPS Works



The roles of registrar and enrollee last only as long as the WPS setup process is active (2 minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the WiFi client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled WiFi clients.

By default, a WPS device is 'un-configured'. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is un-configured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes 'configured'. A configured WiFi client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

8.10.8.3 Example WPS Network Setup

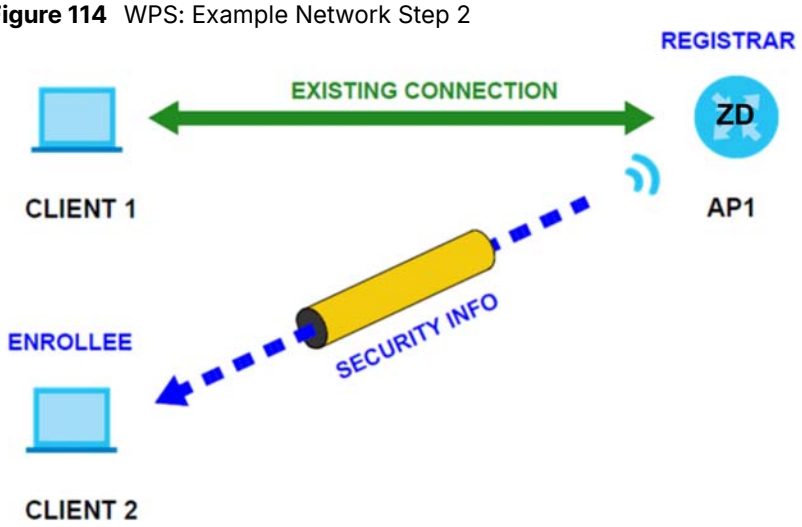
This section shows how security settings are distributed in a sample WPS setup.

The following figure shows a sample network. In step 1, both **AP1** and **Client 1** are un-configured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is un-configured and has no existing information.

Figure 113 WPS: Example Network Step 1

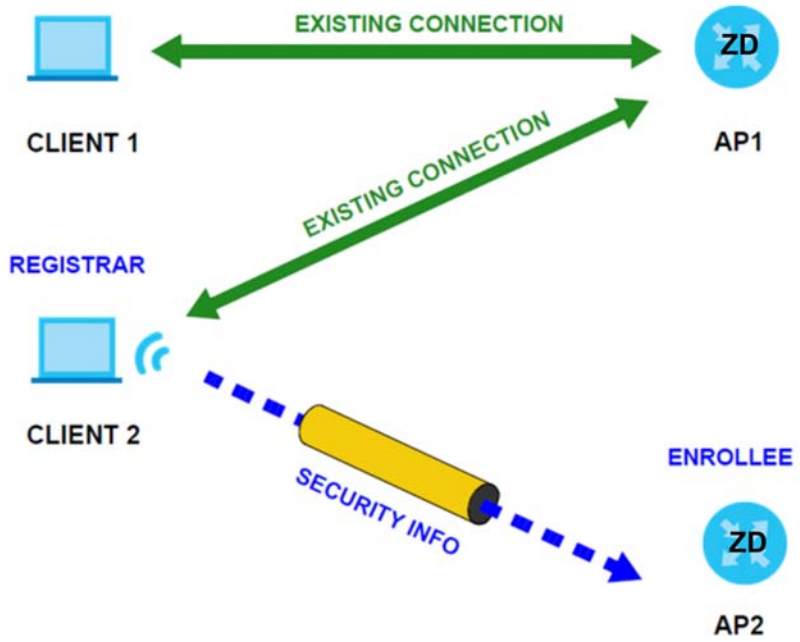
In step 2, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 114 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 115 WPS: Example Network Step 3



8.10.8.4 Limitations of WPS

WPS has some limitations of which you should be aware.

- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it was successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the 'correct' enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS only works simultaneously between two devices, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your WiFi clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

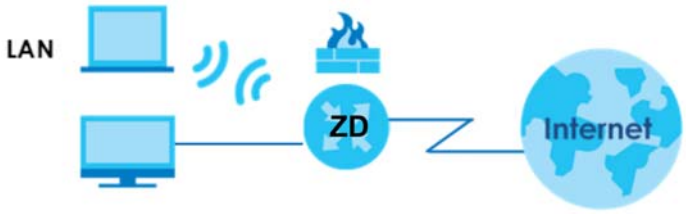
CHAPTER 9
Home Networking

9.1 Home Networking Overview

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

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

Figure 116 Home Networking Example



9.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 9.2 on page 204).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 9.3 on page 209).
- Use the **UPnP** screen to enable UPnP (Section 9.4 on page 211).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 9.5 on page 212).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses (Section 9.6 on page 214).
- Use the **APAS** screen to allow incoming traffic from any port to access any service on a LAN device (Section 9.9 on page 216).

9.1.2 What You Need To Know

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

9.1.2.1 About LAN

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your Zyxel Device will compute the subnet mask automatically based on the IP address that you entered. You do not need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This Zyxel Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

9.1.2.2 About UPnP

How do I know if I am using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows 7). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a Multicast message. For security reasons, the Zyxel Device allows Multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and Zyxel

Zyxel has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC).

See Section 9.11 on page 221 for examples on installing and using UPnP.

9.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

9.2 LAN Setup

A LAN IP address is the IP address of a networking device in the LAN. You can use the Zyxel Device's LAN IP address to access its Web Configurator from the LAN. The DHCP server settings define the rules on assigning IP addresses to LAN clients on your network.

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. Click **Network Setting** > **Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

1. Select the **Interface Group** you want to set up the LAN. To configure an interface group, go to **Network Setting > Interface Grouping**. See Chapter 16 for more details about interface group.
2. Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your Zyxel Device.
3. Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
4. Click **Apply** to save your settings.

Figure 117 Network Setting > Home Networking > LAN Setup

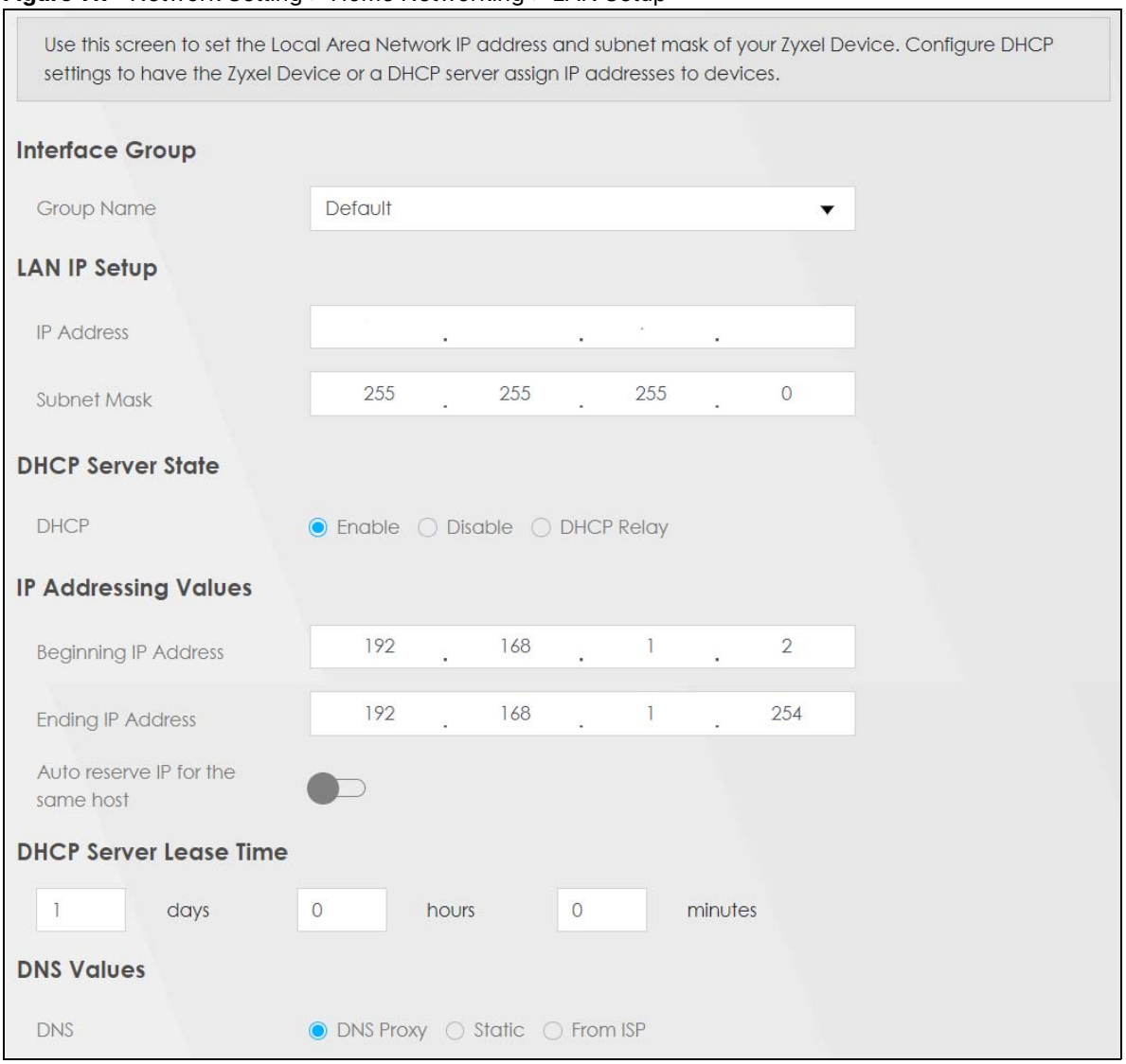
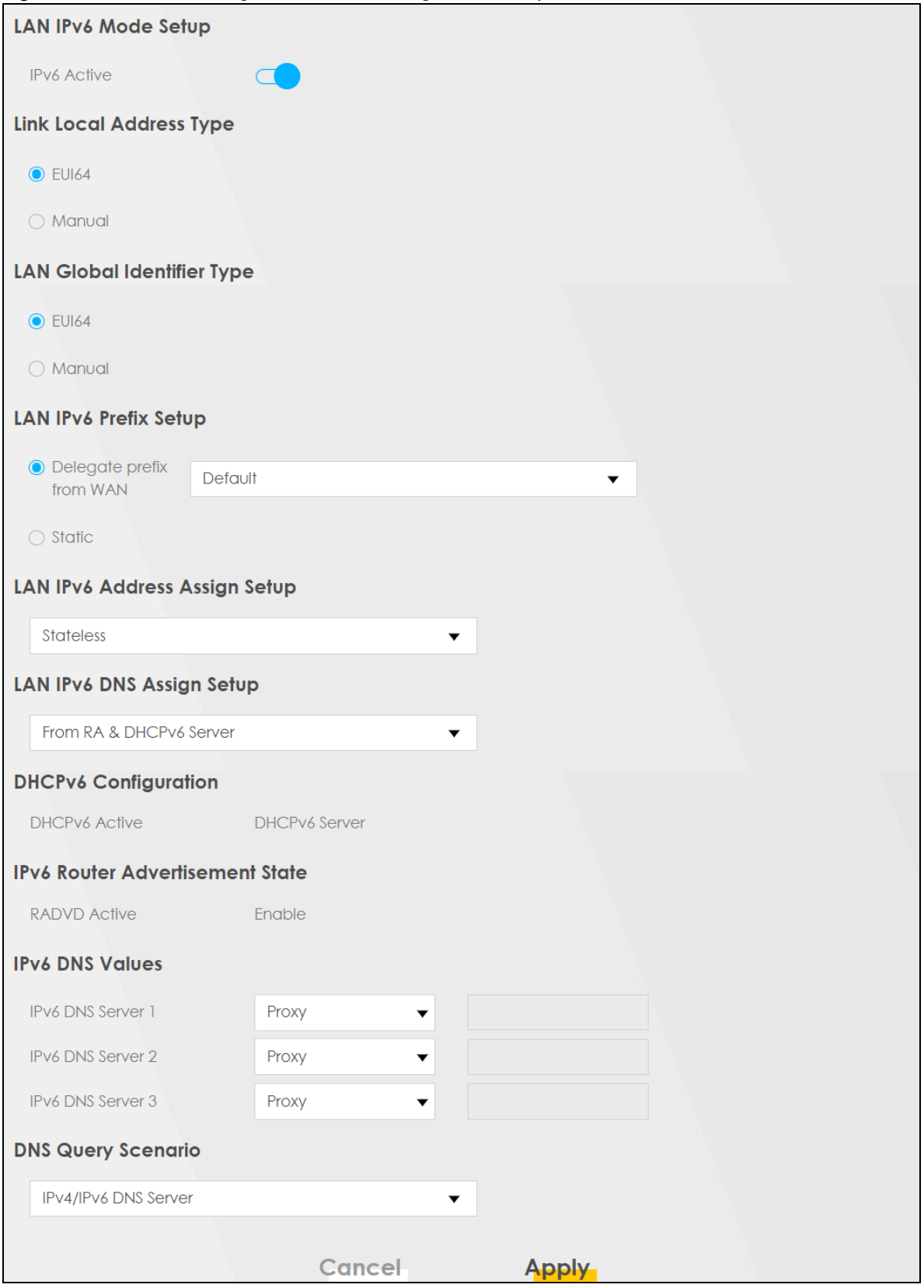


Figure 118 Network Setting > Home Networking > LAN Setup (Continued)



The following table describes the fields in this screen.

Table 53 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group that you want to configure for the LAN settings. You must enable DHCP.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your in dotted decimal notation, for example, (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel 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.
DHCP Server State	
DHCP	Select **Enable** to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. If you select **DHCP Relay**, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
IP Addressing Values The **IP Addressing Values** fields appear only when you select **Enable** in the **DHCP** field.	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
DHCP Server Lease Time This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are “recycled” and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.	
Days/Hours/Minutes	DHCP server leases an address to a new client device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different client device.
DNS Values This field appears only when you select **Enable** in the **DHCP** field.	
DNS	The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client. Select **DNS Proxy** to have the DHCP clients use the Zyxel Device’s own LAN IP address. The Zyxel Device works as a DNS relay. Select **Static** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **From ISP** if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).

Table 53 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 Mode Setup	
IPv6 Active	Use this to enable or disable IPv6 on the Zyxel Device. When IPv6 is used, the following fields need to be set.
Link Local Address Type	A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. 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. Select **EUI64** to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select **Manual**. Link-local Unicast Address Format 1111 1110 10 | 0 | Interface ID 10 bits | 54 bits | 64 bits
EUI64	Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format.
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.
LAN Global Identifier Type	Select **EUI64** to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select **Manual** to manually enter an interface ID for the LAN interface's global IPv6 address.
EUI64	Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address.
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Prefix Setup	Select **Delegate prefix from WAN** to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select **Static** to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: **Stateless**: The Zyxel Device uses IPv6 stateless auto-configuration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. **Stateful**: The Zyxel Device uses IPv6 stateful auto-configuration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6. **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. **From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. **DHCP Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	

Table 53 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 DNS Values	
IPv6 DNS Server 1 – 3	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **User Defined** – Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. **From ISP** – Select this if your ISP dynamically assigns IPv6 DNS server information. **Proxy** – Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay. Otherwise, select **None** if you do not want to configure IPv6 DNS servers.
DNS Query Scenario	Select how the Zyxel Device handles clients' DNS information requests. **IPv4/IPv6 DNS Server**: The Zyxel Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. **IPv6 DNS Server Only**: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. **IPv4 DNS Server Only**: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. **IPv6 DNS Server First**: The Zyxel Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. **IPv4 DNS Server First**: The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

9.3 Static DHCP

When any of the LAN clients in your network want an assigned fixed IP address, add a static lease for each LAN client. Knowing the LAN client's MAC addresses is necessary. This table allows you to assign IP addresses on the LAN to individual computers based on their MAC addresses.

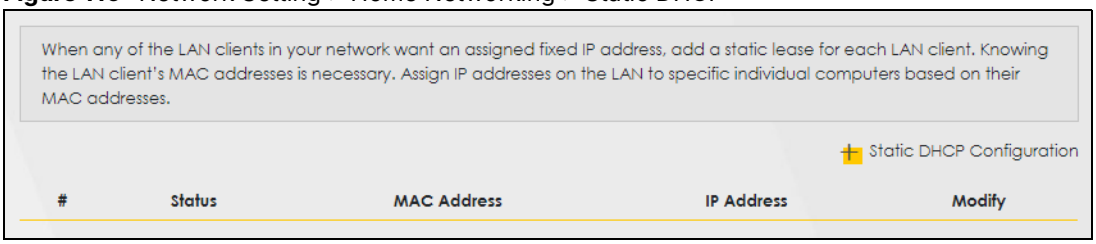
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

9.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your Zyxel Device's static DHCP settings. Click **Network Setting** > **Home Networking** > **Static DHCP** to open the following screen.

Figure 119 Network Setting > Home Networking > Static DHCP



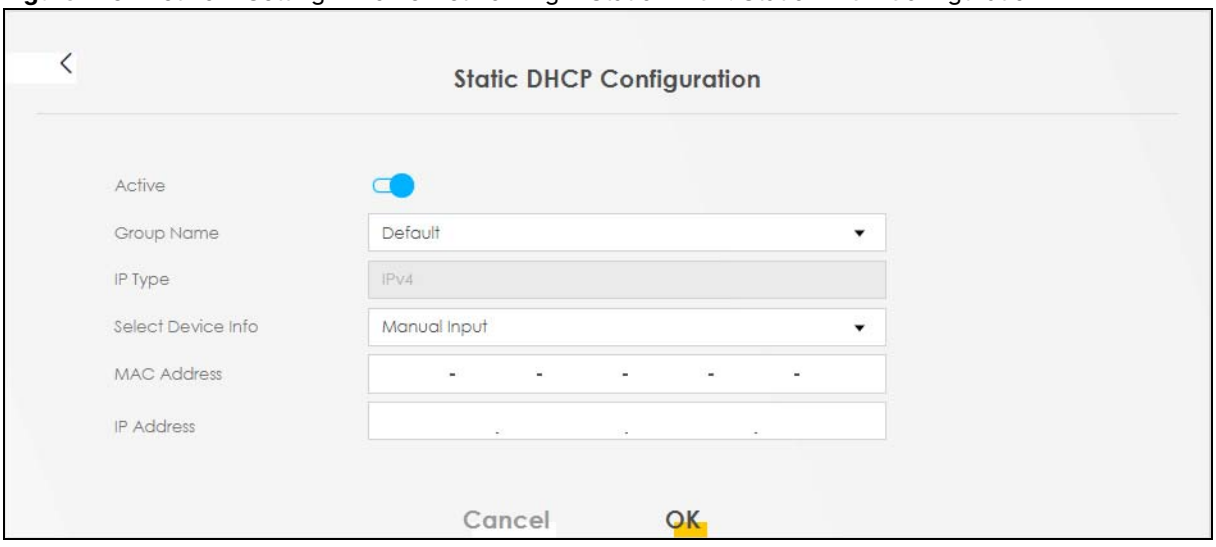
The following table describes the labels in this screen.

Table 54 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to configure a static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the Zyxel Device.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to remove the connection.

If you click **Static DHCP Configuration** in the **Static DHCP** screen, the following screen displays. Using a static DHCP means a LAN client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a client device by selecting the interface group of this client device and its IP address type and selecting the device/computer from a list or manually entering its MAC address and assigned IP address.

Figure 120 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration



The following table describes the labels in this screen.

Table 55 Network Setting > Home Networking > Static DHCP: Configuration

LABEL	DESCRIPTION
Active	Select **Enable** to activate static DHCP in your
Group Name	Select the interface group for which you want to configure the static DHCP settings.
IP Type	The **IP Type** is normally **IPv4** (non-configurable).
Select Device Info	Select between **Manual Input** which allows you to enter the next two fields (**MAC Address** and **IP Address**); or select an existing
MAC Address	Enter the MAC address of a computer on your LAN if you select **Manual Input** in the previous field.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify if you select **Manual Input** in the previous field.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

9.4 UPnP

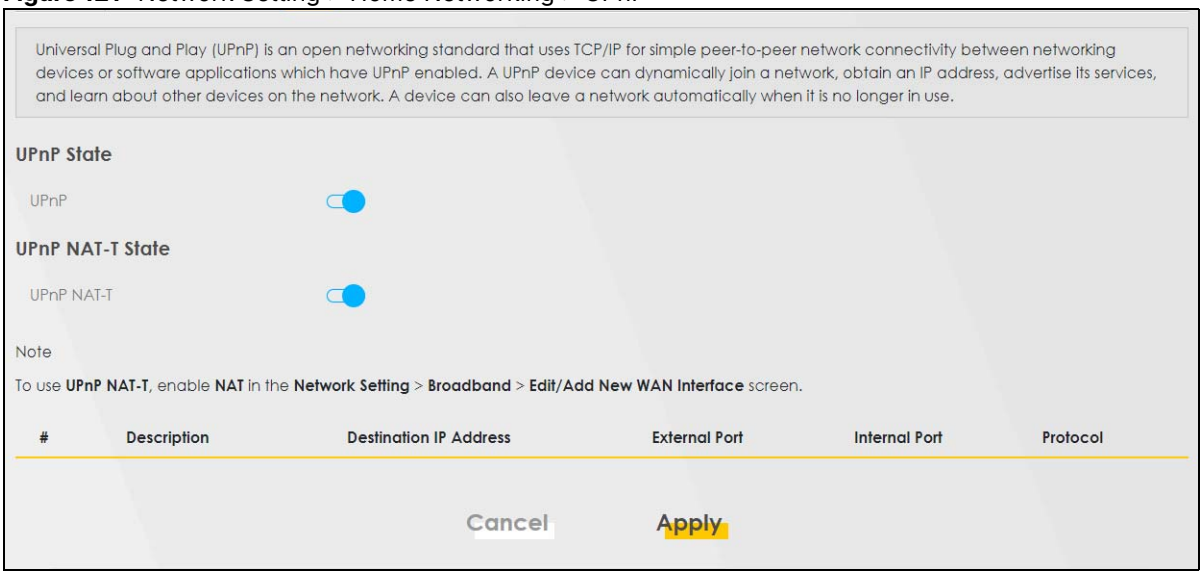
Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn about other devices on the network. A device can also leave a network automatically when it is no longer in use.

See Section 9.11 on page 221 for more information on UPnP.

Note: To use **UPnP NAT-T**, enable **NAT** in the **Network Setting** > **Broadband** > **Edit** or **Add New WAN Interface** screen.

Use the following screen to configure the UPnP settings on your Zyxel Device. Click **Network Setting** > **Home Networking** > **UPnP** to display the screen shown next.

Figure 121 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

Table 56 Network Settings > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP State	
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T State	
UPnP NAT-T	Select **Enable** to activate UPnP with NAT enabled. UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions.
#	This field displays the index number of the entry.
Description	This field displays the description of the UPnP NAT-T connection.
Destination IP Address	This field displays the IP address of the other connected UPnP-enabled device.
External Port	This field displays the external port number that identifies the service.
Internal Port	This field displays the internal port number that identifies the service.
Protocol	This field displays the protocol of the NAT mapping rule. Choices are **TCP** or **UDP**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

9.5 LAN Additional Subnet

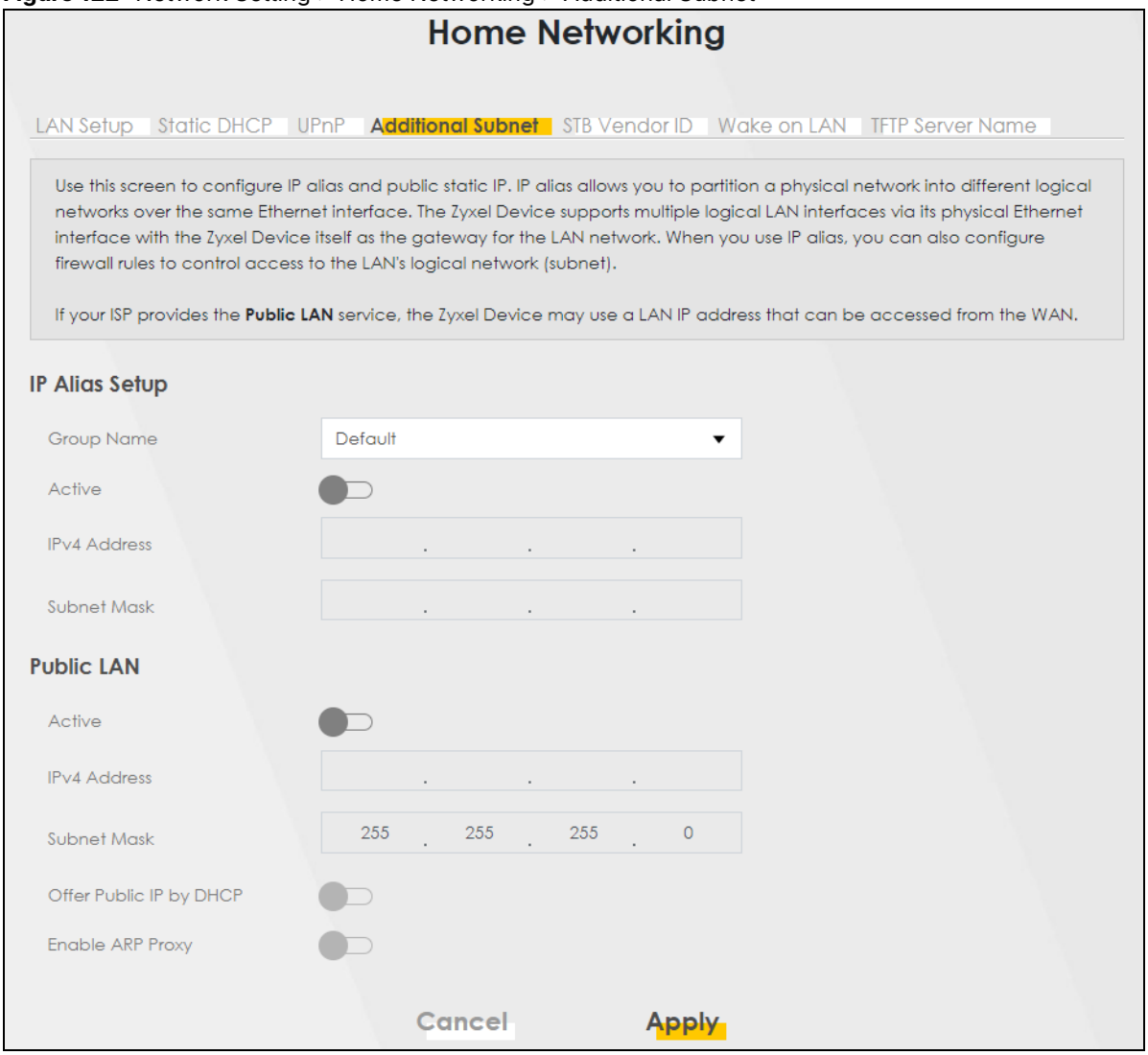
Use this screen to configure IP alias and public static IP.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Zyxel Device supports multiple logical LAN interfaces through its physical Ethernet interface with the Zyxel Device itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

If your ISP provides the **Public LAN** service, the Zyxel Device may use a LAN IP address that can be accessed from the WAN.

Click **Network Setting** > **Home Networking** > **Additional Subnet** to display the screen shown next.

Figure 122 Network Setting > Home Networking > Additional Subnet



The following table describes the labels in this screen.

Table 57 Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings.
Active	Click this switch to enable a logical LAN for the Zyxel Device. When this is enabled, the following fields will be configurable.
IPv4 Address	Enter the IP address of your Zyxel Device in dotted decimal notation.
Subnet Mask	Your Zyxel Device will automatically calculate the subnet mask based on the IPv4 address that you assign. Unless you are implementing subnetting, use this value computed by the Zyxel Device.
Public LAN	
Active	Click this switch to enable or disable the Public LAN feature. Your ISP must support Public LAN and static IP.
IPv4 Address	Enter the public IP address provided by your ISP.

Table 57 Network Setting > Home Networking > Additional Subnet (continued)

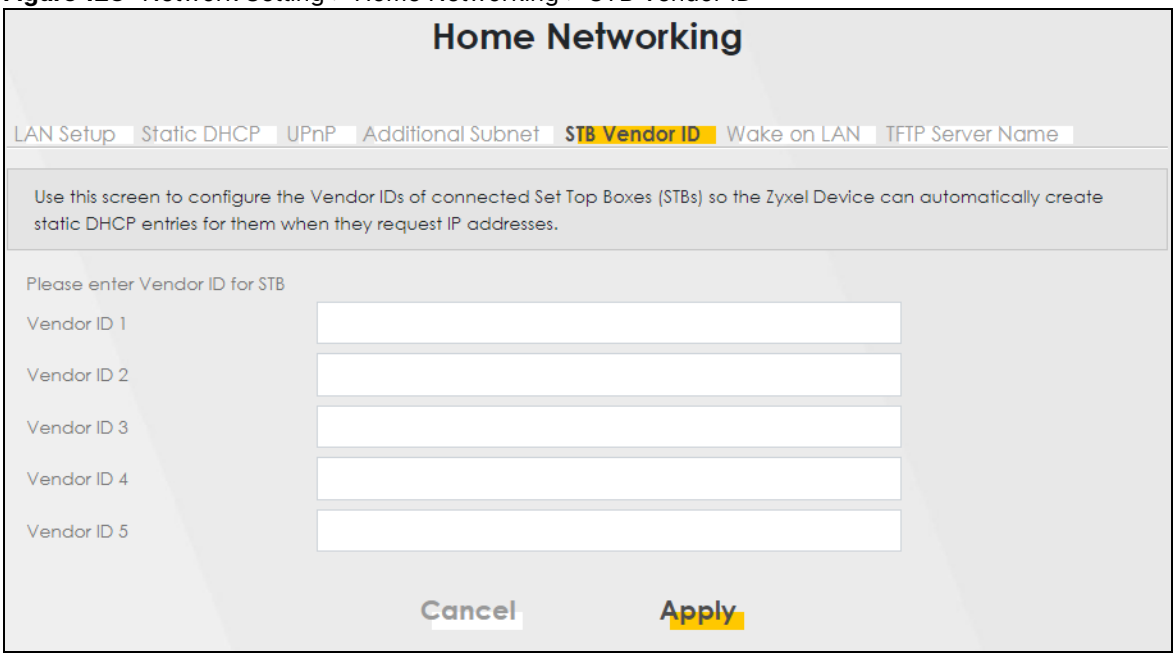
LABEL	DESCRIPTION
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.
Offer Public IP by DHCP	Click this switch to enable the Zyxel Device to provide public IP addresses by DHCP server. Otherwise, click to disable.
Enable ARP Proxy	Click this switch to enable the Address Resolution Protocol (ARP) proxy. Otherwise, click to disable.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

9.6 STB Vendor ID

Use this screen to configure the Vendor IDs of connected Set Top Boxes (STBs) so the Zyxel Device can automatically create static DHCP entries for them when they request IP addresses.

Click **Network Setting** > **Home Networking** > **STB Vendor ID** to open this screen.

Figure 123 Network Setting > Home Networking > STB Vendor ID



The following table describes the labels in this screen.

Table 58 Network Setting > Home Networking > STB Vendor ID

LABEL	DESCRIPTION
Vendor ID 1 – 5	These are STB's Vendor Class Identifiers (DHCP option 60). A Vendor Class Identifier is usually used to inform the DHCP server a DHCP client's vendor and functionality.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

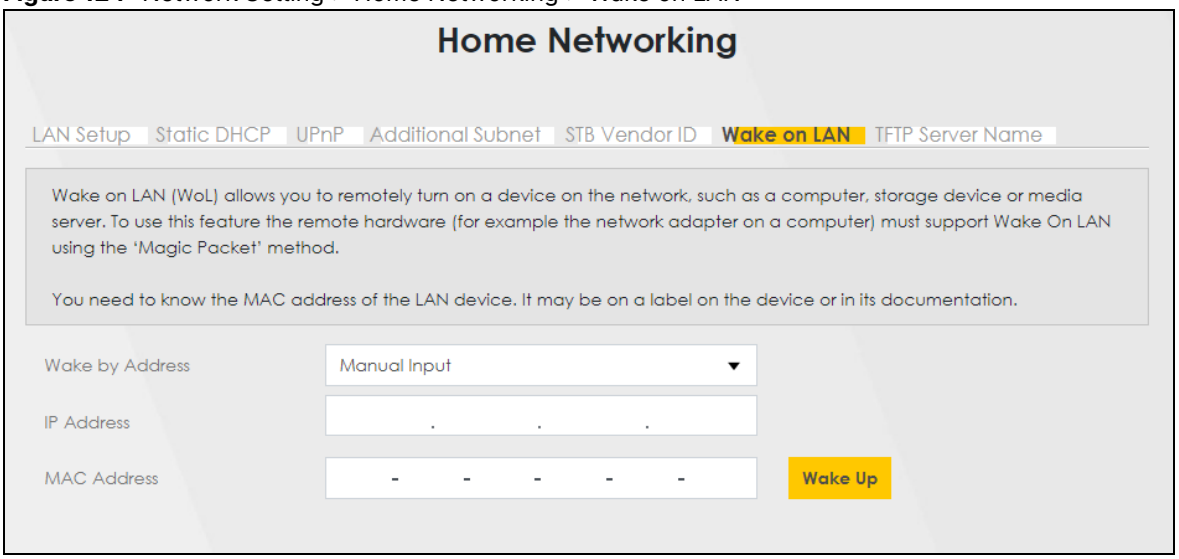
9.7 Wake on LAN

Wake on LAN (WoL) allows you to remotely turn on a device on the network, such as a computer, storage device or media server. To use this feature, the remote hardware (for example the network adapter on a computer) must support Wake on LAN using the 'Magic Packet' method.

You need to know the MAC address of the LAN device. It may be on a label on the LAN device.

Click **Network Setting** > **Home Networking** > **Wake on LAN** to open this screen.

Figure 124 Network Setting > Home Networking > Wake on LAN



The following table describes the labels in this screen.

Table 59 Network Setting > Home Networking > Wake on LAN

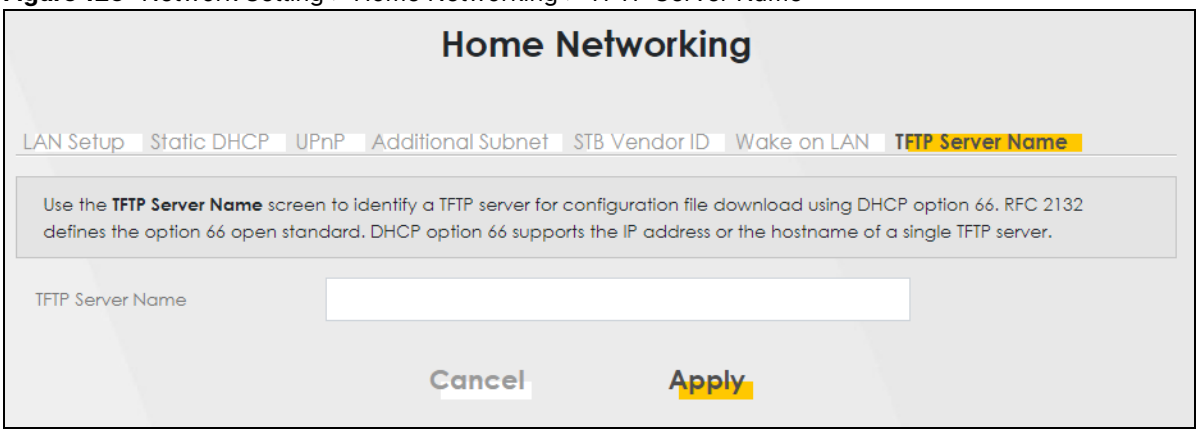
LABEL	DESCRIPTION
Wake by Address	Select **Manual** and enter the IP address or MAC address of the LAN device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the Zyxel Device's ARP table. If you select an IP address, the MAC address of the LAN device with the selected IP address then displays in the **MAC Address** field.
IP Address	Enter the IPv4 IP address of the LAN device to turn it on. This field is not available if you select an IP address in the **Wake by Address** field.
MAC Address	Enter the MAC address of the LAN device to turn it on. A MAC address consists of six hexadecimal character pairs.
Wake Up	Click this to send a WoL magic packet to wake up the specified LAN device.

9.8 TFTP Server Name

Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. RFC 2132 defines the option 66 open standard. DHCP option 66 supports the IP address or the host name of a single TFTP server.

Click **Network Setting** > **Home Networking** > **TFTP Server Name** to open this screen.

Figure 125 Network Setting > Home Networking > TFTP Server Name



The following table describes the labels in this screen.

Table 60 Network Setting > Home Networking > TFTP Server Name

LABEL	DESCRIPTION
TFTP Server Name	Enter the IP address or the host name of a single TFTP server.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

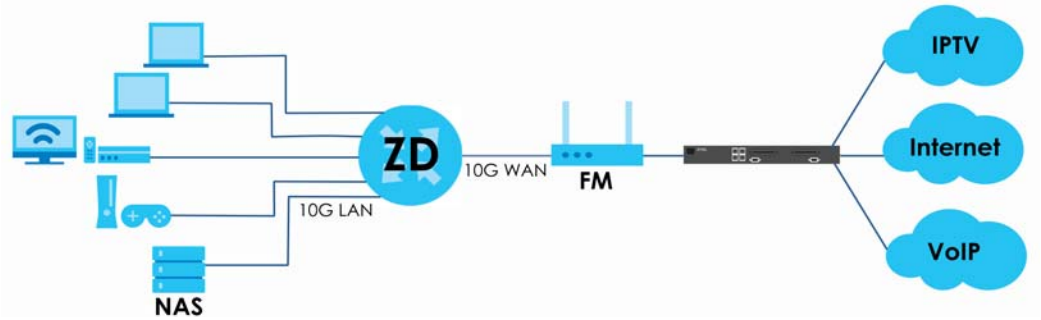
9.9 Any Port Any Service (APAS)

Any Port Any Service (APAS) allows a LAN device to use any available port to access any available service from a remote WAN device. Typically, a LAN device, such as a Set Top Box (STB), would have to use a specific port to access video streams from a video server. With APAS, the video streams only need to be received through the specified Bridge WAN interface for the LAN device specified in the APAS rule. You can connect the LAN device to any LAN port. Other LAN devices can access the Internet using the default gateway.

Unlike **Port Forwarding**, which forwards traffic based on port numbers, you do not need to know the port number for the video traffic from the IPTV server. You just select the LAN device host name or enter its MAC address and select a Bridge WAN interface.

Use the wildcard '*' for a range of MAC addresses for multiple LAN devices. For example, enter 00:13:49:*:*:* for all LAN devices from a vendor with the MAC OUI 00:13:49. (range). Any device with that MAC OUI aa:bb:cc connected to any LAN port on the Zyxel Device can access services or can be accessed for services through the specified Bridge WAN interface. For example, the LAN device could be an STB receiving video streams from a video server, or it could be a server, allowing access to it through the specified Bridge WAN interface.

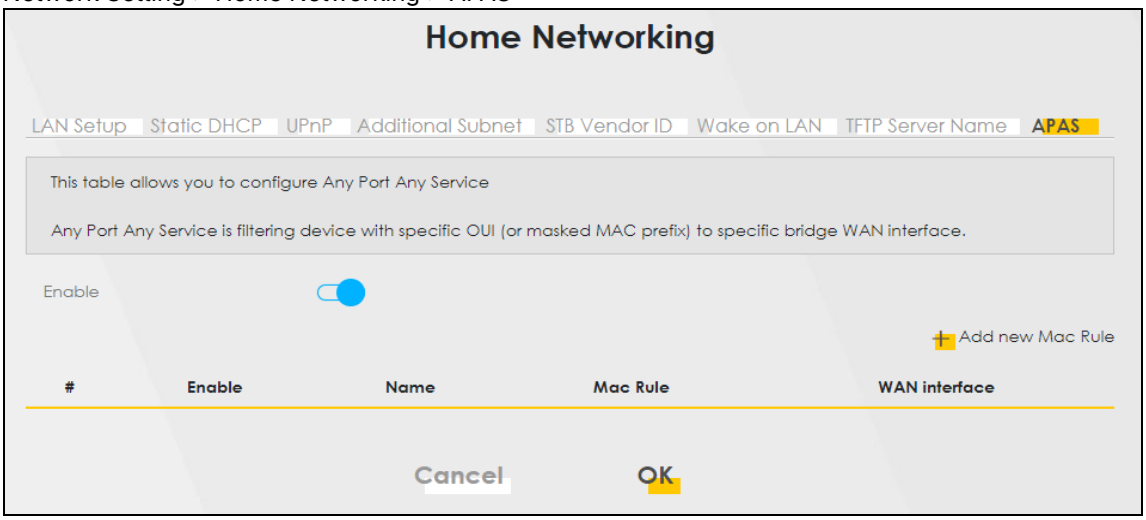
Note: You must configure a Bridge WAN interface in advance.



As APAS allows incoming traffic from any port to access any service on a configured LAN device, it may be difficult to distinguish between appropriate and malicious traffic going to the LAN device. Make sure to properly configure firewall rules to protect the LAN device, and monitor network traffic for suspicious activity.

Click **Network Setting** > **Home Networking** > **APAS** to open this screen.

Network Setting > Home Networking > APAS



The following table describes the labels in this screen.

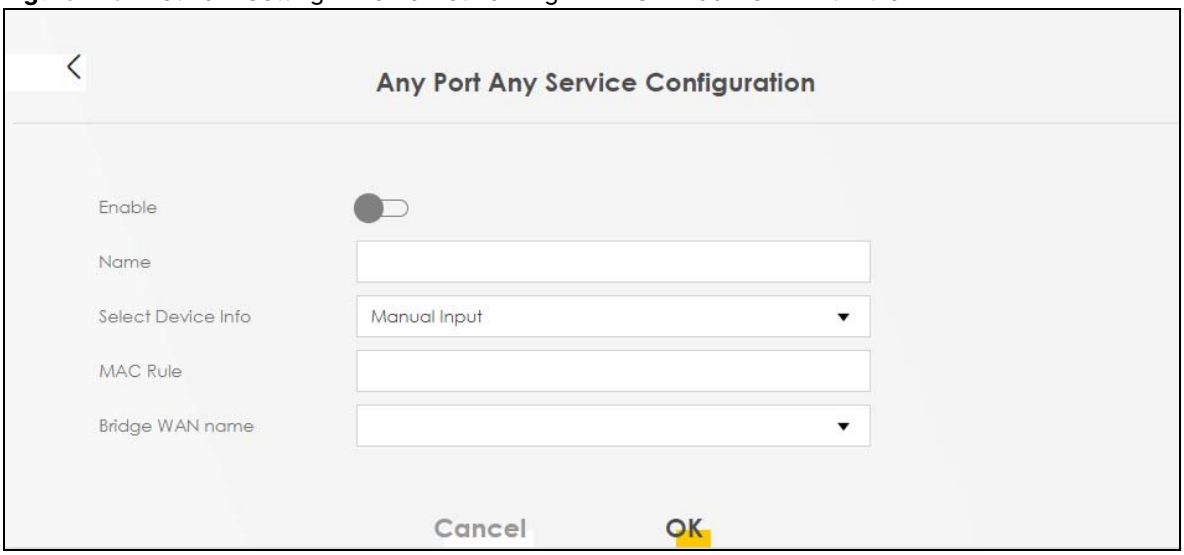
Table 61 Network Setting > Home Networking > APAS

LABEL	DESCRIPTION
Enable	Click **Enable** to activate APAS.
Add new MAC Rule	Click this button to add a new MAC rule. You can create up to eight MAC rules.
#	This is the index number.
Name	This is the name of the rule.
MAC Rule	This is the LAN host MAC address that is applied to the rule.
WAN Interface	This is the bridge WAN interface for incoming traffic.
Cancel	Click **Cancel** to restore your previously saved changes.
OK	Click **OK** to save your changes.

9.9.1 Add APAS

Use this screen to create a new MAC rule. Click **Network Setting** > **Home Networking** > **APAS** > **Add New MAC Rule** to open the following screen.

Figure 126 Network Setting > Home Networking > APAS > Add New MAC Rule



The following table describes the labels in this screen.

Table 62 Network Setting > Home Networking > APAS > Add New MAC Rule

LABEL	DESCRIPTION
Enable	Click this to enable APAS on the Zyxel Device.
Name	Enter a name of up to 64 characters for the **APAS** rule to this host(s). Allowed characters for **Name** include the following within quotes: " !#%()*+,-./ 0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]_abcdefghijklmnopqrstuvw xyz{}~"
Select Device Info	Select a connected LAN host or select **Manual Input** to enter the MAC address of a client that is not yet connected and does not display in **Connection Status** > **Connectivity**.
MAC Rule	If you selected **Manual Input** for **Select Device Info**, then enter the LAN host MAC address here. You can use the wildcard '*' for a MAC address range. For example, enter 00:13:49:*:*:* for all LAN devices from a vendor with the MAC OUI 00:13:49.
Bridge WAN Name	Select a Bridge WAN interface for incoming traffic to apply the rule. You must have created at least one Bridge WAN interface in **Network Setting** > **Broadband** screen.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

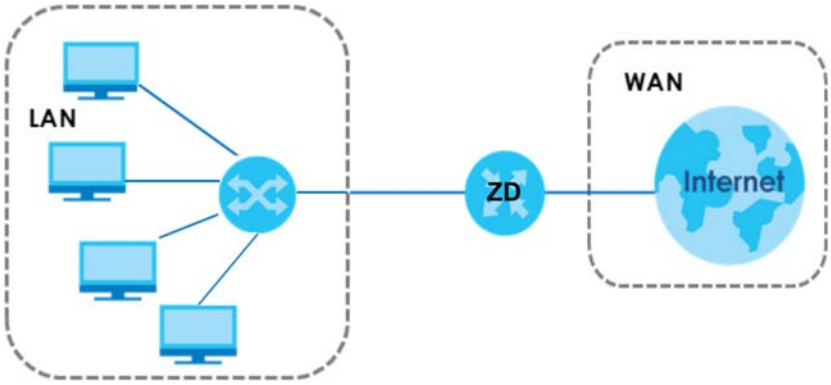
9.10 Technical Reference

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

LANs, WANs and the Zyxel Device

The actual physical connection determines whether the Zyxel Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 127 LAN and WAN IP Addresses



9.10.1 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Zyxel Device as a DHCP server or disable it. When configured as a server, the Zyxel Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The Zyxel Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

9.10.2 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- 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, enter them in the **DNS Server** fields in the **DHCP Setup** screen.

- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Zyxel Device supports the IPCP DNS server extensions through the DNS proxy feature.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

9.10.3 LAN TCP/IP

The Zyxel Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Zyxel Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Zyxel Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Zyxel Device will compute the subnet mask automatically based on the IP address that you entered. You do not need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

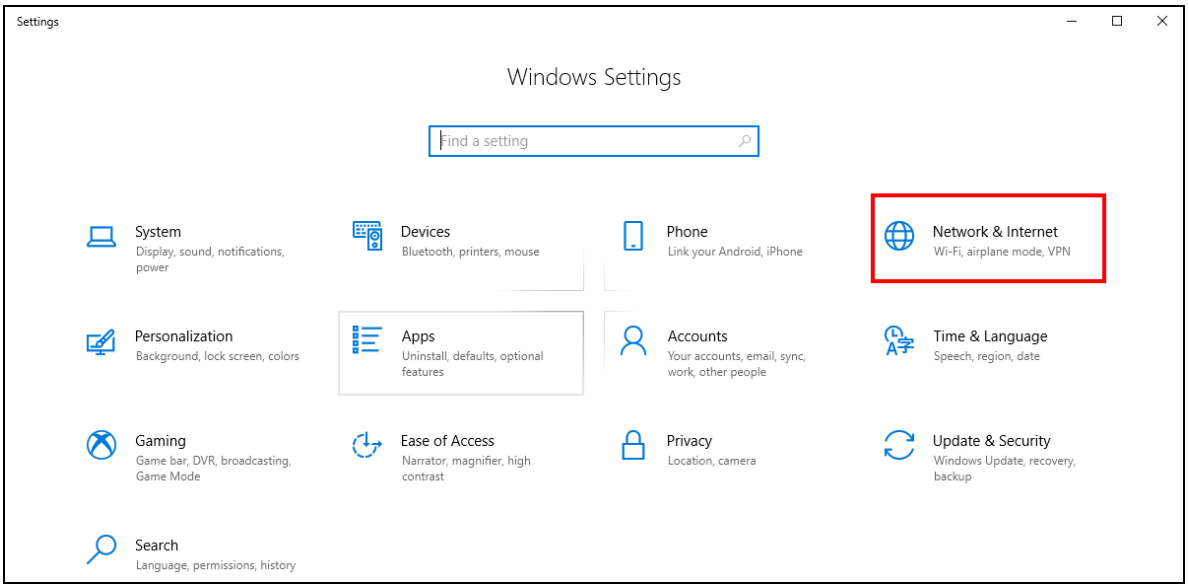
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

9.11 Turn on UPnP in Windows 10 Example

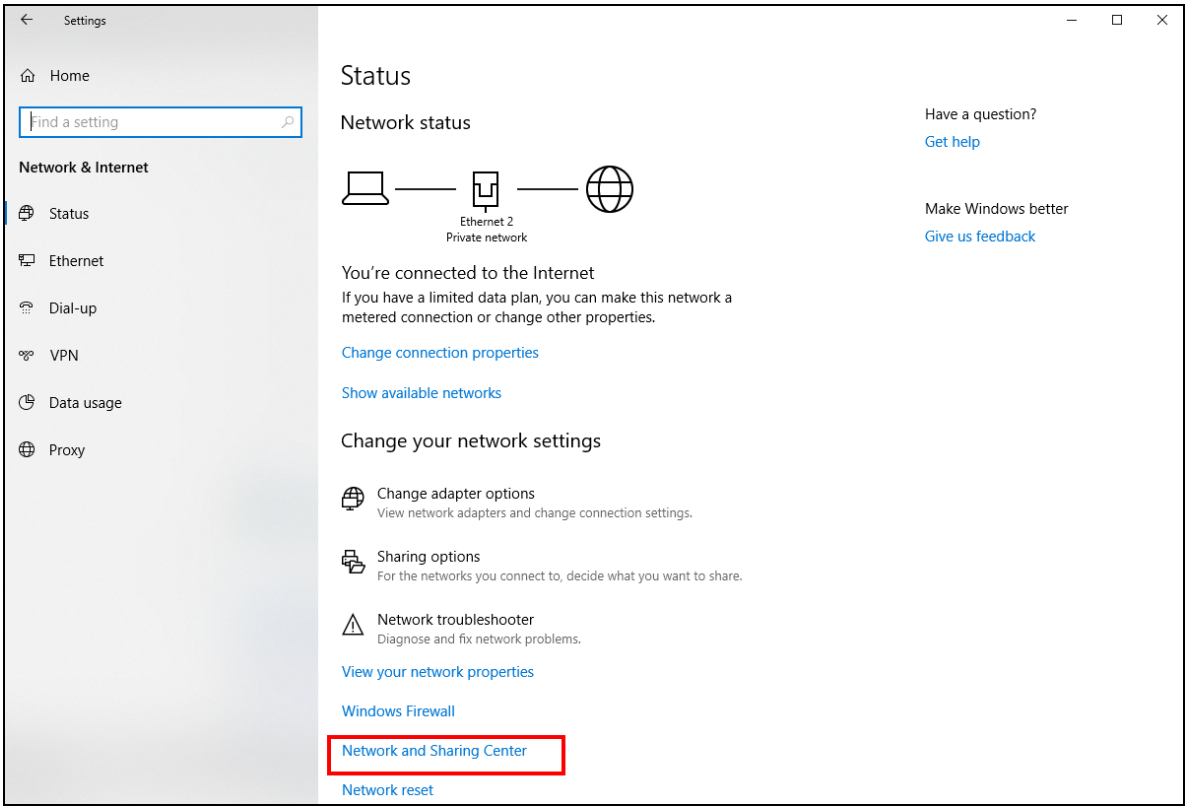
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting** > **Home Networking** > **UPnP**.

Make sure the computer is connected to the LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.

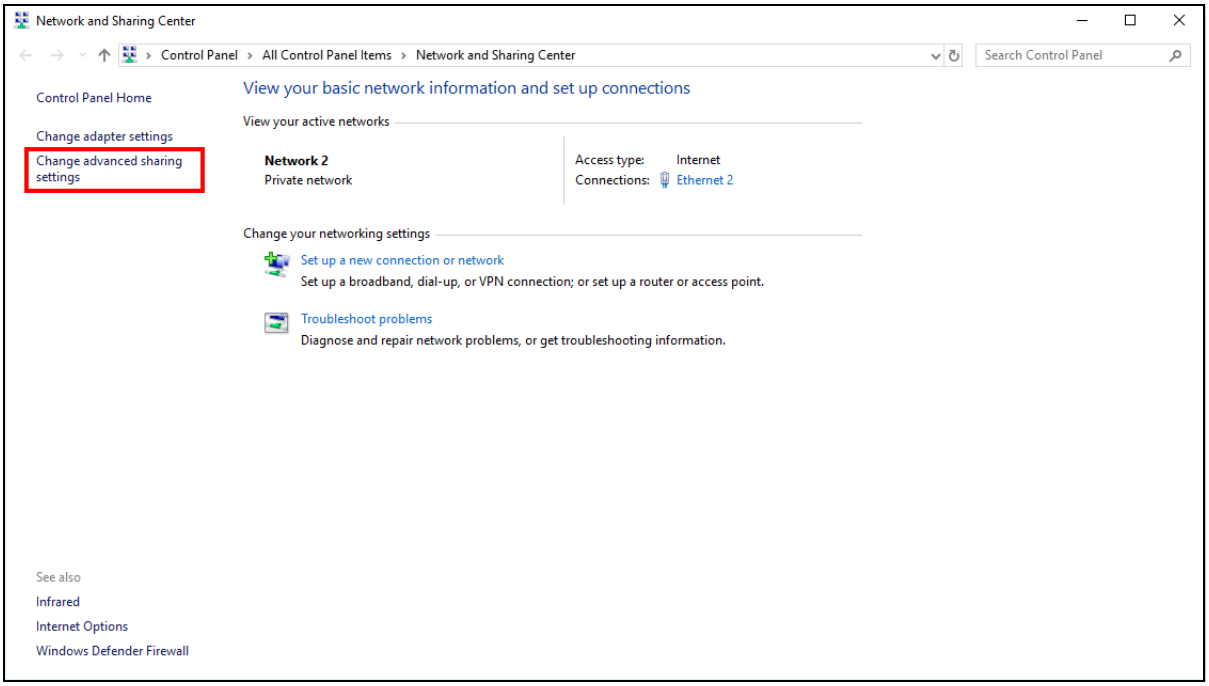
1 Click the start icon, **Settings** and then **Network & Internet**.



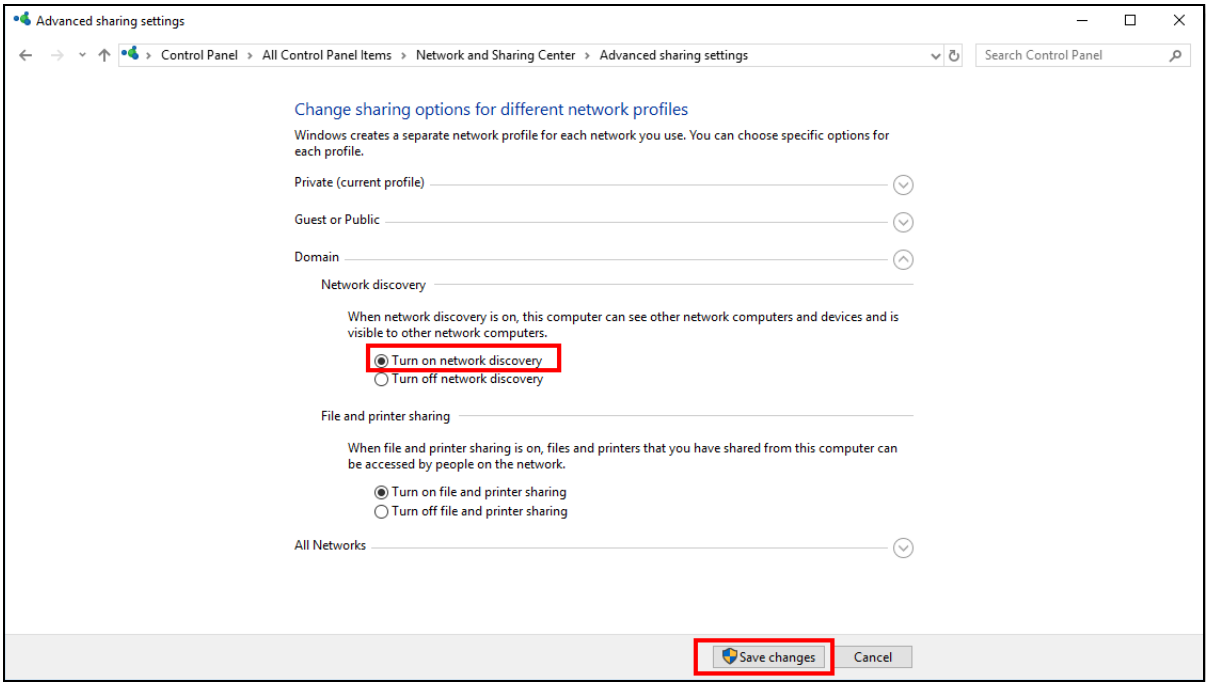
2 Click **Network and Sharing Center**.



3 Click **Change advanced sharing settings**.



4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



9.11.1 Auto-discover Your UPnP-enabled Network Device

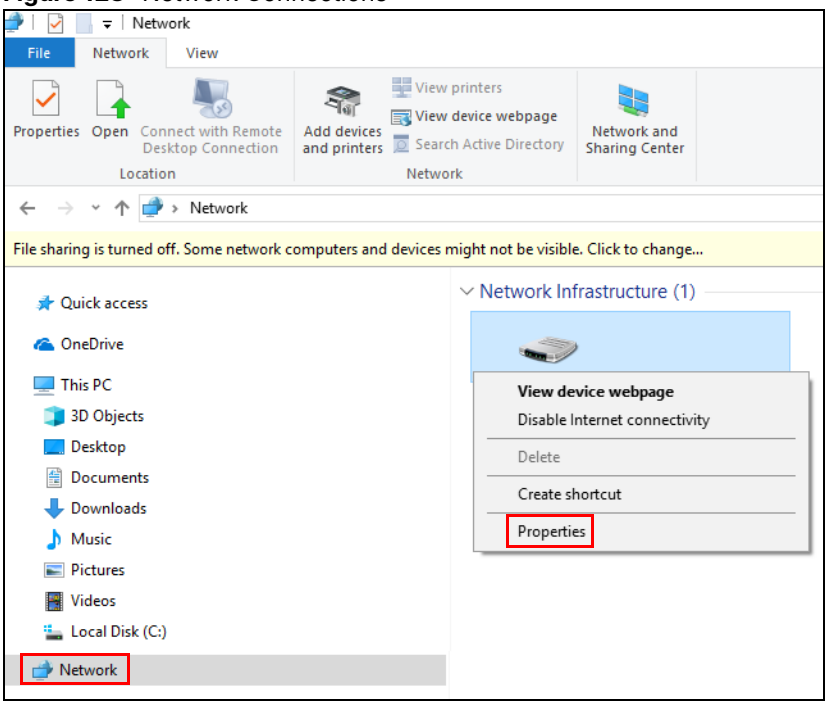
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

Make sure your computer is connected to the LAN port of the Zyxel Device.

1 Open **File Explorer** and click **Network**.

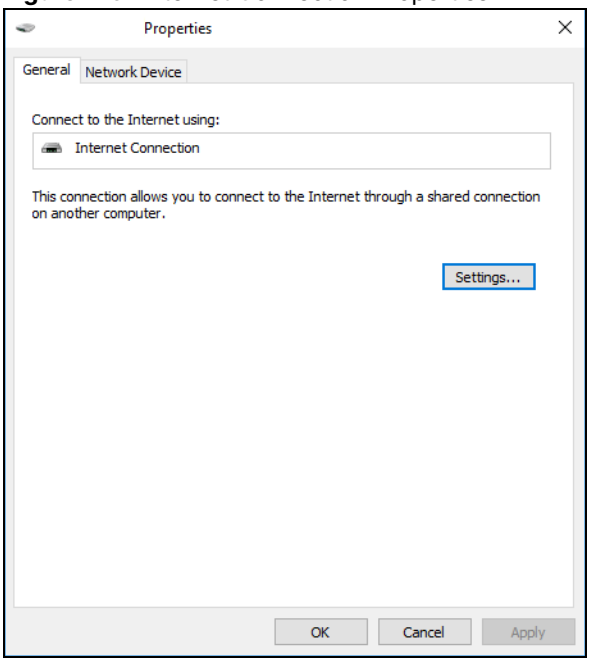
2 Right-click the Zyxel Device icon and select **Properties**.

Figure 128 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 129 Internet Connection Properties



4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 130 Internet Connection Properties: Advanced Settings

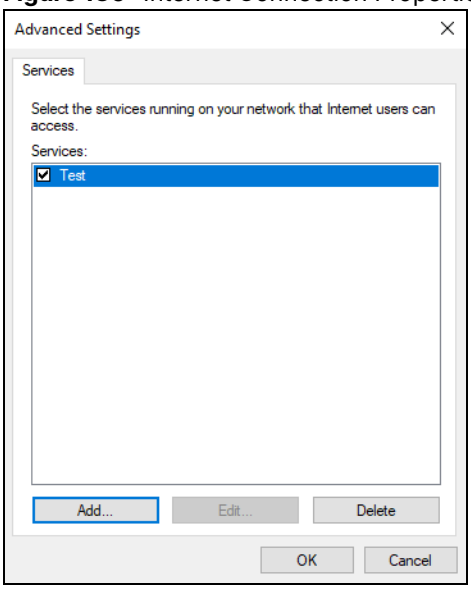
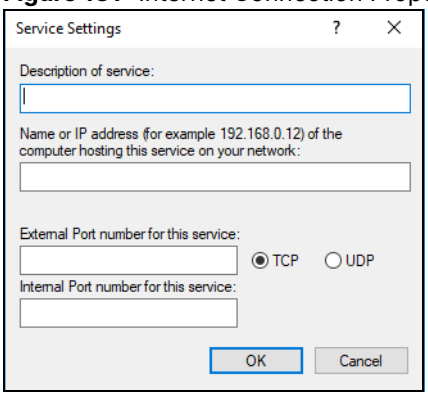


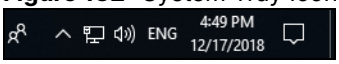
Figure 131 Internet Connection Properties: Advanced Settings: Add



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

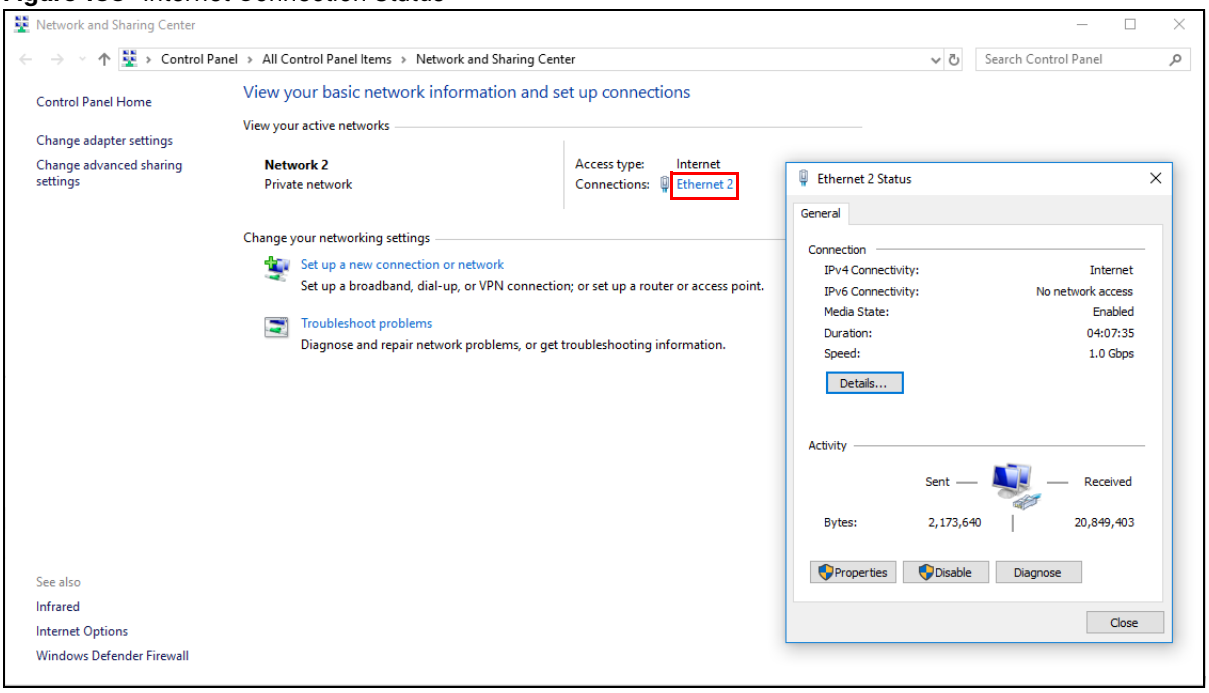
5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 132 System Tray Icon



6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 133 Internet Connection Status



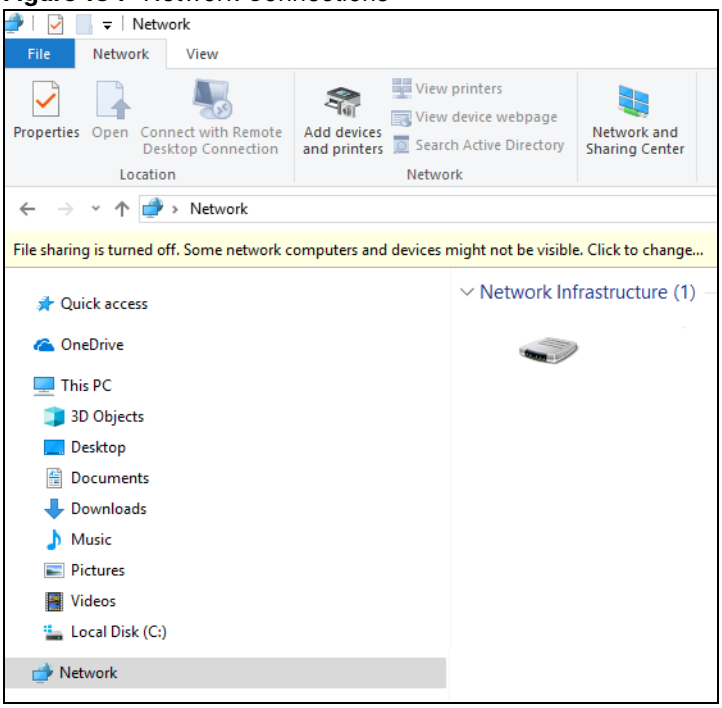
9.12 Web Configurator Access with UPnP in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

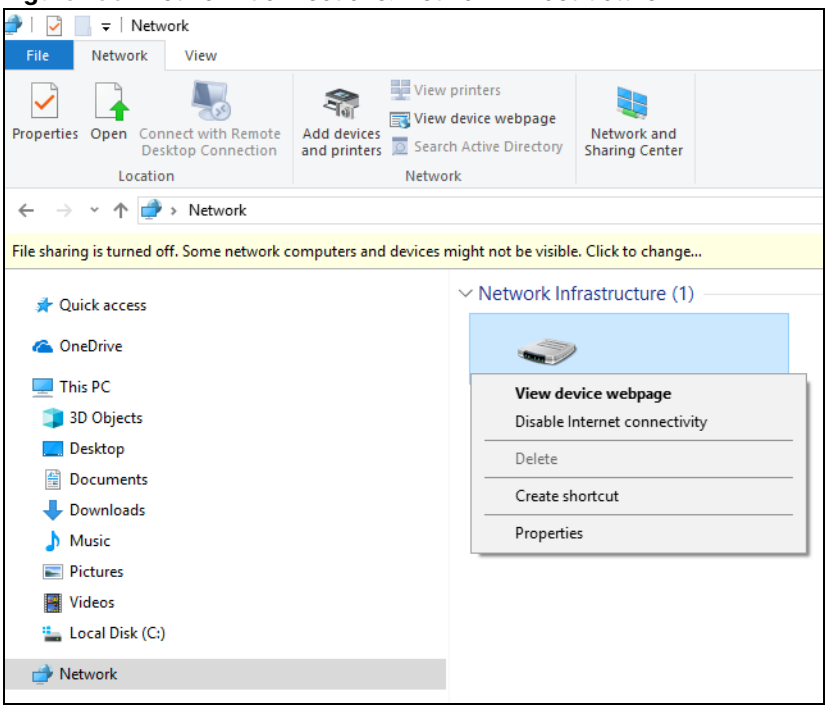
Figure 134 Network Connections



3 An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.

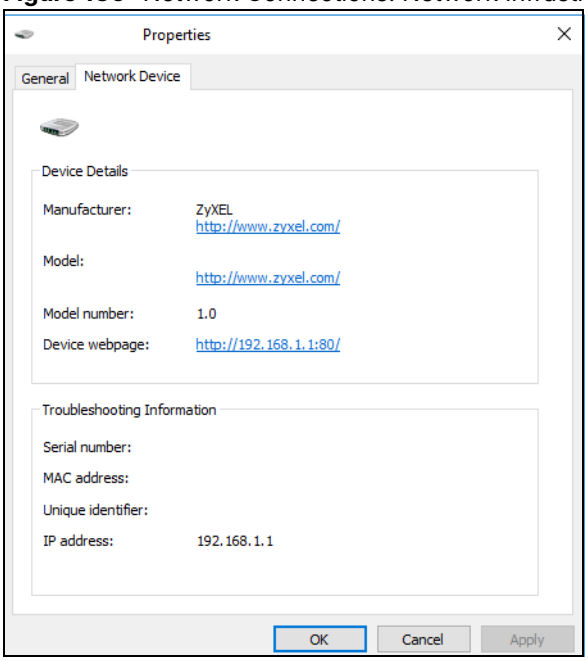
4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

Figure 135 Network Connections: Network Infrastructure



5 Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays information about the Zyxel Device.

Figure 136 Network Connections: Network Infrastructure: Properties: Example



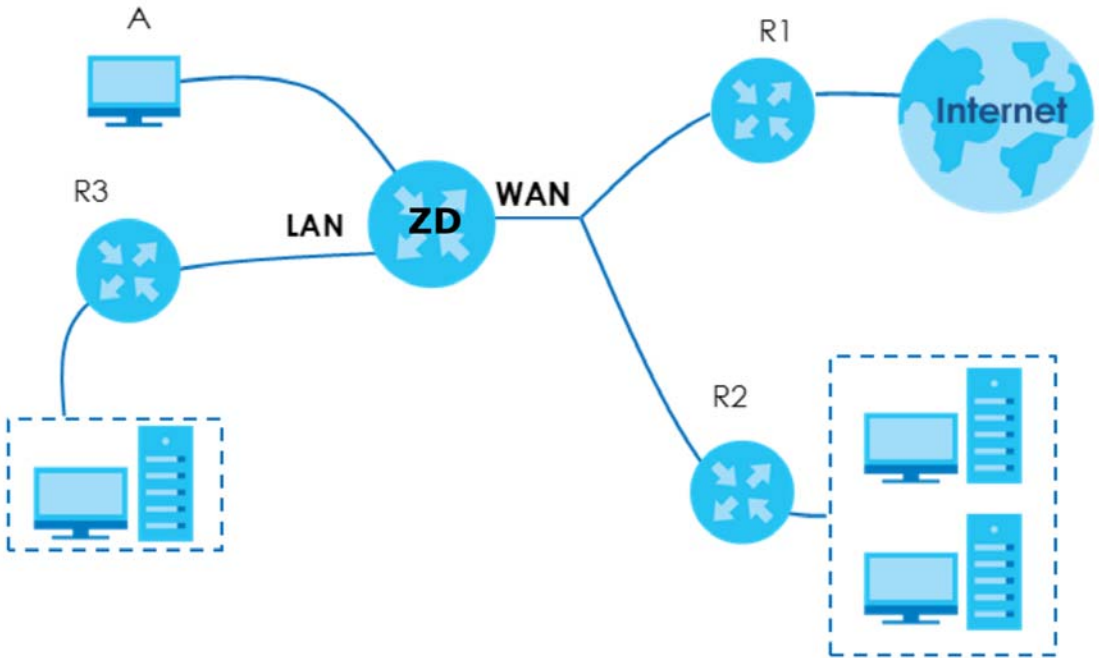
CHAPTER 10
Routing

10.1 Routing Overview

The Zyxel Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Zyxel Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Zyxel Device's LAN interface. The Zyxel Device routes most traffic from **A** to the Internet through the Zyxel Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

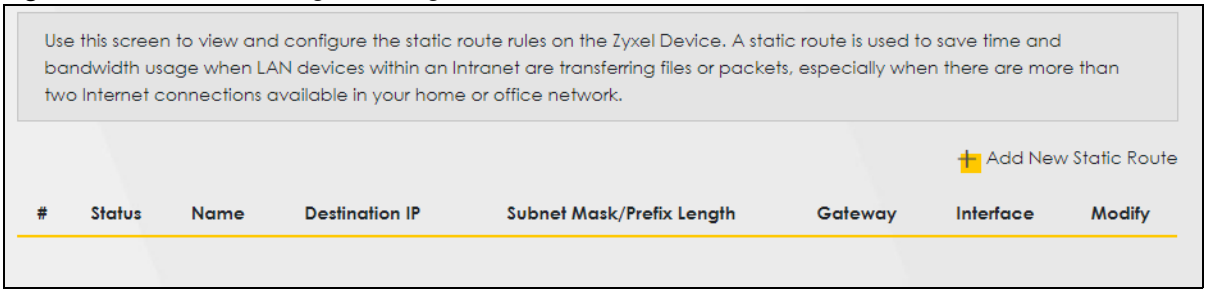
Figure 137 Example of Static Routing Topology



10.2 Configure Static Route

Use this screen to view and configure static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections in your home or office network. Click **Network Setting** > **Routing** to open the **Static Route** screen.

Figure 138 Network Setting > Routing > Static Route



The following table describes the labels in this screen.

Table 63 Network Setting > Routing > Static Route

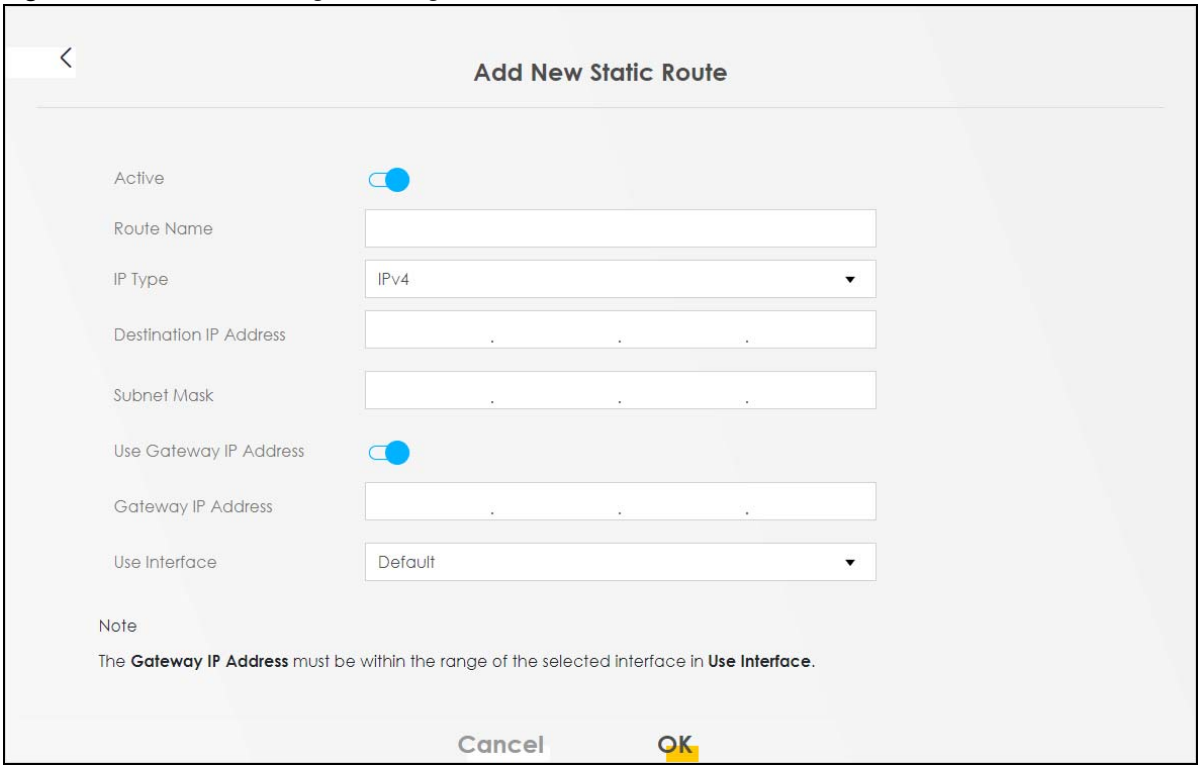
LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Zyxel Device.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This is the name of the static route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask/ Prefix Length	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the Zyxel Device. Click the **Delete** icon to remove a static route from the Zyxel Device.

10.2.1 Add or Edit Static Route

Use this screen to add or edit a static route. Click **Add New Static Route** in the **Static Route** screen, the following screen appears. Configure the required information for a static route.

Note: The **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

Figure 139 Network Setting > Routing > Static Route > Add New Static Route



The following table describes the labels in this screen.

Table 64 Network Setting > Routing > Static Route > Add New Static Route

LABEL	DESCRIPTION
Active	Click this switch to activate static route. Otherwise, click to disable.
Route Name	Enter a name for your static route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
IP Type	Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4**/**IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD).
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here. Note: This field appears only when you select **IPv4** in the **IP Type** field.
Prefix Length	If you are using IPv6, enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address. Note: This field appears only when you select **IPv6** in the **IP Type** field.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.

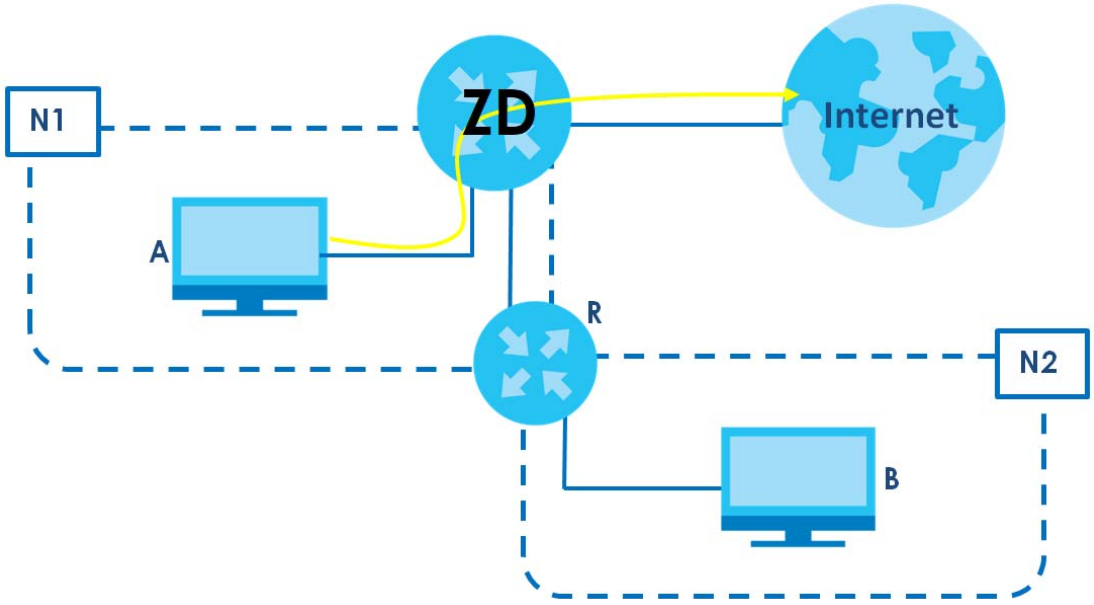
Table 64 Network Setting > Routing > Static Route > Add New Static Route (continued)

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

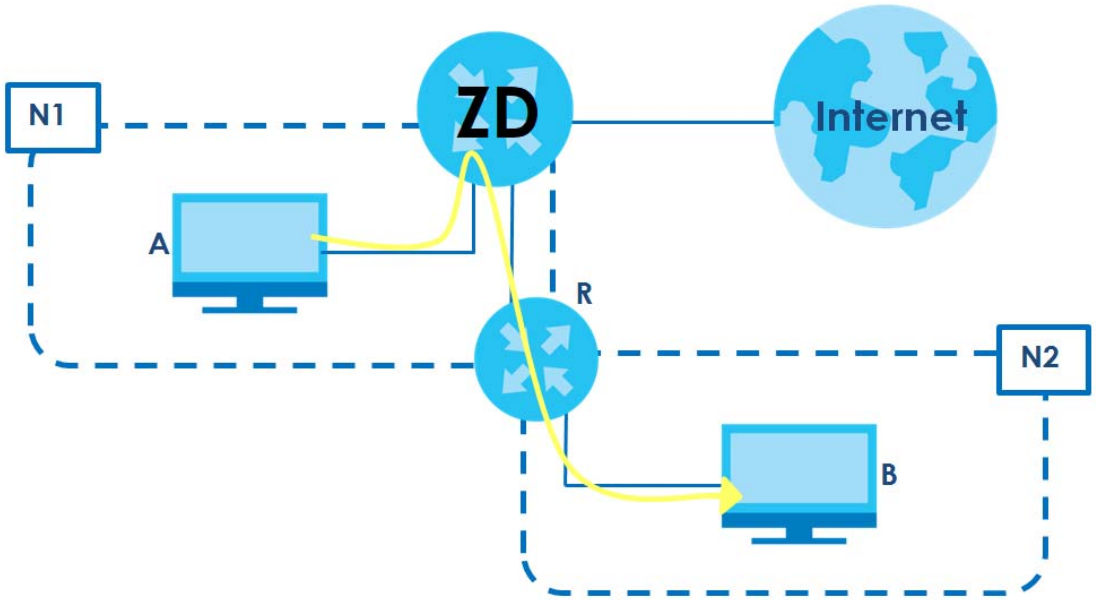
10.2.1.1 An Example of Adding a Static Route

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Zyxel Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Zyxel Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Zyxel Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Zyxel Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Zyxel Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 65 IP Settings in this Tutorial

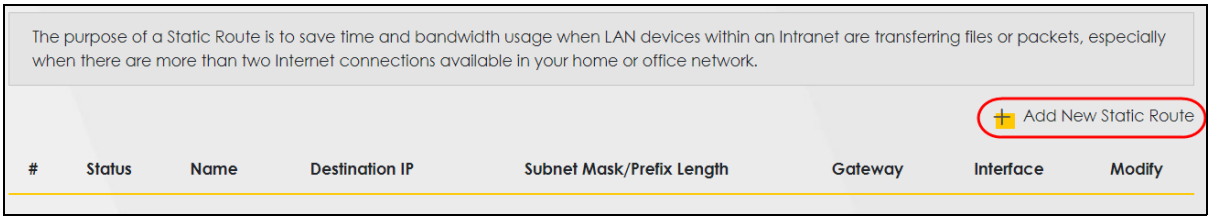
DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	
IP Type	IPv4
Use Interface	Default
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Log into the Zyxel Device's Web Configurator.

2 Click **Network Setting** > **Routing**.

3 Click **Add new Static Route** in the **Static Route** screen.

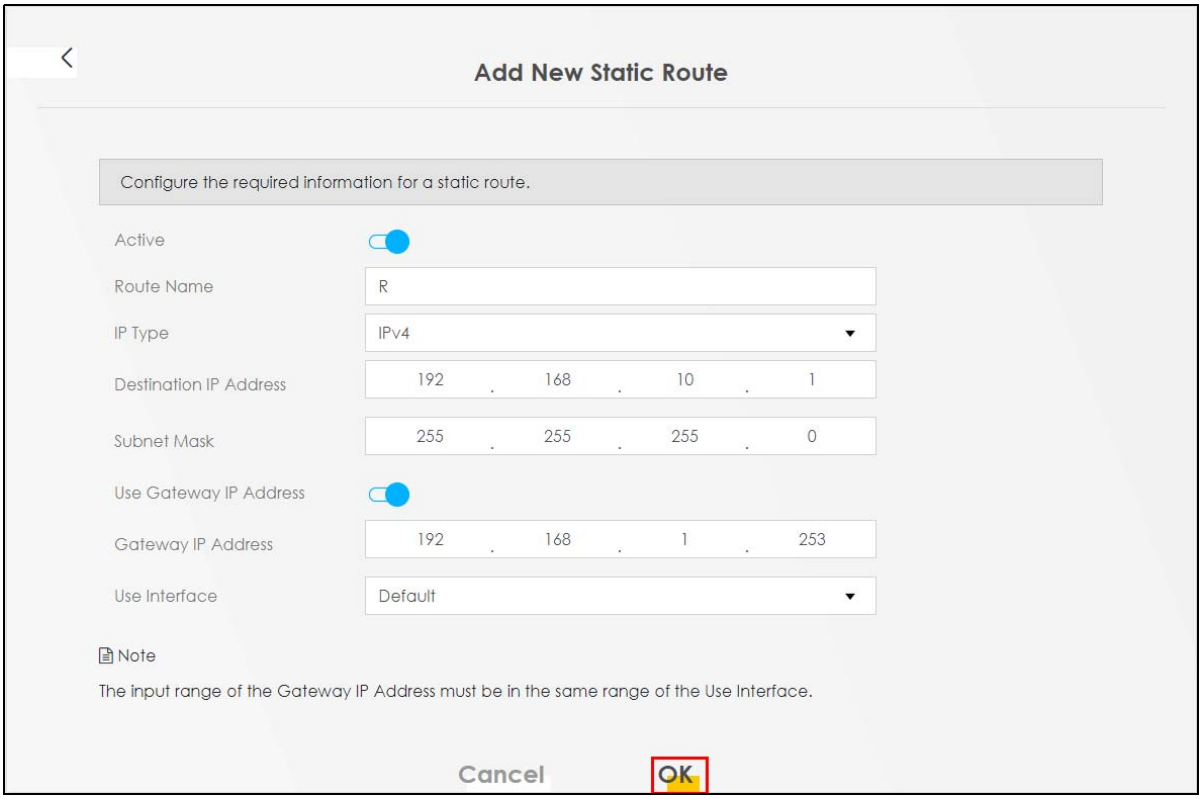


4 Configure the **Static Route Setup** screen using the following settings:

- Click the **Active** button to enable this static route. When the switch goes to the right, the function is enabled. Enter the **Route Name** as **R**.

- Set **IP Type** to **IPv4**.
- Enter the **Destination IP Address 192.168.10.1** and **IP Subnet Mask 255.255.255.0** for the destination, **N2**.
- Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right, the function is enabled. Enter **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
- Select **Default** as the **Use Interface**.
- Click **OK**.

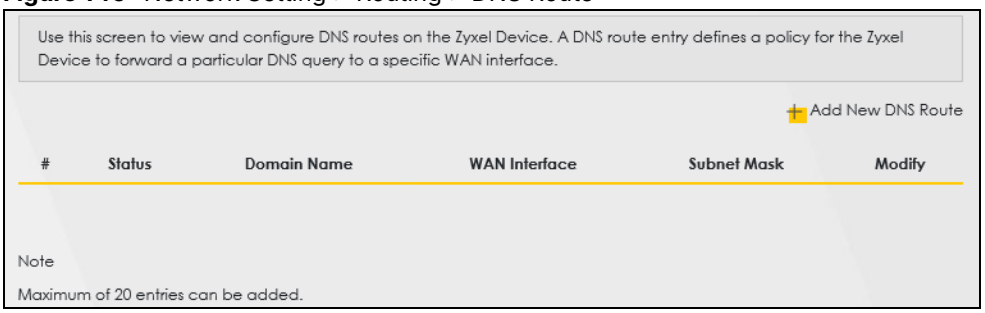
Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.



10.3 DNS Route

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface. Click **Network Setting** > **Routing** > **DNS Route** to open the **DNS Route** screen.

Figure 140 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

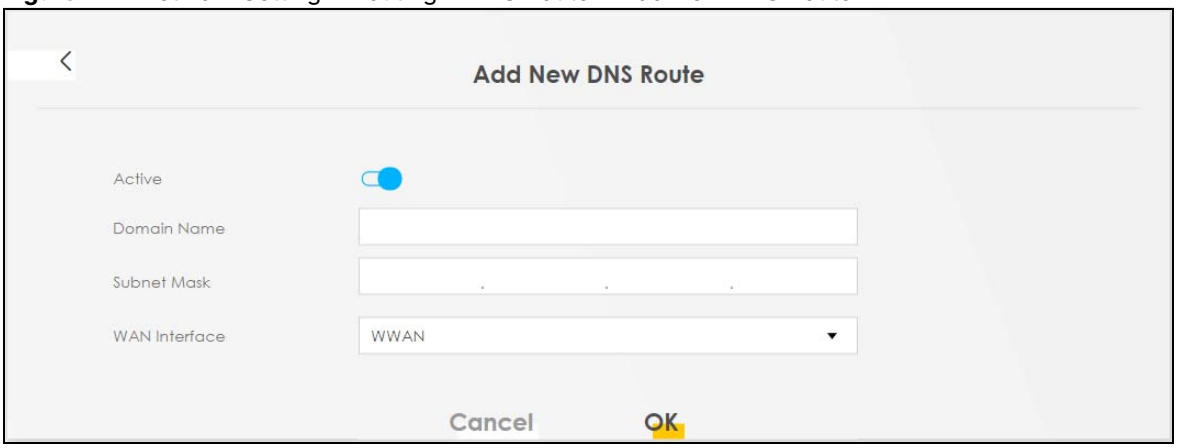
Table 66 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to create a new entry.
#	This is the number of an individual DNS route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Subnet Mask	This parameter specifies the IP network subnet mask.
Modify	Click the **Edit** icon to configure a DNS route on the Zyxel Device. Click the **Delete** icon to remove a DNS route from the Zyxel Device.

10.3.1 Add or Edit DNS Route

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **DNS Route** screen, use this screen to configure the required information for a DNS route.

Figure 141 Network Setting > Routing > DNS Route > Add New DNS Route



The following table describes the labels in this screen.

Table 67 Network Setting > Routing > DNS Route > Add New DNS Route

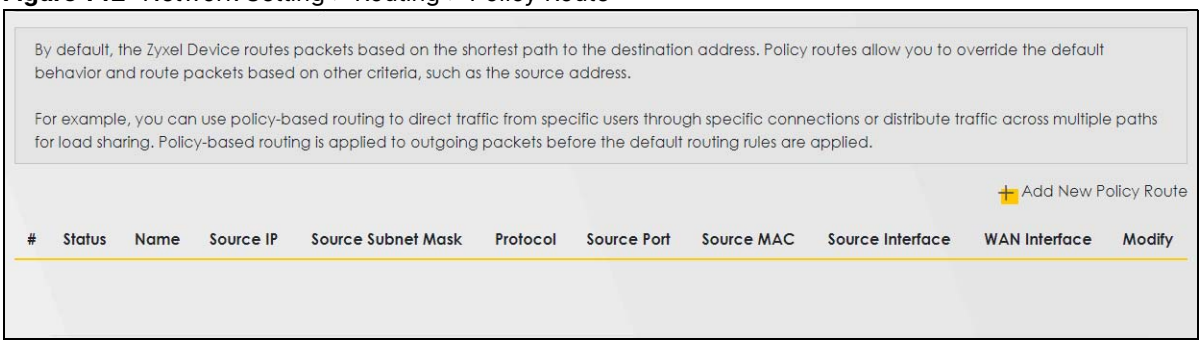
LABEL	DESCRIPTION
Active	Enable DNS route in your Zyxel Device.
Domain Name	Enter the domain name you want to resolve. You can use up to 64 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Zyxel Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
Subnet Mask	Enter the subnet mask of the network for which to use the DNS route in dotted decimal notation, for example 255.255.255.255.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interfaces already configured in the **Broadband** screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

10.4 Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address. For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.

The **Policy Route** screen let you view and configure routing policies on the Zyxel Device. Click **Network Setting** > **Routing** > **Policy Route** to open the following screen.

Figure 142 Network Setting > Routing > Policy Route



The following table describes the labels in this screen.

Table 68 Network Setting > Routing > Policy Route

LABEL	DESCRIPTION
Add New Policy Route	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.

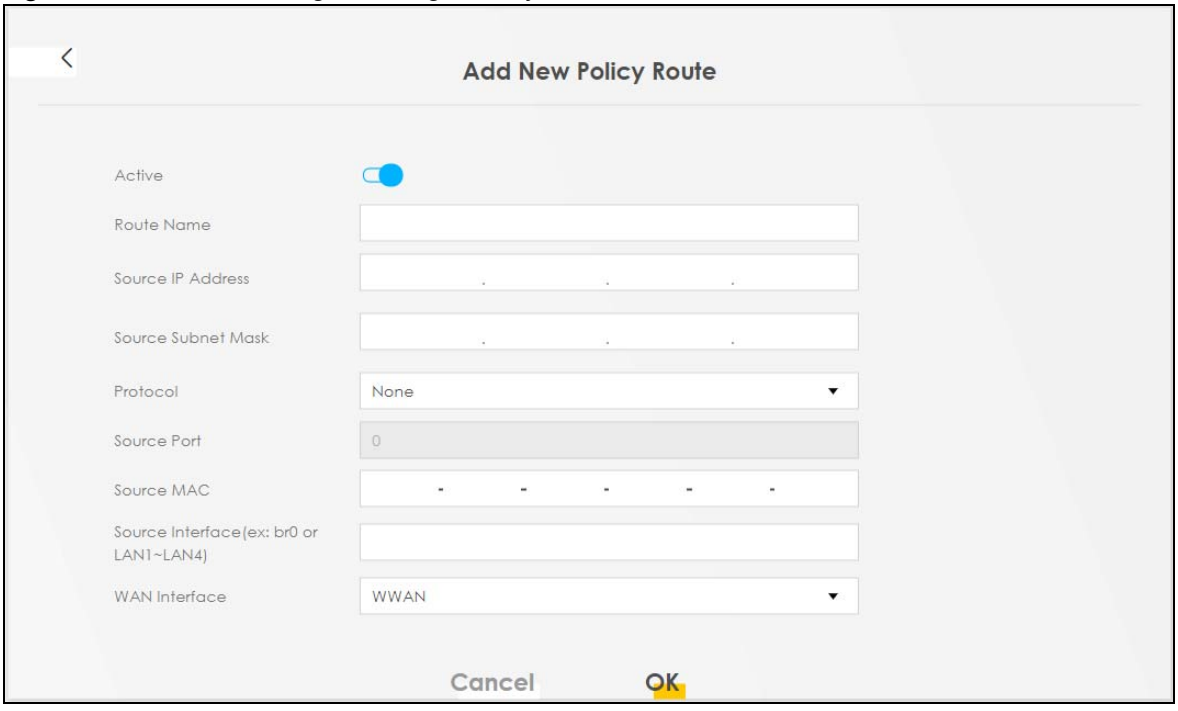
Table 68 Network Setting > Routing > Policy Route (continued)

LABEL	DESCRIPTION
Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Source MAC	This is the source MAC address.
Source Interface	This is the interface from which the matched traffic is sent.
WAN Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to edit this policy. Click the **Delete** icon to remove a policy from the Zyxel Device. A window displays asking you to confirm that you want to delete the policy.

10.4.1 Add or Edit Policy Route

Click **Add New Policy Route** in the **Policy Route** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 143 Network Setting > Routing > Policy Route: Add or Edit



The following table describes the labels in this screen.

Table 69 Network Setting > Routing > Policy Route: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this policy route. Otherwise, click to disable.
Route Name	Enter a descriptive name of this policy route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP**, **UDP, or None**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (example: br0 or LAN1 – LAN4)	Enter the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interfaces already configured in the **Broadband** screens.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

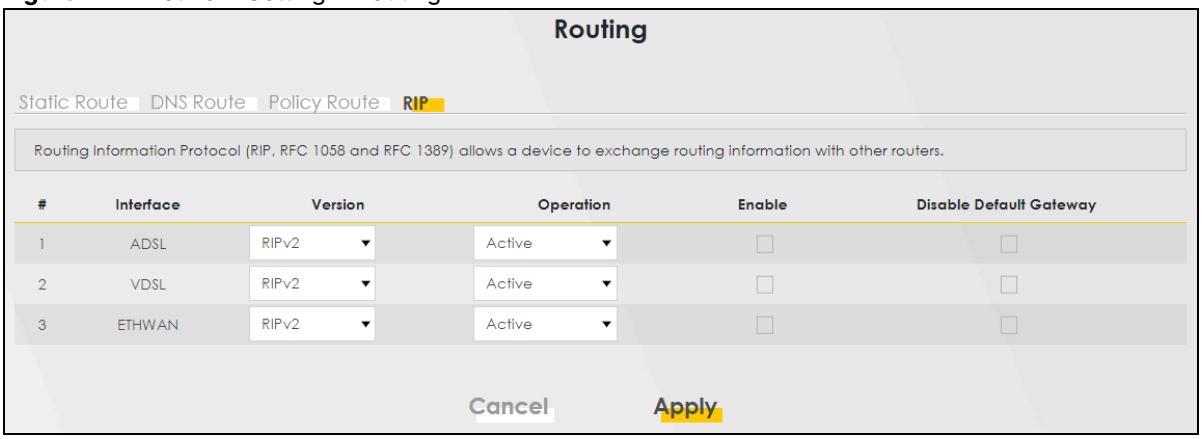
10.5 RIP Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows the Zyxel Device to exchange routing information with other routers. To activate RIP for the WAN interface, select the supported RIP version and operation.

10.5.1 RIP

Click **Network Setting** > **Routing** > **RIP** to open the **RIP** screen. Select the desired RIP version and operation by clicking the checkbox. To stop RIP on the WAN interface, clear the checkbox. Click the **Apply** button to start or stop RIP and save the configuration.

Figure 144 Network Setting > Routing > RIP



The following table describes the labels in this screen.

Table 70 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). **RIPv1** is universally supported but **RIPv2** carries more information. **RIPv1** is probably adequate for most networks, unless you have an unusual network topology. When set to **Both**, the Zyxel Device will broadcast its routing table periodically and incorporate the RIP information that it receives
Operation	Select **Passive** to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the checkbox to activate the settings.
Disable Default Gateway	Select the checkbox to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 11
Quality of Service (QoS)

11.1 QoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

Configure QoS on the Zyxel Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1 Configure classifiers to sort traffic into different flows.

2 Assign priority and define actions to be performed for a classified traffic flow.

The Zyxel Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video. There are eight priority levels, with 1 having the highest priority.

This chapter contains information about configuring QoS and editing classifiers.

11.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 11.3 on page 242).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 11.4 on page 243).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers (Section 11.5 on page 246).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface (Section 11.6 on page 251).

11.2 What You Need to Know

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

QoS versus CoS

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of

traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

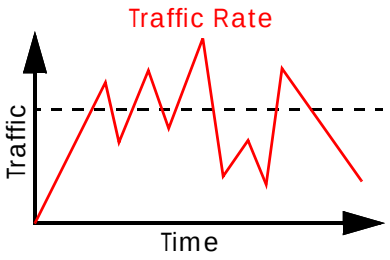
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of 3 bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

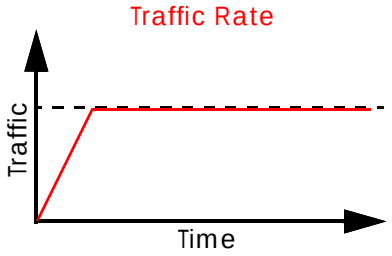
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Zyxel Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



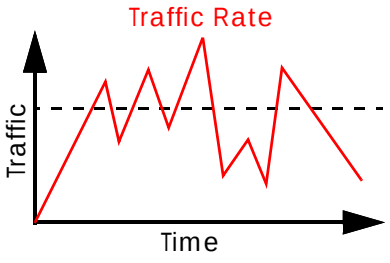
(Before Traffic Shaping)



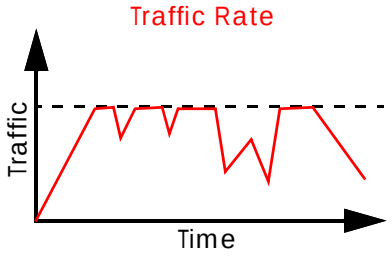
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

The Zyxel Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 11.9 on page 257 for more information on each metering algorithm.

Strictly Priority

Strictly Priority (SP) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

Weighted Round Robin Schedule (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

11.3 Quality of Service General Settings

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See Section 11.1 on page 240 for more information.

When one of the following situations happens, the current WAN linkup rate will be used instead:

1. **WAN Managed Upstream Bandwidth** is set to 0
2. **WAN Managed Upstream Bandwidth** is empty
3. **WAN Managed Upstream Bandwidth** is higher than the current WAN interface linkup rate

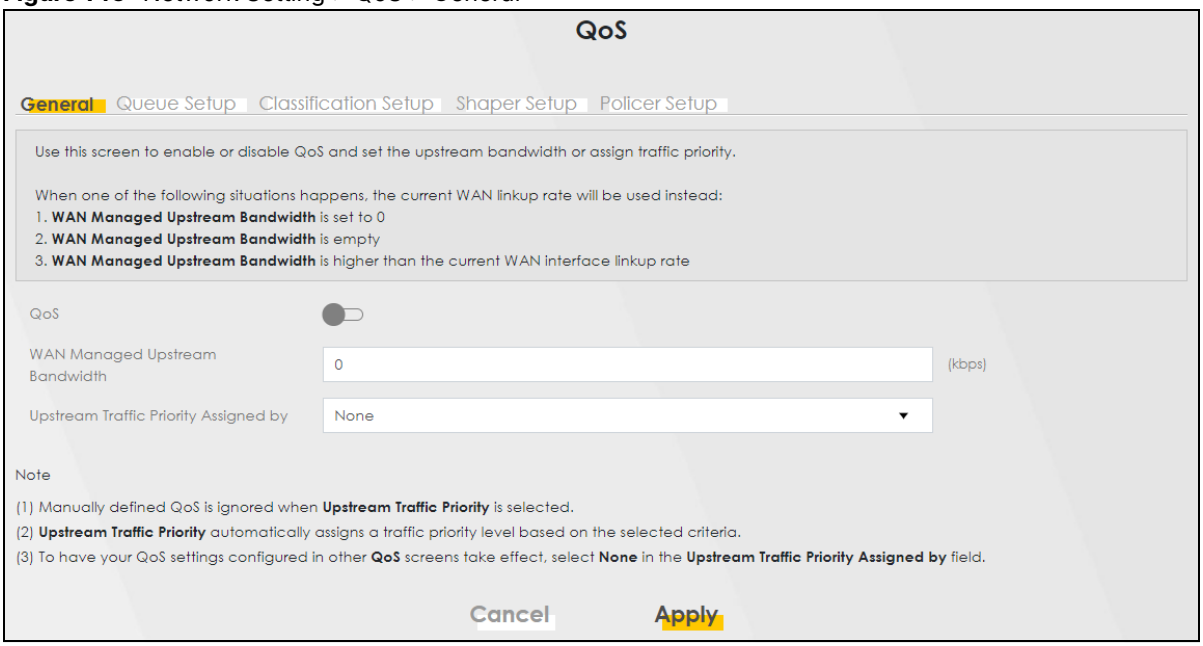
Note: Manually defined QoS is ignored when **Upstream Traffic Priority** is selected.

Note: **Upstream Traffic Priority** automatically assigns a traffic priority level based on the selected criteria.

Note: To have your QoS settings configured in other **QoS** screens take effect, select **None** in the **Upstream Traffic Priority Assigned by** field.

Click **Network Setting** > **QoS** > **General** to open the screen as shown next.

Figure 145 Network Setting > QoS > General



The following table describes the labels in this screen.

Table 71 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Click this switch to enable QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can also set this number lower than the interfaces' actual transmission speed. This will cause the Zyxel Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the Zyxel Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

11.4 Queue Setup

Click **Network Setting** > **QoS** > **Queue Setup** to open the screen as shown next.

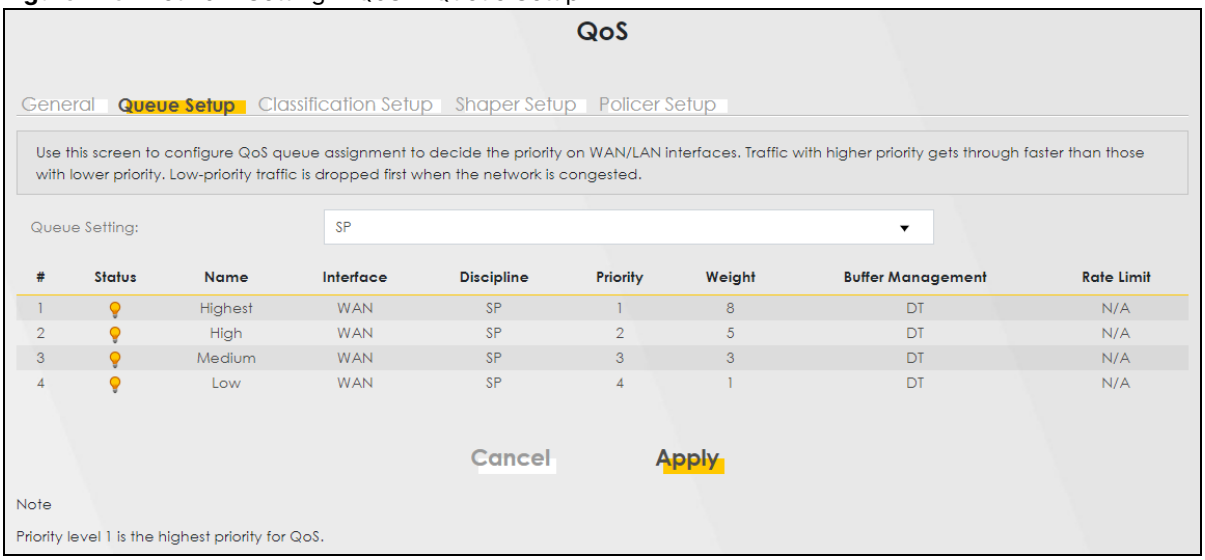
Use this screen to configure QoS queue assignment to decide the priority on WAN or LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

Note: Configure the priority level for a QoS queue from 1 to 8. The smaller the number in the **Priority** column, the higher the priority.

Note: The corresponding classifiers will be removed automatically if a queue is deleted.

Note: Rate limit 0 means there is no rate limit on a queue.

Figure 146 Network Setting > QoS > Queue Setup



The following table describes the labels in this screen.

Table 72 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Queue Setting	Select between **SP** (Strict Priority), **SP+WRR**, or **WRR** (Weighted Round Robin). **SP** scheduling singles out the highest priority queue and ensures all queued traffic in this queue is transmitted before servicing the lower priority queues. WRR scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field. Queues with larger weights get more service than queues with smaller weights. If you choose **SP+WRR**, the first and second queue will be **SP**, and the third and fourth queue will be **WRR**.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this queue passes.
Discipline	This shows the discipline of the queue. The discipline is changed according to the option chosen in **Queue Setting**. If you choose **SP**, the discipline will be SP. If you choose **SP+WRR**, the discipline of the first and second queue will be SP, and the third and fourth queue will be WRR. If you choose **WRR**, the discipline will be WRR. Strict Priority scheduling services the remaining queues using WRR. WRR scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights. Note: Queue weights can only be changed when Weighted Round Robin is selected.
Priority	This shows the priority of this queue. The lower the number, the higher the priority level.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Zyxel Device should handle packets when it receives too many (network congestion).

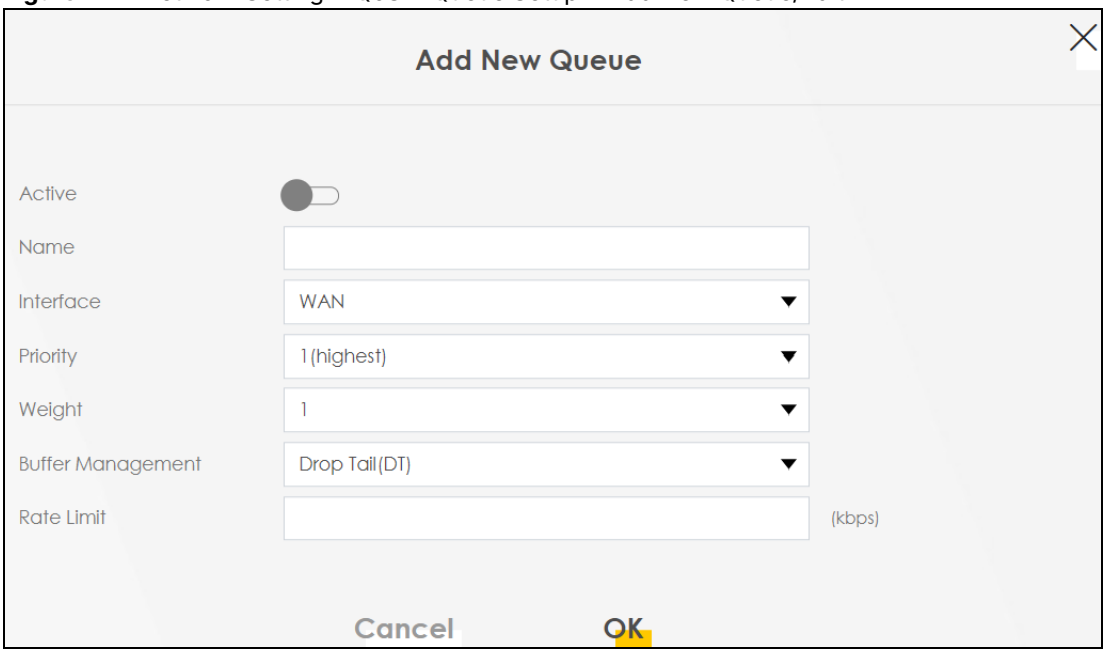
Table 72 Network Setting > QoS > Queue Setup (continued)

LABEL	DESCRIPTION
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

11.4.1 Add a QoS Queue

Click **Add New Queue** or the **Edit** icon in the **Queue Setup** screen to configure a queue.

Figure 147 Network Setting > QoS > Queue Setup > Add New Queue/Edit



The following table describes the labels in this screen.

Table 73 Network Setting > QoS > Queue Setup > Add New Queue/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable the queue.
Name	Enter a descriptive name for this queue. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 8) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Zyxel Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.

Table 73 Network Setting > QoS > Queue Setup > Add New Queue/Edit (continued)

LABEL	DESCRIPTION
Buffer Management	This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the Zyxel Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue. If you enter 0 here, this means there's no rate limit on this queue.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

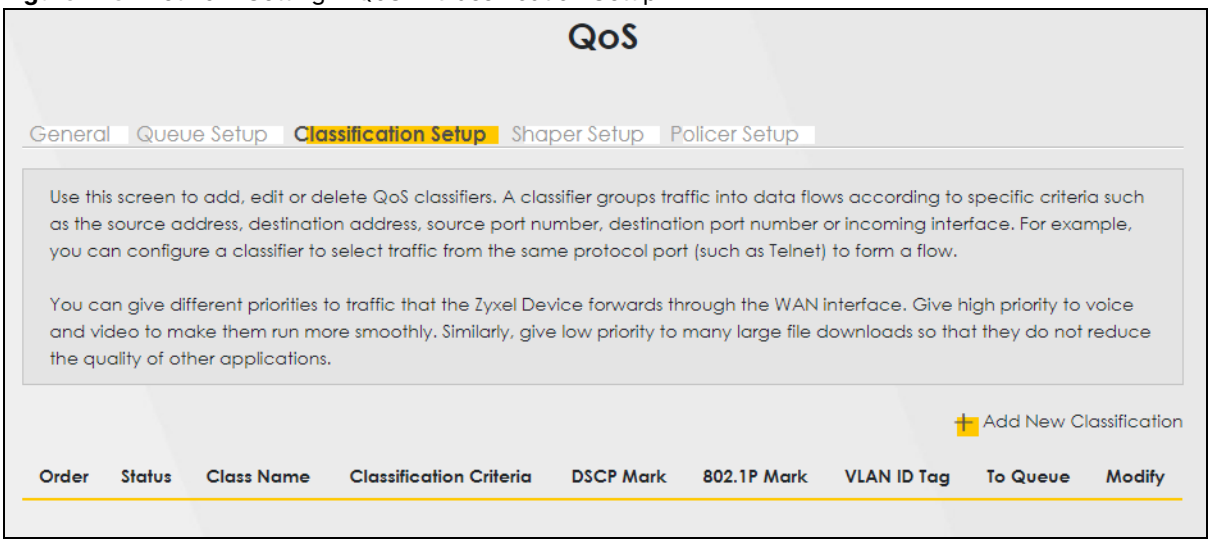
11.5 QoS Classification Setup

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Zyxel Device forwards through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting** > **QoS** > **Classification Setup** to open the following screen.

Figure 148 Network Setting > QoS > Classification Setup



The following table describes the labels in this screen.

Table 74 Network Setting > QoS > Classification Setup

LABEL	DESCRIPTION
Add New Classification	Click this to create a new classifier.
Order	This is the index number of the entry. The classifiers are applied in order of their numbering.

Table 74 Network Setting > QoS > Classification Setup (continued)

LABEL	DESCRIPTION
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

11.5.1 Add or Edit QoS Class

Click **Add New Classification** in the **Classification Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 149 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step1

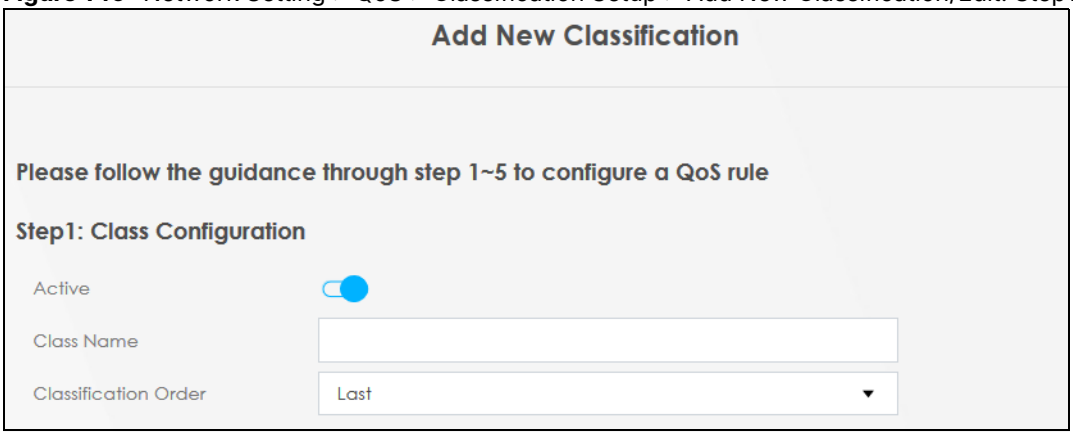


Figure 150 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step2

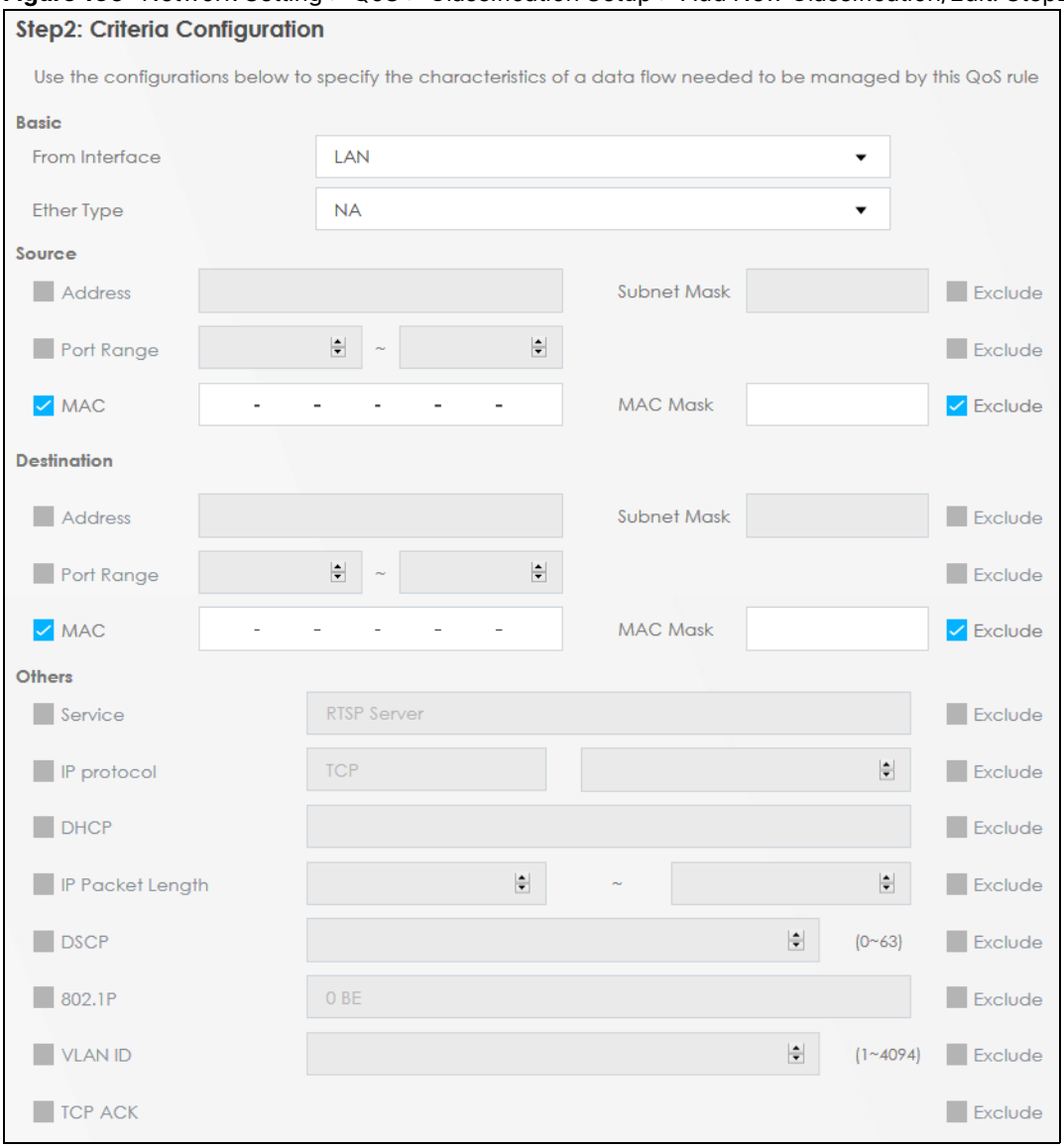


Figure 151 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step3

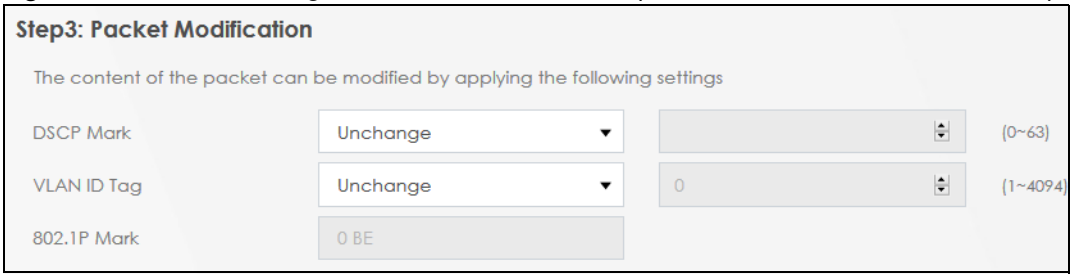


Figure 152 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step4

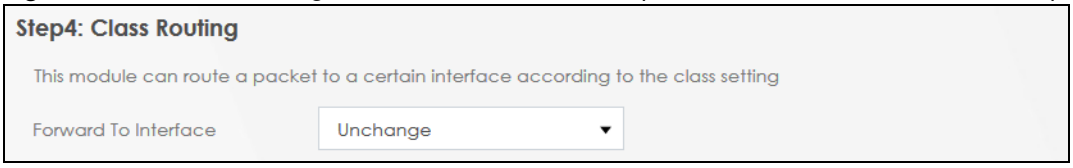
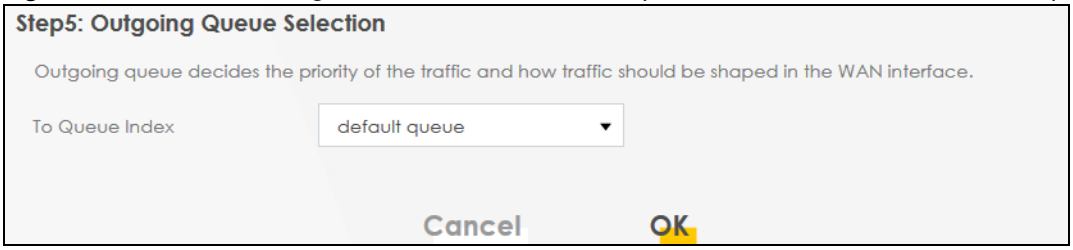


Figure 153 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step5



The following table describes the labels in this screen.

Table 75 Network Setting > QoS > Classification Setup > Add New Classification/Edit

LABEL	DESCRIPTION
Step1: Class Configuration	
Active	Click this switch to enable the classifier.
Class Name	Enter a descriptive name for this class. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Step2: Criteria Configuration	
Basic	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the **From Interface** drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. Traffic will be classified with the Ether Type of Ethernet frames. Ether Type is a field in an Ethernet frame used to identify the protocol encapsulated in the frame. Select **NA** to specify traffic that does not belong to any Ether type. If you select **IP**, you also need to configure source or destination, IP address, DHCP options, DSCP value or the protocol type. If you select **IPv6**, you also need to configure source or destination, IPv6 address, DSCP value or the protocol type. If you select **802.1Q**, you can configure an 802.1p priority level.
Source	
Address	Select the checkbox and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the checkbox and enter the port numbers of the source.
MAC	Select the checkbox and enter the source MAC address of the packet.
MAC Mask	Enter the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the checkbox and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.

Table 75 Network Setting > QoS > Classification Setup > Add New Classification/Edit (continued)

LABEL	DESCRIPTION
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the checkbox and enter the port numbers of the source.
MAC	Select the checkbox and enter the source MAC address of the packet.
MAC Mask	Enter the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **Client ID (DHCP Option 61)**, enter the Identity Association IDentifier (IAD Option 61) of the matched traffic, such as the MAC address of the device. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets. If you select **Vendor Specific Info (DHCP Option 125)**, enter the vendor specific information of the matched traffic, such as the product class, model name, and serial number of the device.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Step3: Packet Modification	
802.1P Mark	Select a priority level with which the Zyxel Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the Zyxel Device keep the 802.1p priority field in the packets.
Step4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the Zyxel Device forward traffic of this class according to the default routing table.
Step5: Outgoing Queue Selection	
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.

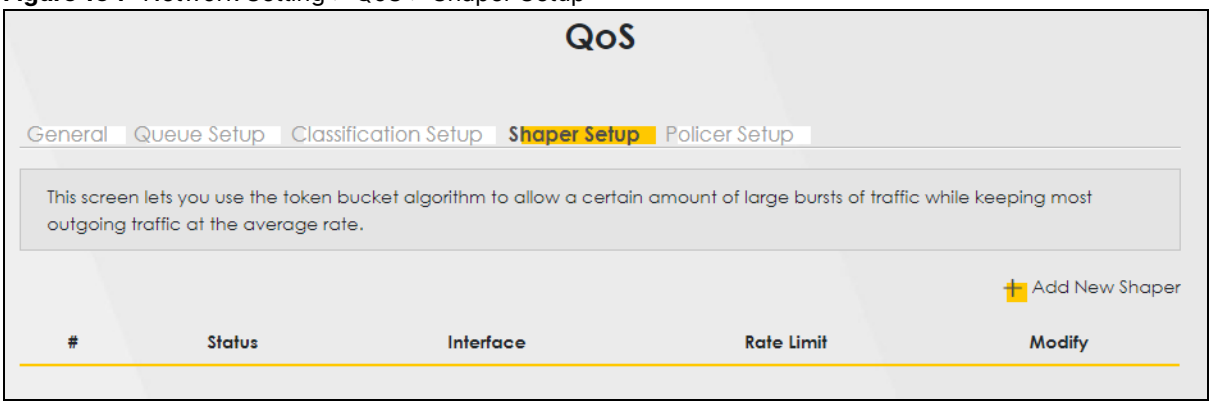
Table 75 Network Setting > QoS > Classification Setup > Add New Classification/Edit (continued)

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

11.6 QoS Shaper Setup

This screen lets you use the token bucket algorithm to allow a certain amount of large bursts of traffic while keeping most outgoing traffic at the average rate. Click **Network Setting** > **QoS** > **Shaper Setup**. The screen appears as shown.

Figure 154 Network Setting > QoS > Shaper Setup



The following table describes the labels in this screen.

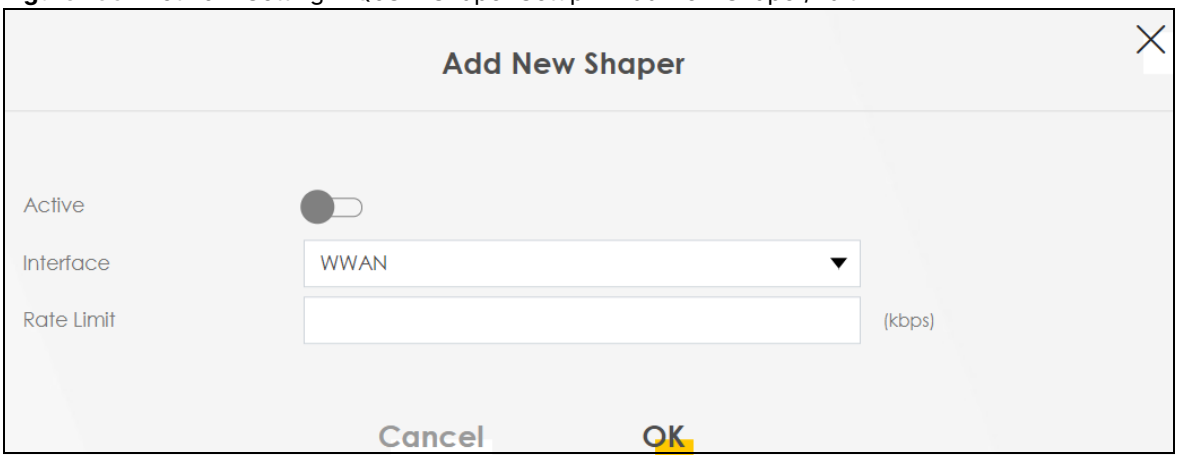
Table 76 Network Setting > QoS > Shaper Setup

LABEL	DESCRIPTION
Add New Shaper	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the shaper is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this shaper is not active.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	This shows the average rate limit of traffic bursts for this shaper.
Modify	Click the **Edit** icon to edit the shaper. Click the **Delete** icon to delete an existing shaper. Note that subsequent rules move up by one when you take this action.

11.6.1 Add or Edit a QoS Shaper

Click **Add New Shaper** in the **Shaper Setup** screen or the **Edit** icon next to a shaper to show the following screen.

Figure 155 Network Setting > QoS > Shaper Setup > Add New Shaper/Edit



The following table describes the labels in this screen.

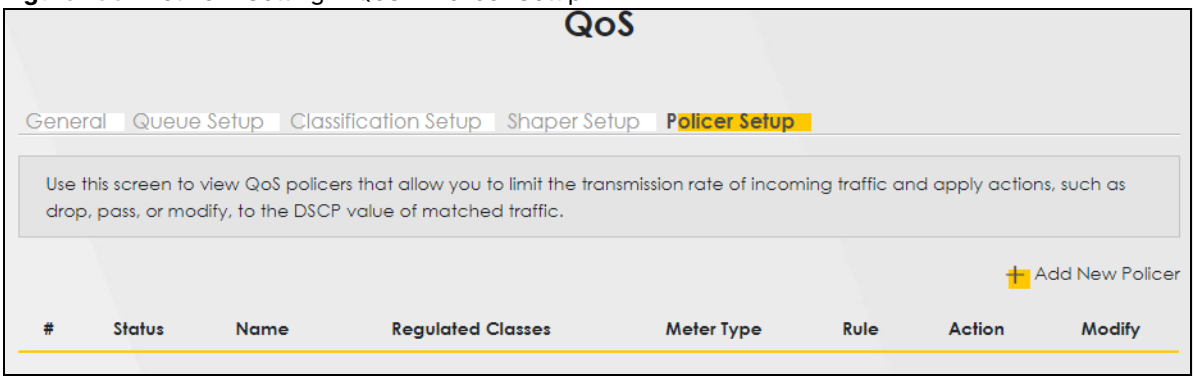
Table 77 Network Setting > QoS > Shaper Setup > Add New Shaper/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable the shaper.
Interface	Select a Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

11.7 QoS Policer Setup

Use this screen to view QoS policers that allow you to limit the transmission rate of incoming traffic and apply actions, such as drop, pass, or modify, to the DSCP value of matched traffic. Click **Network Setting** > **QoS** > **Policer Setup**. The screen appears as shown.

Figure 156 Network Setting > QoS > Policer Setup



The following table describes the labels in this screen.

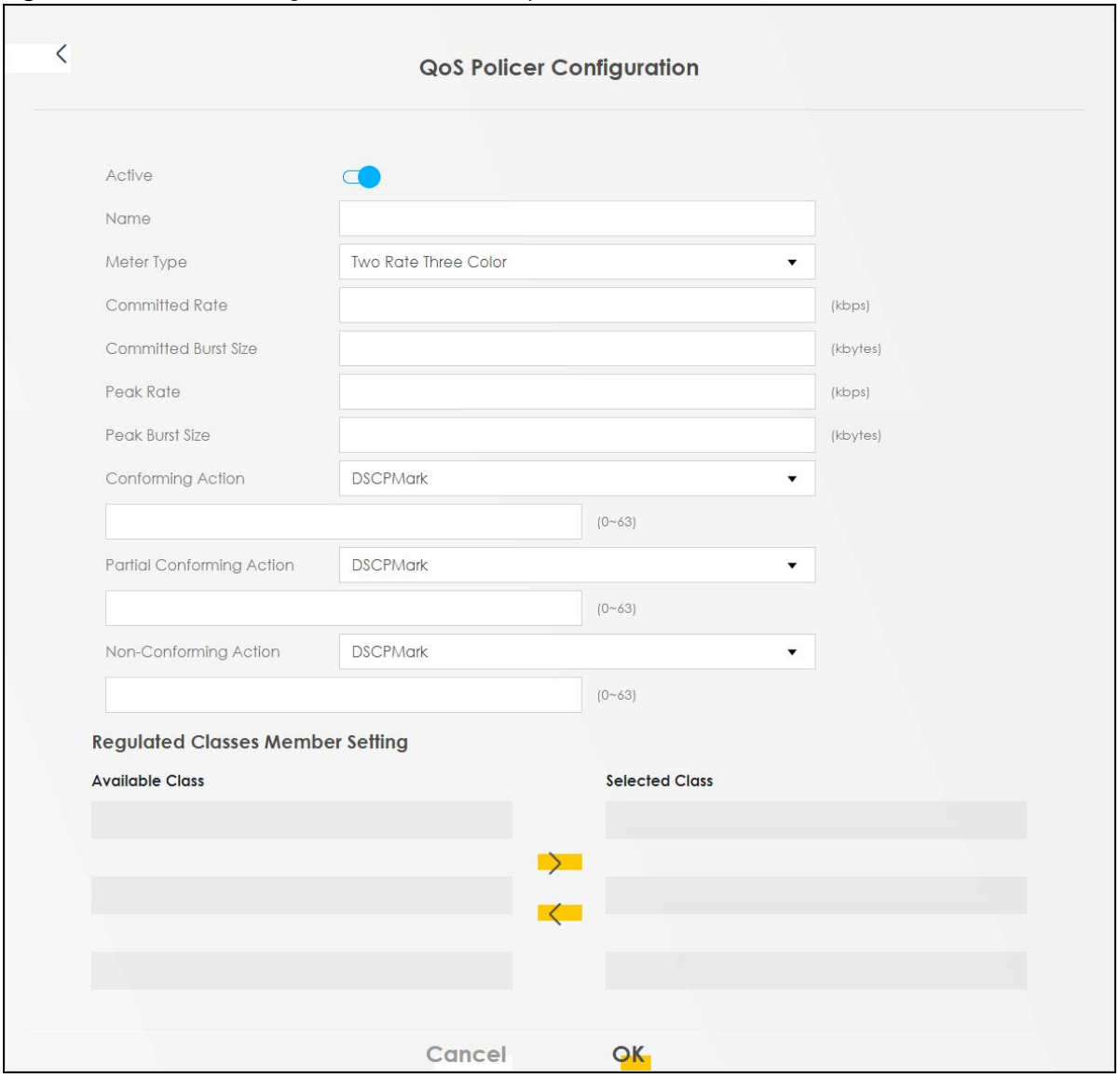
Table 78 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add New Policer	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows how the policer has the Zyxel Device treat different types of traffic belonging to the policer's member QoS classes.
Modify	Click the **Edit** icon to edit the policer. Click the **Delete** icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

11.7.1 Add or Edit a QoS Policer

Click **Add New Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 157 Network Setting > QoS > Policer Setup > Add New Policer/Edit



The following table describes the labels in this screen.

Table 79 Network Setting > QoS > Policer Setup > Add New Policer/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable the policer.
Name	Enter a descriptive name for this policer. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.

Table 79 Network Setting > QoS > Policer Setup > Add New Policer/Edit (continued)

LABEL	DESCRIPTION
Meter Type	This shows the traffic metering algorithm used in this policer. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size. The **Single Rate Three Color** Marker (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The **Two Rate Three Color** Marker (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Excess Burst Size	Specify the additional amount of bytes that are admitted at the committed rate besides the committed burst size. This is the maximum size of the second token bucket in the srTCM. This field is only available when you select **Single Rate Three Color** in the **Meter Type** field.
Peak Rate	Specify the maximum rate at which packets are admitted to the network. The peak rate should be greater than or equal to the committed rate. This is to specify how many bytes of tokens are added to the second bucket every second in the trTCM. This field is only available when you select **Two Rate Three Color** in the **Meter Type** field.
Peak Burst Size	Specify the maximum amount of bytes that are admitted at the committed rate. This is the maximum size of the second token bucket in the trTCM. This field is only available when you select **Two Rate Three Color** in the **Meter Type** field.
Conforming Action	Specify what the Zyxel Device does for packets within the committed rate and burst size (green-marked packets). • **Pass:** Send the packets without modification. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Partial Conforming Action	Specify the action that the Zyxel Device takes on yellow-marked packets. Select **Pass** to forward the packets. Select **Drop** to discard the packets. Select **DSCP Mark** to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network. This field is only available when you select **Single**/**Two Rate Three Color** in the **Meter Type** field.
Non-Conforming Action	Specify what the Zyxel Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). • **Drop:** Discard the packets. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Regulated Classes Member Setting	

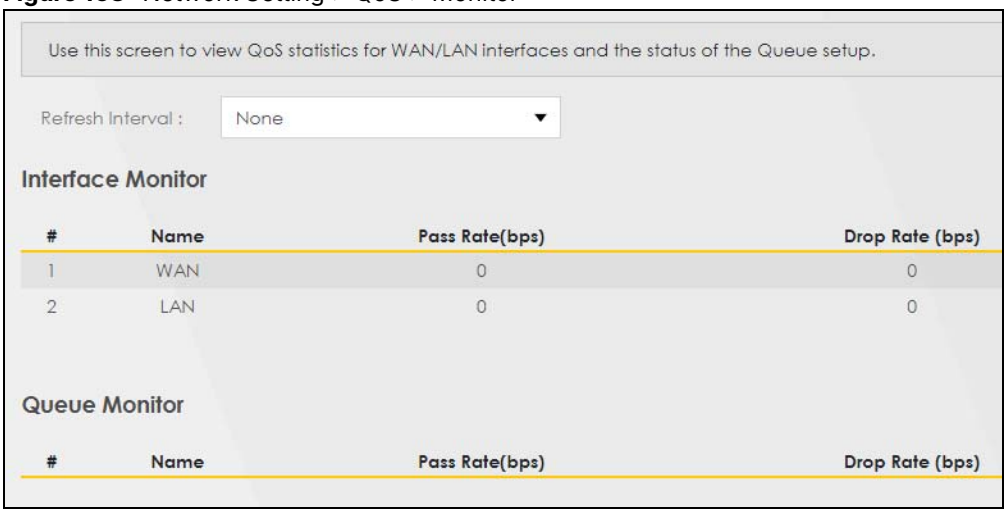
Table 79 Network Setting > QoS > Policer Setup > Add New Policer/Edit (continued)

LABEL	DESCRIPTION
Available Class Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

11.8 QoS Monitor

To view the Zyxel Device's QoS packet statistics, click **Network Setting** > **QoS** > **Monitor**. The screen appears as shown.

Figure 158 Network Setting > QoS > Monitor



The following table describes the labels in this screen.

Table 80 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Select how often you want theZyxel Device to update this screen. Select **None** to stop refreshing
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the interface on the Zyxel Device.
Pass Rate (bps)	This shows how many packets forwarded to this interface are transmitted successfully.
Drop Rate (bps)	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.

Table 80 Network Setting > QoS > Monitor (continued)

LABEL	DESCRIPTION
Pass Rate (bps)	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how many packets assigned to this queue are dropped.

11.9 Technical Reference

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

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 81 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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

DSCP and Per-Hop Behavior

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

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

DSCP (6 bits)	Unused (2 bits)

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

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the Zyxel Device, the Zyxel Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the Zyxel Device. On the Zyxel Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 82 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250 – 1100
4	4	2	010110 010100 010010 010000	

Table 82 Internal Layer2 and Layer3 QoS Mapping (continued)

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Zyxel Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Zyxel Device treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The Zyxel Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the Zyxel Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.

- If the PBS bucket has enough tokens, the Zyxel Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 12
Network Address Translation (NAT)

12.1 NAT Overview

NAT (Network Address Translation – NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

12.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the servers on your local network (Section 12.2 on page 263).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings (Section 12.3 on page 266).
- Use the **DMZ** screen to configure a default server (Section 12.4 on page 270).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 12.5 on page 270).
- Use the **Address Mapping** screen to enable and disable the NAT Address Mapping in the Zyxel Device (Section 12.6 on page 271).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section 12.7 on page 274).

12.1.2 What You Need To Know

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

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the Zyxel Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

12.2 Port Forwarding

Use **Port Forwarding** to forward incoming service requests from the Internet to the servers on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

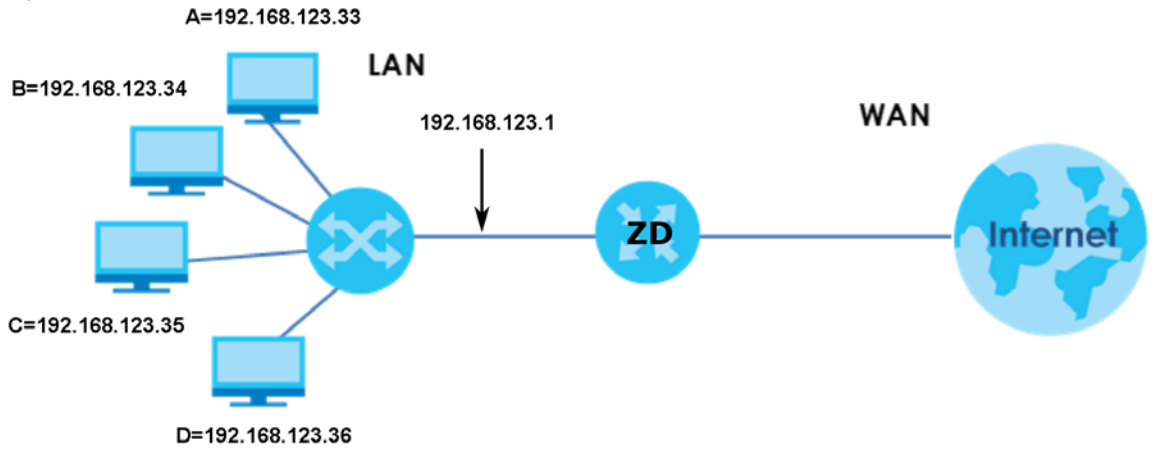
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configure Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example), a default server IP address of 192.168.1.35 to a third (**C** in the example), and a default server IP address of 192.168.1.36 to a fourth (**D** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 159 Multiple Servers Behind NAT Example

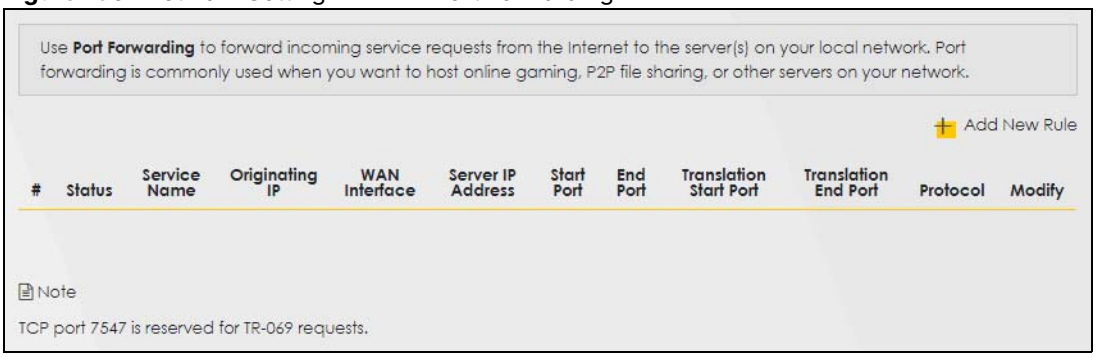


12.2.1 Port Forwarding

Click **Network Setting** > **NAT** to open the **Port Forwarding** screen.

Note: TCP port 7547 is reserved for system use.

Figure 160 Network Setting > NAT > Port Forwarding



The following table describes the fields in this screen.

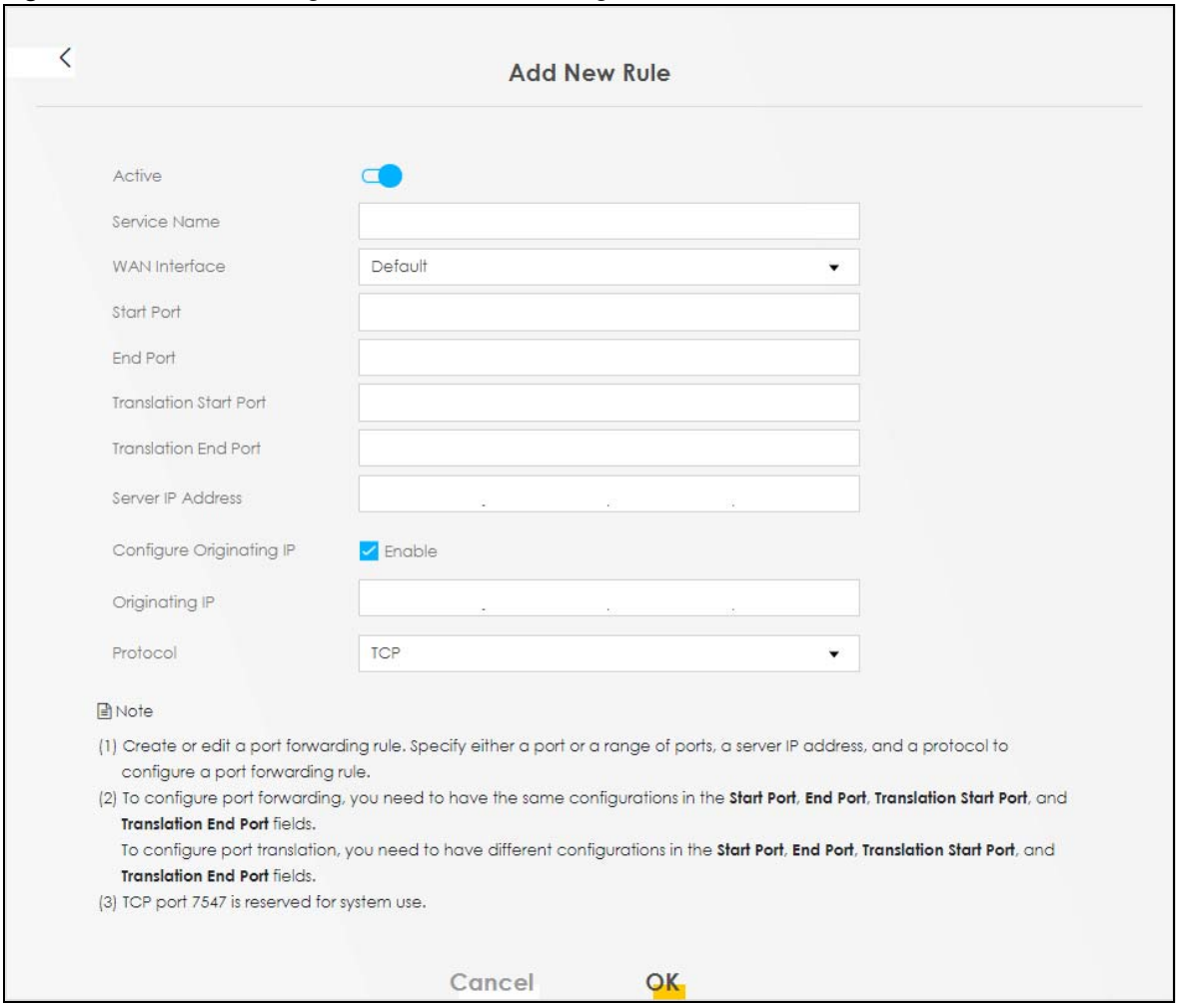
Table 83 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
Originating IP	This is the source's IP address.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP) used to transport the packets for which you want to apply the rule.
Modify	Click the **Edit** icon to edit the port forwarding rule. Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

12.2.2 Add or Edit Port Forwarding

Create or edit a port forwarding rule. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule. Click **Add New Rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 161 Network Setting > NAT > Port Forwarding: Add or Edit



Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
Here is an example to configure port translation. Configure **Start Port** to 100, **End Port** to 120, **Translation Start Port** to 200, and **Translation End Port** to 220.

Note: TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 84 Network Setting > NAT > Port Forwarding: Add or Edit

LABEL	DESCRIPTION
Active	Click to turn the port forwarding rule on or off.
Service Name	Enter a name for the service to forward. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.

Table 84 Network Setting > NAT > Port Forwarding: Add or Edit (continued)

LABEL	DESCRIPTION
Start Port	Configure this for a user-defined entry. Enter the original destination port for the packets. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Configure this for a user-defined entry. Enter the last port of the original destination port range. To forward only one port, enter the port number in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Translation Start Port	Configure this for a user-defined entry. This shows the port number to which you want the Zyxel Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	Configure this for a user-defined entry. This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Configure Originating IP	Click the **Enable** checkbox to enter the source IP in the next field.
Originating IP	Enter the source IP address here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

12.3 Port Triggering

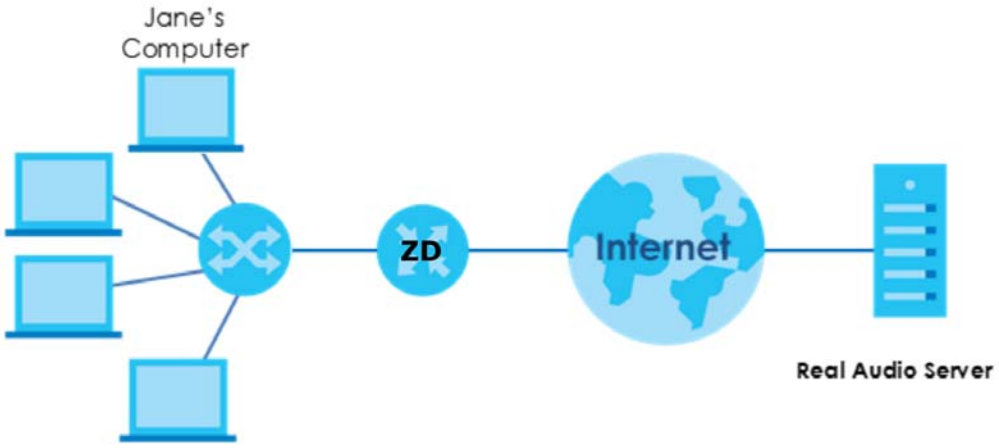
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service.

The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a \"trigger\" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol (\"open\" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 162 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a “trigger” port and causes the Zyxel Device to record Jane’s computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970 – 7170.

3 The Real Audio server responds using a port number ranging between 6970 – 7170.

4 The Zyxel Device forwards the traffic to Jane’s computer IP address.

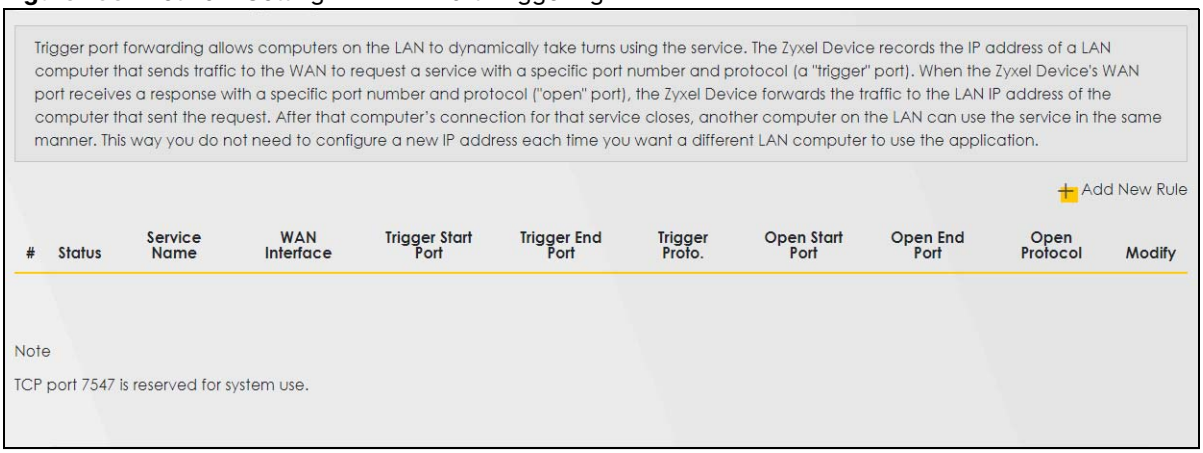
5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in 3 minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting** > **NAT** > **Port Triggering** to open the following screen. Use this screen to view your Zyxel Device’s trigger port settings.

Note: TCP port 7547 is reserved for system use.

Note: The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.

Figure 163 Network Setting > NAT > Port Triggering



The following table describes the labels in this screen.

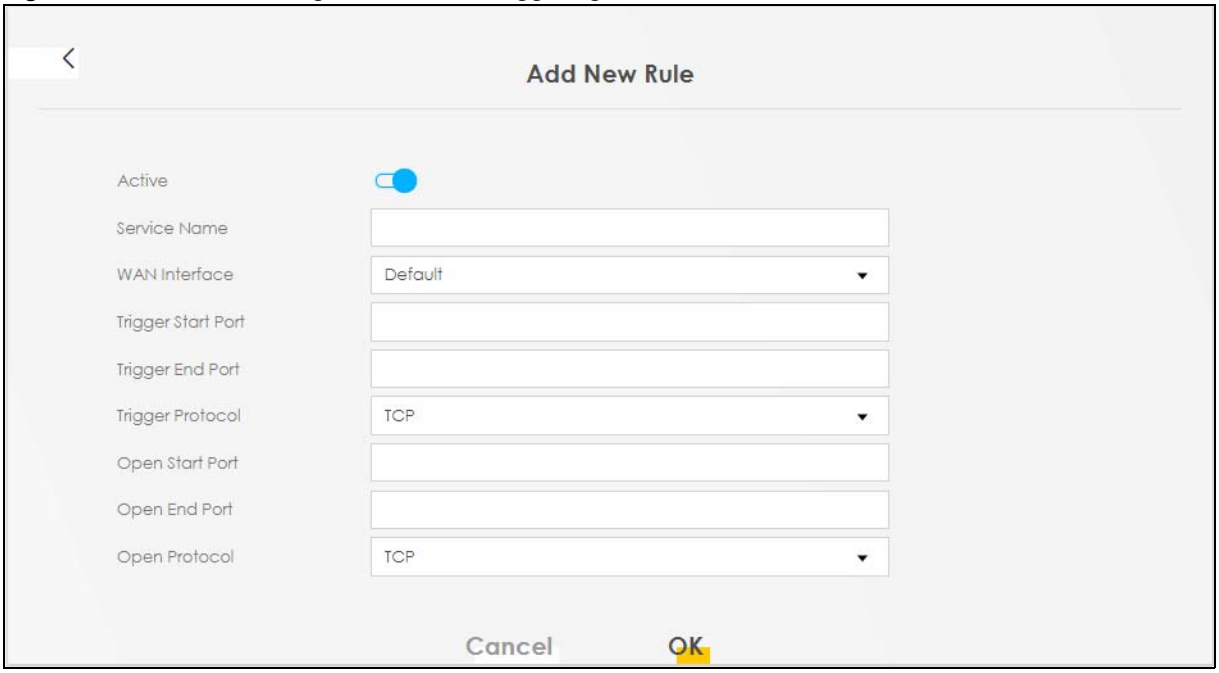
Table 85 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Protocol	This is the open transport layer protocol.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

12.3.1 Add or Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add New Rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen. Use this screen to configure a port or range of ports and protocols for sending out requests and for receiving responses.

Figure 164 Network Setting > NAT > Port Triggering: Add or Edit



The following table describes the labels in this screen.

Table 86 Network Setting > NAT > Port Triggering: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this rule.
Service Name	Enter a name to identify this rule. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter a port number or the starting port number in a range of port numbers.
Trigger End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Enter a port number or the starting port number in a range of port numbers.
Open End Port	Enter a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

12.4 DMZ

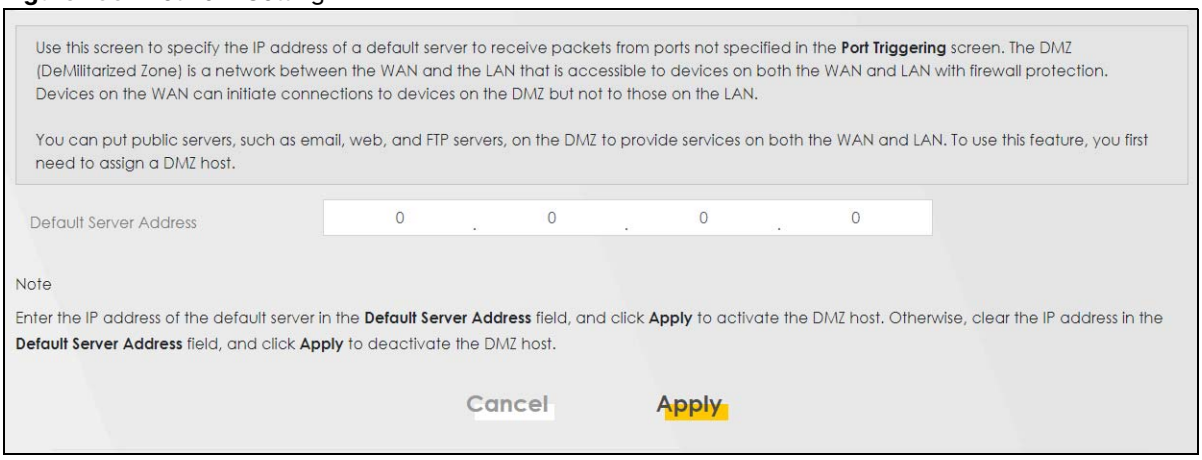
Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (DeMilitarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on the WAN can initiate connections to devices on the DMZ but not to those on the LAN.

You can put public servers, such as email and web servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host. Click **Network Setting** > **NAT** > **DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address of the default server in the **Default Server Address** field, and click **Apply** to activate the DMZ host. Otherwise, clear the IP address in the **Default Server Address** field, and click **Apply** to deactivate the DMZ host.

Figure 165 Network Setting > NAT > DMZ



The following table describes the fields in this screen.

Table 87 Network Setting > NAT > DMZ

LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **Port Forwarding** screen. Note: If you do not assign a default server, the Zyxel Device discards all packets received for ports not specified in the virtual server configuration.
Apply	Click this to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

12.5 ALG

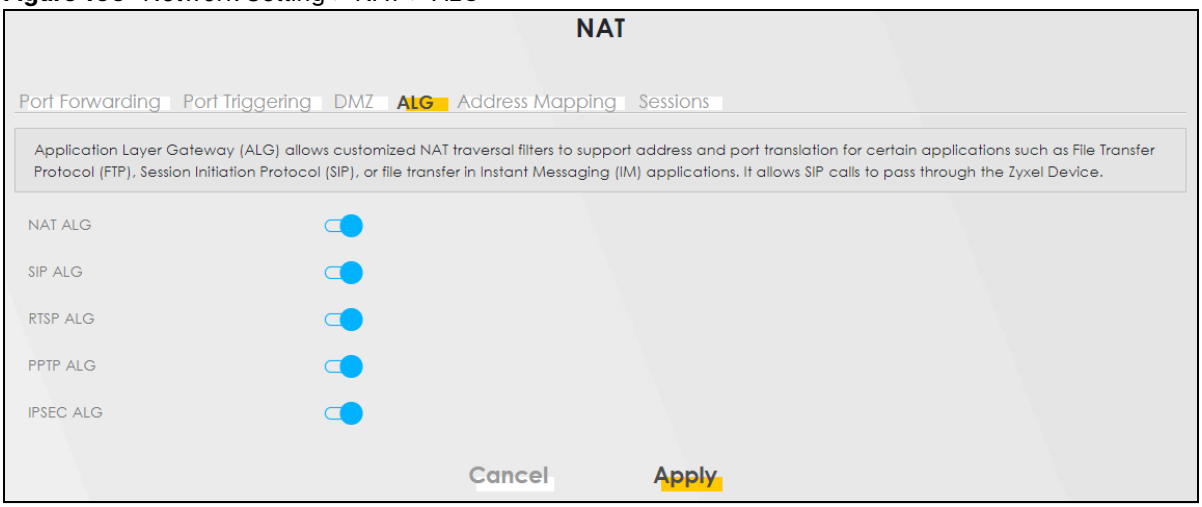
Application Layer Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain applications such as Session Initiation Protocol (SIP) or file transfer in Instant Messaging (IM) applications. It allows SIP calls to pass through the Zyxel Device. When the Zyxel Device

registers with the SIP register server, the SIP ALG translates the Zyxel Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Zyxel Device is behind a SIP ALG.

Click **Network Setting** > **NAT** > **ALG** to open the **ALG** screen. Use this screen to enable and disable the NAT Application Layer Gateway (ALG) in the Zyxel Device.

Application Layer Gateway (ALG) allows certain applications such as Session Initiation Protocol (SIP) or file transfer in Instant Messaging (IM) applications to pass through the Zyxel Device.

Figure 166 Network Setting > NAT > ALG



The following table describes the fields in this screen.

Table 88 Network Setting > NAT > ALG

LABEL	DESCRIPTION
SIP ALG	Click this switch to enable SIP ALG to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
PPTP ALG	Click this switch to enable the PPTP ALG on the Zyxel Device to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

12.6 Address Mapping

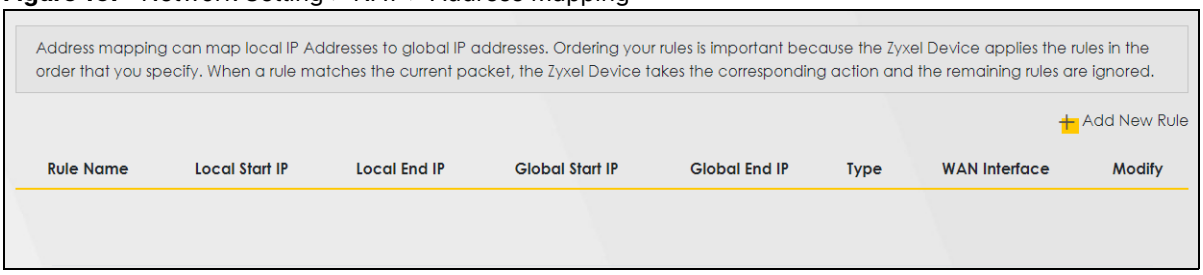
Address mapping can map local IP Addresses to global IP addresses. Ordering your rules is important because the Zyxel Device applies the rules in the order that you specify. When a rule matches the current packet, the Zyxel Device takes the corresponding action and the remaining rules are ignored.

Use this screen to enable or disable the NAT Address Mapping in the Zyxel Device.

12.6.1 Address Mapping Screen

Click **Network Setting** > **NAT** > **Address Mapping** to open the **Address Mapping** screen.

Figure 167 Network Setting > NAT > Address Mapping



The following table describes the fields in this screen.

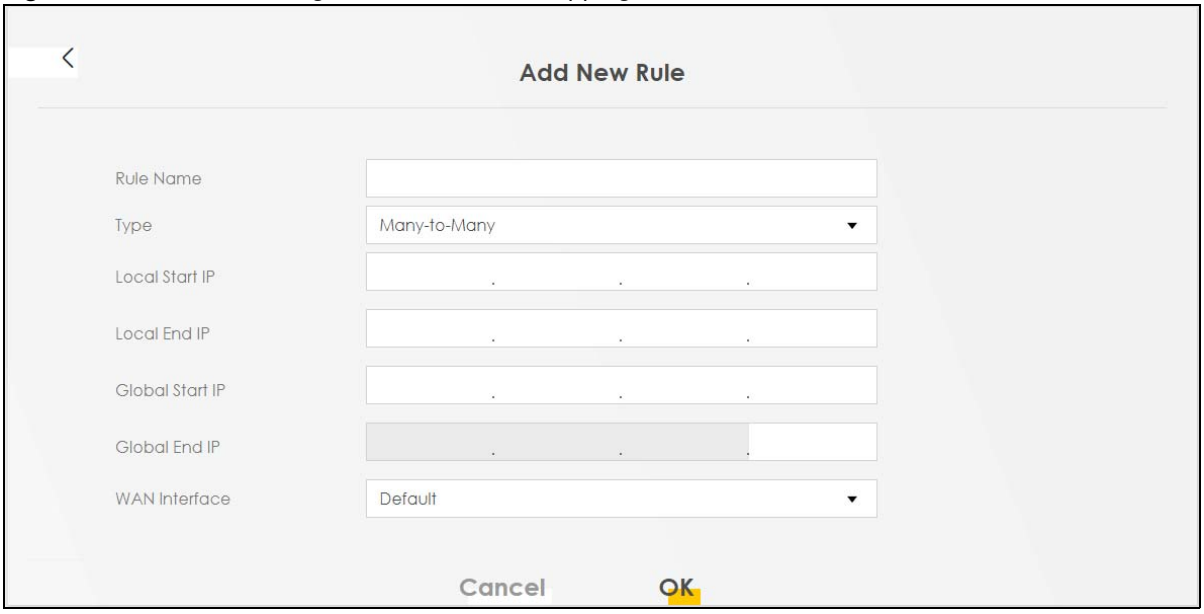
Table 89 Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
Rule Name	This is the name of the rule.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
Type	This is the address mapping type. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
WAN Interface	This is the WAN interface to which the address mapping rule applies.
Modify	Click the **Edit** icon to go to the screen where you can edit the address mapping rule. Click the **Delete** icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

12.6.2 Add New Rule Screen

To add or edit an address mapping rule, click **Add New Rule** or the **Modify** icon in the **Address Mapping** screen to display the screen shown next.

Figure 168 Network Setting > NAT > Address Mapping > Add New Rule



The following table describes the fields in this screen.

Table 90 Network Setting > NAT > Address Mapping > Add New Rule

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name for this rule. You can use up to 20 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Type	Choose the IP or port mapping type from one of the following. **One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
WAN Interface	Select a WAN interface to which the address mapping rule applies.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

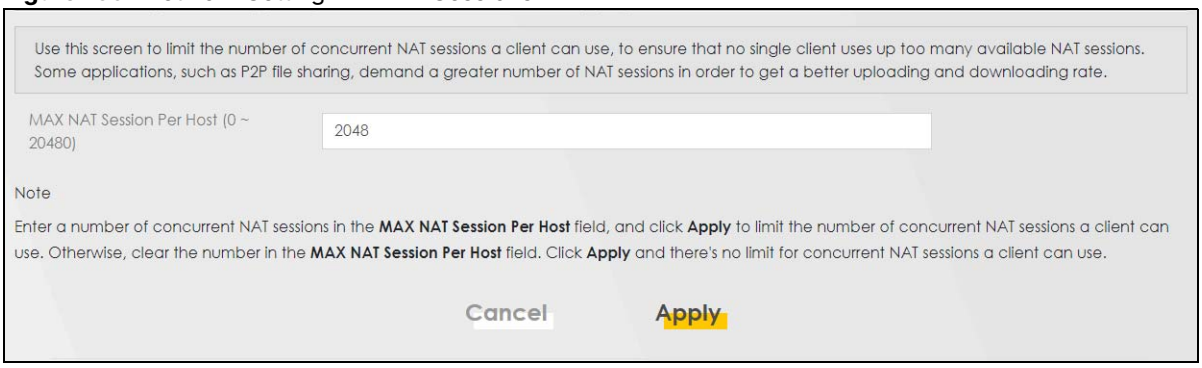
12.7 Sessions

Use this screen to limit the number of concurrent NAT sessions a client can use, to ensure that no single client uses up too many available NAT sessions. Some applications, such as P2P file sharing, demand a greater number of NAT sessions in order to get a better uploading and downloading rate. Click **Network Setting** > **NAT** > **Sessions** to display the following screen.

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use. Click **Network Setting** > **NAT** > **Sessions** to open the **Sessions** screen.

Note: Enter a number of concurrent NAT sessions in the **MAX NAT Session Per Host** field, and click **Apply** to limit the number of concurrent NAT sessions a client can use. Otherwise, clear the number in the **MAX NAT Session Per Host** field. Click **Apply** and there is no limit for concurrent NAT sessions a client can use.

Figure 169 Network Setting > NAT > Sessions



The following table describes the fields in this screen.

Table 91 Network Setting > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Session Per Host	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

12.8 Port Control Protocol (PCP)

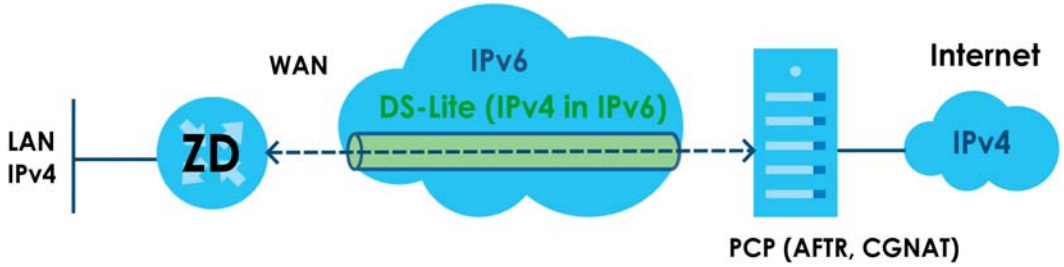
Use this screen to view, add, or delete PCP rules. Port Control Protocol (PCP) allows devices such as web or file sharing servers behind the Zyxel Device to receive incoming traffic.

Example Applications

- Some remote access applications, such as remote desktop or SSH, require incoming traffic to be routed to the user's device in order to establish a remote connection. Use PCP to dynamically map incoming traffic to the user's device, allowing them to establish remote connections.

The PCP server allows dynamic mapping of external ports to internal IP addresses and ports. PCP allows devices to request and release mappings for specific ports, and to specify the lifetime of those mappings. This allows devices to dynamically open and close ports just as needed, and does not need keepalive packets that can drain battery life of home devices such as smartphones.

In the following figure, the Zyxel Device is the PCP client. DS-Lite tunnels IPv4 packets over an IPv6 network to an AFTR (Address Family Transition Router) and Carrier-Grade NAT (CGNAT) which includes the PCP server, then sends traffic to its external IPv4 network. The Port Control Protocol with DS Lite allows you to create PCP mapping rules with the PCP server.



Requirement

You must enable DS Lite (Dual-Stack Lite) in **Network Setting** > **Broadband** > **Edit WAN Interface** to use PCP.

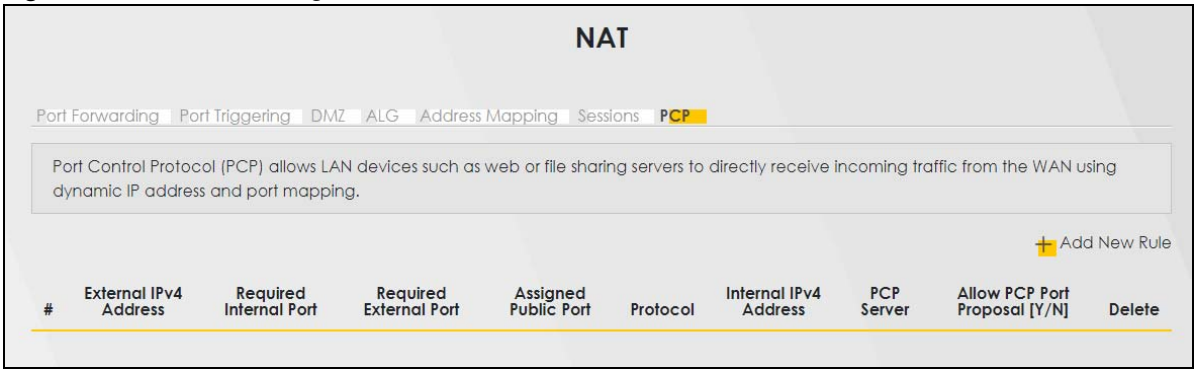
- If you select **Automatically configured by DHCPC**, then the IP address of the PCP server is in assigned to the Zyxel Device using DCHP Option 64.

- If you select **Manually Configured**, then you must enter the IPv6 address of the PCP server in the **DS-Lite Relay server IP** field.

Configuring PCP

Click **Network Setting** > **NAT** > **PCP** to display the following screen.

Figure 170 Network Setting > NAT > PCP



The following table describes the fields in this screen.

Table 92 Network Setting > NAT > PCP

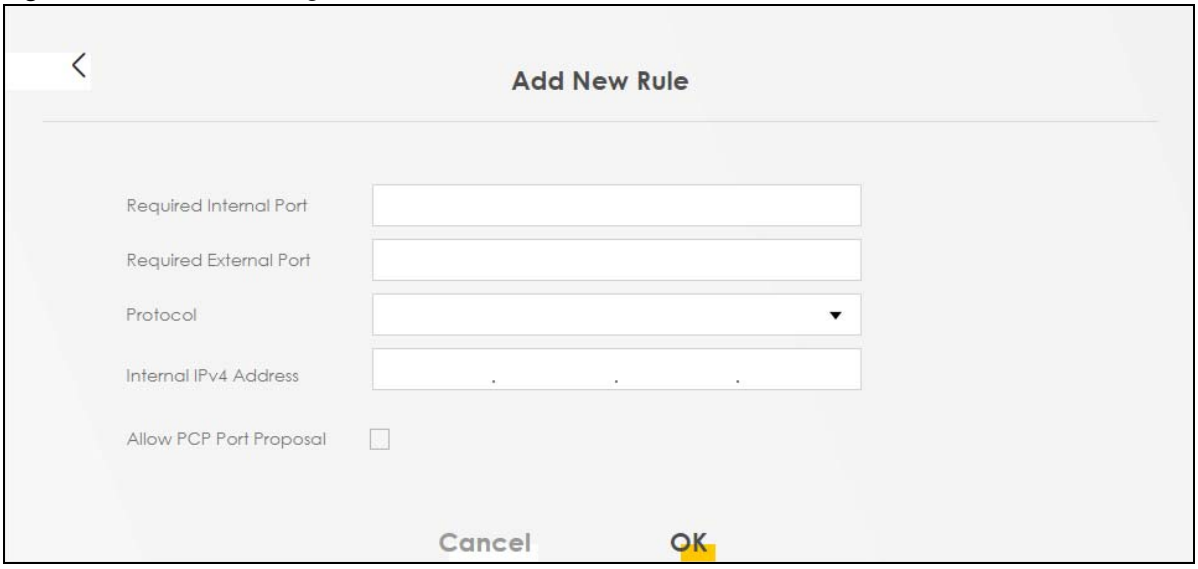
LABEL	DESCRIPTION
Add New Rule	Click this to add a new PCP rule.
#	This is the index number of the rule.
External IPv4 Address	This displays the external IP address assigned by the PCP server. PCP maps from this IP address to the LAN device IP address.
Required Internal Port	This displays the internal port number that the PCP server maps to, from the external port.
Required External Port	This displays the proposed external port number that the PCP server maps from, to the internal port.
Assigned Public Port	This displays the allocated external port number assigned by the PCP server for the service on the WAN if Allow PCP Port Proposal is enabled. PCP maps from this port number to the internal port number.
Protocol	This is the protocol (**TCP** or **UDP**) for port number that identifies a service.
Internal IPv4 Address	This is the LAN device IP address. PCP maps the external IP address to this IP address.
PCP Server	This field displays the status of the PCP mapping request to the PCP server. • **Succeeded** - The PCP server successfully mapped the external IP address and port to the internal IP address and port. • **Failed** - The PCP server failed to map the external IP address and port to the internal IP address and port. Make sure to select Allow PCP Port Proposal to allow the PCP server to assign an external IP address and port if the configured ones are not available.
Allow PCP Port Proposal (Y/N)	This displays **Y** if the PCP server can assign a different external IP address and port to the required ones you configured.
Delete	Select a rule, then click this icon to remove the rule from the Zyxel Device.

12.8.1 Add New Rule Screen

To add a new PCP rule, click **Add New Rule**. To edit an existing rule, select the rule, then click the **Modify** icon. The following screen displays.

Note: Be careful not to configure conflicting mapping between PCP and NAT port forwarding for incoming traffic.

Figure 171 Network Setting > NAT > PCP > Add New Rule



The following table describes the fields in this screen.

Table 93 Network Setting > NAT > PCP > Add New Rule

LABEL	DESCRIPTION
Required Internal Port	Enter an internal port number that the PCP server maps to, from the external port.
Required External Port	Enter a proposed external port number that the PCP server maps from, to the internal port.
Protocol	Select the transport layer protocol. Choices are **TCP** and **UDP**. See the Service Appendix to see what services require what protocol and port number.
Internal IPv4 Address	Enter the IP address of the LAN device. PCP maps the external IP address to this IP address.
Allow PCP Port Proposal	Select this to allow the PCP server to assign an external IP address and port. If you clear this, PCP mapping will fail if the required ones configured are not available on the PCP server.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

12.9 Technical Reference

This part contains more information regarding NAT.

12.9.1 NAT Definitions

Inside or outside denotes where a host is located relative to the Zyxel Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global or local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside or outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 94 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

12.9.2 What NAT Does

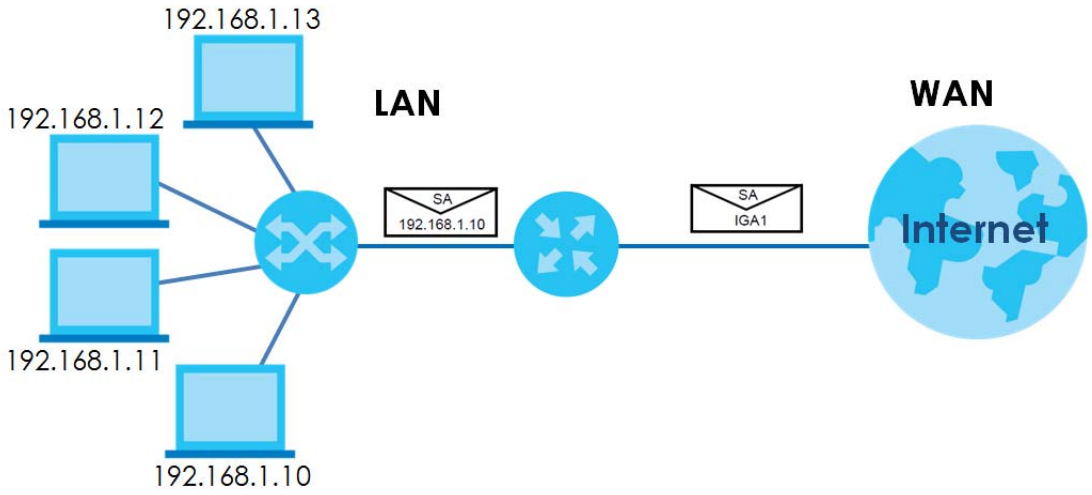
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Zyxel Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

12.9.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Zyxel Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

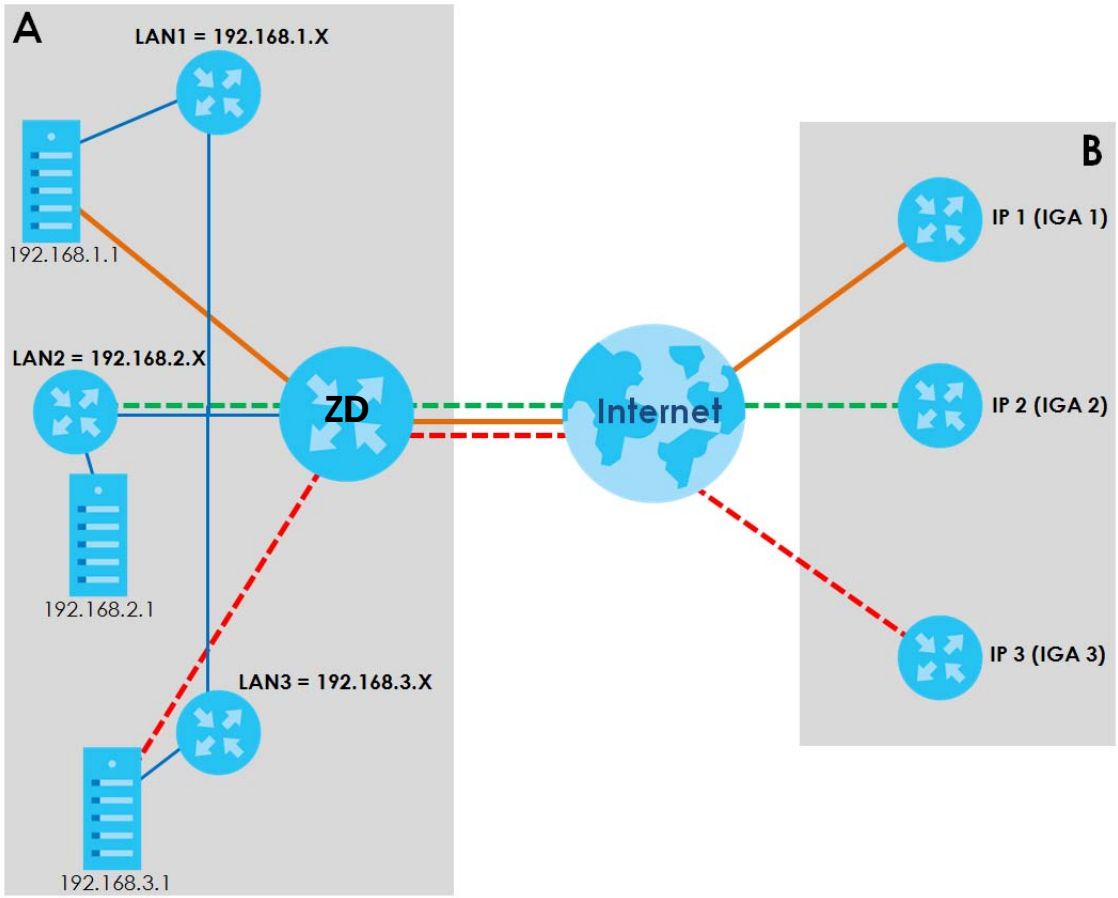
Figure 172 How NAT Works



12.9.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the Zyxel Device can communicate with three distinct WAN networks.

Figure 173 NAT Application With IP Alias



Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

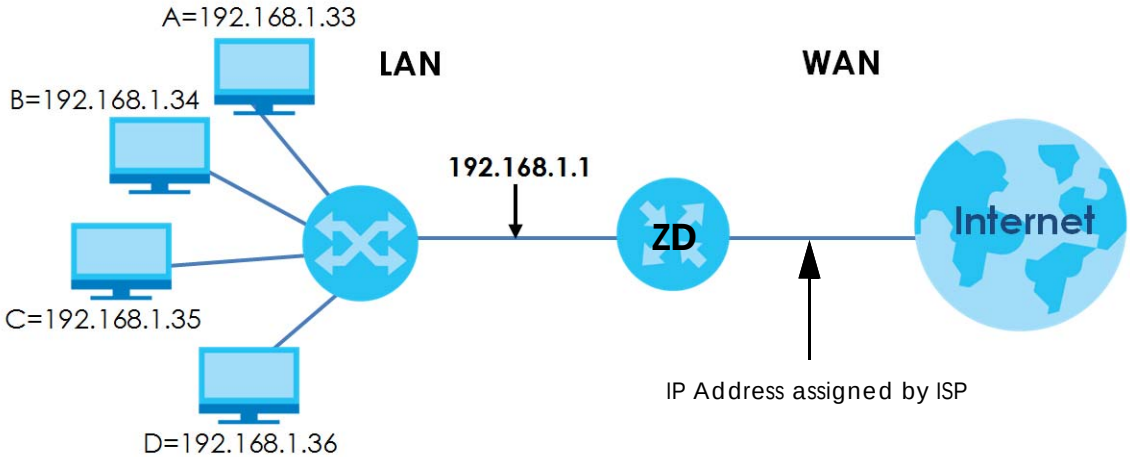
Table 95 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21 – 25 to one Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 174 Multiple Servers Behind NAT Example



CHAPTER 13
DNS

13.1 DNS Overview

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS servers, each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. The Zyxel Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Zyxel Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, and so on). You can also access your Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they do not know your IP address.

You first need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

13.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 13.2 on page 282).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device (Section 13.3 on page 283).

13.1.2 What You Need To Know

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

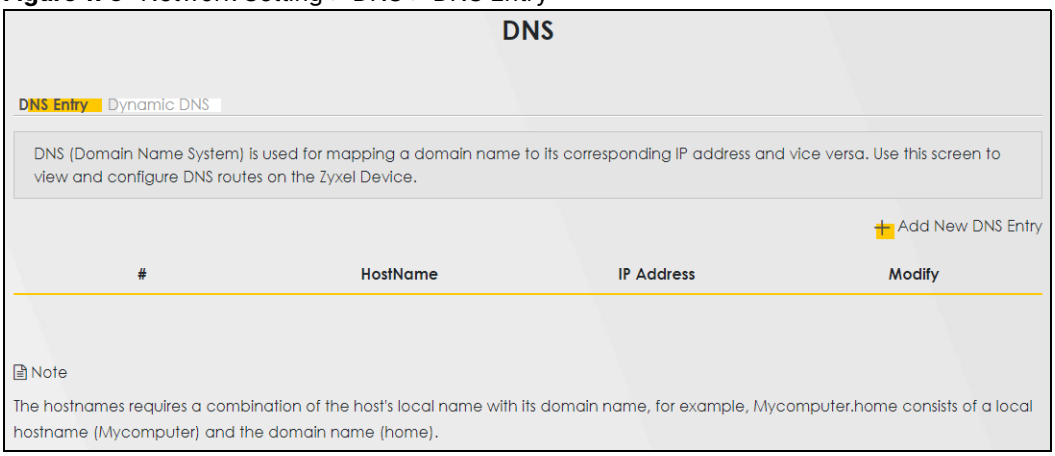
If you have a private WAN IP address, then you cannot use Dynamic DNS.

13.2 DNS Entry (DNS)

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure manual DNS entires on the Zyxel Device. Click **Network Setting** > **DNS** to open the **DNS Entry** screen.

Note: The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.

Figure 175 Network Setting > DNS > DNS Entry



The following table describes the fields in this screen.

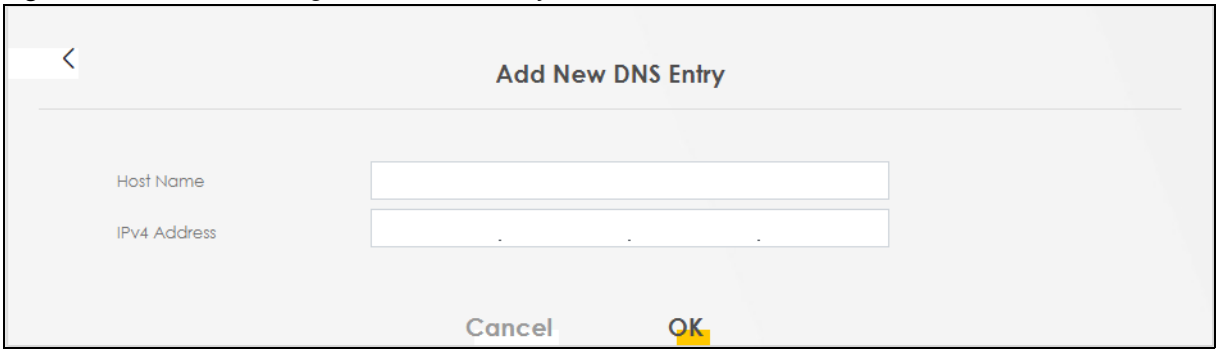
Table 96 Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
HostName	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule.

13.2.1 Add or Edit DNS Entry

You can manually add or edit the Zyxel Device's DNS name and IP address entry. Click **Add New DNS Entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 176 Network Setting > DNS > DNS Entry: Add



The following table describes the labels in this screen.

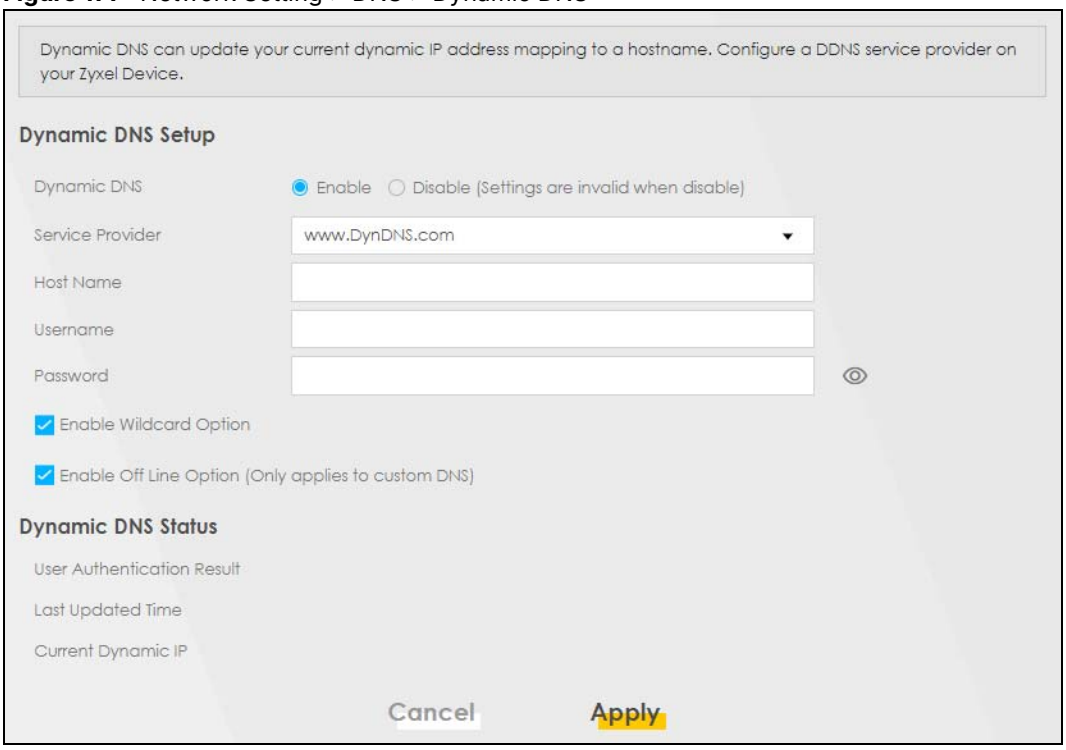
Table 97 Network Setting > DNS > DNS Entry: Add or Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com.
IPv4 Address	Enter the IPv4 address of the DNS entry.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

13.3 Dynamic DNS

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Configure a DDNS service provider on your Zyxel Device. Click **Network Setting** > **DNS** > **Dynamic DNS**. The screen appears as shown.

Figure 177 Network Setting > DNS > Dynamic DNS



The following table describes the fields in this screen.

Table 98 Network Setting > DNS > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Enter the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the checkbox to enable DynDNS Wildcard.
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	
User Authentication Result	This shows **Success** if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.

Table 98 Network Setting > DNS > Dynamic DNS (continued)

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

CHAPTER 14
IGMP/MLD

14.1 IGMP/MLD Overview

Multicast delivers IP packets to a group of hosts on the network defined by multicast groups. Membership to these multicast groups are established using IGMP/MLD.

Use the **IGMP/MLD** screen to configure IGMP/MLD group settings.

14.1.1 What You Need To Know

Multicast and IGMP

See Multicast on page 170 for more information.

Multicast Listener Discovery (MLD)

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 hosts 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.
- An MLD Report message is equivalent to an IGMP Report message, and an MLD Done message is equivalent to an IGMP Leave message.

IGMP Fast Leave

When a host leaves a multicast group (224.1.1.1), it sends an IGMP leave message to inform all routers (224.0.0.2) in the multicast group. When a router receives the leave message, it sends a specific query message to all multicast group (224.1.1.1) members to check if any other hosts are still in the group. Then the router deletes the host's information.

With the IGMP fast leave feature enabled, the router removes the host's information from the group member list once it receives a leave message from a host and the fast leave timer expires.

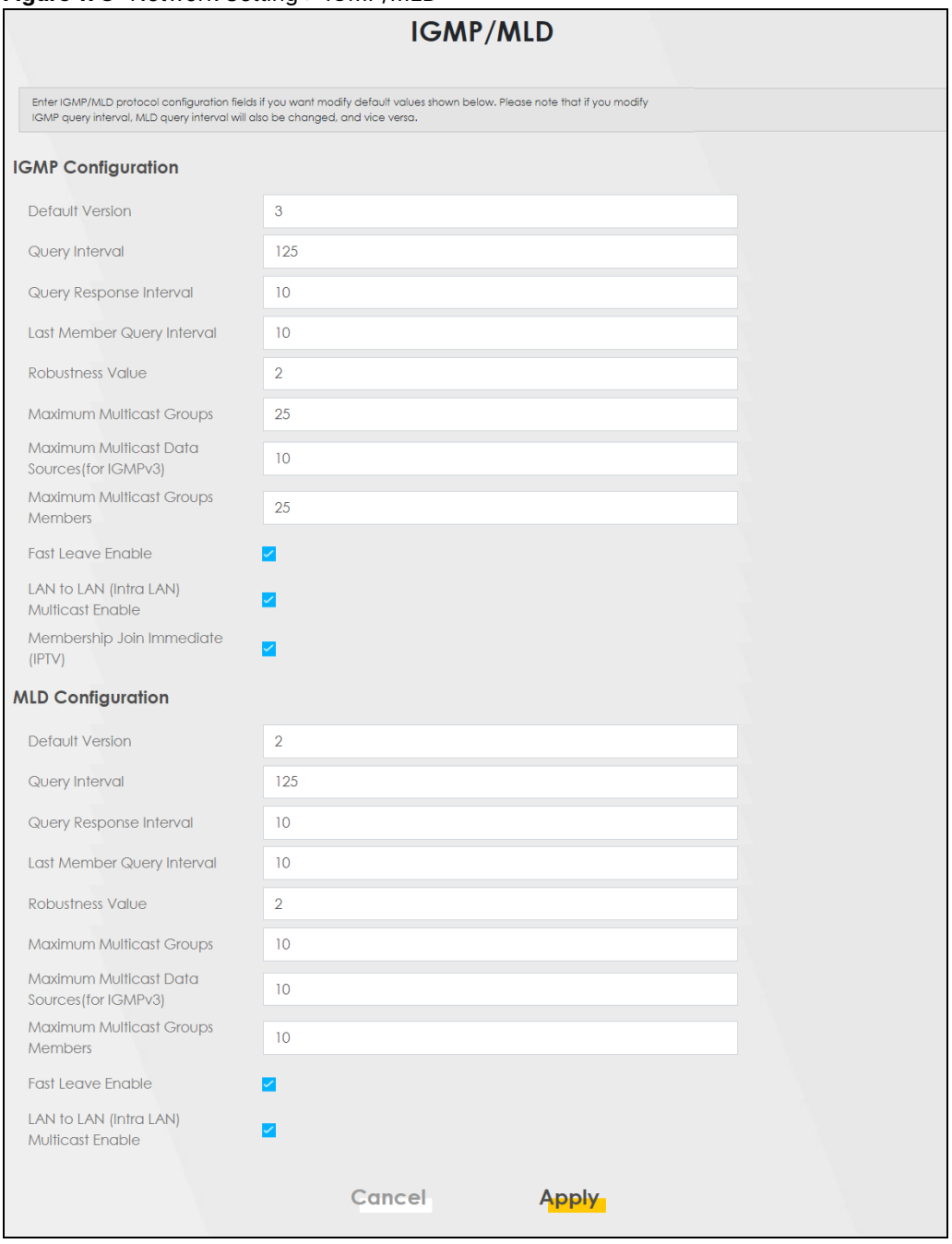
14.2 The IGMP/MLD Screen

Use this screen to configure multicast groups that the Zyxel Device manages through IGMP/MLD settings. To open this screen, click **Network Setting** > **IGMP/MLD**.

Note: Some models only support IGMP/MLD **Default Version** configuration.

Note: For DX3300/3301-T0, IGMP/MLD are enabled by default and are not configurable. The default IGMP version is 3. The default MLD version is 2.

Figure 178 Network Setting > IGMP/MLD



The following table describes the labels in this screen.

Table 99 Network Setting > IGMP/MLD

LABEL	DESCRIPTION
IGMP/MLD Configuration	
Default Version	Enter the version of IGMP (1~3) and MLD (1~2) that you want the Zyxel Device to use on the WAN.
Query Interval	Enter the number of seconds the Zyxel Device sends a query message to hosts to get the group membership information.
Query Response Interval	Enter the maximum number of seconds the Zyxel Device can wait for receiving a General Query message. Multicast routers use general queries to learn which multicast groups have members.
Last Member Query Interval	Enter the maximum number of seconds the Zyxel Device can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group.
Robustness Value	Enter the number of times (1~7) the Zyxel Device can resend a packet if packet loss occurs due to network congestion.
Maximum Multicast Groups	Enter a number to limit the number of multicast groups an interface on the Zyxel Device is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface.
Maximum Multicast Data Sources(for IGMPv3)	Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2.
Maximum Multicast Group Members	Enter a number to limit the number of multicast members a multicast group can have.
Fast Leave Enable	Select this option to set the Zyxel Device to remove a port from the multicast tree immediately (without sending an IGMP or MLD membership query message) once it receives an IGMP or MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications.
LAN to LAN (Intra LAN) Multicast Enable	Select this to enable LAN to LAN IGMP snooping capability.
Membership Join Immediate (IPTV)	Select this to have the Zyxel Device add a host to a multicast group immediately once the Zyxel Device receives an IGMP or MLD join message.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 15
VLAN Group

15.1 VLAN Group Overview

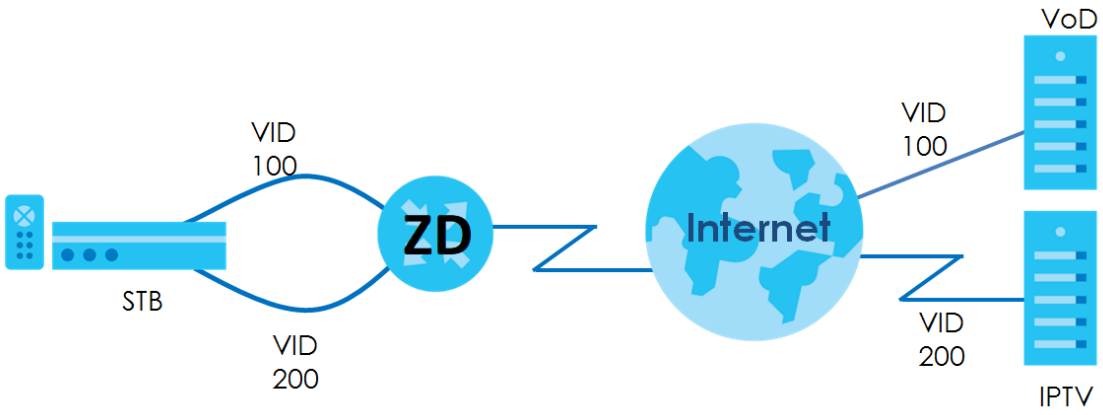
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same groups;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

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. Shared resources such as a server can be used by all ports in the same VLAN as the server. Ports can belong to other VLAN groups too. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges. The VLAN ID associates a frame with a specific VLAN and provides the information that switches the need to process the frame across the network.

In the following example, VLAN IDs (VIDs) 100 and 200 are added to identify Video-on-Demand and IPTV traffic respectively coming from the VoD and IPTV multicast servers. The Zyxel Device can also tag outgoing requests to the servers with these VLAN IDs.

Figure 179 VLAN Group Example



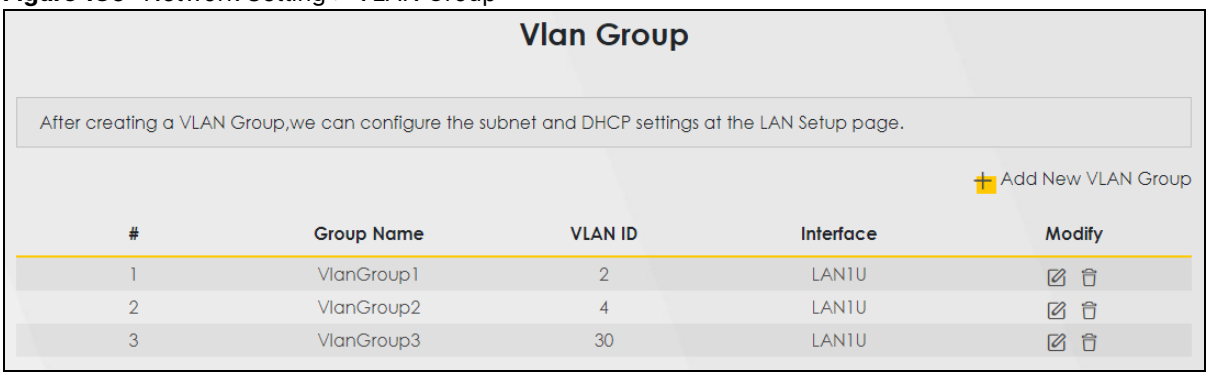
15.1.1 What You Can Do in this Chapter

Use these screens to manage VLAN groups on the Zyxel Device.

15.2 VLAN Group Settings

This screen shows the VLAN groups created on the Zyxel Device. Click **Network Setting** > **VLAN Group** to open the following screen.

Figure 180 Network Setting > VLAN Group



The following table describes the fields in this screen.

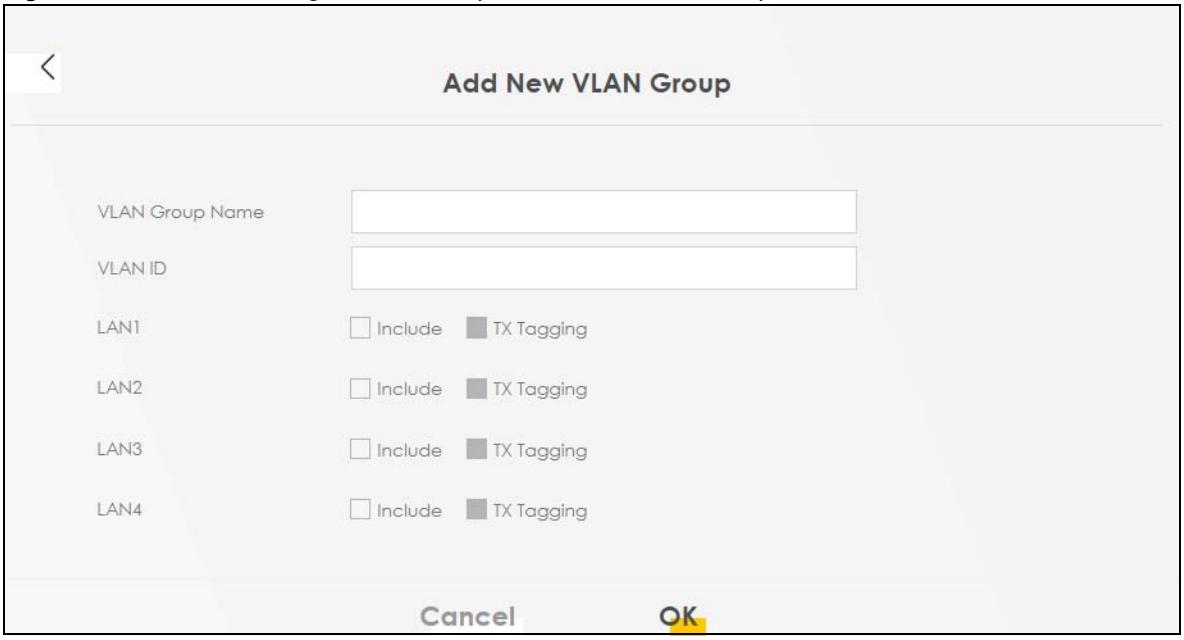
Table 100 Network Setting > VLAN Group

LABEL	DESCRIPTION
Add New VLAN Group	Click this button to create a new VLAN group.
#	This is the index number of the VLAN group.
Group Name	This shows the descriptive name of the VLAN group.
VLAN ID	This shows the unique ID number that identifies the VLAN group.
Interface	This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID.
Modify	Click the **Edit** icon to change an existing VLAN group setting or click the **Delete** icon to remove the VLAN group.

15.2.1 Add or Edit a VLAN Group

Click the **Add New VLAN Group** button in the **VLAN Group** screen to open the following screen. Use this screen to create a new VLAN group.

Figure 181 Network Setting > VLAN Group > Add New VLAN Group/Edit



The following table describes the fields in this screen.

Table 101 Network Setting > VLAN Group > Add New VLAN Group/Edit

LABEL	DESCRIPTION
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify this VLAN group. Outgoing traffic is tagged with this ID if **TX Tagging** is selected below.
LAN	Select **Include** to add the associated LAN interface to this VLAN group. Note: Select **TX Tagging** to tag outgoing traffic from the associated LAN port with the **VLAN ID** number entered above.
10G LAN	Select **Include** to add the associated LAN interface to this VLAN group. Note: Select **TX Tagging** to tag outgoing traffic from the associated LAN port with the **VLAN ID** number entered above.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 16
Interface Grouping

16.1 Interface Grouping Overview

By default, all LAN and WAN interfaces on the Zyxel Device are in the default group. Client devices in the default group can communicate with all devices in the default and other groups. Create interface groups to have the Zyxel Device assign IP addresses in different domains. Each group acts as an independent network on the Zyxel Device. Client devices in the same group can communicate with each other directly. Interfaces that do not belong to any user-defined group belong to the default group.

16.1.1 What You Can Do in this Chapter

The **Interface Grouping** screen lets you create multiple networks on the Zyxel Device (Section 16.2 on page 292).

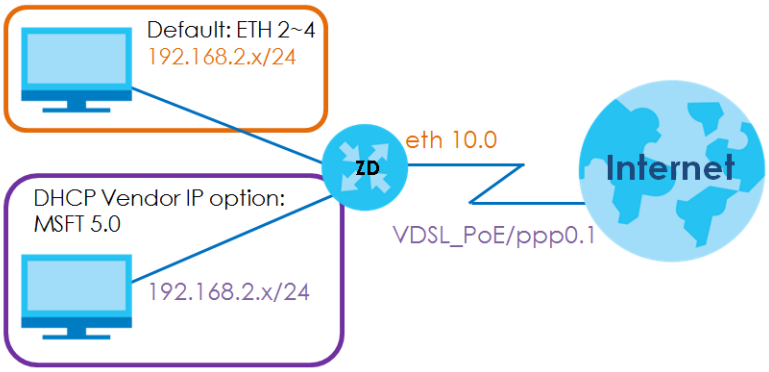
16.2 Interface Grouping

You can manually add a LAN interface to a new group. Alternatively, you can have the Zyxel Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN Setup** screen to configure the private IP addresses the DHCP server on the Zyxel Device assigns to the clients in the default and/or user-defined groups. If you set the Zyxel Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 9 on page 202 for more information.

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

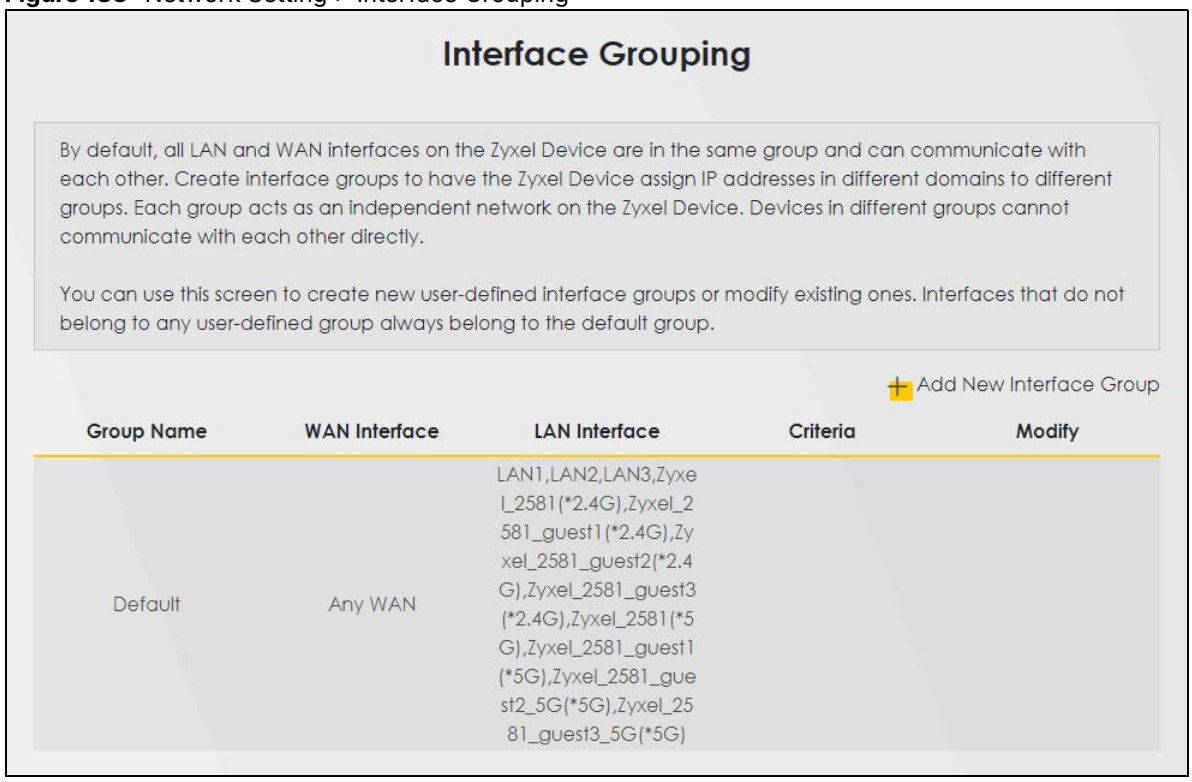
Figure 182 Interface Grouping Application



You can use this screen to create new user-defined interface groups or modify existing ones. Interfaces that do not belong to any user-defined group always belong to the default group.

Click **Network Setting** > **Interface Grouping** to open the following screen.

Figure 183 Network Setting > Interface Grouping



The following table describes the fields in this screen.

Table 102 Network Setting > Interface Grouping

LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Modify	Click the **Edit** icon to modify an existing Interface group setting or click the **Delete** icon to remove the Interface group.

16.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group. If you want to automatically add LAN clients to a new group, use filtering criteria.

Note: An interface can belong to only one group at a time.

Note: After configuring a vendor ID, reboot the client device attached to the Zyxel Device to obtain an appropriate IP address.

Figure 184 Network Setting > Interface Grouping > Add New Interface Group (for DSL routers)

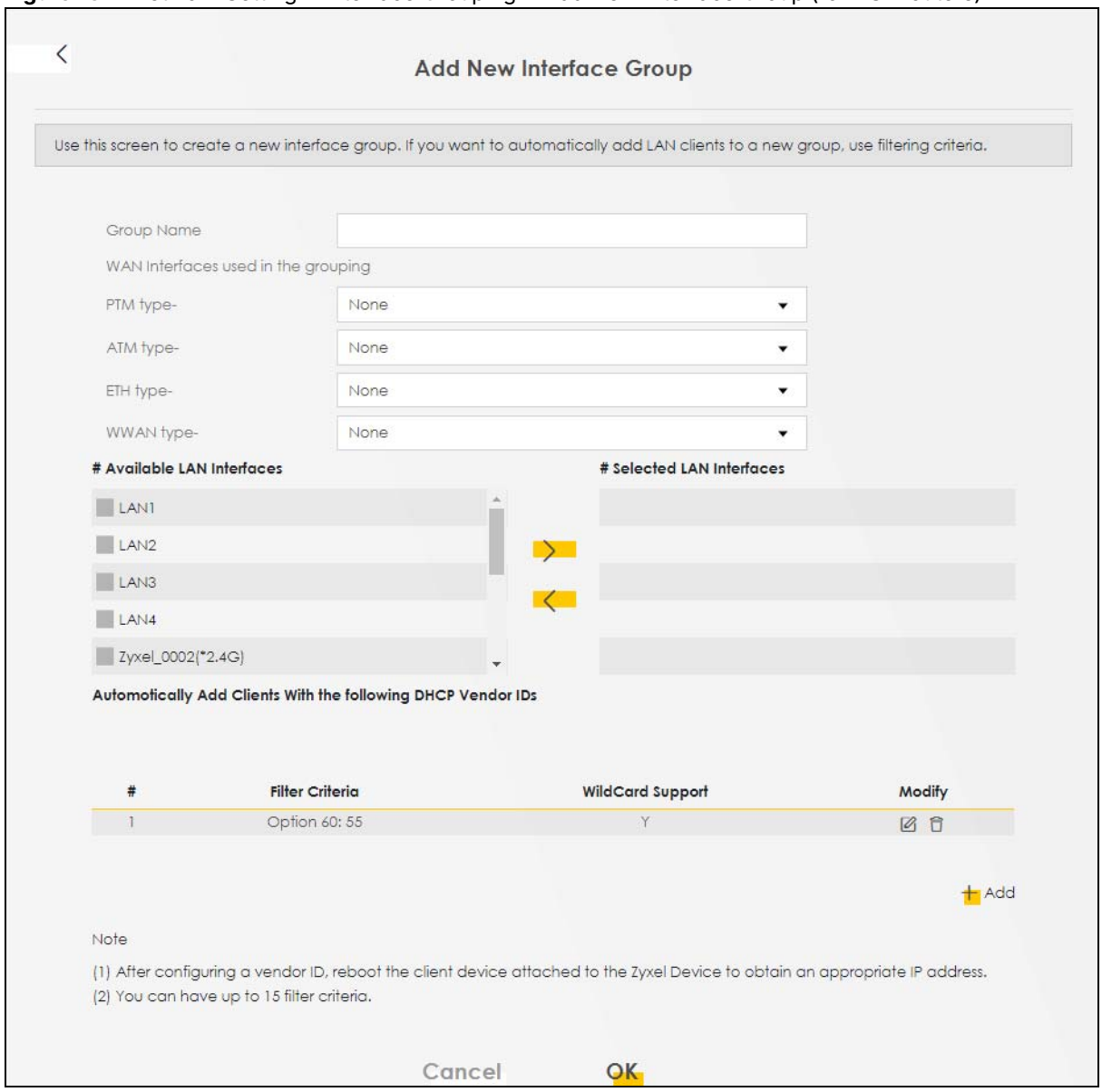


Figure 185 Network Setting > Interface Grouping > Add New Interface Group (for Ethernet routers)

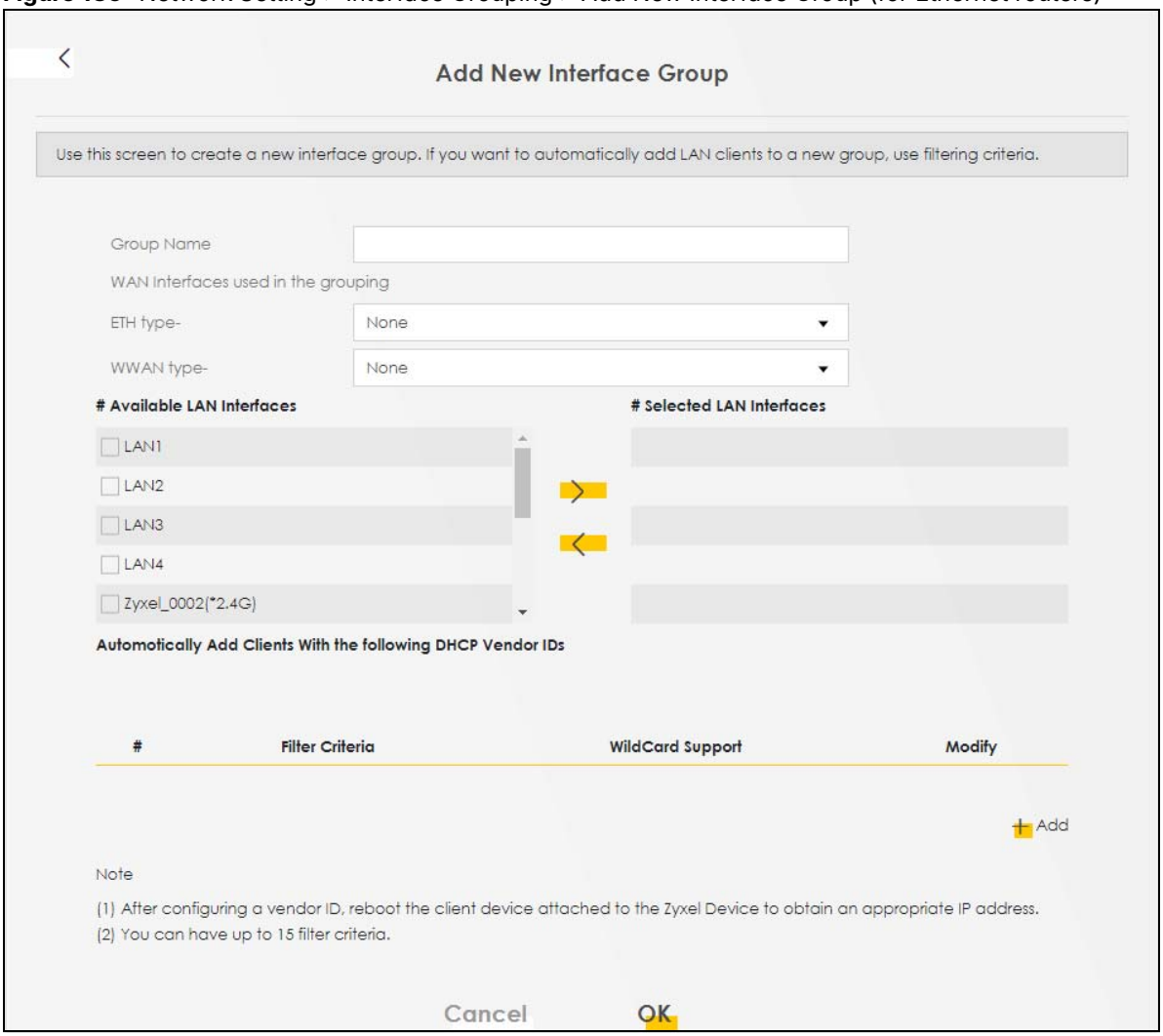
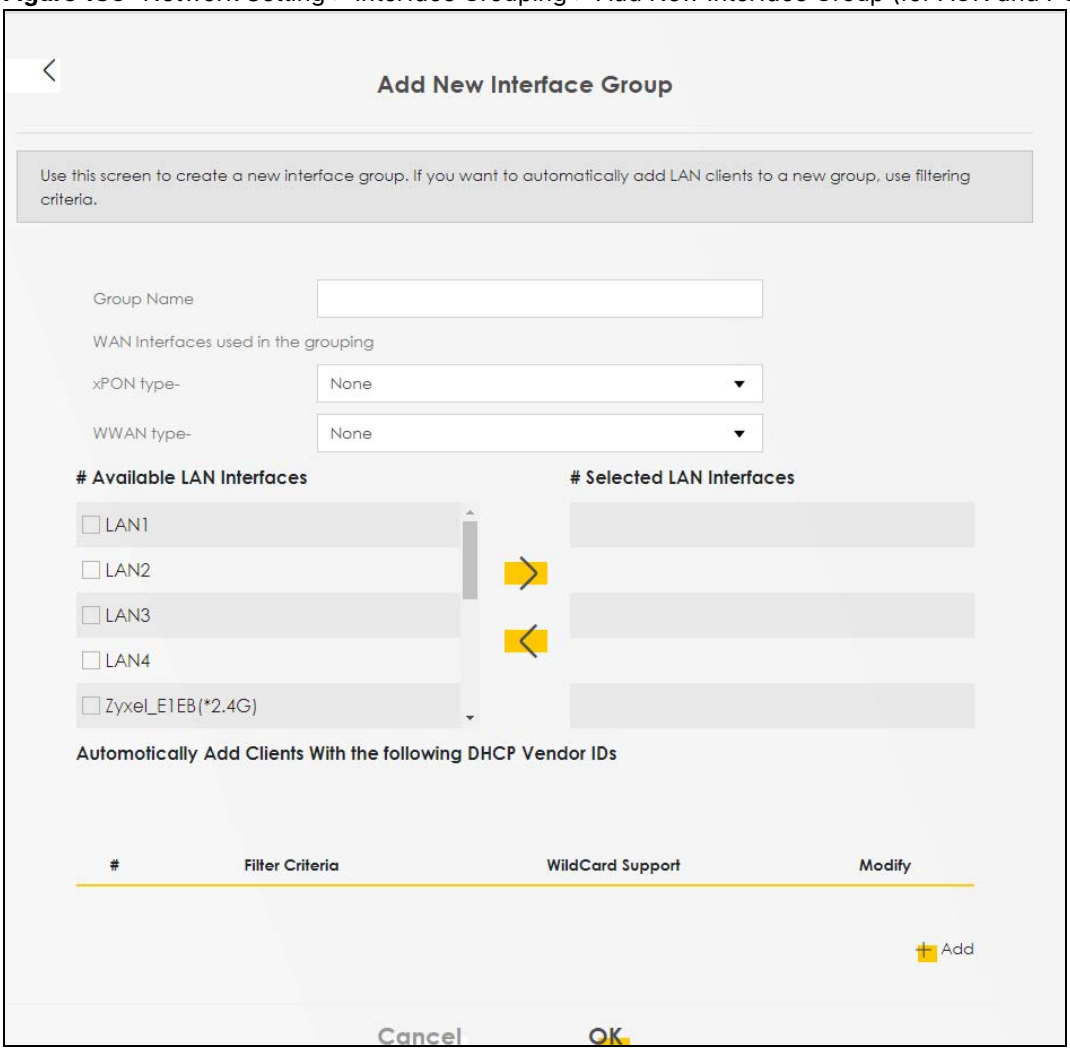


Figure 186 Network Setting > Interface Grouping > Add New Interface Group (for AON and PON routers)



The following table describes the fields in this screen.

Table 103 Network Setting > Interface Grouping > Add New Interface Group/Edit

LABEL	DESCRIPTION
Group Name	Enter a descriptive name for this interface group. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface. Select **None** to not add a WAN interface to this group.
Selected LAN Interfaces Available LAN Interfaces	Select one or more interfaces (Ethernet LAN, wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Selected LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Selected LAN Interfaces**, use the right-facing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	Click **Add** to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 16.2.2 on page 297 for more information.

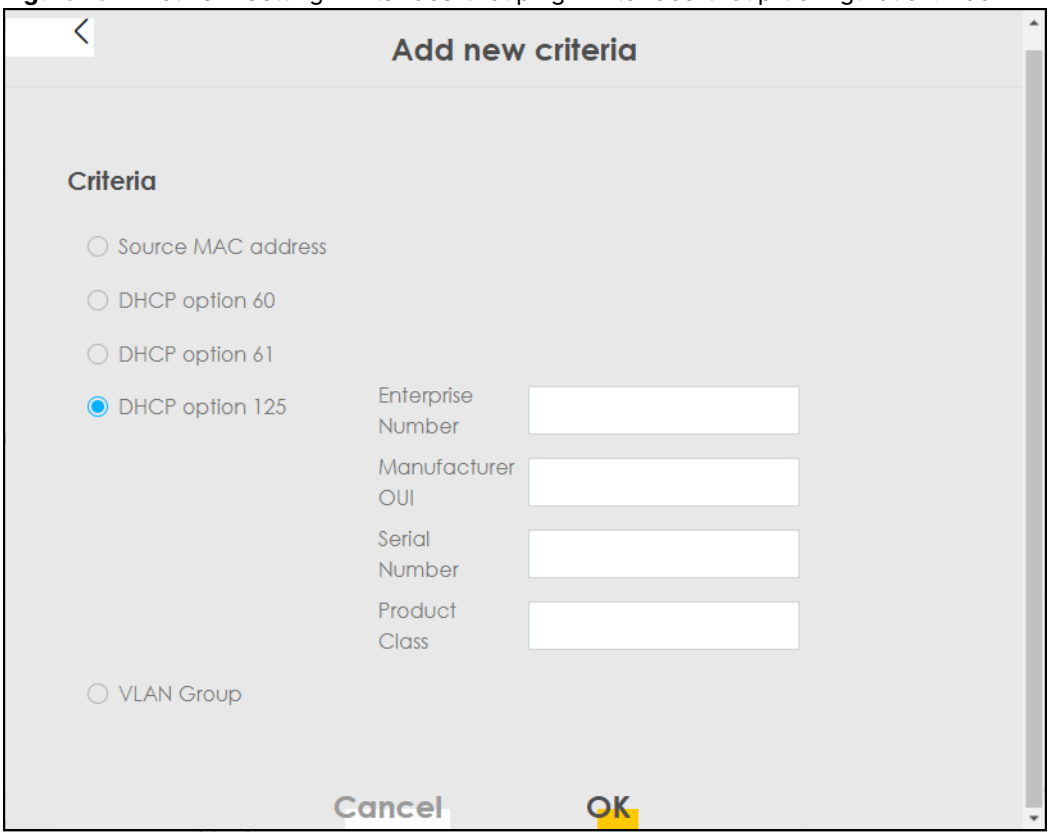
Table 103 Network Setting > Interface Grouping > Add New Interface Group/Edit (continued)

LABEL	DESCRIPTION
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
WildCard Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the **Edit** icon to change the group setting. Click the **Delete** icon to delete this group from the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click OK to save your changes.

16.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen. Use this screen to automatically add clients to an interface group based on specified criteria. You can choose to define a group based on a MAC address, a vendor ID (DHCP option 60), an Identity Association Identifier (DHCP option 61), vendor specific information (DHCP option 125), or a VLAN group.

Figure 187 Network Setting > Interface Grouping > Interface Group Configuration: Add



The following table describes the fields in this screen.

Table 104 Network Setting > Interface Grouping > Interface Group Configuration: Add

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
APAS MAC Filter	Select this option and enter the MAC address of the matched LAN host.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first 3 bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
VLAN Group	Select this and the VLAN group of the matched traffic from the drop-down list box. A VLAN group can be configured in **Network Setting** > **VLAN Group**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

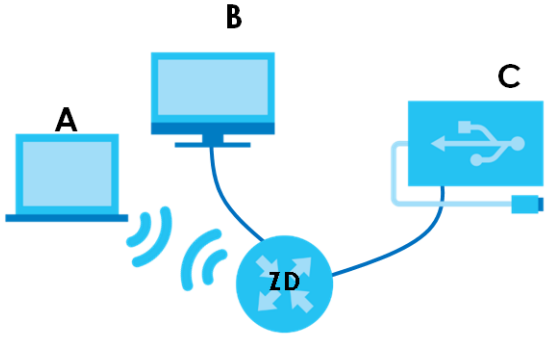
CHAPTER 17
USB Service

17.1 USB Service Overview

You can share files on a USB memory stick or hard drive connected to your Zyxel Device with users on your network.

The following figure is an overview of the Zyxel Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Zyxel Device.

Figure 188 File Sharing Overview



The Zyxel Device will not be able to join a workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

17.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server (Section 17.2 on page 300).
- Use the **Media Server** screen to enable or disable the sharing of media files (Section 17.3 on page 304).

17.1.2 What You Need To Know

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

17.1.3 Section 7.3 on page 160File Sharing

Workgroup Name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Zyxel Device is given a folder, called a “share”. If a USB hard drive connected to the Zyxel Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Zyxel Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Zyxel Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Zyxel Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

17.1.4 Before You Begin

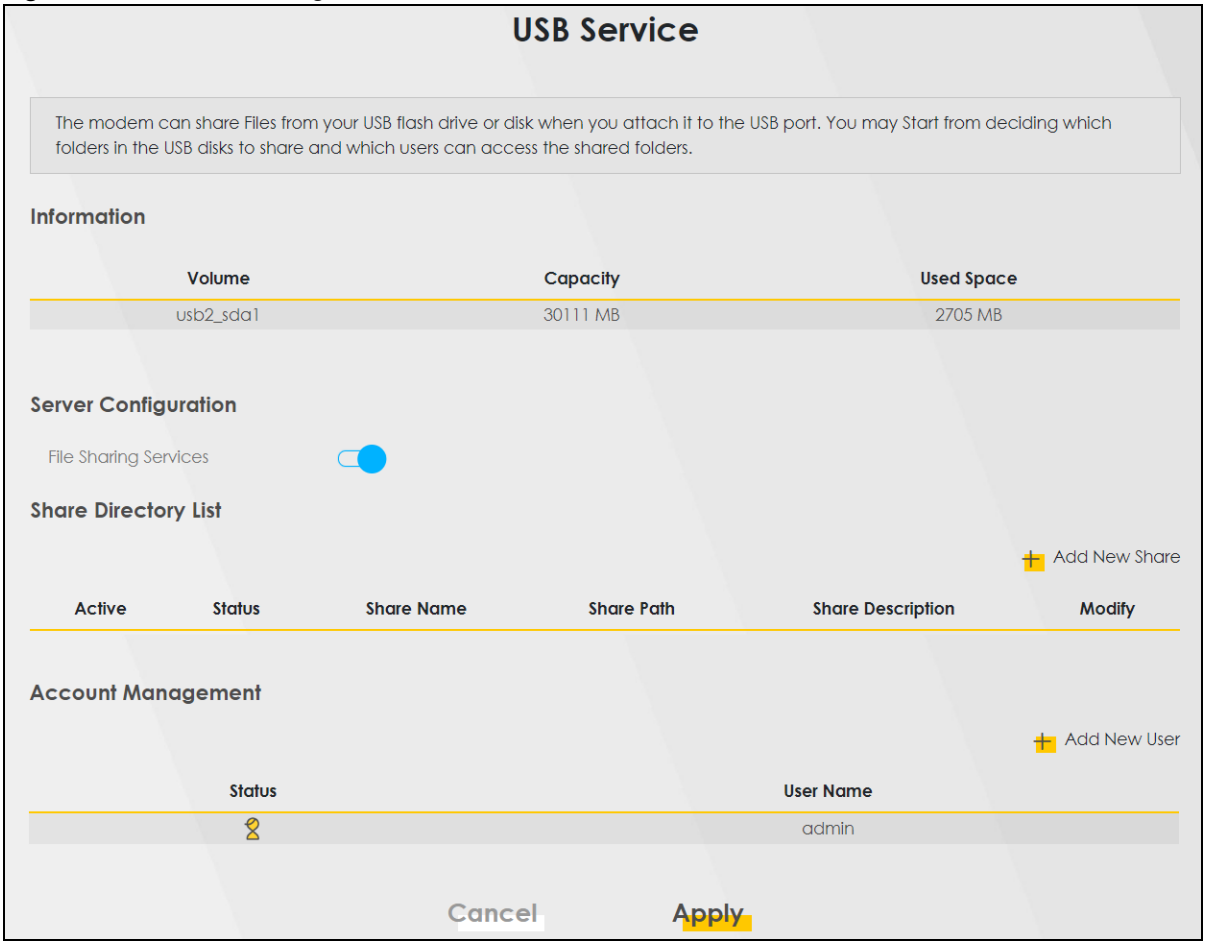
1. Make sure the Zyxel Device is connected to your network and turned on.
2. Connect the USB device to one of the Zyxel Device’s USB port. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source.
3. The Zyxel Device detects the USB device and makes its contents available for browsing.

   Note: If your USB device cannot be detected by the Zyxel Device, see the troubleshooting for suggestions.

17.2 USB Service

Use this screen to set up file sharing through the Zyxel Device. The Zyxel Device’s LAN users can access the shared folder (or share) from the USB device inserted in the Zyxel Device. To access this screen, click **Network Setting** > **USB Service**.

Figure 189 Network Setting > USB Service



Note: The **Share Directory List** is only visible when you connect a USB device.

Each field is described in the following table.

Table 105 Network Setting > USB Service

LABEL	DESCRIPTION
Information	
Volume	This is the volume name the Zyxel Device gives to an inserted USB device.
Capacity	This is the total available memory size (in megabytes) on the USB device.
Used Space	This is the memory size (in megabytes) already used on the USB device.
Server Configuration	
File Sharing Services	Click this switch to enable file sharing through the Zyxel Device.
Share Directory List This only appears when you have inserted a USB device.	
Add New Share	Click this to set up a new share on the Zyxel Device.
Active	Select this to allow the share to be accessed.

Table 105 Network Setting > USB Service (continued)

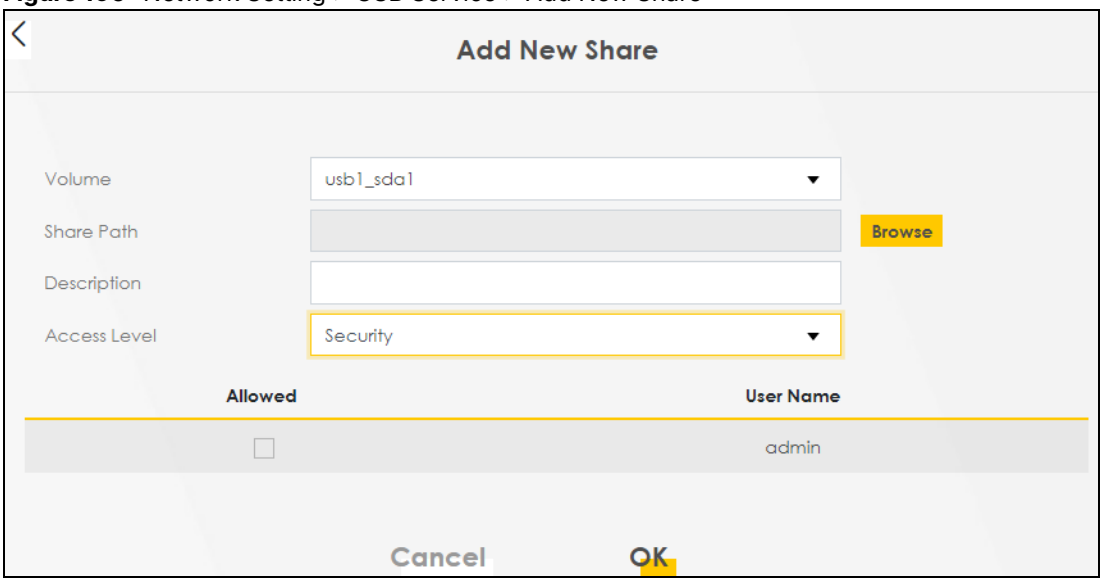
LABEL	DESCRIPTION
Status	This field shows the status of the share  : The share is not activated.  : The share is activated.
Share Name	This field displays the name of the file you shared.
Share Path	This field displays the location in the USB of the file you shared.
Share Description	This field displays a description of the file you shared.
Modify	Click the **Edit** icon to change the settings of an existing share. Click the **Delete** icon to delete this share in the list.
Account Management	
Add New User	Click this button to create a user account to access the secured shares. This button redirects you to **Maintenance** > **User Account.**
Status	This field shows the status of the user.  : The user account is not activated for the share.  : The user account is activated for the share.
User Name	This is the name of a user who is allowed to access the secured shares on the USB device.
Cancel	Click this to restore your previously saved settings.
Apply	Click this to save your changes to the Zyxel Device.

17.2.1 Add New Share

Use this screen to set up a new share or edit an existing share on the Zyxel Device. Click **Add New Share** in the **File Sharing** screen or click the **Edit** or **Modify** icon next to an existing share.

Please note that you need to set up shared folders on the USB device before enabling file sharing in the Zyxel Device. Spaces and the following special characters, ["], [`], ['], [<], [>], [^], [$], [|], [&], [;], are not allowed for the USB share name.

Figure 190 Network Setting > USB Service > Add New Share



The following table describes the labels in this menu.

Table 106 Network Setting > USB Service > Add New Share

LABEL	DESCRIPTION
Volume	Select the volume in the USB storage device that you want to add as a share in the Zyxel Device. This field is read-only when you are editing the share.
Share Path	Manually enter the file path for the share, or click the **Browse** button and select the folder that you want to add as a share. This field is read-only when you are editing the share.
Description	You can either enter a short description of the share, or leave this field blank. You can use up to 128 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Access Level	Select **Public** if you want the share to be accessed by users connecting to the Zyxel Device. Otherwise, select **Security**.
Allowed	If **Security** is selected in the **Access Level** field, select this checkbox to allow/prohibit access to the share.
User Name	This field specifies the user for which the **Allowed** setting applies. Users can be added or modified in **Maintenance** > **User Account.**
Cancel	Click **Cancel** to return to the previous screen.
OK	Click **OK** to save your changes.

17.2.2 Add New User Screen

Once you click the **Add New User** button, you will be directed to the **User Account** screen. To create a user account that can access the secured shares on the USB device, click the **Add New Account** button in the **Network Setting** > **USB Service** > **User Account screen**.

Please see Chapter 35 on page 395, for detailed information about **User Account** screen.

17.3 Media Server

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your Zyxel Device without having to copy them to another computer. The Zyxel Device can function as a DLNA-compliant media server, where the Zyxel Device streams files to DLNA-compliant media clients like Windows Media Player. The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

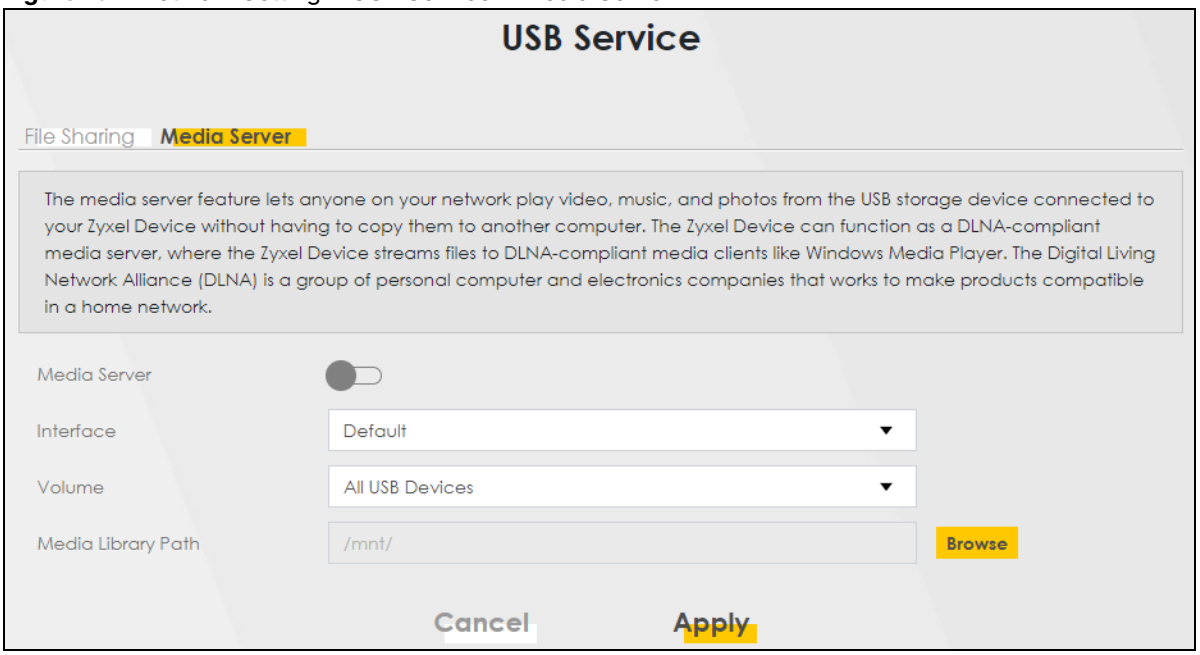
The Zyxel Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Zyxel Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your Zyxel Device's media server settings, click **Network Setting** > **USB Service** > **Media Server**. The screen appears as shown.

Figure 191 Network Setting > USB Service > Media Server



The following table describes the labels in this menu.

Table 107 Network Setting > USB Service > Media Server

LABEL	DESCRIPTION
Media Server	Click this switch to have the Zyxel Device function as a DLNA-compliant media server. When the switch goes to the right  , the function is enabled. Otherwise, it is not. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares.
Interface	Select an interface on which you want to enable the media server function. An interface can be added or modified in **Network Setting** > **Interface Grouping.**
Media Library Path	Enter the path clients use to access the media files on a USB storage device connected to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 18
Firewall

18.1 Firewall Overview

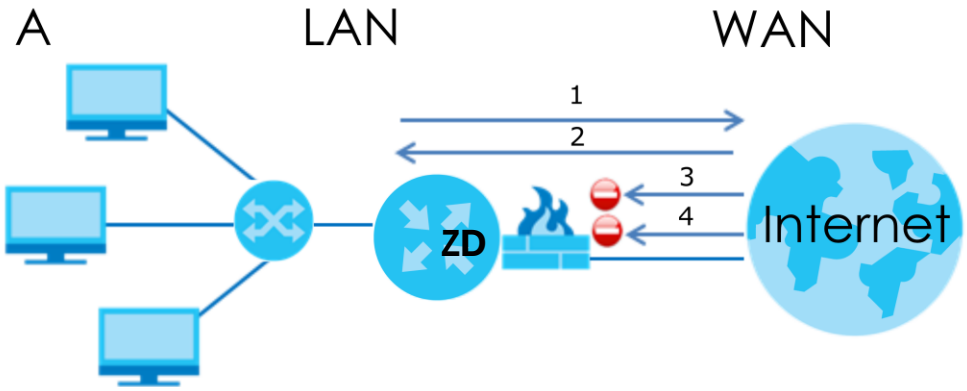
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

By default, the Zyxel Device blocks DoS attacks whether the firewall is enabled or disabled.

The following figure illustrates the firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 192 Default Firewall Action



18.1.1 What You Need to Know About Firewall

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denial-of-Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to

network resources. The Zyxel Device is pre-configured to automatically detect and thwart all known DoS attacks.

DoS Thresholds

For DoS attacks, the Zyxel Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

DDoS

A Distributed Denial-of-Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a 'ping' utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

18.2 Firewall

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it.

18.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device (Section 18.3 on page 308).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 18.4 on page 309).

- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules (Section 18.5 on page 310).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 18.6 on page 313).

18.3 General

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets. A higher firewall level means more restrictions on the Internet activities you can perform. Click **Security** > **Firewall** > **General** to display the following screen. Use the slider to select the level of firewall protection.

Figure 193 Security > Firewall > General

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.
When the security level is set to **High**, Telnet, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

The following table describes the labels in this screen.

Table 108 Security > Firewall > General

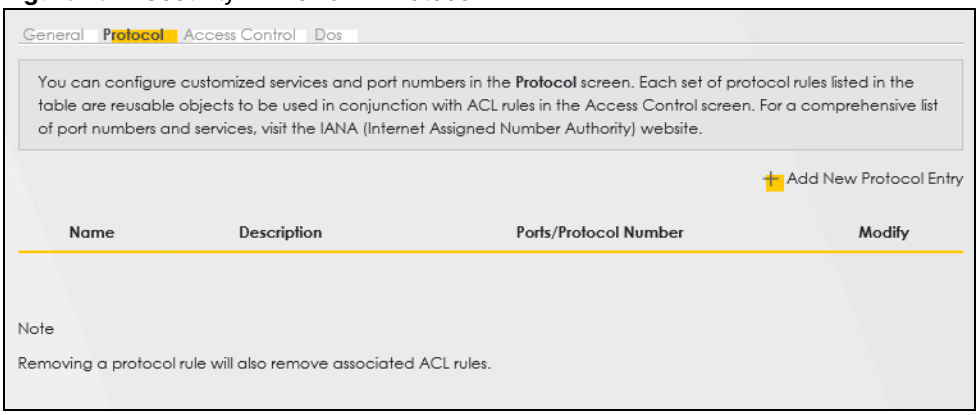
LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using **IPv4** (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using **IPv6** (Internet Protocol version 6).
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.
Medium	This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.
Low	This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

18.4 Protocol (Customized Services)

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security** > **Firewall** > **Protocol** to display the following screen.

Note: Removing a protocol rule will also remove associated ACL rules.

Figure 194 Security > Firewall > Protocol



The following table describes the labels in this screen.

Table 109 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to configure a customized service.
Name	This is the name of your customized service.
Description	This is a description of your customized service.

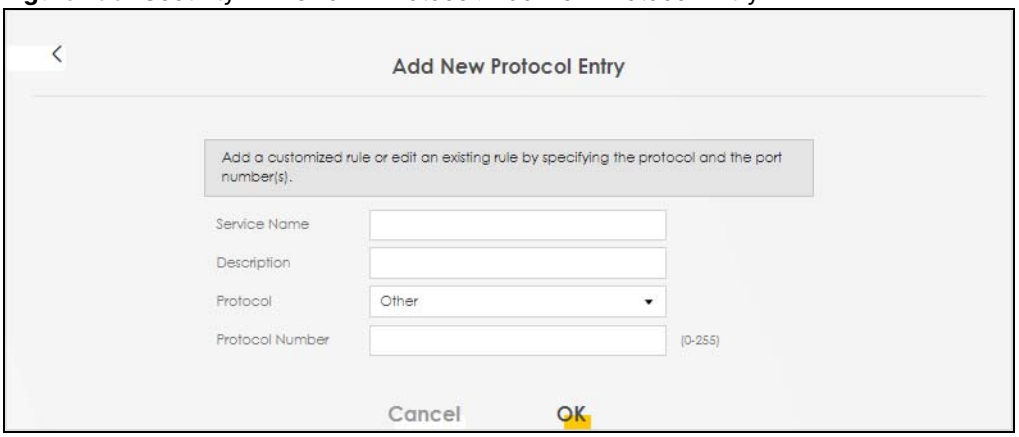
Table 109 Security > Firewall > Protocol (continued)

LABEL	DESCRIPTION
Ports/Protocol Number	This shows the port number or range and the IP protocol (**TCP** or **UDP**) that defines your customized service.
Modify	Click this to edit a customized service.

18.4.1 Add Customized Service

Add a customized rule or edit an existing rule by specifying the protocol and the port numbers. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

Figure 195 Security > Firewall > Protocol: Add New Protocol Entry



The following table describes the labels in this screen.

Table 110 Security > Firewall > Protocol: Add New Protocol Entry

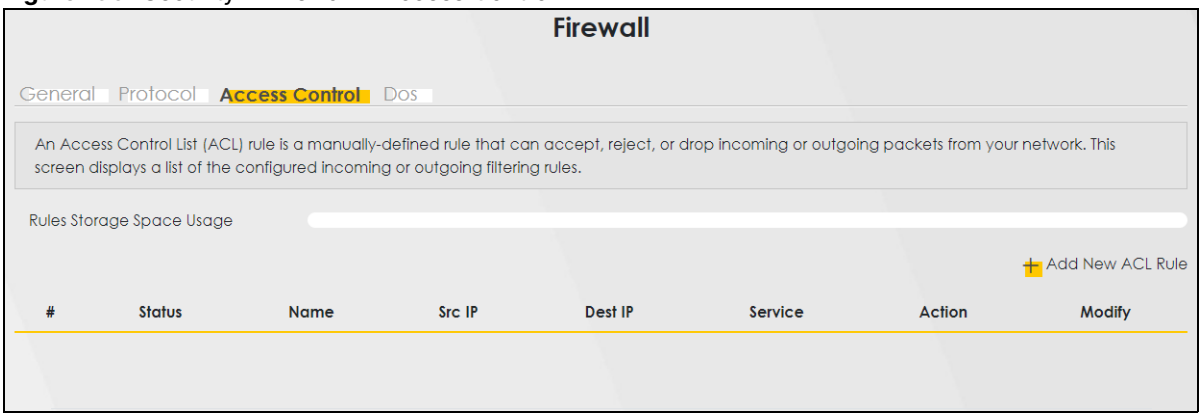
LABEL	DESCRIPTION
Service Name	Enter a descriptive name for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Description	Enter a description for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Protocol	Select the protocol (**TCP**, **UDP**, **ICMP**, **ICMPv6**, or **Other**) that defines your customized port from the drop down list box.
Protocol Number	Enter a single port number or the range of port numbers (**0** – **255**) that define your customized service.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

18.5 Access Control (Rules)

An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed. Click **Security** > **Firewall** > **Access Control** to display the following screen.

Note: The ordering of your rules is very important as rules are applied in turn.

Figure 196 Security > Firewall > Access Control



The following table describes the labels in this screen.

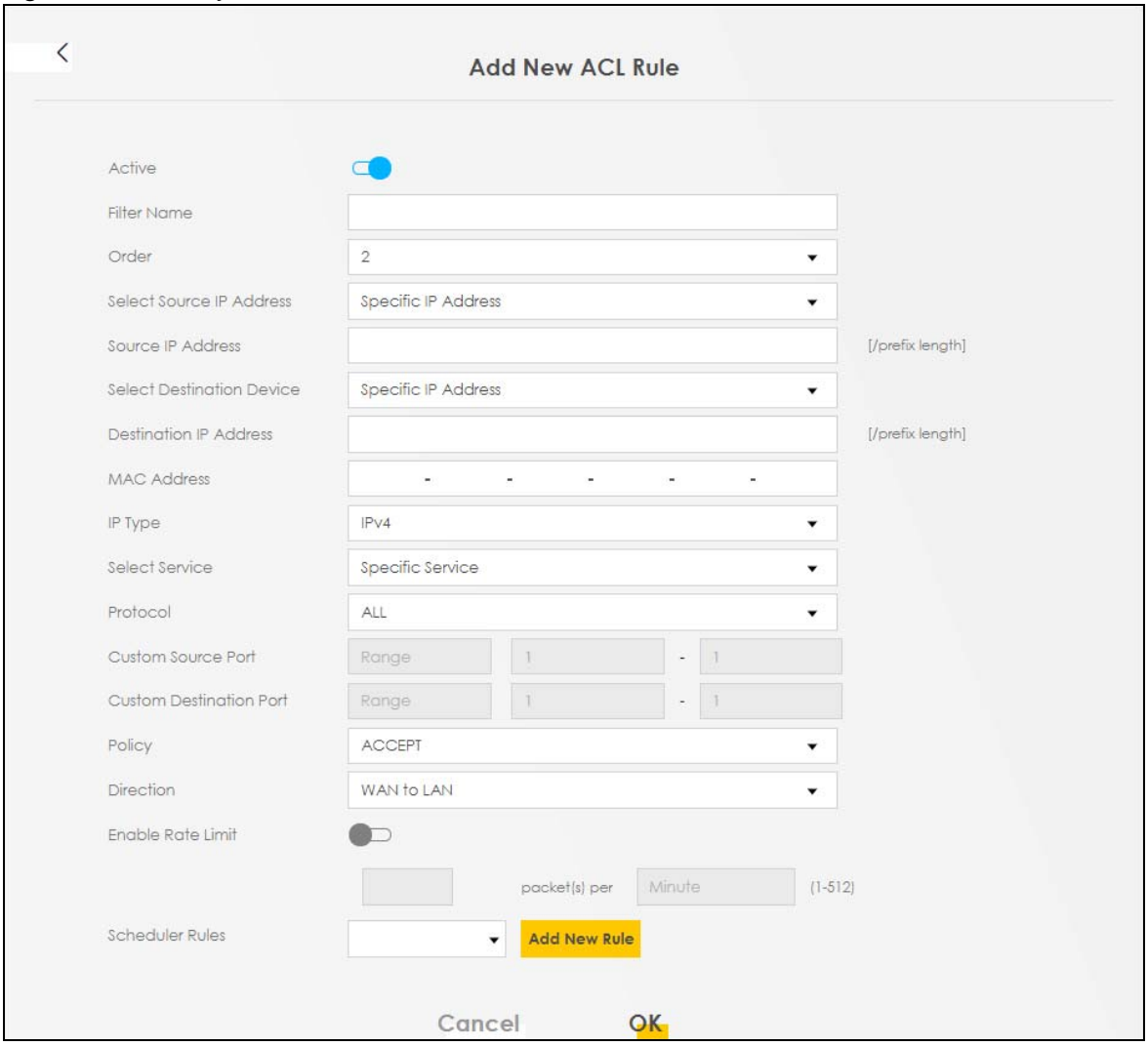
Table 111 Security > Firewall > Access Control

LABEL	DESCRIPTION
Rules Storage Space Usage	This read-only bar shows how much of the Zyxel Device's memory is in use for recording firewall rules. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Add New ACL Rule	Select an index number and click **Add New ACL Rule** to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
#	This field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Name	This field displays the rule name.
Src IP	This field displays the source IP addresses to which this rule applies.
Dest IP	This field displays the destination IP addresses to which this rule applies.
Service	This field displays the protocol (All, TCP, UDP, TCP/UDP, ICMP, ICMPv6, or any) used to transport the packets for which you want to apply the rule.
Action	Displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule.
Modify	Click the **Edit** icon to edit the firewall rule. Click the **Delete** icon to delete an existing firewall rule.

18.5.1 Add New ACL Rule

Click **Add new ACL** rule or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays. Use this screen to accept, reject, or drop packets based on specified parameters, such as source and destination IP address, IP Type, service, and direction. You can also specify a limit as to how many packets this rule applies to at a certain period of time or specify a schedule for this rule.

Figure 197 Security > Firewall > Access Control > Add New ACL Rule



The following table describes the labels in this screen.

Table 112 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name for your filter rule. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Order	Assign the order of your rules as rules are applied in turn.
Source IP Address	If you selected **Specific IP Address** in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select **Specific IP Address**. If not, select a detected device.
Destination IP Address	If you selected **Specific IP Address** in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.
IP Type	Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4**/**IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD).

Table 112 Security > Firewall > Access Control > Add New ACL Rule (continued)

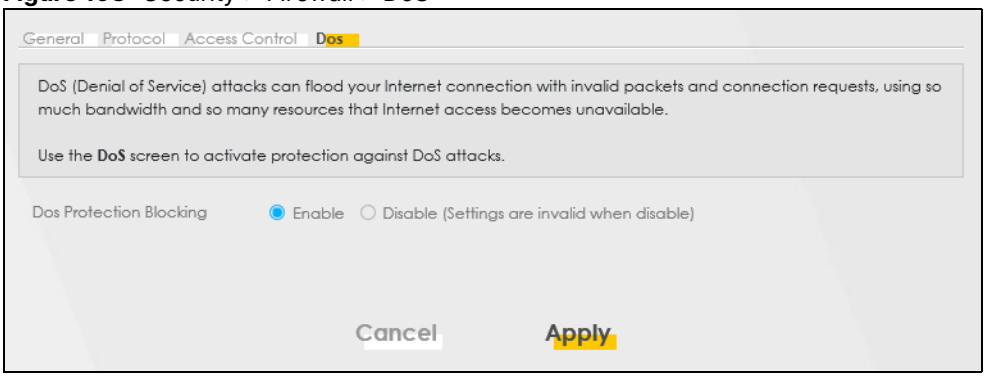
LABEL	DESCRIPTION
Select Service	Select a service from the **Select Service** box.
Protocol	Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
Policy	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule.
Direction	Select **WAN to LAN** to apply the rule to traffic from WAN to LAN. Select **LAN to WAN** to apply the rule to traffic from LAN to WAN. Select **WAN to Router** to apply the rule to traffic from WAN to router. Select **LAN to Router** to apply the rule to traffic from LAN to router.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

18.6 DoS

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Use the **DoS** screen to activate protection against DoS attacks.

Click **Security** > **Firewall** > **DoS** to display the following screen.

Figure 198 Security > Firewall > DoS



The following table describes the labels in this screen.

Table 113 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Enable this to protect against DoS attacks. The Zyxel Device will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

18.7 Firewall Technical Reference

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

18.7.1 Firewall Rules Overview

Your customized rules take precedence and override the Zyxel Device's default settings. The Zyxel Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the Zyxel Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to Router
- LAN to WAN
- WAN to LAN
- WAN to Router

By default, the Zyxel Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to Router

  These rules specify which computers on the LAN can manage the Zyxel Device (remote management).

Note: You can also configure the remote management settings to allow only a specific computer to manage the Zyxel Device.

- LAN to WAN

  These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the Zyxel Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN

  These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to Router

  By default the Zyxel Device stops computers on the WAN from managing the Zyxel Device. You could configure one of these rules to allow a WAN computer to manage the Zyxel Device.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the Zyxel Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.

- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the Zyxel Device's default rules.

18.7.2 Guidelines For Security Enhancement With Your Firewall

1. Change the default password through the Web Configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your router.
4. Do not enable any local service (such as telnet) that you do not use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

18.7.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Zyxel Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC (Internet Relay Chat) is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the Web Configurator screens.

CHAPTER 19
MAC Filter

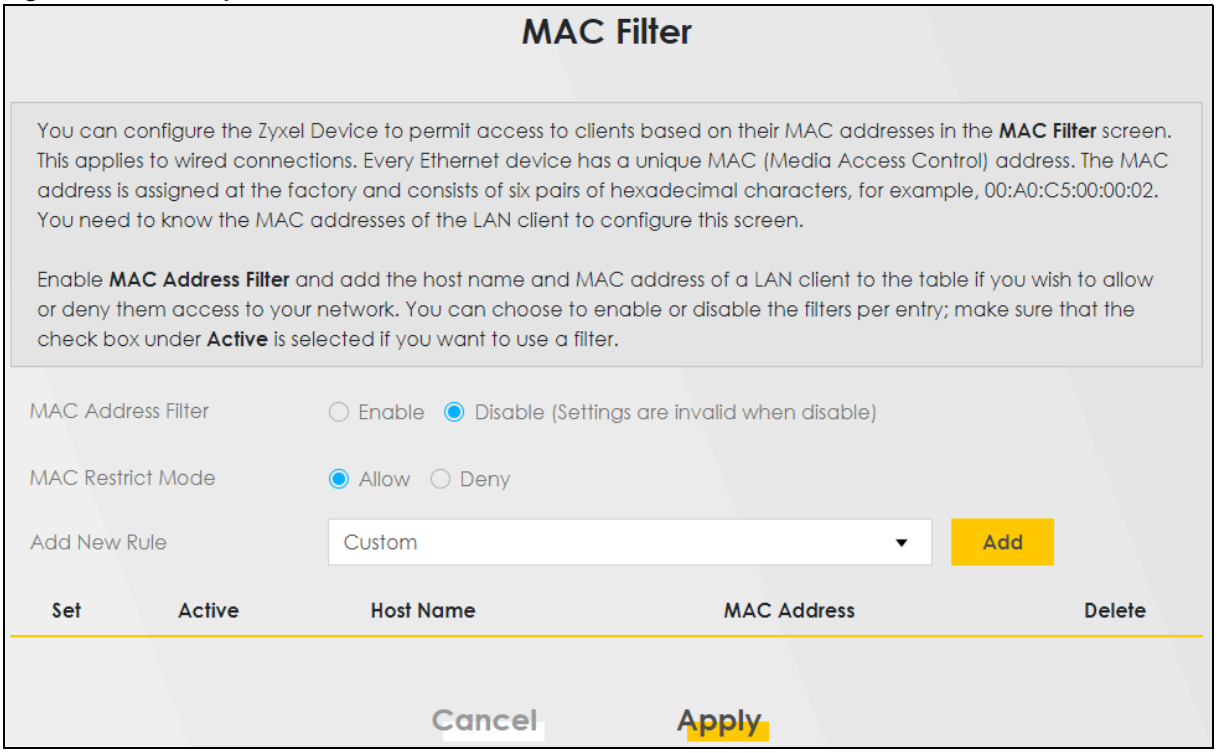
19.1 MAC Filter Overview

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of wired LAN client to configure this screen.

19.2 MAC Filter

Enable **MAC Address Filter** and add the host name and MAC address of a wired LAN client to the table if you wish to allow or deny them access to your network. You can choose to enable or disable the filters per entry; make sure that the checkbox under **Active** is selected if you want to use a filter. Select **Security** > **MAC Filter**. The screen appears as shown.

Figure 199 Security > MAC Filter



The following table describes the labels in this screen.

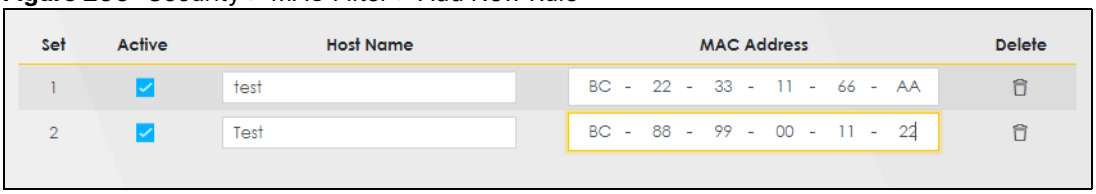
Table 114 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate the MAC filter function.
MAC Restrict Mode	Select **Allow** to only permit the listed MAC addresses access to the Zyxel Device. Select **Deny** to permit anyone access to the Zyxel Device except the listed MAC addresses.
Set	This is the index number of the MAC address.
Active	Select **Active** to enable the MAC filter rule. The rule will not be applied if **Allow** is not selected under **MAC Restrict Mode**.
Host Name	Enter the host name of a wired LAN client that you want to allow access to the Zyxel Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC address of a wired LAN client that you want to allow access to the Zyxel Device. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the **Delete** icon to delete an existing rule.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

19.2.1 Add New Rule

You can choose to enable or disable the filters per entry; make sure that the checkbox under **Active** is selected if you want to use a filter, as shown in the example below. Select **Security** > **MAC Filter** > **Add New Rule**. The screen appears as shown.

Figure 200 Security > MAC Filter > Add New Rule



The following table describes the labels in this screen.

Table 115 Security > MAC Filter > Add New Rule

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
Active	Select **Active** to enable the MAC filter rule. The rule will not be applied if **Allow** is not selected under **MAC Restrict Mode**.
Host Name	Enter the host name of a wired LAN client that you want to allow access to the Zyxel Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC addresses of a wired LAN client that you want to allow access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the **Delete** icon to delete an existing rule.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 20
Home Security

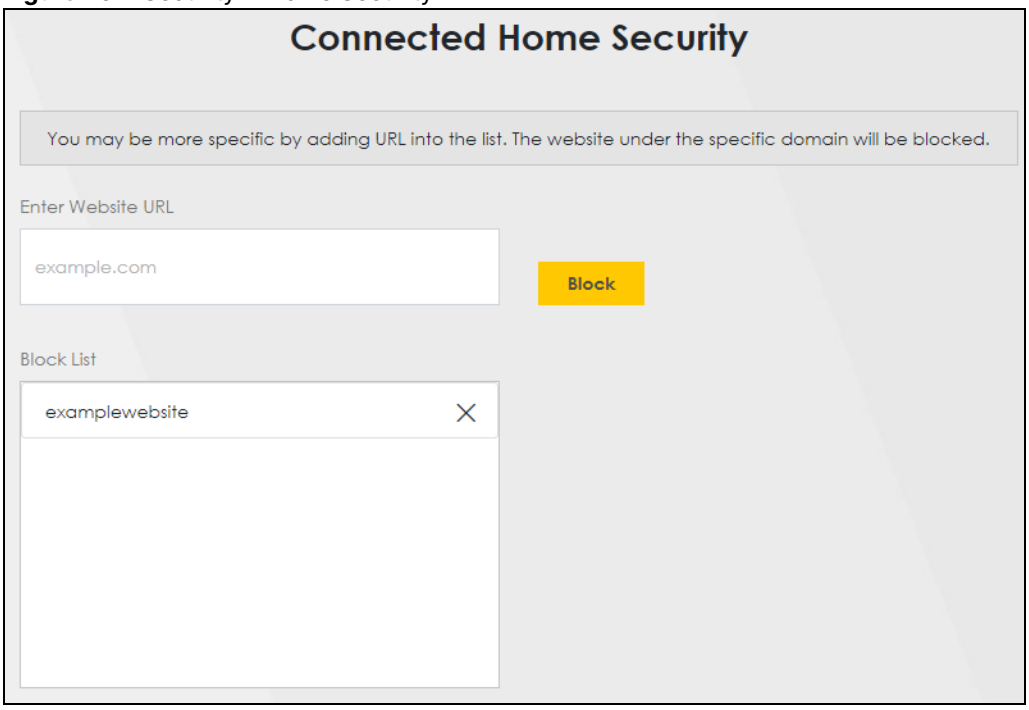
20.1 Home Security Overview

The Zyxel Device supports URL (Uniform Resource Locator) filtering that allows you to block user access to specific websites containing inappropriate or harmful content. Users on your network will not be able to enter the websites with URL domain names, keywords or full URLs you specify. Check Section 1.1 on page 19 to see if your Zyxel Device supports the Home Security feature.

20.2 Home Security

Use this screen to configure URL filtering settings to block users on your network from accessing certain websites. To access this screen, click **Security** > **Home Security**.

Figure 201 Security > Home Security



The following table describes the labels in this screen.

Table 116 Security > Home Security

LABEL	DESCRIPTION
Enter Website URL	Enter the URL of a website or URL keyword to which the Zyxel Device blocks access. Click **Block** to add the website to the **Block List**. Use keywords, domain names, or full URLs to block websites. For example, if you want to block a website with the domain name “www.exampleWeb.com”, you can use the following input formats: • http://exampleWeb.com • https://exampleWeb.com • exampleWeb.com • www.exampleWeb.com • example
Block List	The Zyxel Device prohibits users on your network from viewing the websites with the URLs/keywords in this block list. Click **x** to remove the entry from the list.

CHAPTER 21
Parental Control

21.1 Parental Control Overview

Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

Your parental control screens may be different depending on the model you are using. Some Zyxel Devices support scheduling, some support scheduling and URL filtering.

See Section 1.1 on page 19 for more information.

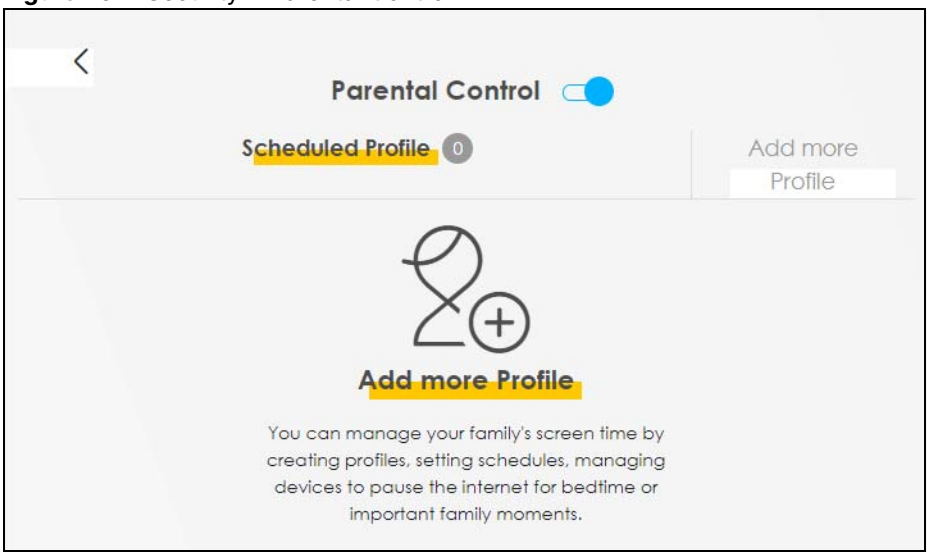
21.2 Parental Control Schedule

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet. These rules are defined in a Parental Control Profile (PCP).

Click **Security** > **Parental Control** to open the following screen.

Note: For some Zyxel Device models, you need to disable MESH to add a new parental control profile.

Figure 202 Security > Parental Control



The following table describes the fields in this screen.

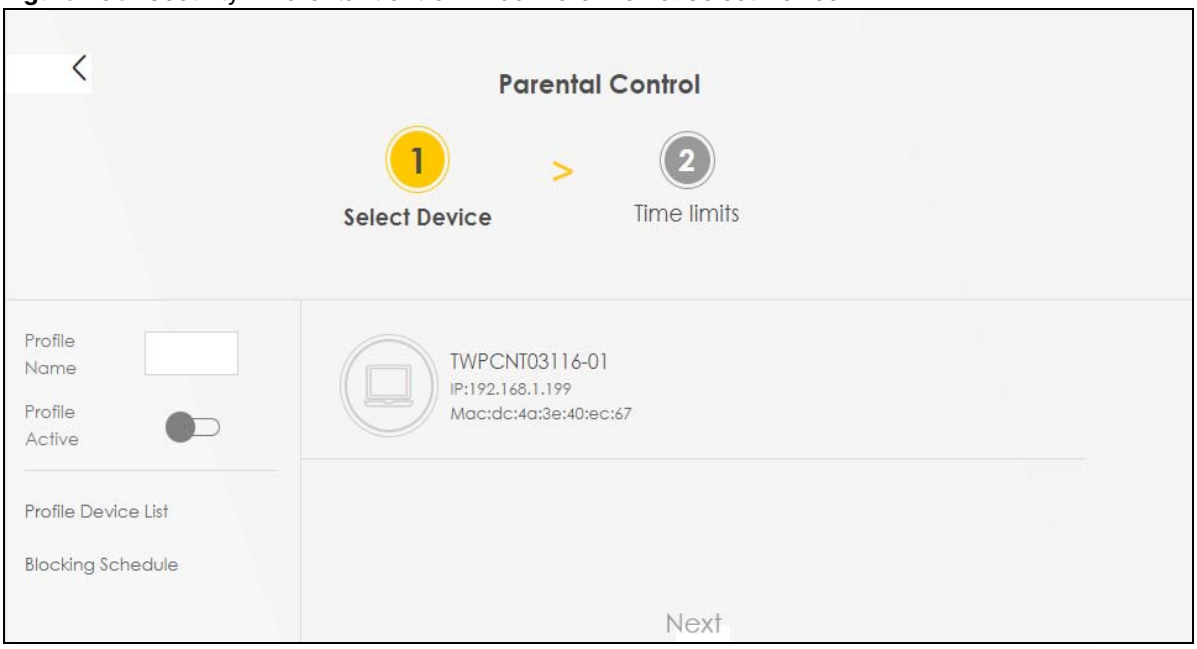
Table 117 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control.
Scheduled Profile	This screen shows all the created profiles.
Add more Profile	Click this button to create a new profile.

21.2.1 Add or Edit a Parental Control Profile

Click **Add more Profile** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule.

Figure 203 Security > Parental Control > Add more Profile: Select Device



The following table describes the fields in this screen.

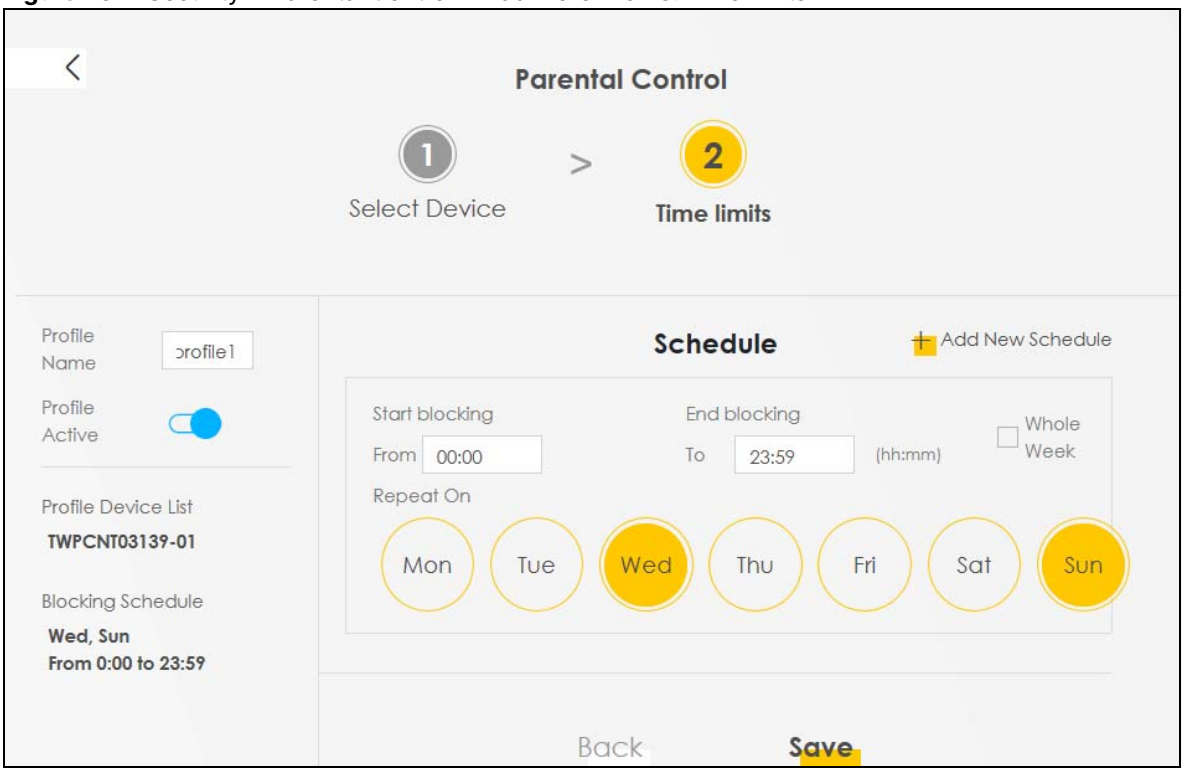
Table 118 Security > Parental Control > Add more Profile: Select Device

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Profile Active	Click this switch to enable or disable this profile.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile devices.
Next	Click **Next** to go to the next step to set a schedule for this profile.

21.2.2 Define a Schedule

This screen allow you to define time periods and days during which Internet access is blocked on the profile devices. Finish the settings in the **Select Device** step and click **Next** to access this screen.

Figure 204 Security > Parental Control > Add more Profile: Time limits



The following table describes the fields in this screen.

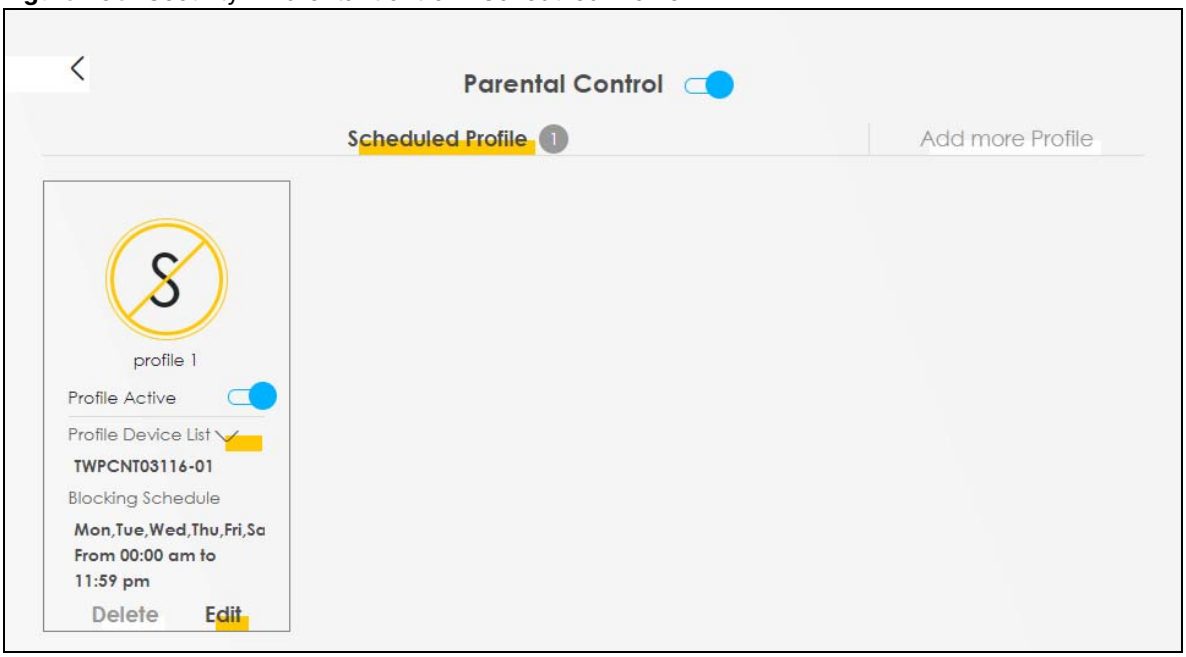
Table 119 Security > Parental Control > Add more Profile: Time limits

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable this profile. When the switch goes to the right ( ), this profile is active. Otherwise, it is not.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile devices.
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Start/End blocking	Select the time period when Internet access is blocked on the profile devices.
Repeat On	Select the days when Internet access is blocked on the profile devices. Select **Whole Week** and the scheduler rule will be activated for the whole week.
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save your changes.

21.2.3 Parental Control Scheduled Profile

Use this screen to view and manage the created parental control profiles.

Figure 205 Security > Parental Control > Scheduled Profile



The following table describes the fields in this screen.

Table 120 Security > Parental Control > Scheduled Profile

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not.
Profile Active	Click this switch to enable or disable a created profile. When the switch goes to the right ( ), this profile is active. Otherwise, it is not.
Scheduled Profile	This screen shows all the created profiles. Click beside **Profile Device List** to view more information about the profile. You can click **Delete** to remove the profile or click **Edit** to change the profile settings. Only the **Add more Profile** button displays if there is no profile created.
Add more Profile	Click this button to create a new profile.

CHAPTER 22
Scheduler Rule

22.1 Scheduler Rule Overview

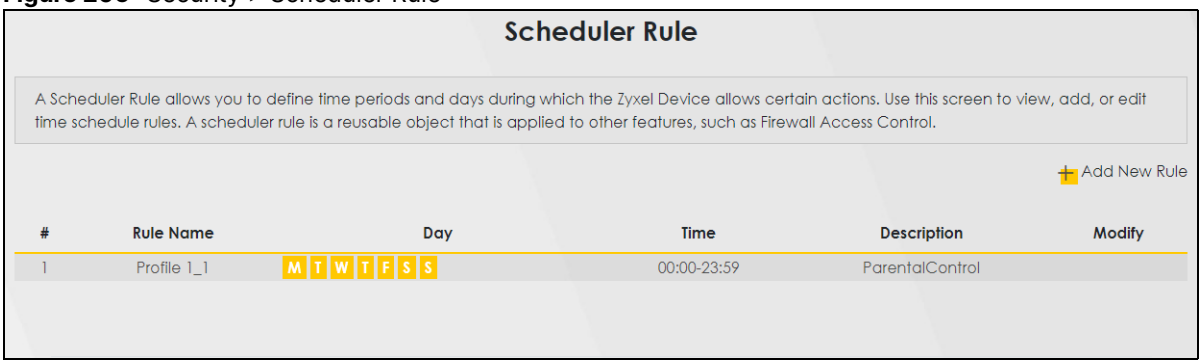
A Scheduler Rule allows you to define time periods and days during which the Zyxel Device allows certain actions.

22.2 Scheduler Rule Settings

Use this screen to view, add, or edit time schedule rules. A scheduler rule is a reusable object that is applied to other features, such as Firewall Access Control.

Click **Security** > **Scheduler Rule** to open the following screen.

Figure 206 Security > Scheduler Rule



The following table describes the fields in this screen.

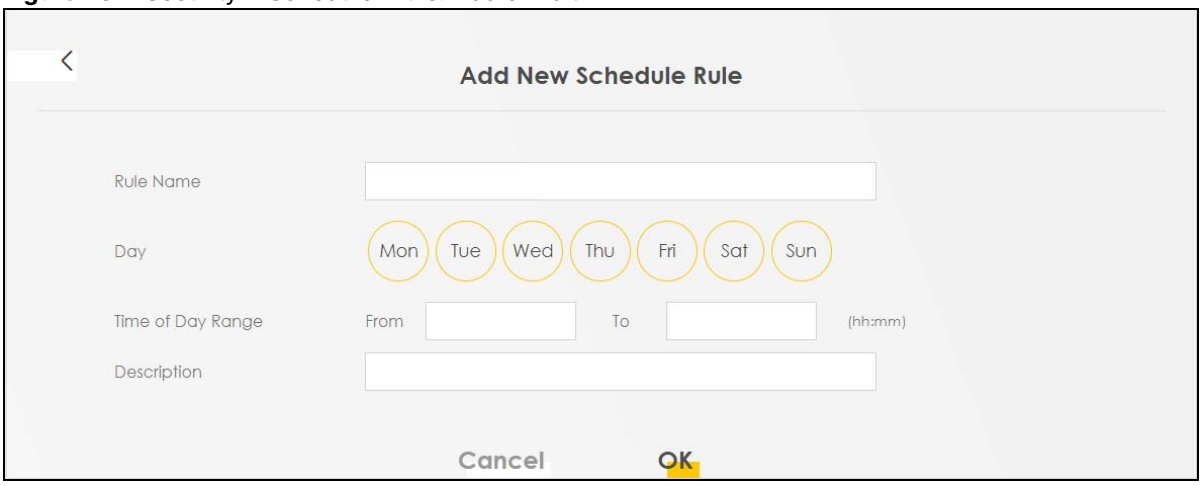
Table 121 Security > Scheduler Rule

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the days on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the **Edit** icon to edit the schedule. Click the **Delete** icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

22.2.1 Add or Edit a Schedule Rule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

Figure 207 Security > Scheduler Rule: Add or Edit



The following table describes the fields in this screen.

Table 122 Security > Scheduler Rule: Add or Edit

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name for this schedule. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Day	Select check boxes for the days that you want the Zyxel Device to perform this scheduler rule.
Time of Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
Description	Enter a description for this scheduler rule. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

CHAPTER 23
Certificates

23.1 Certificates Overview

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.

23.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Zyxel Device's CA-signed (Certification Authority) certificates (Section 23.3 on page 326).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer (Section 23.4 on page 331).

23.2 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 Zyxel Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

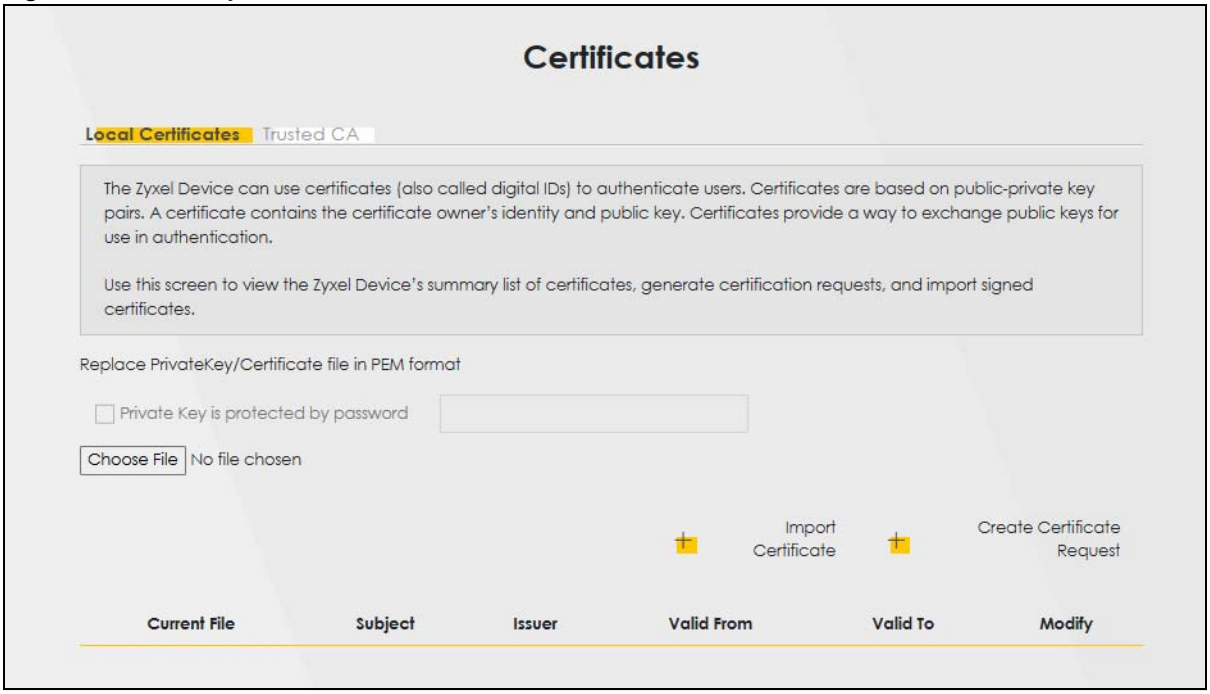
23.3 Local Certificates

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

- Web Server – This certificate secures HTTP connections.
- SSH – This certificate secures remote connections.

Click **Security** > **Certificates** to open the **Local Certificates** screen.

Figure 208 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

Table 123 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by password	Select the checkbox and enter the private key into the text box to store it on the Zyxel Device. You can use up to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
Choose File/ Browse	Click this button 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 Zyxel Device.
Create Certificate Request	Click this button to go to the screen where you can have the Zyxel Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have a unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.

Table 123 Security > Certificates > Local Certificates (continued)

LABEL	DESCRIPTION
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate. For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

23.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state or province name, and the default US two-letter country code (The US country code is by default and not changeable when sold in the U.S.) for the certificate.

Figure 209 Security > Certificates > Local Certificates: Create Certificate Request

The following table describes the labels in this screen.

Table 124 Security > Certificates > Local Certificates: Create Certificate Request

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

Table 124 Security > Certificates > Local Certificates: Create Certificate Request

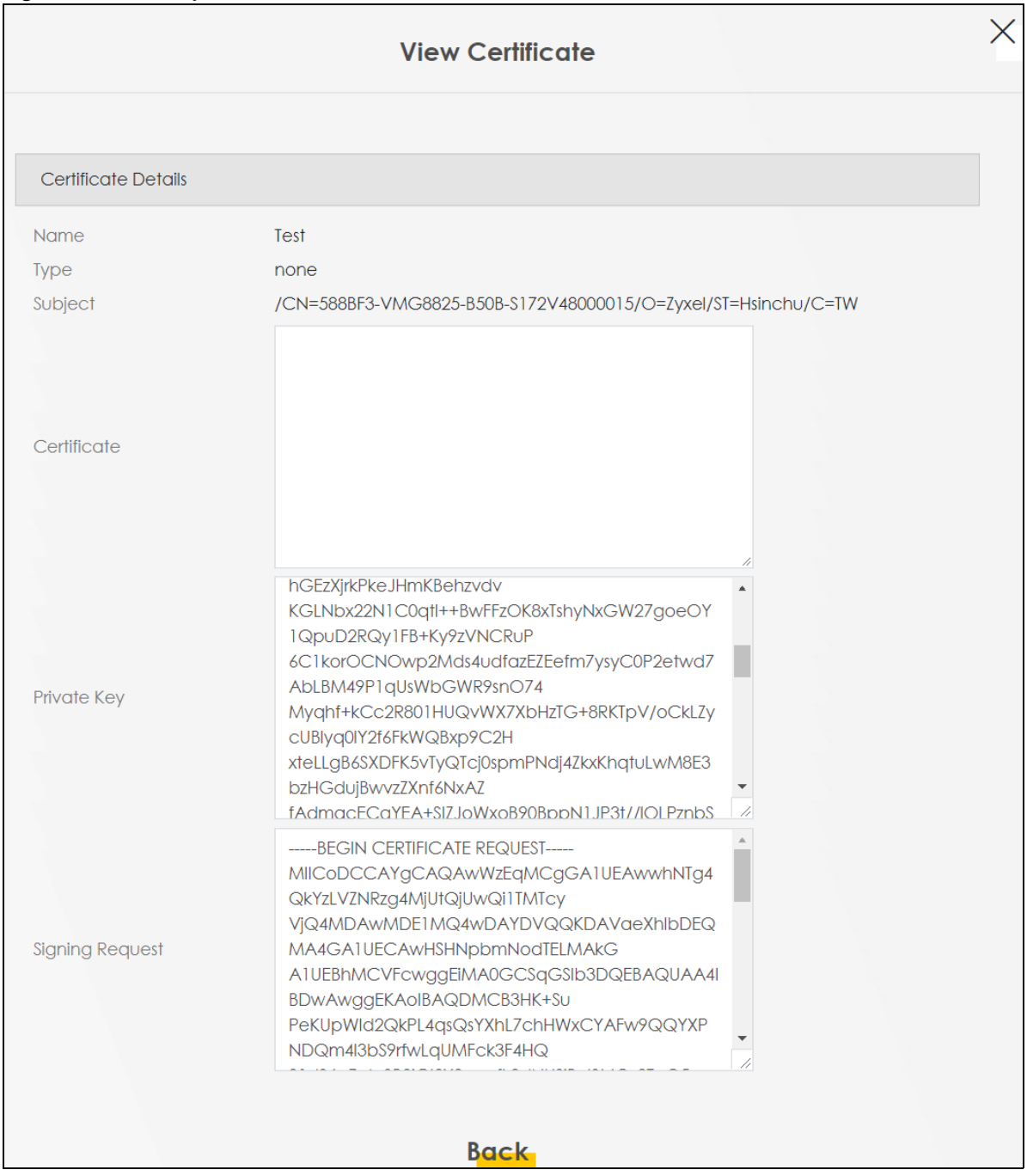
LABEL	DESCRIPTION
State/Province Name	Enter a descriptive name to identify the state or province where the certificate owner is located. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

23.3.2 View Certificate Request

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. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

Click the **View** icon in the **Local Certificates** screen to open the following screen.

Figure 210 Security > Certificates > Local Certificates: View Certificate



The following table describes the fields in this screen.

Table 125 Security > Certificates > Local Certificates: View Certificate

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

Table 125 Security > Certificates > Local Certificates: View Certificate (continued)

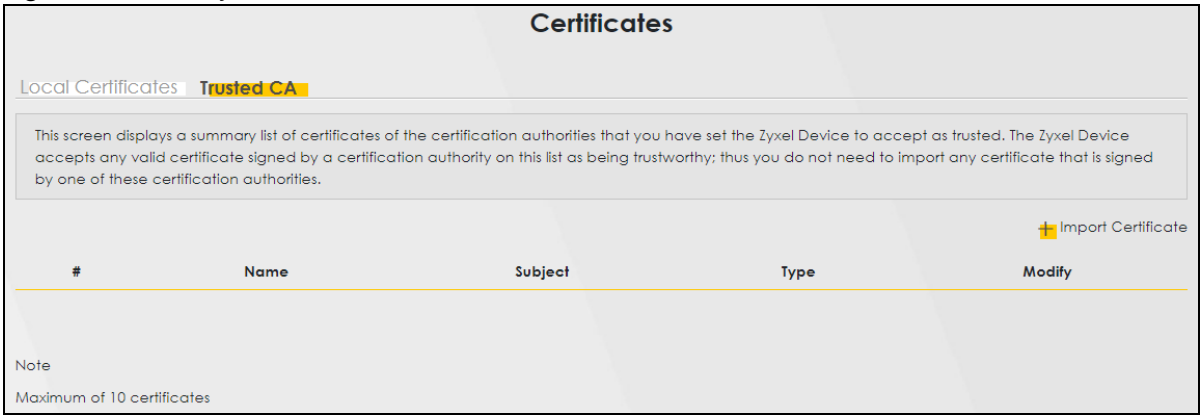
LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste 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.

23.4 Trusted CA

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

Note: A maximum of ten certificates can be added.

Figure 211 Security > Certificates > Trusted CA



The following table describes the labels in this screen.

Table 126 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this to open a screen where you can save the certificate of a certification authority that you trust to the Zyxel Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have a unique subject information.

Table 126 Security > Certificates > Trusted CA (continued)

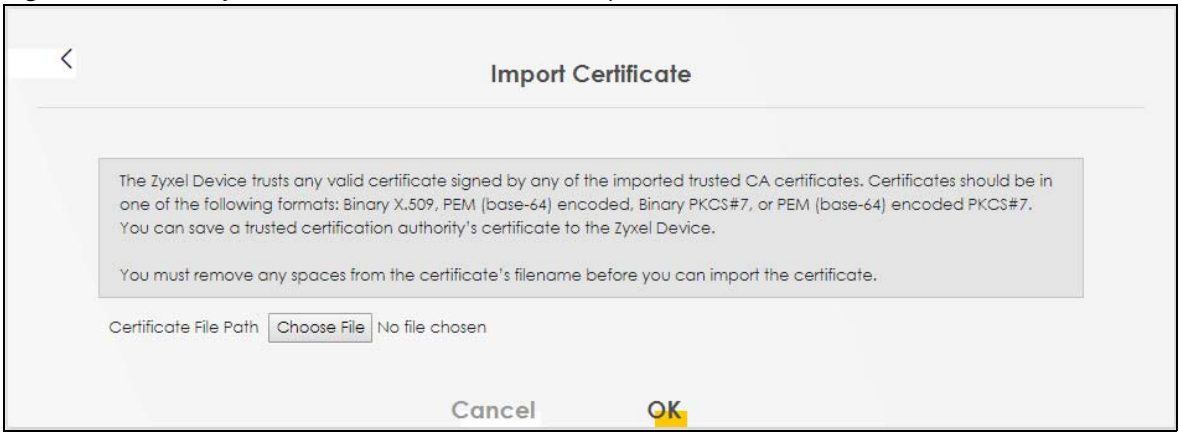
LABEL	DESCRIPTION
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

23.5 Import Trusted CA Certificate

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. The Zyxel 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.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 212 Security > Certificates > Trusted CA > Import Certificate



The following table describes the labels in this screen.

Table 127 Security > Certificates > Trusted CA > Import Certificate

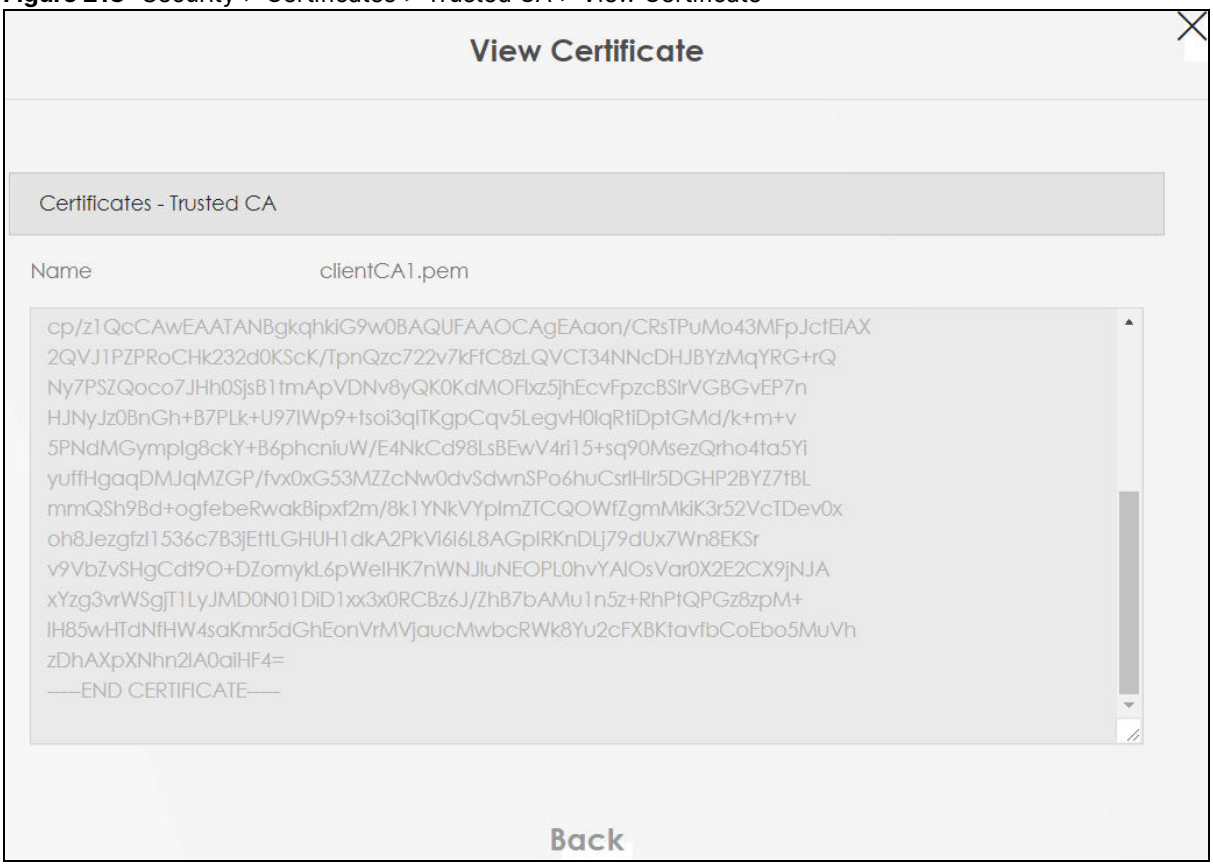
LABEL	DESCRIPTION
Certificate File Path	Enter the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it.
Choose File/ Browse	Click this to find the certificate file you want to upload.
OK	Click this to save the certificate on the Zyxel Device.
Cancel	Click this to exit this screen without saving.

23.6 View Trusted CA Certificate

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.

Click **Security** > **Certificates** > **Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 213 Security > Certificates > Trusted CA > View Certificate



The following table describes the labels in this screen.

Table 128 Security > Certificates > Trusted CA > View Certificate

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through USB thumb drive for example).
Back	Click this to return to the previous screen.

23.7 Certificates 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 Zyxel 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 Zyxel 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.

23.7.1 Verify a Certificate

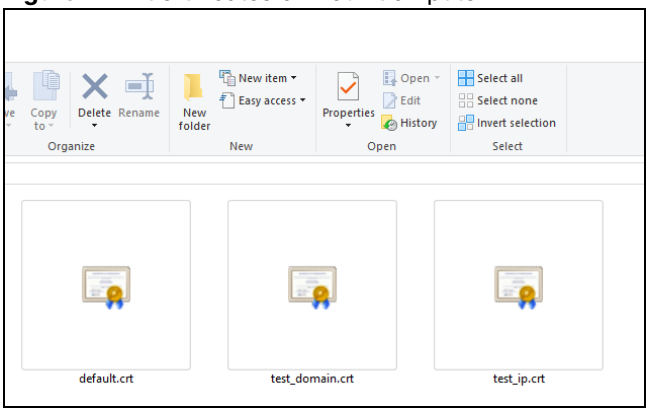
Before you import a trusted CA or trusted remote host certificate into the Zyxel Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the Zyxel Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

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.

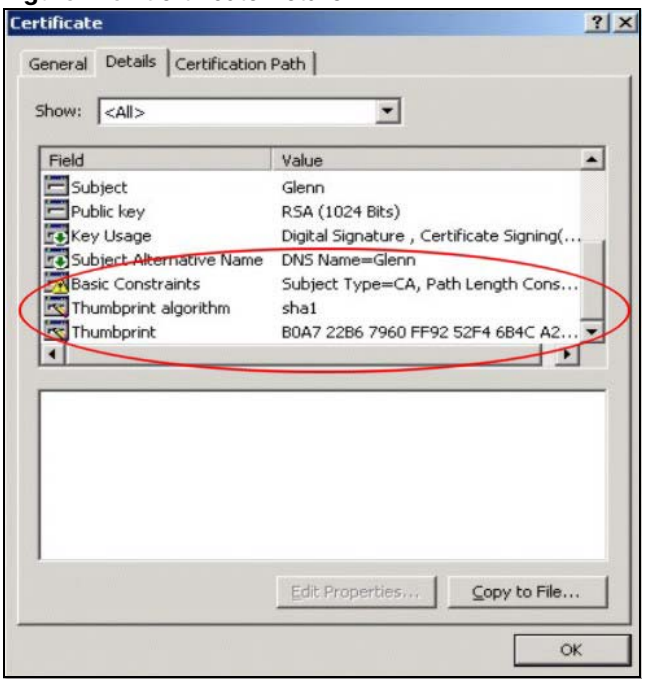
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 214 Certificates on Your Computer



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.

Figure 215 Certificate Details



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 24
Voice

24.1 Voice Overview

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

Use this chapter to:

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

24.1.1 What You Can Do in this Chapter

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

- Use the **SIP Account** screen to set up information about your SIP account, control which SIP accounts the phones connected to the Zyxel Device use, and configure audio settings such as volume levels for the phones connected to the Zyxel Device (Section 24.3 on page 338).
- Use the **SIP Service Provider** screen to configure the SIP server information, and the numbers for certain phone functions (Section 24.4 on page 345).
- Use the **SIP TLS Common** screen to change the default TLS local port if you need to, and select a local certificate for the SIP server to verify the Zyxel Device.(Section 24.5 on page 351).
- Use the **Phone** screens to change settings that depend on which region of the world the Zyxel Device is in (Section 24.6 on page 352).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 24.8 on page 355).
- Use the **Call History** screen to view a call history list (Section 24.9 on page 356).

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

24.1.2 What You Need to Know About VoIP

VoIP

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

SIP

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

SIP Accounts

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

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

SIP Address

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

24.2 Before You Begin

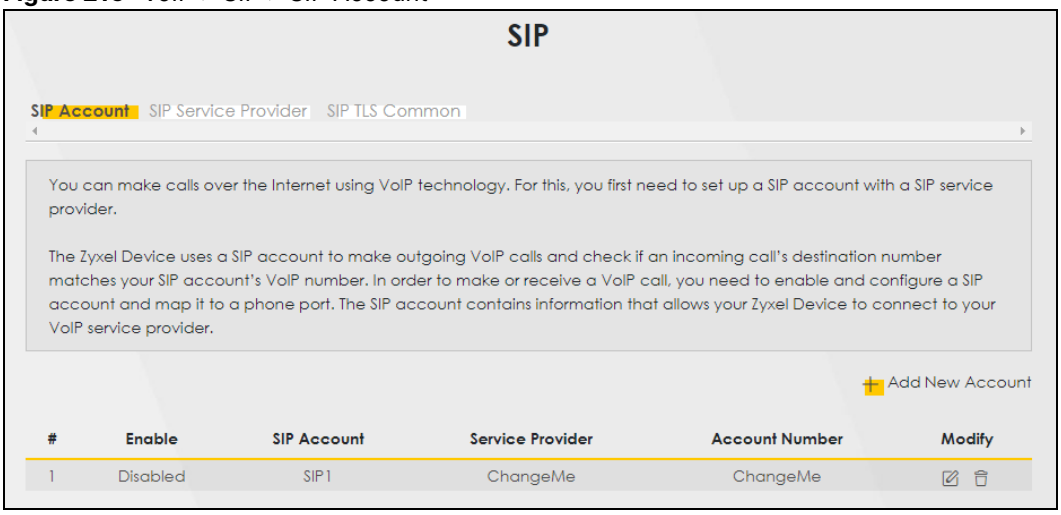
- Before you can use these screens, you need to have a VoIP account already set up. If you do not have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the Zyxel Device.

24.3 SIP Account

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

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

Figure 216 VoIP > SIP > SIP Account



The following table describes the labels in this screen.

Table 129 VoIP > SIP > SIP Account

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

24.3.1 Add or Edit SIP Account

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

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

Figure 217 VoIP > SIP > SIP Account > Add Account or Edit

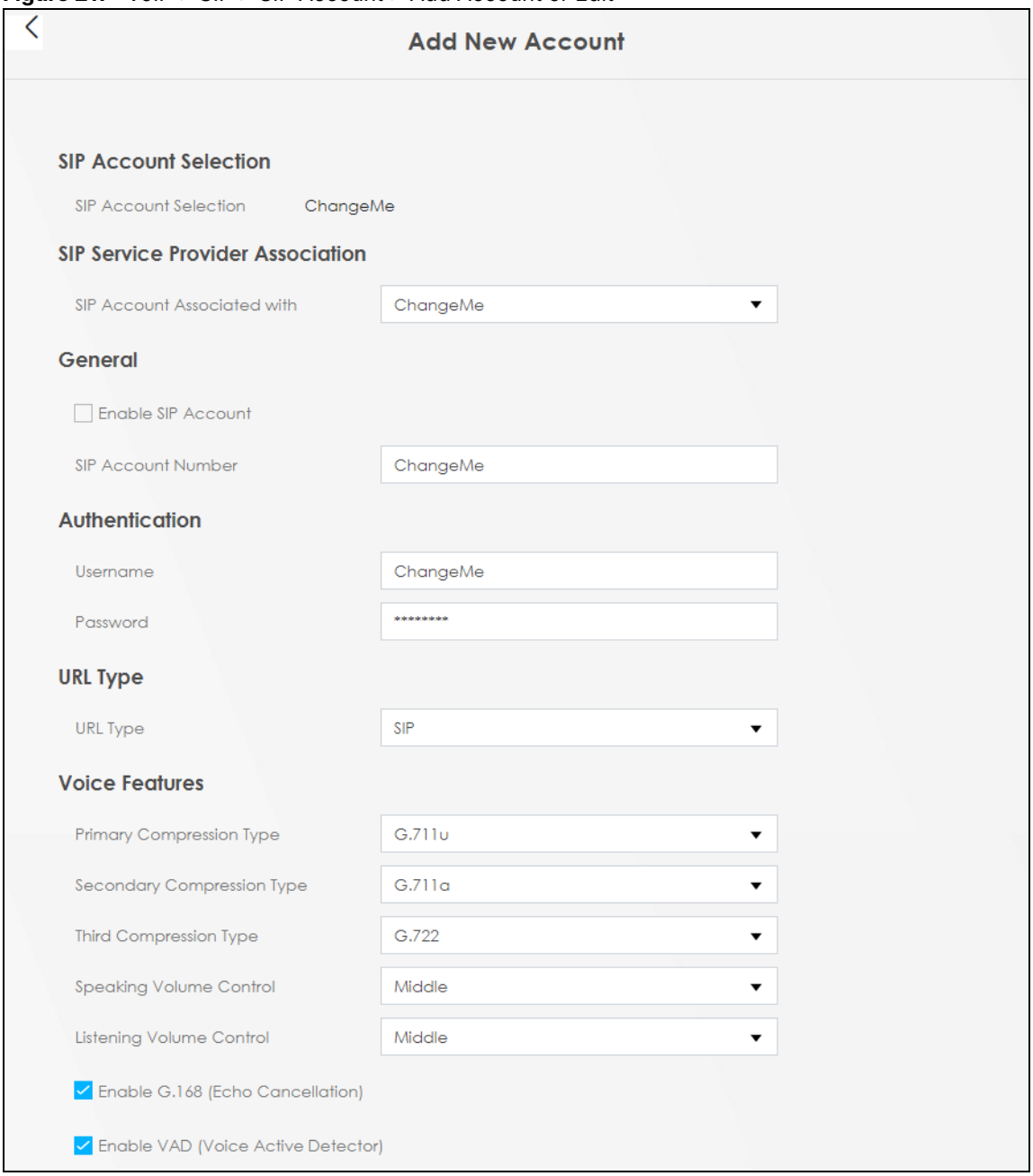


Figure 218 VoIP > SIP > SIP Account > Add Account or Edit (Call Features)

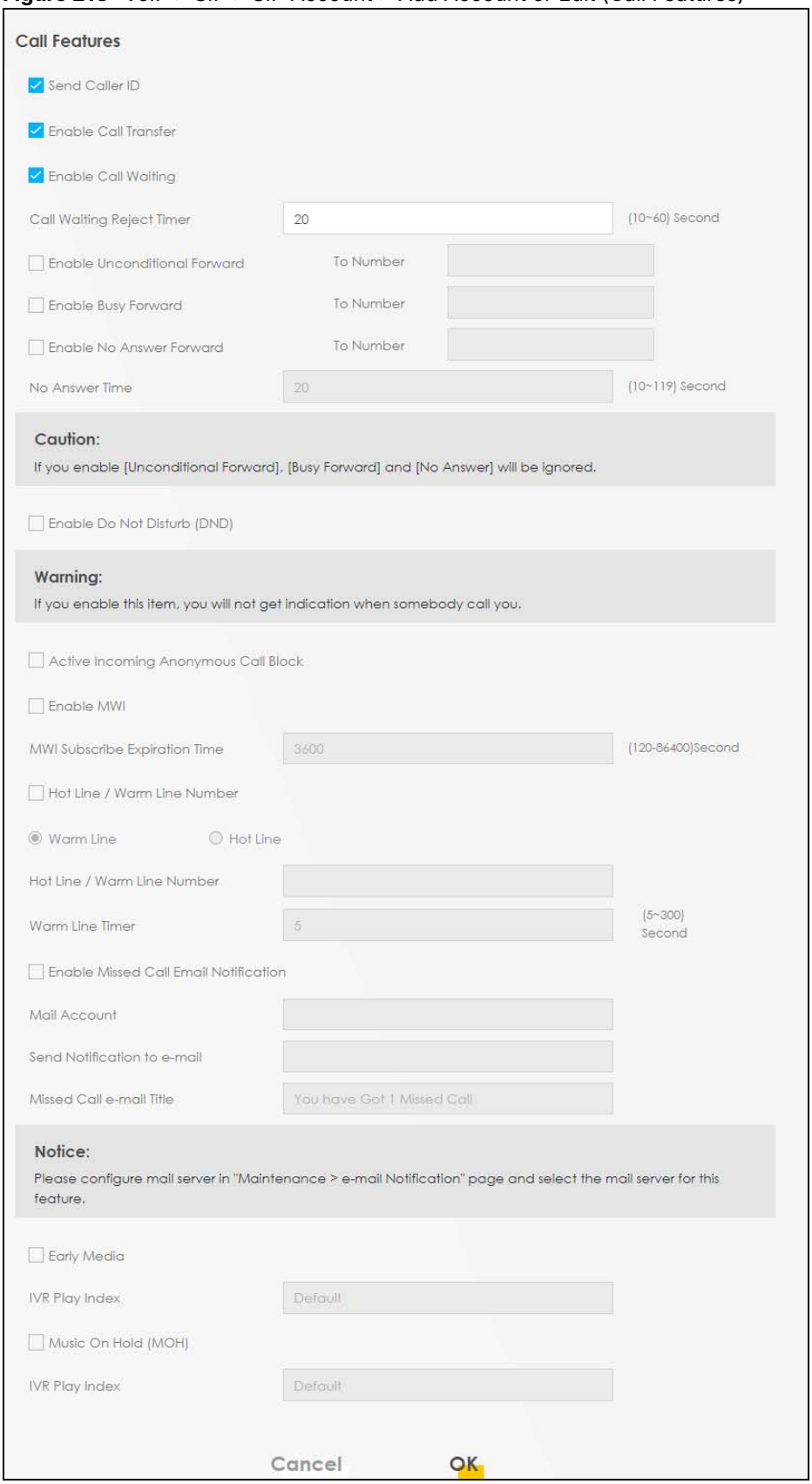
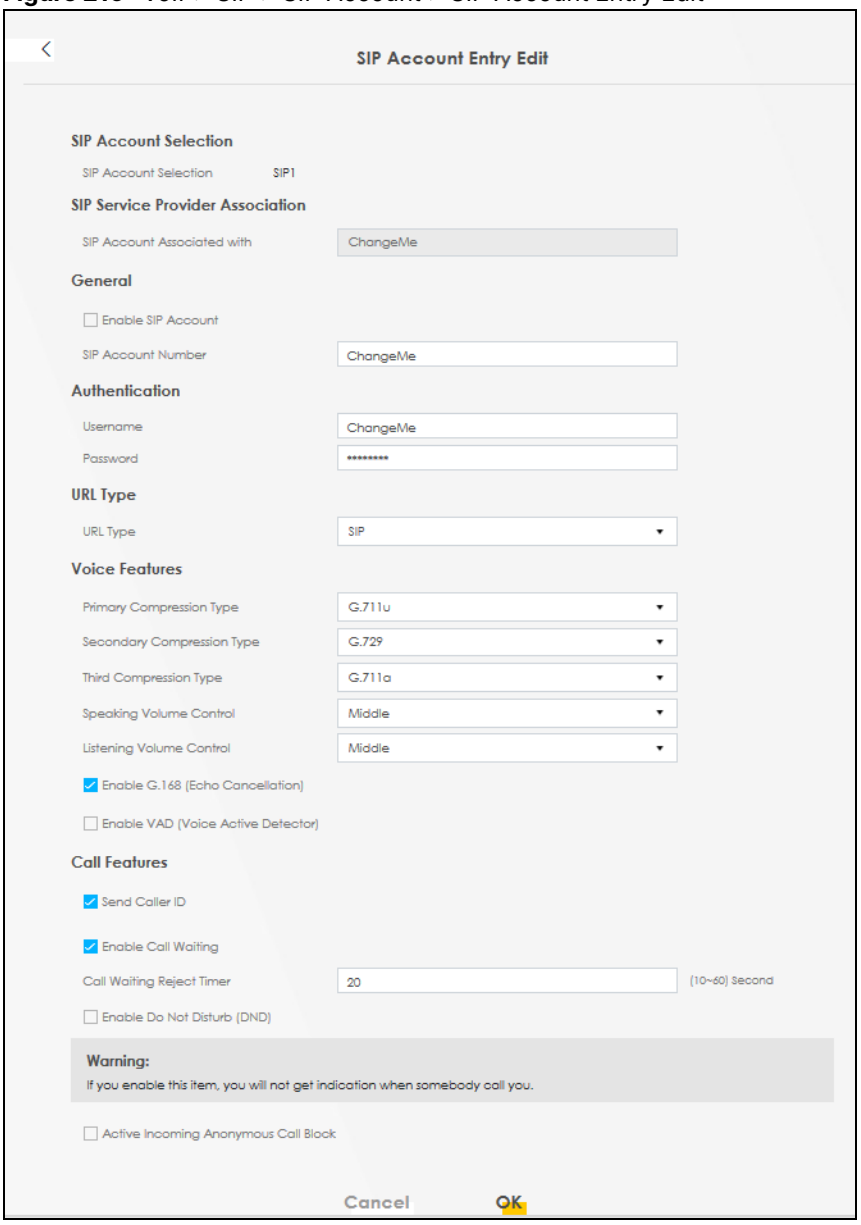


Figure 219 VoIP> SIP > SIP Account > SIP Account Entry Edit



The following table describes the labels in this screen.

Table 130 VoIP > SIP > SIP Account > SIP Account Entry Edit

LABEL	DESCRIPTION
SIP Account Selection	
SIP Account Selection	This field displays **ChangeMe** if you are creating a new SIP account or the SIP account you are modifying.
SIP Service Provider Association	
SIP Account Associated with	Select the SIP service provider profile to use for the SIP account you are configuring in this screen. You should already have configured a SIP service provider profile in the **SIP Service Provider** screen. This field is read-only when you are modifying an existing SIP account.
General	

Table 130 VoIP > SIP > SIP Account > SIP Account Entry Edit (continued)

LABEL	DESCRIPTION
Enable SIP Account	Select this if you want the Zyxel Device to use this account. Clear it if you do not want the Zyxel Device to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable characters and spaces.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 alphanumeric (0-9, a-z, A-Z), printable special characters and spaces.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 alphanumeric (0-9, a-z, A-Z), printable special characters and spaces.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the Zyxel Device sends the SIP number. **SIP** – include the SIP service domain name. **TEL** – do not include the SIP service domain name.
Voice Features	
Primary/Secondary/Third Compression Type	Select the type of voice coder or decoder (codec) that you want the Zyxel Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • **G.729** provides good sound quality and reduces the required bandwidth to 8 kbps. • **G.711a** is typically used in Europe. • **G.711u** is typically used in North America and Japan. • **G.726-24** operates at 24 kbps. • **G.726-32** operates at 32 kbps. • **G.722** operates at 6.3 kbps or 5.3 kbps. When two SIP devices start a SIP session, they must agree on a codec. Select the Zyxel Device's first choice for voice coder or decoder. Select the Zyxel Device's second choice for voice coder or decoder. Select **None** if you only want the Zyxel Device to accept the first choice. Select the Zyxel Device's third choice for voice coder or decoder. Select **None** if you only want the Zyxel Device to accept the first or second choice.
Speaking Volume Control	Select the loudness that the Zyxel Device uses for speech that it sends to the peer device. Choices are **Minimum**, **Middle**, and **Maximum**.
Listening Volume Control	Select the loudness that the Zyxel Device uses for speech that it receives from the peer device. Choices are **Minimum**, **Middle**, and **Maximum**.
Enable G. 168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Enable VAD (Voice Active Detector)	Select this if the Zyxel Device should stop transmitting when you are not speaking. This reduces the bandwidth the Zyxel Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Enable Call Transfer	Select this to enable call transfer on the Zyxel Device. This allows you to transfer an incoming call (that you have answered) to another phone.

Table 130 VoIP > SIP > SIP Account > SIP Account Entry Edit (continued)

LABEL	DESCRIPTION
Enable Call Waiting	Select this to enable call waiting on the Zyxel Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Call Waiting Reject Timer	Specify a time of seconds that the Zyxel Device waits before rejecting the second call if you do not answer it.
Enable Unconditional Forward	Select this if you want the Zyxel Device to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Enable Busy Forward	Select this if you want the Zyxel Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Enable No Answer Forward	Select this if you want the Zyxel Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the Zyxel Device should wait for you to answer an incoming call before it considers the call unanswered.
Enable Do Not Disturb (DND)	Select this to turn the do not disturb feature on. This has the Zyxel Device reject all calls destined to the phone line.
Active Incoming Anonymous Call Block	Select this to have the phone not ring for incoming calls with caller ID deactivated.
Enable MWI	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
MWI Subscribe Expiration Time	Keep the default value of this field unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the Zyxel Device subscribes to the service. Before this time passes, the Zyxel Device automatically subscribes again.
Hot Line / Warm Line Number	Select this to enable the hot line or warm line feature on the Zyxel Device.
Hot Line	Select this to have the Zyxel Device dial the specified hot line number immediately when you pick up the telephone.
Warm Line	Select this to have the Zyxel Device dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line / Warm Line Number	Enter the number of the hot line or warm line that you want the Zyxel Device to dial.
Warm Line Timer	Enter a number of seconds that the Zyxel Device waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Enable Missed Call Email Notification	Select this option to have the Zyxel Device email you a notification when there is a missed call.
Mail Account	Select a mail account for the email address specified below. If you select **None** here, email notifications will not be sent through email. You must have configured a mail account already in the **Email Notification** screen.
Send Notification to e-mail	Notifications are sent to the email address specified in this field. If this field is left blank, notifications will not be sent through email.

Table 130 VoIP > SIP > SIP Account > SIP Account Entry Edit (continued)

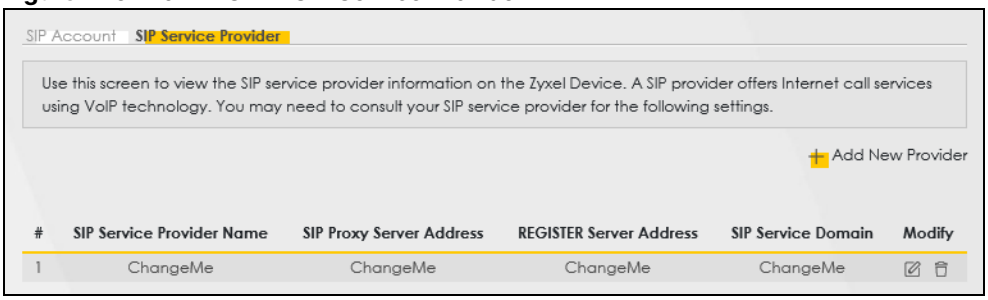
LABEL	DESCRIPTION
Missed Call e-mail Title	Type a title that you want to be in the subject line of the email notifications that the Zyxel Device sends.
Early Media	Select this if you want people to hear a customized recording when they call you.
IVR Play Index	Select the tone you want people to hear when they call you. This field is configurable only when you select **Early Media**. See Section 24.10 on page 358 for information on how to record these tones.
Music On Hold (MOH)	Select this to play a customized recording when you put people on hold.
IVR Play Index	Select the tone to play when you put someone on hold. This field is configurable only when you select **Music on Hold**, See Section 24.10 on page 358 for information on how to record these tones.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

24.4 SIP Service Provider

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

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

Figure 220 VoIP > SIP > SIP Service Provider



The following table describes the labels in this screen.

Table 131 VoIP > SIP > SIP Service Provider

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

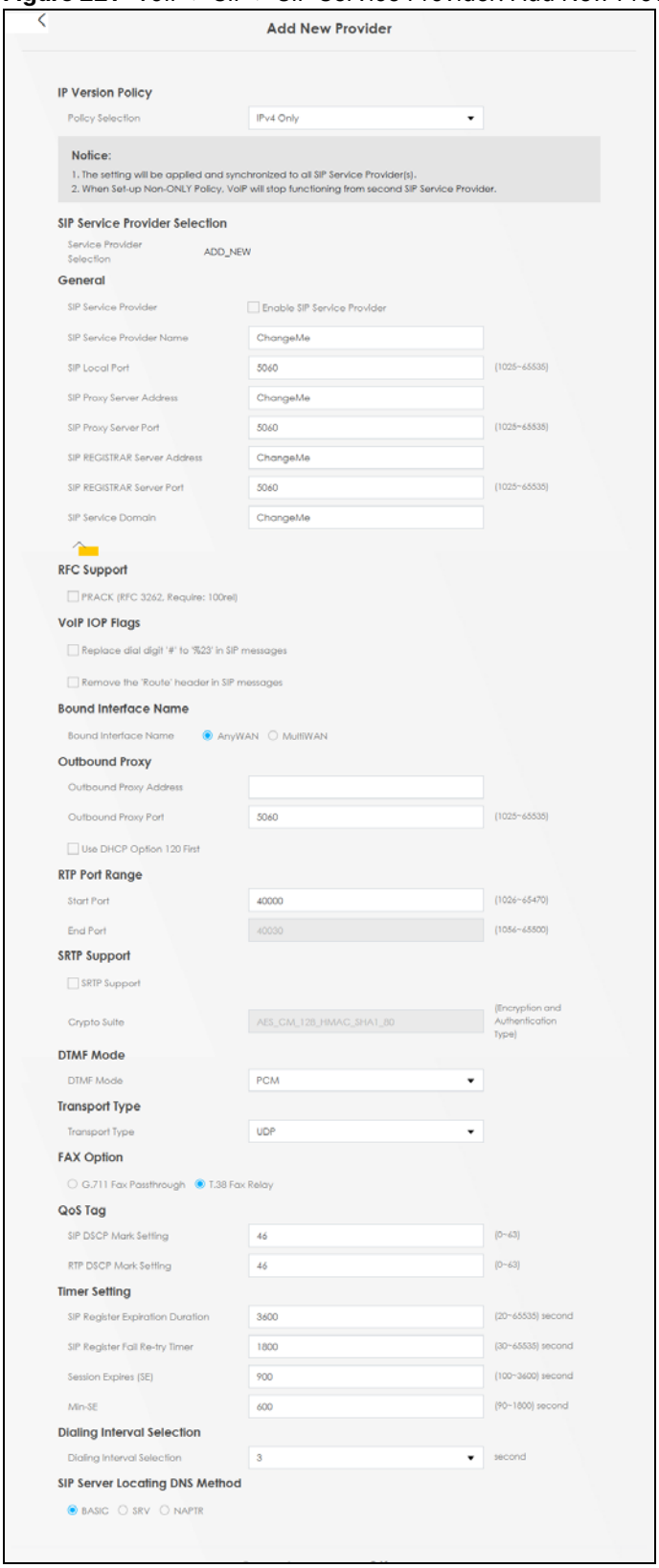
24.4.1 Provider Entry Add/Edit

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

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

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

Figure 221 VoIP > SIP > SIP Service Provider: Add New Provider or Edit



The following table describes the labels in this screen.

Table 132 VoIP > SIP > SIP Service Provider > Add New Provider or Edit

<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>IP Version Policy</td><td></td></tr>
<tr><td>Policy Selection</td><td>Select the Internet Protocol version that the SIP service provider supports.
• Select IPv4 Only if the SIP service provider supports an IPv4 IP address.
• Select IPv6 Only if the SIP service provider supports an IPv6 IP address.
• Select IPv4 Prefer to use an IPv4 address over an IPv6 address. If an IPv4 address is not available on the interface, the SIP service provider uses an IPv6 address. The SIP service provider changes to an IPv4 address whenever an IPv4 address is available. This selection applies only to the first service provider.
• Select IPv6 Prefer to use an IPv6 address over an IPv4 address. If an IPv6 address is not available on the interface, the SIP service provider uses an IPv4 address. The SIP service provider changes to an IPv6 address whenever an IPv6 address is available. This selection applies only to the first service provider.
• Select IPv4 First to use an IPv4 address over an IPv6 address. If an IPv4 address is not available on the interface, the SIP service provider uses an IPv6 address. The SIP service provider selects the IP version based on the first available IP version. This selection applies only to the first service provider.
• Select IPv6 First to use an IPv6 address over an IPv4 address. If an IPv6 address is not available on the interface, the SIP service provider uses an IPv4 address. The SIP service provider selects the IP version based on the first available IP version. This selection applies only to the first service provider.
Note: Rebooting or resetting the Zyxel Device may cause the SIP service provider to use a different IP version.
<table>
<tr><th></th><th>ISP supports an IPv4 address</th><th>ISP supports an IPv6 address</th><th>ISP supports both IPv4 and IPv6 addresses</th></tr>
<tr><td>IPv4 Only</td><td>V</td><td>X</td><td>IPv4</td></tr>
<tr><td>IPv6 Only</td><td>X</td><td>V</td><td>IPv6</td></tr>
<tr><td>IPv4 Prefer</td><td>V</td><td>V</td><td>IPv4 ↔ IPv6</td></tr>
<tr><td>IPv6 Prefer</td><td>V</td><td>V</td><td>IPv6 ↔ IPv4</td></tr>
<tr><td>IPv4 First</td><td>V</td><td>V</td><td>IPv4; otherwise IPv6</td></tr>
<tr><td>IPv6 First</td><td>V</td><td>V</td><td>IPv6; otherwise IPv4</td></tr>
</table>
</td></tr>
<tr><td>SIP Service Provider Selection</td><td></td></tr>
<tr><td>General</td><td></td></tr>
<tr><td>SIP Service Provider</td><td>Select this if you want the Zyxel Device to use this SIP provider. Clear it if you do not want the Zyxel Device to use this SIP provider.</td></tr>
<tr><td>SIP Service Provider Name</td><td>Enter the name of your SIP service provider.</td></tr>
<tr><td>SIP Local Port</td><td>Enter the Zyxel Device’s listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.</td></tr>
<tr><td>SIP Proxy Server Address</td><td>Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. It does not matter whether the SIP server is a proxy, redirect or register server.</td></tr>
<tr><td>SIP Proxy Server Port</td><td>Enter the SIP server’s listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.</td></tr>
</table>

Table 132 VoIP > SIP > SIP Service Provider > Add New Provider or Edit (continued)

LABEL	DESCRIPTION
SIP REGISTRAR Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].
SIP REGISTRAR Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].
RFC Support	
VoIP IOP Flags – Select VoIP inter-operability settings.	
Replace dial digit '#' to '%23' in SIP messages	Replace a dial digit "#" with "%23" in the INVITE messages.
Remove the 'Route' header in SIP messages	Remove the 'Route' header in SIP packets.
Bound Interface Name	
Bound Interface Name	If you select **AnyWAN**, the Zyxel Device automatically activates the VoIP service when any WAN connection is up. If you select **MultiWAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Zyxel Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Zyxel Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
Use DHCP Option 120 first	Select this to have the Zyxel Device use DHCP Option 120 first.
RTP Port Range	
Start/End Port	Enter the listening port numbers for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
SRTP Support	

Table 132 VoIP > SIP > SIP Service Provider > Add New Provider or Edit (continued)

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

Table 132 VoIP > SIP > SIP Service Provider > Add New Provider or Edit (continued)

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

24.5 SIP TLS Common

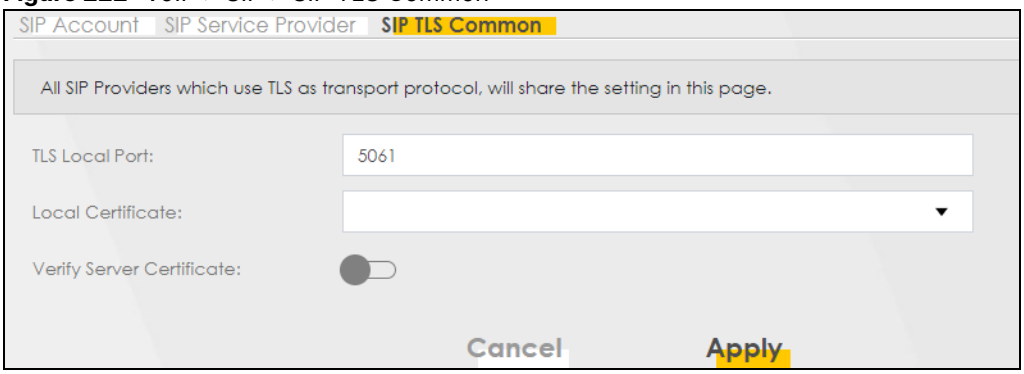
Use this screen to:

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

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

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

Figure 222 VoIP > SIP > SIP TLS Common



The following table describes the labels in this screen.

Table 133 VoIP > SIP > SIP TLS Common

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

24.6 Phone

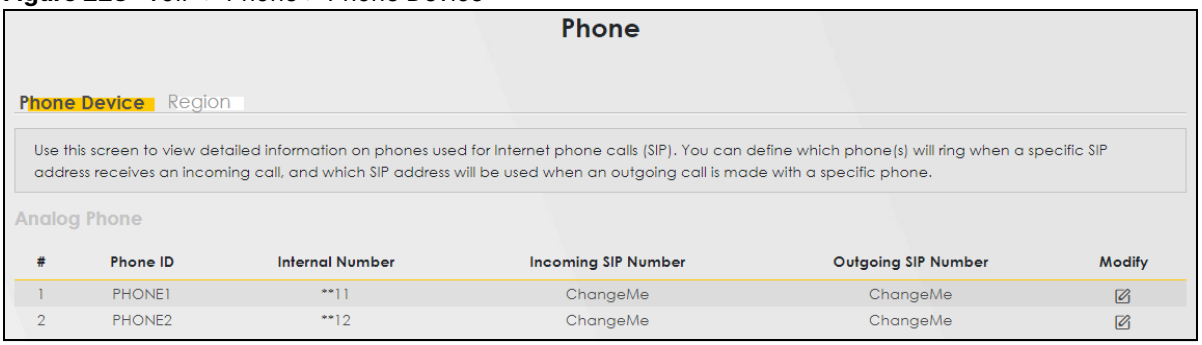
Use these screens to configure SIP numbers and regions for IP phones that are connected to the Zyxel Device.

24.6.1 Phone Device

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

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

Figure 223 VoIP > Phone > Phone Device



Each field is described in the following table.

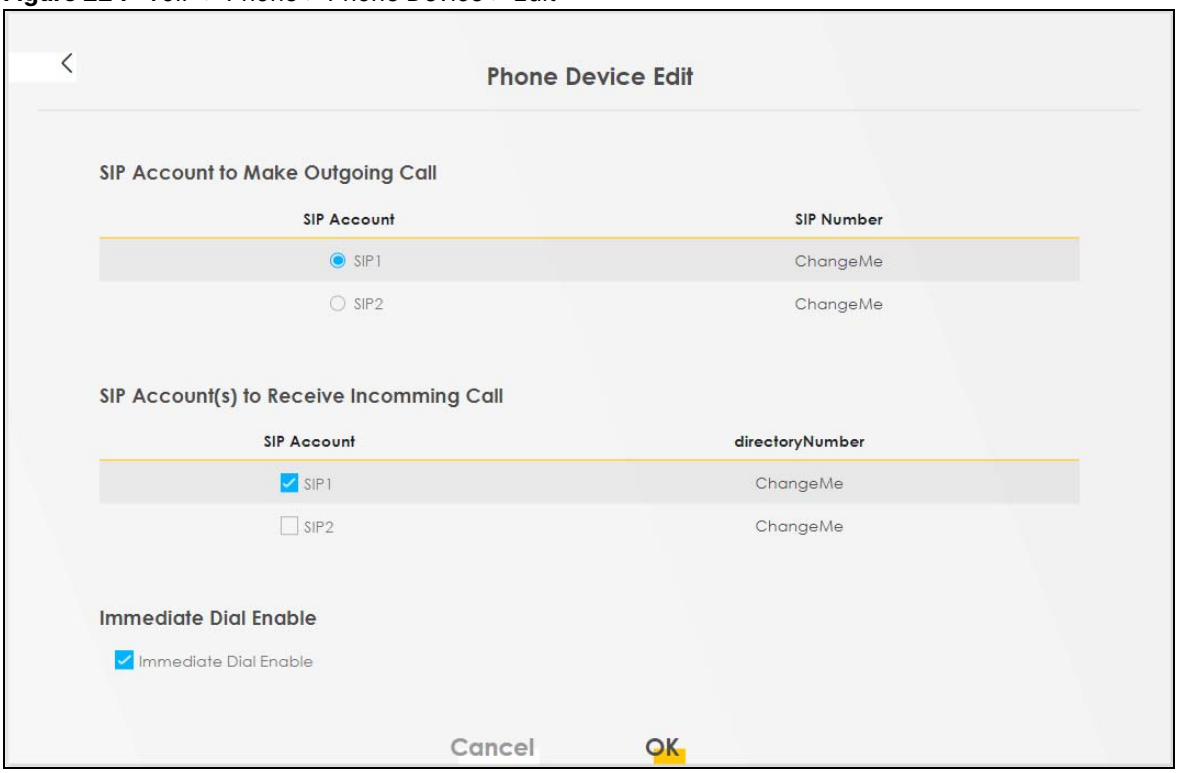
Table 134 VoIP > Phone > Phone Device

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

24.6.2 Phone Device Edit

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

Figure 224 VoIP > Phone > Phone Device > Edit



Each field is described in the following table.

Table 135 VoIP > Phone > Phone Device > Edit

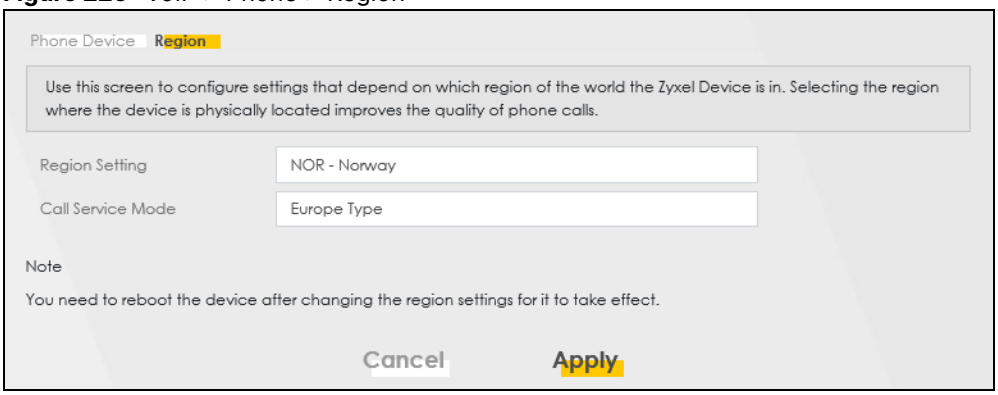
LABEL	DESCRIPTION
SIP Account to Make Outgoing Call	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Account(s) to Receive Incoming Call	Select a SIP account if you want to receive phone calls for the selected SIP account on this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

24.7 Phone Region

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

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

Figure 225 VoIP > Phone > Region



The following table describes the labels in this screen.

Table 136 VoIP > Phone > Region

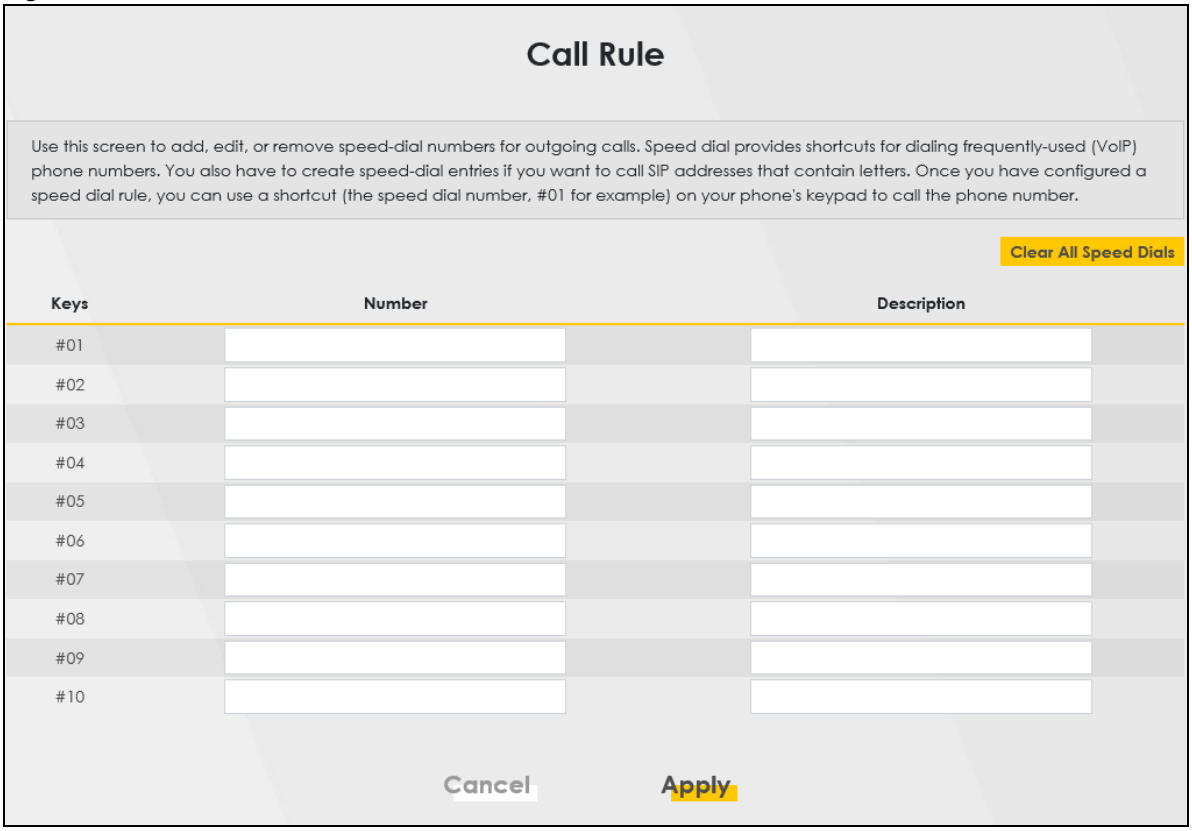
LABEL	DESCRIPTION
Region Setting	Select the place in which the Zyxel Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. • **Europe Type** – use supplementary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

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

24.8 Call Rule

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

Figure 226 VoIP > Call Rule



The following table describes the labels in this screen.

Table 137 VoIP > Call Rule

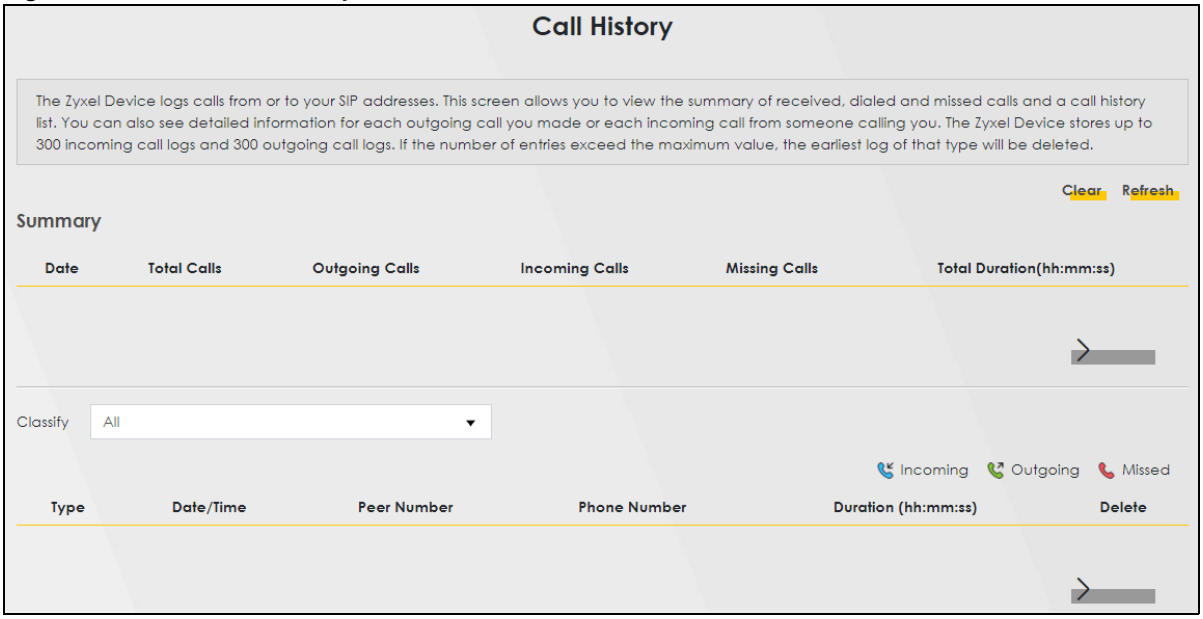
LABEL	DESCRIPTION
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the Zyxel Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number.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

24.9 Call History

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

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

Figure 227 VoIP > Call History



Each field is described in the following table.

Table 138 VoIP > Call History

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

Table 138 VoIP > Call History

LABEL	DESCRIPTION
Duration (hh:mm:ss)	This displays how long the call lasted.
Modify	Click the **Delete** icon to remove the call history.
Delete	Click the **Delete** icon to remove the call history.

24.10 Technical Reference

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

VoIP

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

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

SIP

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

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

SIP Identities

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

SIP Number

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

SIP Service Domain

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

SIP Registration

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

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

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

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

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

Authorization Requirements

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

SIP Servers

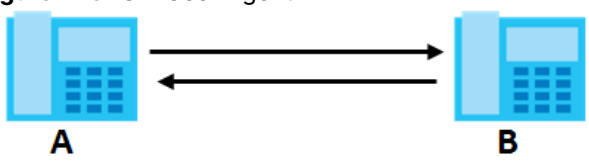
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

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

SIP User Agent

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

Figure 228 SIP User Agent



SIP Proxy Server

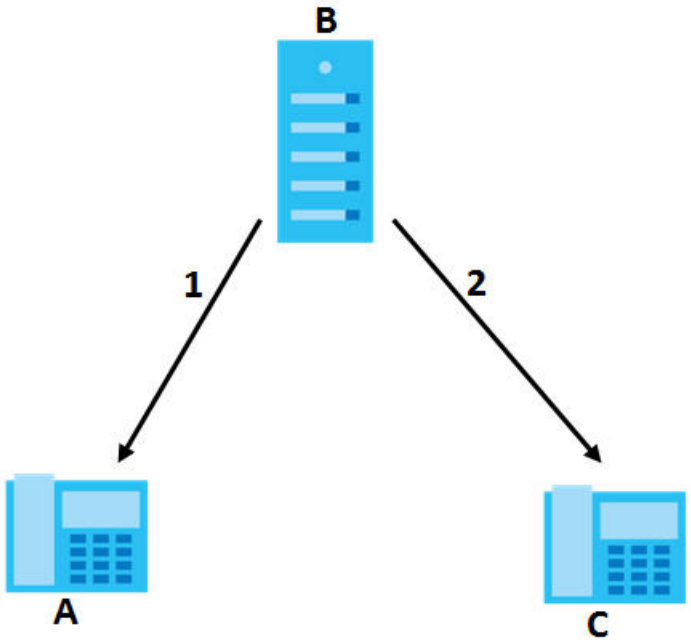
A SIP proxy server receives requests from clients and forwards them to another server.

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

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

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

Figure 229 SIP Proxy Server



SIP Redirect Server

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

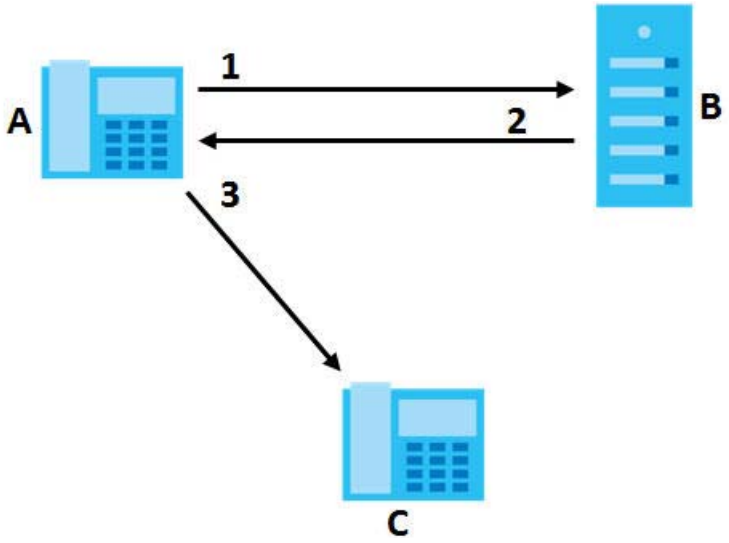
In the following example, you want to use client device **A** to call someone who is using client device **C**.

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

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

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

Figure 230 SIP Redirect Server



SIP Register Server

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

RTP

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

Pulse Code Modulation

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

SIP Call Progression

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

Table 139 SIP Call Progression

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

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

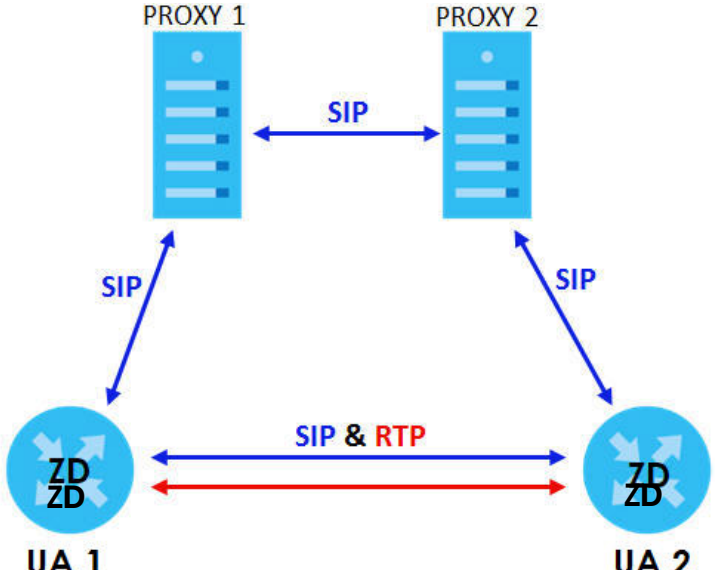
SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

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

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

Figure 231 SIP Call Through Proxy Servers

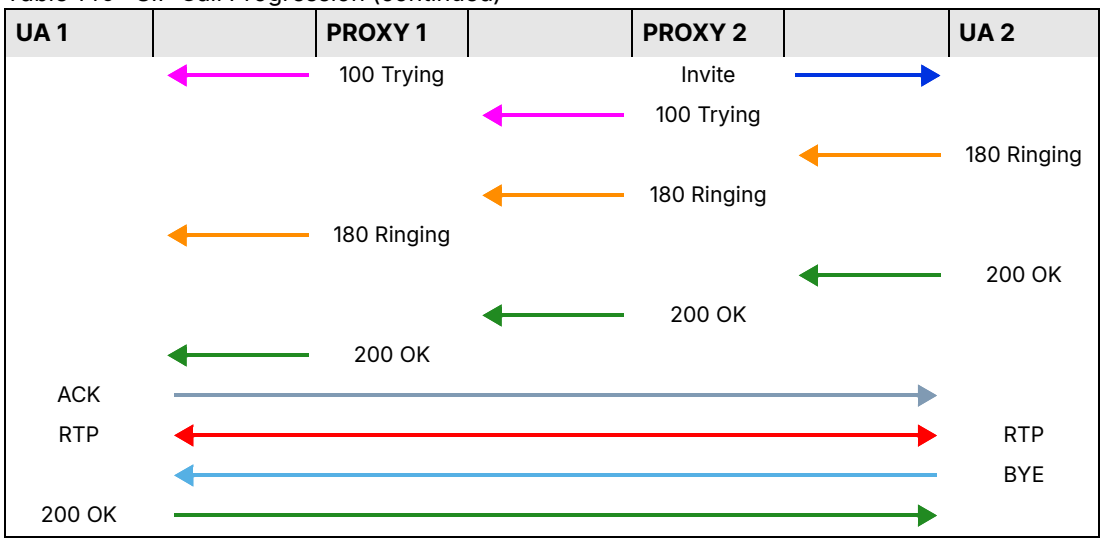


The following table shows the SIP call progression.

Table 140 SIP Call Progression

UA 1		PROXY 1		PROXY 2		UA 2
Invite →						
		Invite →				

Table 140 SIP Call Progression (continued)



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

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

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

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

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

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

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

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

Voice Coding

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

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

- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

Voice Activity Detection/Silence Suppression

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

Comfort Noise Generation

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

Echo Cancellation

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

MWI (Message Waiting Indication)

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

Custom Tones (IVR)

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

Table 141 Custom Tones Details

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

Recording Custom Tones

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

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

2 Press a number from 1101 – 1105 on your phone followed by the “#” key.

3 Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.

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

Listening to Custom Tones

Do the following to listen to a custom tone:

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

2 Press a number from 1201 – 1208 followed by the "#" key to listen to the tone.

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

Deleting Custom Tones

Do the following to delete a custom tone:

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

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

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

24.10.1 Quality of Service (QoS)

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

Type of Service (ToS)

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

DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[3]

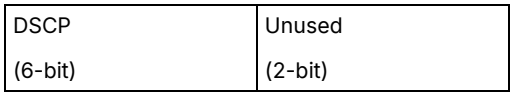
3. The Zyxel Device does not support DiffServ at the time of writing.

DSCP and Per-Hop Behavior

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

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

Figure 232 DiffServ: Differentiated Service Field



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

24.10.2 Phone Services Overview

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

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

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

24.10.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the

same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Zyxel Device.

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

24.10.2.2 Europe Type Supplementary Phone Services

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

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

Table 142 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

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

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

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

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

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

European Call Waiting

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

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

- Reject the second call.

  Press the flash key and then press “0”.

- Disconnect the first call and answer the second call.

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

  Press the flash key and then “2”.

European Call Transfer

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

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

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

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

European Three-Way Conference

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

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

2 Dial a phone number directly to make another call.

3 When the second call is answered, press the flash key and press “3” to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

24.10.2.3 USA Type Supplementary Services

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

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

Table 143 USA Flash Key Commands

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

USA Call Hold

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

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

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

USA Call Waiting

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

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

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

USA Call Transfer

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

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

USA Three-Way Conference

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

1. When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call (to party B).
3. When party B answers the second call, press the flash key to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.
6. If you want to go back to the three-way conversation, press the flash key again.
7. If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

24.10.2.4 Phone Functions Summary

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

Table 144 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
*98#	Call transfer	Transfer a call to another phone. See Section 24.10.2.2 on page 367 (Europe type) and Section 24.10.2.3 on page 368 (USA type).
*66#	Call return	Place a call to the last person who called you.
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off.
#95#	Disable Do Not Disturb	
*41#	Enable Call Waiting	Use these to allow you to put a call on hold when you are answering another, or to turn this function off.
#41#	Disable Call Waiting	
****	IVR	Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold).
####	Internal Call	Call the phone(s) connected to the Zyxel Device.
*82	One Shot Caller Display Call	Activate or deactivate caller ID for the next call only.
*67	One Shot Caller Hidden Call	

CHAPTER 25
Log

25.1 What You Need To Know

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

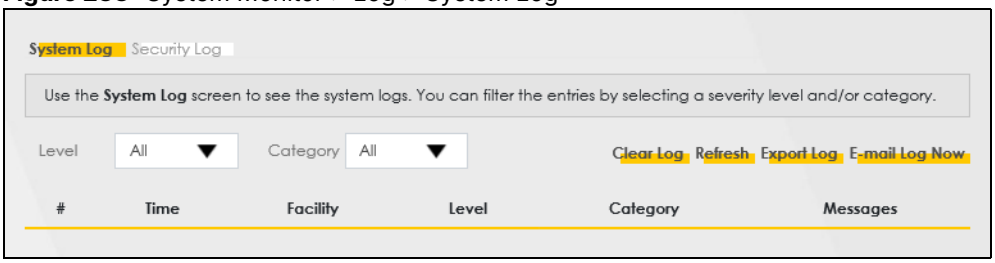
Alerts and Logs

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.

25.2 System Log

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

Figure 233 System Monitor > Log > System Log



The following table describes the fields in this screen.

Table 145 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 Zyxel 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 selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.

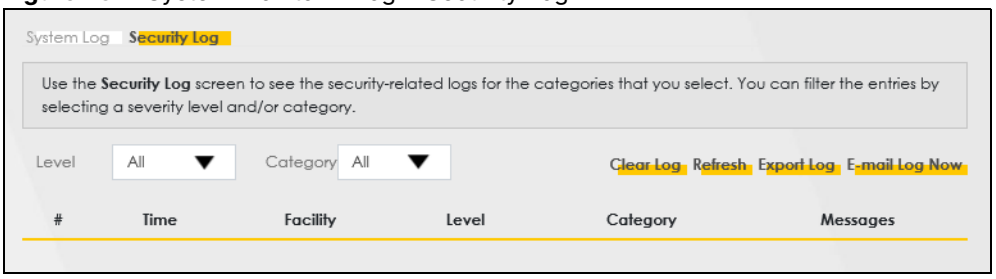
Table 145 System Monitor > Log > System Log (continued)

LABEL	DESCRIPTION
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 Zyxel 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.

25.3 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. Click **System Monitor** > **Log** > **Security Log** to open the following screen.

Figure 234 System Monitor > Log > Security Log



The following table describes the fields in this screen.

Table 146 System Monitor > Log > Security 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 Zyxel 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 selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen.
#	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 Zyxel 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 26
Traffic Status

26.1 Traffic Status Overview

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

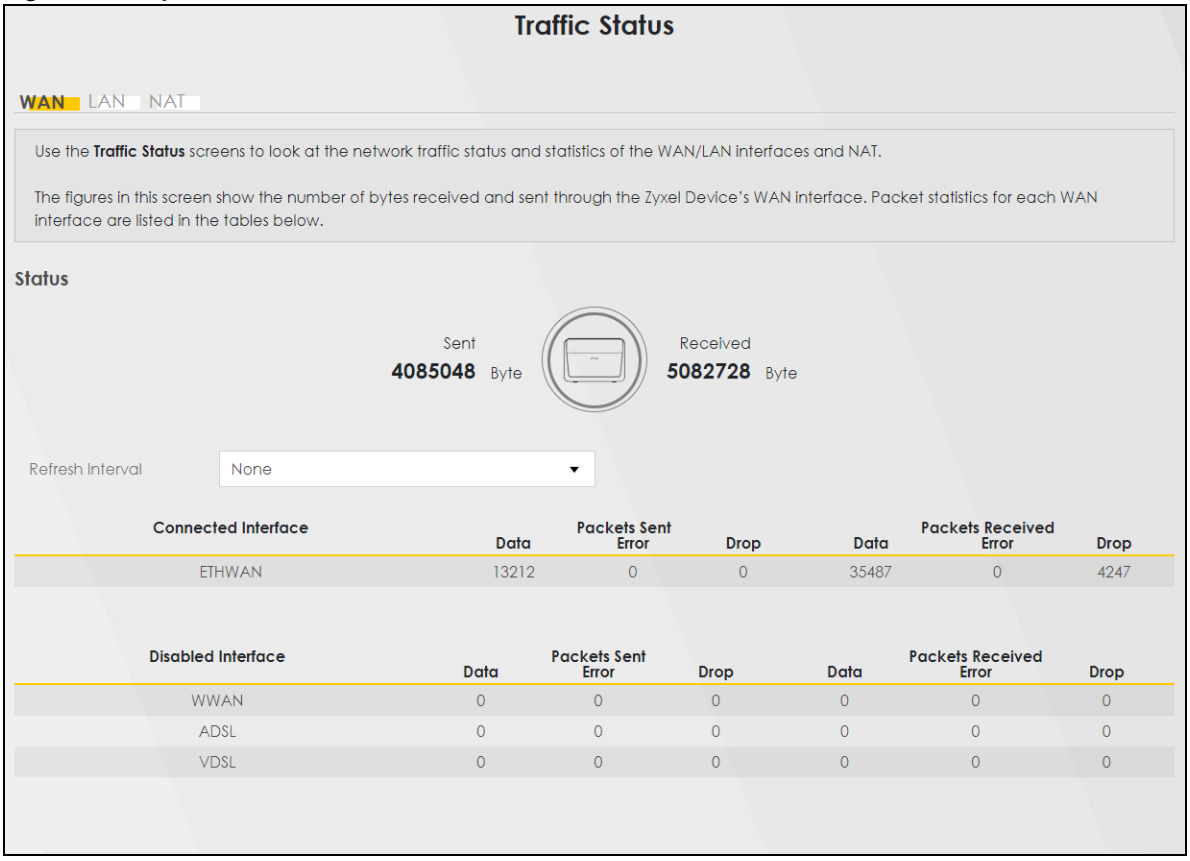
26.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 26.2 on page 373).
- Use the **LAN** screen to view the LAN traffic statistics (Section 26.3 on page 375).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's clients (Section 26.4 on page 376).

26.2 WAN Status

Click **System Monitor** > **Traffic Status** to open the **WAN** screen. The figures in this screen show the number of bytes received and sent through the Zyxel Device's WAN interface. The table below shows packet statistics for each WAN interface.

Figure 235 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 147 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel 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.

Table 147 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
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.

26.3 LAN Status

Click **System Monitor** > **Traffic Status** > **LAN** to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.

Figure 236 System Monitor > Traffic Status > LAN

The following table describes the fields in this screen.

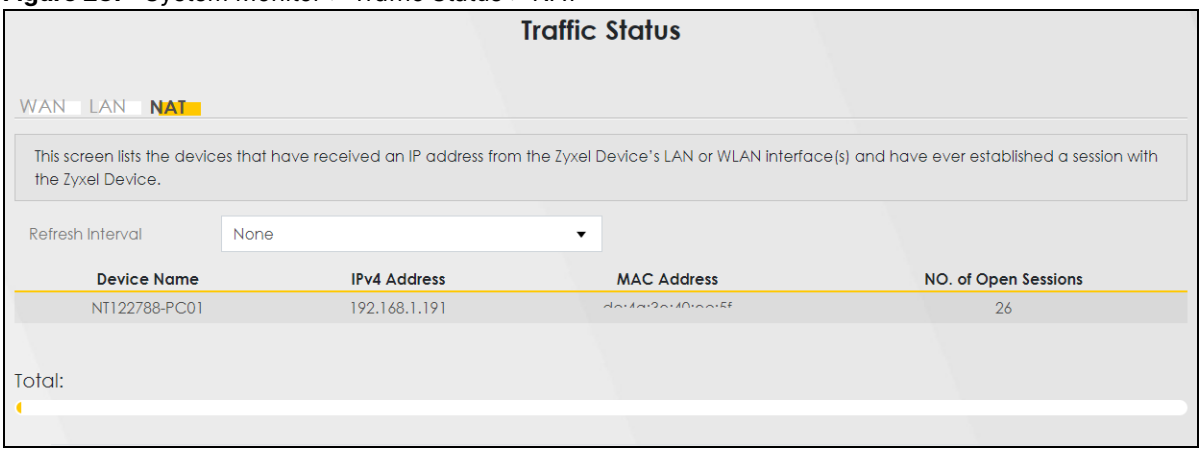
Table 148 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or WLAN interface.
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 or WLAN interfaces.
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.

26.4 NAT Status

Click **System Monitor** > **Traffic Status** > **NAT** to open the following screen. This screen lists the devices that have received an IP address from the Zyxel Device LAN or WLAN interfaces and have ever established a session with the Zyxel Device.

Figure 237 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 149 System Monitor > Traffic Status > NAT

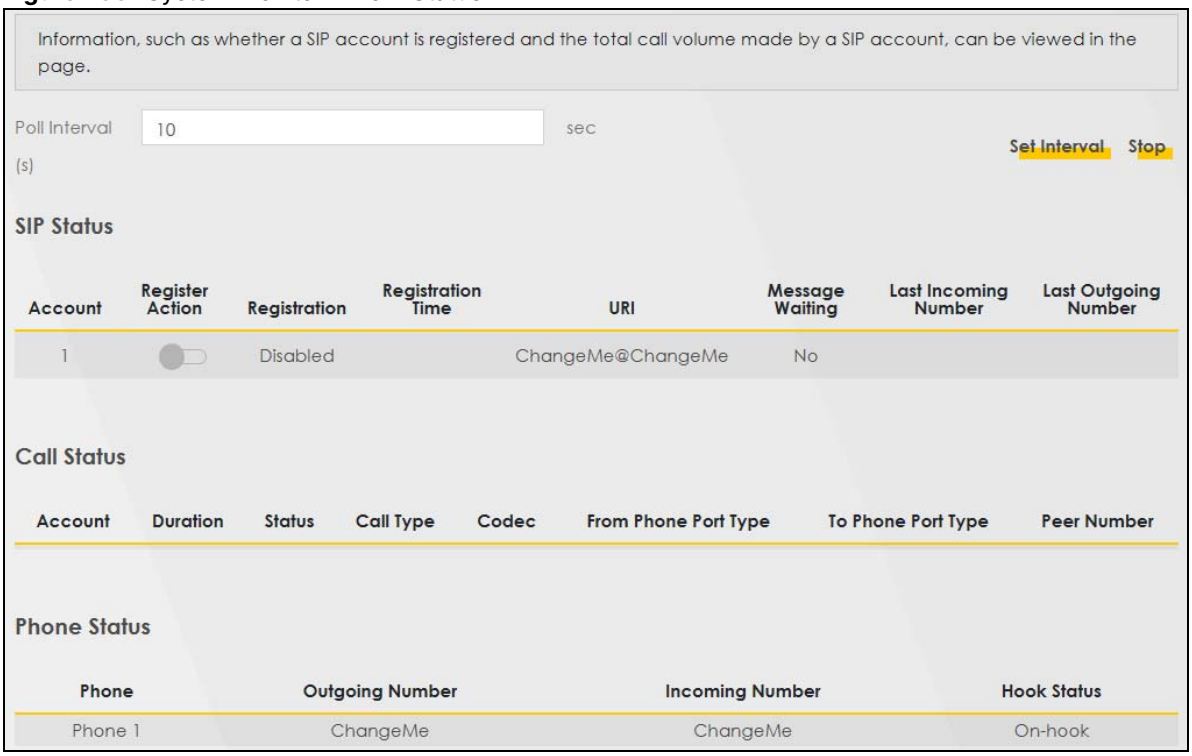
LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Device Name	This displays the name of the connected host.
IPv4 Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open Sessions	This displays the number of NAT sessions currently opened for the connected host.
Total	This displays what percentage of NAT sessions the Zyxel Device can support is currently being used by all connected hosts. You can also see the number of active NAT sessions and the maximum number of NAT sessions the Zyxel Device can support

CHAPTER 27
VoIP Status

27.1 VoIP Status Screen

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

Figure 238 System Monitor > VoIP Status



The following table describes the labels in this screen.

Table 150 System Monitor > VoIP Status

LABEL	DESCRIPTION
Poll Interval	Enter the number of seconds the Device needs to wait before updating this screen and then click **Set Interval**. Click **Stop** to have the Device stop updating this screen.
SIP Status	
Account	This column displays each SIP account in the Device.
Register Action	Click on this switch to register/unregister the SIP account. This switch will turn blue if a registration attempt is successful; otherwise, it will revert to its unregistered setting. Unregistering an account does not delete the SIP account itself, but removes the mapping between your SIP identity and your IP address or domain name,
Registration Time	This field displays the last time the Device successfully registered the SIP account. The field is blank if the Device has never successfully registered this account.

Table 150 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP** > **SIP** screen.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** – There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** – The callee's phone is ringing. **Ring** – The phone is ringing for an incoming VoIP call. **Process** – There is a VoIP call in progress. **DISC** – The callee's line is busy, the callee hung up or your phone was left off the hook.
Call Type	This field displays the call direction type of the current VoIP call. Outgoing Call – It is a SIP VoIP call made by local phone ports, and this SIP account is able to issue a (SIP-based) call setup to the SIP account of remote peers for a VoIP call establishment. This (SIP-based) call setup signal is sent to the SIP server first, and then the SIP server would relay it to the target peer after correctly resolving and locating the target peer. During the call setup (signaling) phase, Calling state is displayed in the Status field, and it turns to InCall state once the call is successfully established. Incoming Call – It is a SIP VoIP call made or originated by remote SIP accounts to connect to this local SIP account. One or more local phone ports can be configured to receive this type of call, see the Incoming Number below, and all of them should begin to ring during the call setup (signaling phase), see the Status above. Once some remote SIP accounts start to ring one local phone, answer by off-hook to the call, and the call is successfully established. The other ringing local phone ports will stop ringing and turning to InCall state in the Status field. Internal Call – It is a local VoIP call between two different local phone ports. No SIP signaling is needed and thus no SIP server is involved to establish this type of call. This type of call is established through the Internal and Non-SIP local setup signaling procedure between the call-originating and call-terminating local phone ports. In general, one or more local phone ports can be designed to receive this type of call, and once any of the ringing phones answer the call, the other ringing ones will stop ringing. During the call setup phase (signaling phase), Calling state is displayed in Status field, and turns to InCall state once the call is successfully established.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
From Phone Port Type	This field displays the phone ports type used to originate, start, or create the current VoIP call. Type Two possible type values will be displayed here: SIP – For the current call which is categorized as Incoming Call in the Call Type filed, this field will show the type SIP. FXS – As for the other cases: Outgoing Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device.
To Phone Port Type	This field displays the phone ports type used to receive the current VoIP call. Three possible type Type values will be displayed here: SIP – For the current call which is categorized as Outgoing Call in the Call Type field, this field will show the type SIP. FXS and Unknown – As for the other cases: Incoming Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device. While the call is established, this field shows Unknown during the call setup phase (signaling phase). This is because one or more local phone ports can be configured or designed to receive these two types of calls, see the Call Type above, and the local phone port will answer the call that hasn't been determined yet at that time.

Table 150 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays the name of a phone port on the Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Hook Status	This field displays whether the phone is in the on or off hook status. **Off-Hook** means a telephone connected to one of the phone port has its receiver off the hook. **On-Hook** means a telephone connected to one of the phone port has its receiver on the hook.

CHAPTER 28
ARP Table

28.1 ARP Table Overview

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

An IP version 4 address is 32 bits long. MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

28.1.1 How ARP Works

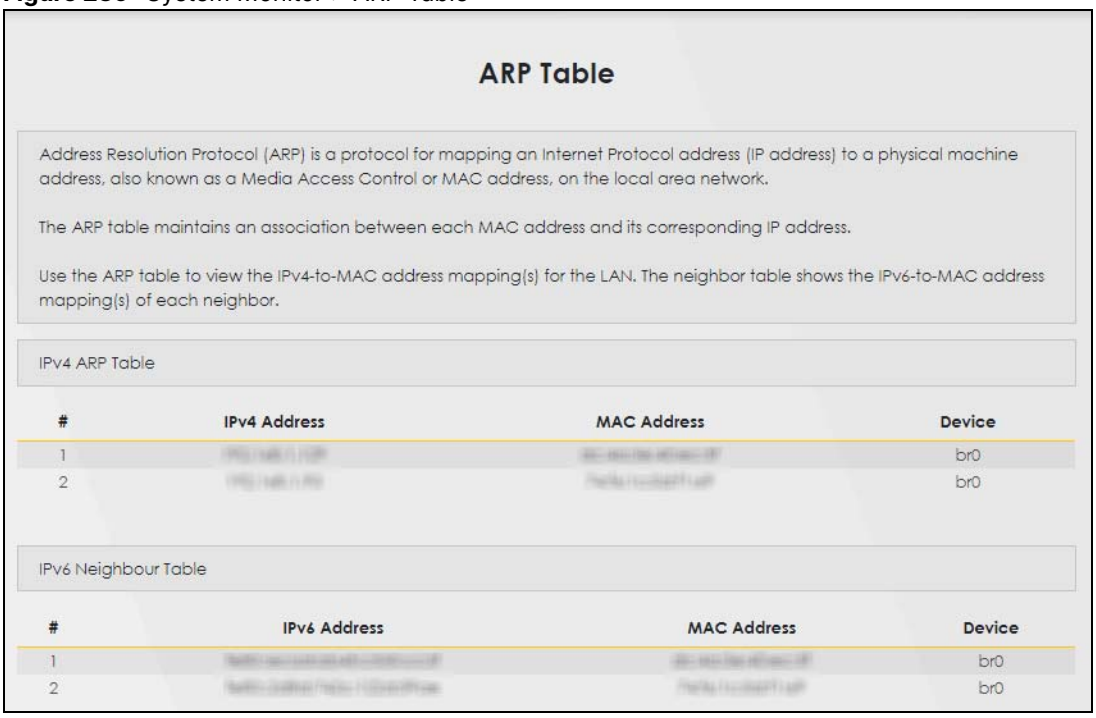
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

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

28.2 ARP Table

Use the ARP table to view the IPv4-to-MAC address mappings for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mappings of each IPv6 neighbor. To open this screen, click **System Monitor** > **ARP Table**.

Figure 239 System Monitor > ARP Table



The following table describes the labels in this screen.

Table 151 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IPv4 / IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to the Zyxel Device.
MAC Address	This is the MAC address of the connected device with the listed IP address.
Device	This is the type of interface used by the connected device. You can click the device type to go to its configuration screen.

CHAPTER 29
Routing Table

29.1 Routing Table Overview

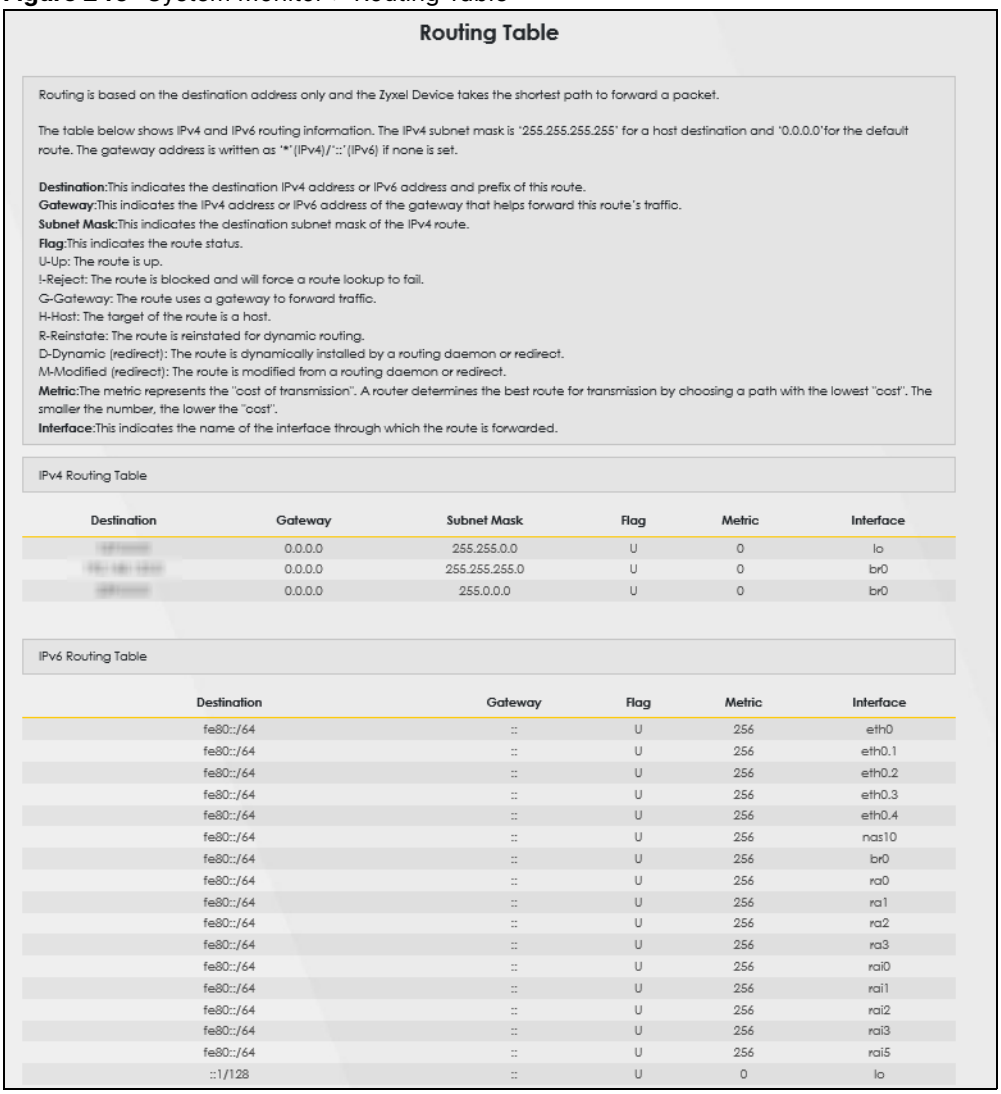
Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

29.2 Routing Table

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is ‘255.255.255.255’ for a host destination and ‘0.0.0.0’ for the default route. The gateway address is written as ‘*’(IPv4)/‘::’(IPv6) if none is set.

Click **System Monitor** > **Routing Table** to open the following screen.

Figure 240 System Monitor > Routing Table



Routing Table

Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0'for the default route. The gateway address is written as '*'(IPv4)/'::'(IPv6) if none is set.

Destination:This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway:This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask:This indicates the destination subnet mask of the IPv4 route.
Flag:This indicates the route status.
U-Up: The route is up.
!-Reject: The route is blocked and will force a route lookup to fail.
G-Gateway: The route uses a gateway to forward traffic.
H-Host: The target of the route is a host.
R-Reinstate: The route is reinstated for dynamic routing.
D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.
M-Modified (redirect): The route is modified from a routing daemon or redirect.
Metric:The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface:This indicates the name of the interface through which the route is forwarded.

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
[redacted]	0.0.0.0	255.255.0.0	U	0	lo
[redacted]	0.0.0.0	255.255.255.0	U	0	br0
[redacted]	0.0.0.0	255.0.0.0	U	0	br0

IPv6 Routing Table

Destination	Gateway	Flag	Metric	Interface
fe80::/64	::	U	256	eth0
fe80::/64	::	U	256	eth0.1
fe80::/64	::	U	256	eth0.2
fe80::/64	::	U	256	eth0.3
fe80::/64	::	U	256	eth0.4
fe80::/64	::	U	256	nas10
fe80::/64	::	U	256	br0
fe80::/64	::	U	256	ra0
fe80::/64	::	U	256	ra1
fe80::/64	::	U	256	ra2
fe80::/64	::	U	256	ra3
fe80::/64	::	U	256	rai0
fe80::/64	::	U	256	rai1
fe80::/64	::	U	256	rai2
fe80::/64	::	U	256	rai3
fe80::/64	::	U	256	rai5
::1/128	::	U	0	lo

The following table describes the labels in this screen.

Table 152 System Monitor > Routing Table

LABEL	DESCRIPTION
IPv4 / IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.

Table 152 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	This indicates the route status. **U–Up:** The route is up. **!–Reject:** The route is blocked and will force a route lookup to fail. **G–Gateway:** The route uses a gateway to forward traffic. **H–Host:** The target of the route is a host. **R–Reinstate:** The route is reinstated for dynamic routing. **D–Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect. **M–Modified (redirect):** The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission." A router determines the best route for transmission by choosing a path with the lowest "cost." The smaller the number, the lower the "cost."
Interface	This indicates the name of the interface through which the route is forwarded. • **brx** indicates a LAN interface where x can be 0 – 3 to represent LAN1 to LAN4 respectively. • **ethx** indicates an Ethernet WAN interface using IPoE or in bridge mode. • **ppp0** indicates a WAN interface using PPPoE. • **wlx** indicates a wireless interface where x can be 0 – 1.

CHAPTER 30
Multicast Status

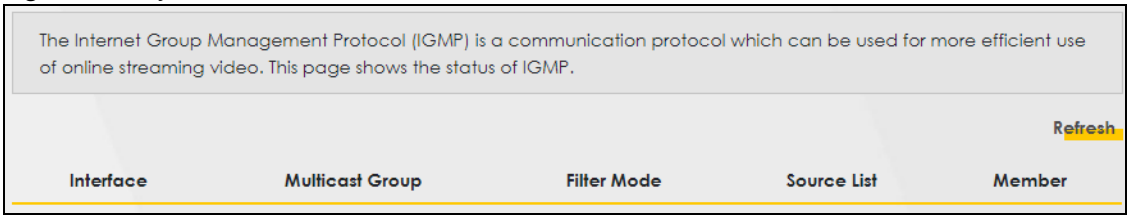
30.1 Multicast Status Overview

Use the **Multicast Status** screens to look at IGMP/MLD group status and traffic statistics.

30.2 The IGMP Status Screen

Use this screen to look at the current list of multicast groups the Zyxel Device manages through IGMP. Configure IGMP in **Network Setting** > **IGMP/MLD**. To open this screen, click **System Monitor** > **Multicast Status** > **IGMP Status**.

Figure 241 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

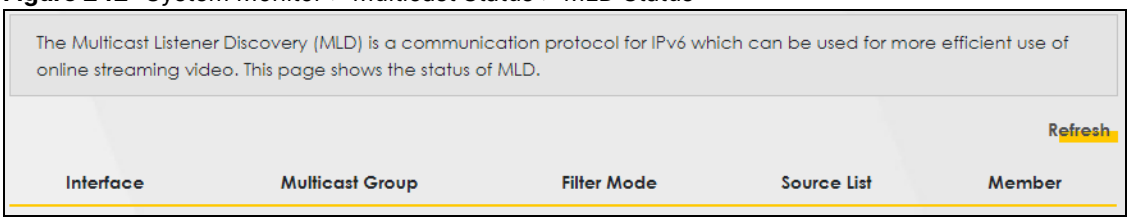
Table 153 System Monitor > Multicast Status > IGMP Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information on this screen.
Interface	This field displays the name of an interface on the Zyxel Device that belongs to an IGMP multicast group.
Multicast Group	This field displays the name of the IGMP multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of the members of the multicast group.

30.3 The MLD Status Screen

Use this screen to look at the current list of multicast groups the Zyxel Device manages through MLD. Configure MLD in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 242 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 154 System Monitor > Multicast Status > MLD Status

LABEL	DESCRIPTION
Refresh	Click this button to update the status on this screen.
Interface	This field displays the name of an interface on the Zyxel Device that belongs to an MLD multicast group.
Multicast Group	This field displays the name of the MLD multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of members in the multicast group.

CHAPTER 31
WLAN Station Status

31.1 WLAN Station Status Overview

Click **System Monitor** > **WLAN Station Status** to open the following screen. Use this screen to view information and status of the WiFi stations (WiFi clients) that are currently associated with the Zyxel Device. Being associated means that a WiFi client (for example, your computer with a WiFi network card installed) has connected successfully to an AP (or WiFi router) using the same SSID, channel, and WiFi security settings.

Figure 243 System Monitor > WLAN Station Status (For 2.4 GHz and 5 GHz models)

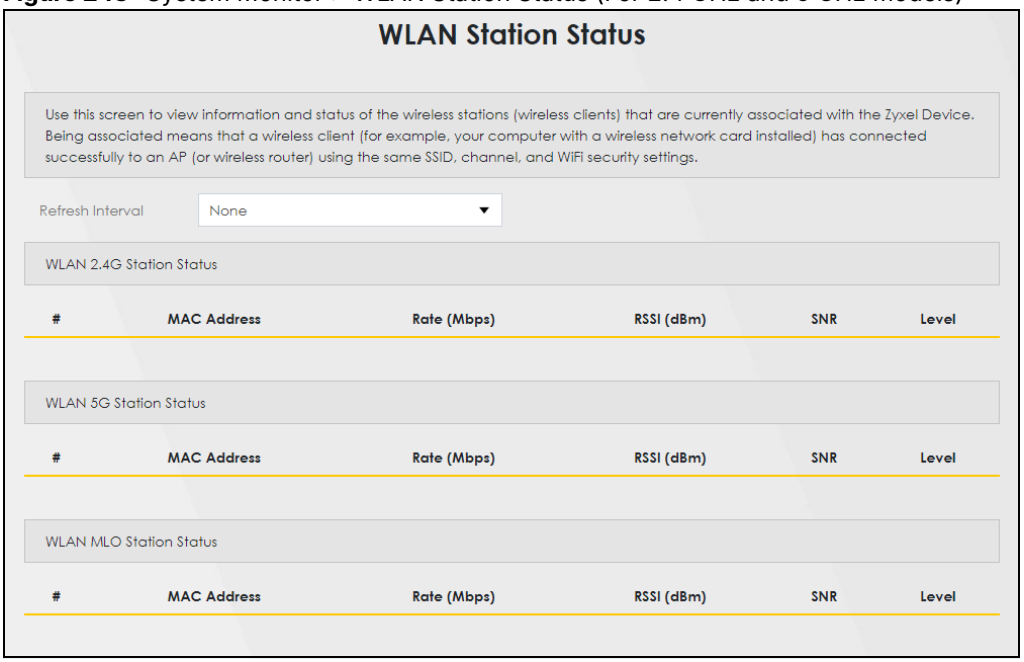
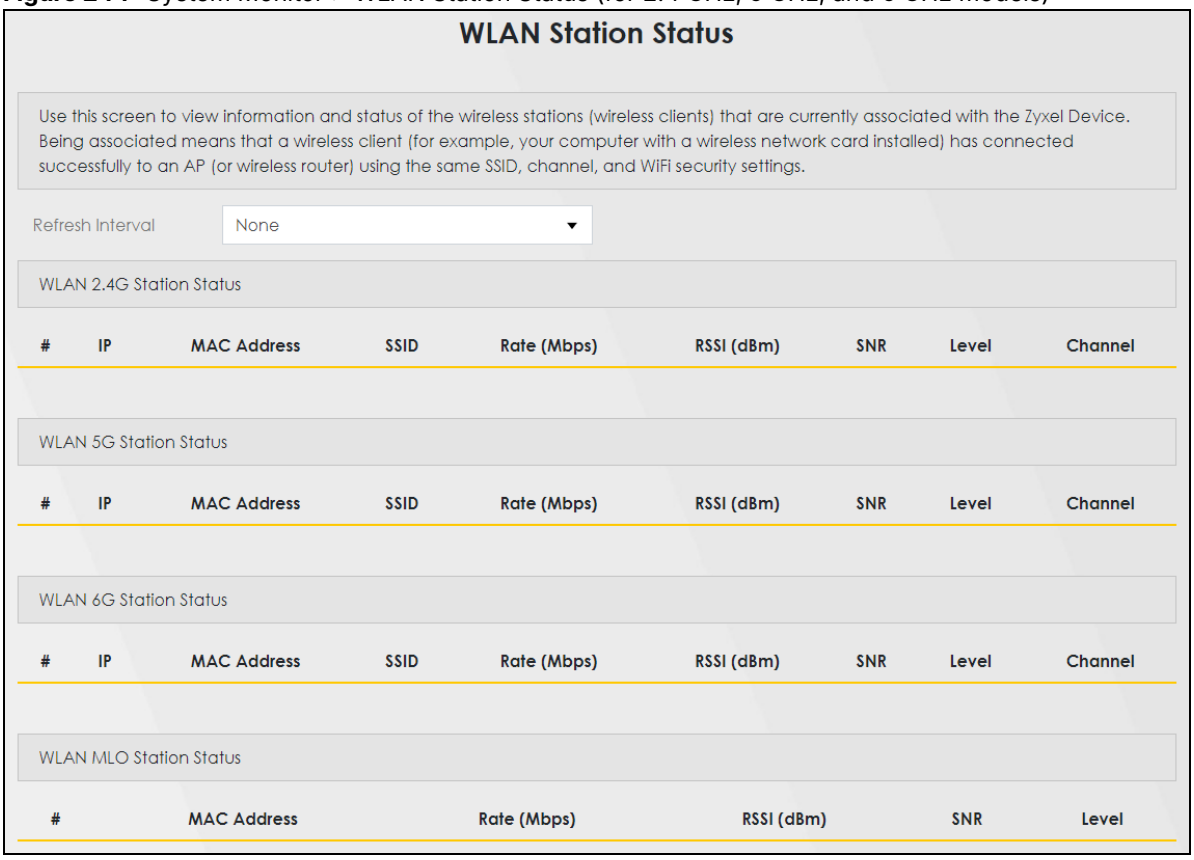


Figure 244 System Monitor > WLAN Station Status (for 2.4 GHz, 5 GHz, and 6 GHz models)



The following table describes the labels in this screen.

Table 155 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated WiFi station.
IP	This field displays the IP address of an associated WiFi station.
MAC Address	This field displays the MAC address of an associated WiFi station.
SSID	This field displays the SSID (Service Set IDentifier) this WiFi station is associated with.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated WiFi station and the Zyxel Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's WiFi connection. The normal range is –30dBm to –79dBm. If the value drops below –80dBm, try moving the associated WiFi station closer to the Zyxel Device to get better signal strength.
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The greater the number, the better the quality of WiFi. The normal range is 15 to 40. If the value drops below 15, try moving the associated WiFi station closer to the Zyxel Device to get better quality WiFi.

Table 155 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
Level	This field displays a number which represents the strength of the WiFi signal between an associated WiFi station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the Zyxel Device is receiving an excellent WiFi signal. **4** means the Zyxel Device is receiving a very good WiFi signal. **3** means the Zyxel Device is receiving a weak WiFi signal, **2** means the Zyxel Device is receiving a very weak WiFi signal. **1** means the Zyxel Device is not receiving a WiFi signal.
Channel	This field displays the wireless channel bandwidth of an associated WiFi station.

CHAPTER 32
Cellular Statistics

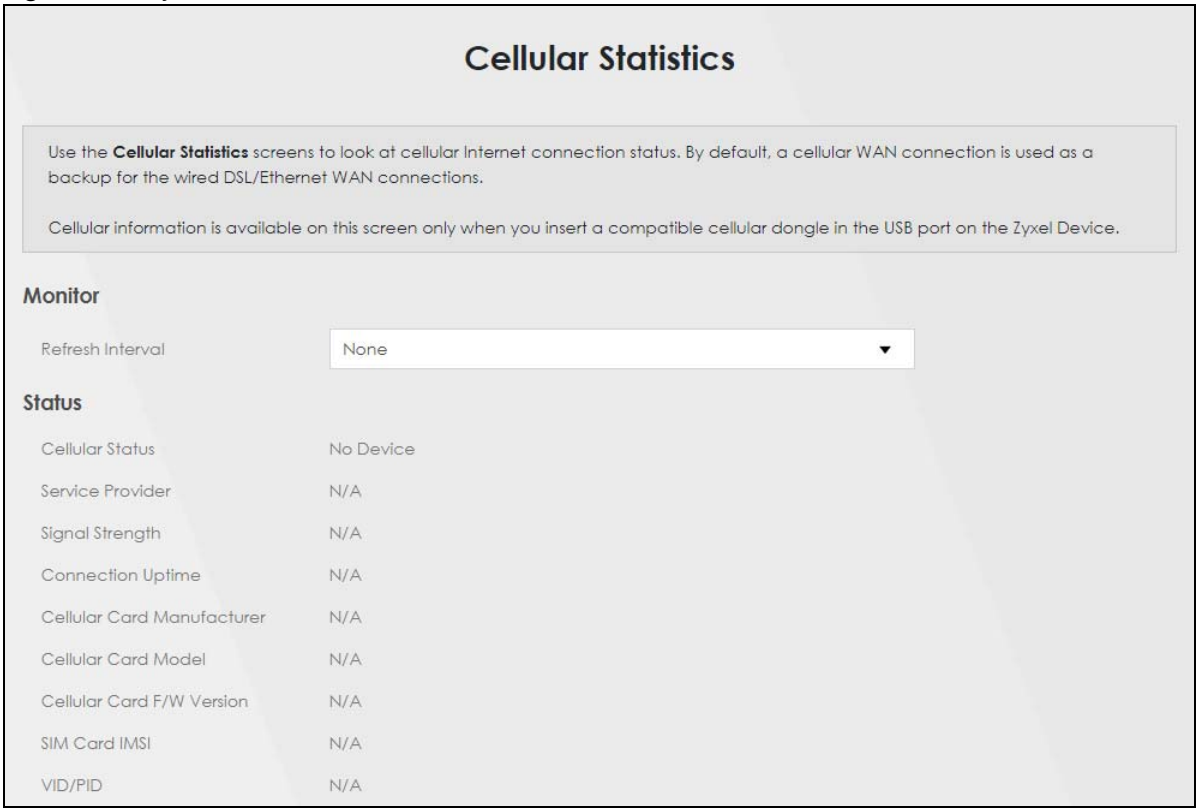
32.1 Cellular Statistics Overview

Use the **Cellular Statistics** screens to look at cellular Internet connection status. By default, a cellular WAN connection is used as a backup for the wired DSL or Ethernet WAN connections.

32.2 Cellular Statistics Settings

To open this screen, click **System Monitor** > **Cellular Statistics**. Cellular information is available on this screen only when you insert a compatible cellular dongle in the USB port on the Zyxel Device.

Figure 245 System Monitor > Cellular Statistics



The following table describes the labels in this screen.

Table 156 System Monitor > Cellular Statistics

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Select how often you want the Zyxel Device to update this screen. Select **None** to stop refreshing.
Status	
Cellular Status	This field displays the status of the cellular Internet connection. This field can display: **GSM** – Global System for Mobile Communications, 2G **GPRS** – General Packet Radio Service, 2.5G **EDGE** – Enhanced Data rates for GSM Evolution, 2.75G **WCDMA** – Wideband Code Division Multiple Access, 3G **HSDPA** – High-Speed Downlink Packet Access, 3.5G **HSUPA** – High-Speed Uplink Packet Access, 3.75G **HSPA** – HSDPA+HSUPA, 3.75G
Service Provider	This field displays the name of the service provider.
Signal Strength	This field displays the strength of the signal in dBm.
Connection Uptime	This field displays the time the connection has been up.
Cellular Card Manufacturer	This field displays the manufacturer of the cellular card.
Cellular Card Model	This field displays the model name of the cellular card.
Cellular Card F/W Version	This field displays the firmware version of the cellular card.
SIM Card IMSI	The International Mobile Subscriber Identity or IMSI is a unique identification number associated with all cellular networks. This number is provisioned in the SIM card.
VID/PID	This field displays the USB Vendor ID and Product ID of the cellular card.

CHAPTER 33
Optical Signal Status

33.1 Overview

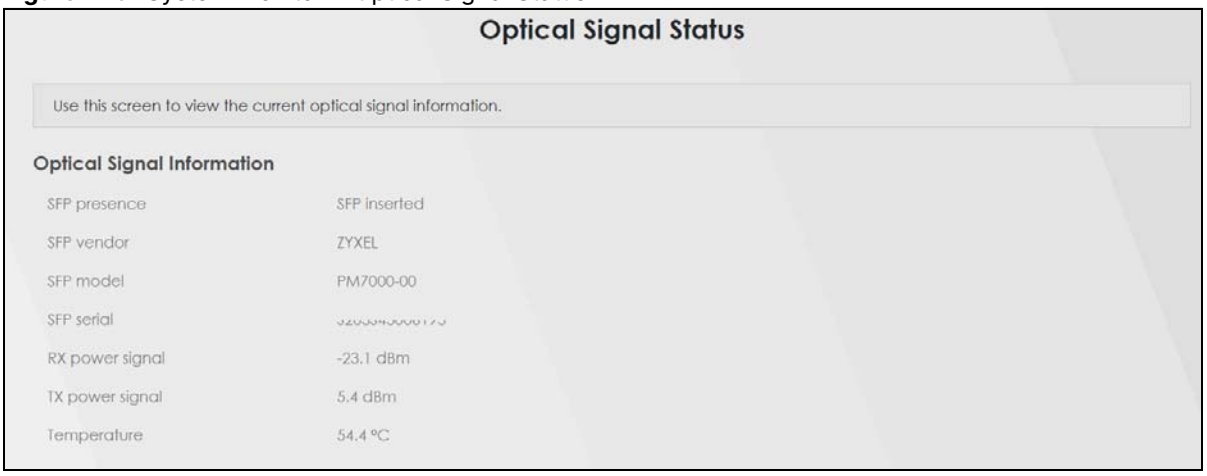
Use this screen to view the PON (Passive Optical Network) transceiver's TX power and RX power level and temperature.

33.2 The Optical Signal Status Screen

Click **System Monitor** > **Optical Signal Status** to open the **Optical Signal Status** screen to see the real-time DDMI (Digital Diagnostics Monitoring Interface) parameters.

The PON transceiver's support for the 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 246 System Monitor > Optical Signal Status



The following table describes the labels in this screen.

Table 157 System Monitor > Optical Signal Status

LABEL	DESCRIPTION
Optical Signal Information	
SFP presence	This displays whether the SFP transceiver is inserted.
SFP vendor	This displays the vendor name of the inserted SFP transceiver.
SFP model	This displays the model name of the inserted SFP transceiver.
SFP serial	This displays the serial number of the inserted SFP transceiver.
RX power signal	This displays the PON transceiver's receiving power in dBm.

Table 157 System Monitor > Optical Signal Status (continued)

LABEL	DESCRIPTION
TX power signal	This displays the PON transceiver’s transmitting power in dBm.
Temperature	This displays the PON transceiver’s temperature in degrees Celsius.

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

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

Table 158 Normal Range of Optical Signal Information

LABEL	NORMAL RANGE
RX power signal	-9 to -28 dBm Note: The higher the value, the stronger the signal as there is less background noise. For example, -9 dBm is a stronger signal than -28 dBm.
TX power signal	4 to 9 dBm
Temperature	0 to 85 degrees Celsius (185 degrees Fahrenheit)

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

CHAPTER 34
System

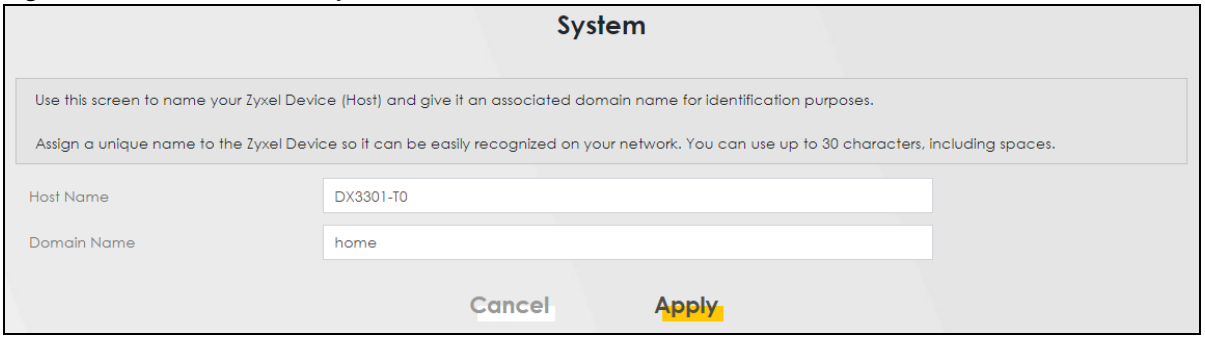
34.1 System Overview

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

34.2 System

Click **Maintenance** > **System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network.

Figure 247 Maintenance > System



The following table describes the labels in this screen.

Table 159 Maintenance > System

LABEL	DESCRIPTION
Host Name	Enter a descriptive host name for your Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. For some models, the supported maximum input length is 16 alphanumeric characters.
Domain Name	Enter a domain name for your host Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Cancel	Click **Cancel** to abandon this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 35
User Account

35.1 User Account Overview

In the **User Account** screen, you can view the settings of the “admin” that you use to log into the Zyxel Device to manage it.

The number of accounts you can create:

Administrator Account	4
User Account	4

The privileges of administrator and user accounts differ. Some features are available only to the administrator accounts but are not accessible to user accounts.

Below is an example of the account privilege.

Table 160 Account Privilege Comparison Table - Example

	ADMINISTRATOR	USER
Wizard		
Quick Start	YES	NO
Configuration		
Connection Status	YES	YES
Network		
Broadband	YES	NO
Wireless	YES	NO
Home Networking	YES	NO
Routing	YES	NO
QoS	YES	NO
NAT	YES	NO
DNS	YES	NO
IGMP/MLD	YES	NO
Interface Grouping	YES	NO
Security		
Firewall	YES	NO
Mac Filter	YES	NO
Certificates	YES	NO
System Monitor		
Log	YES	YES

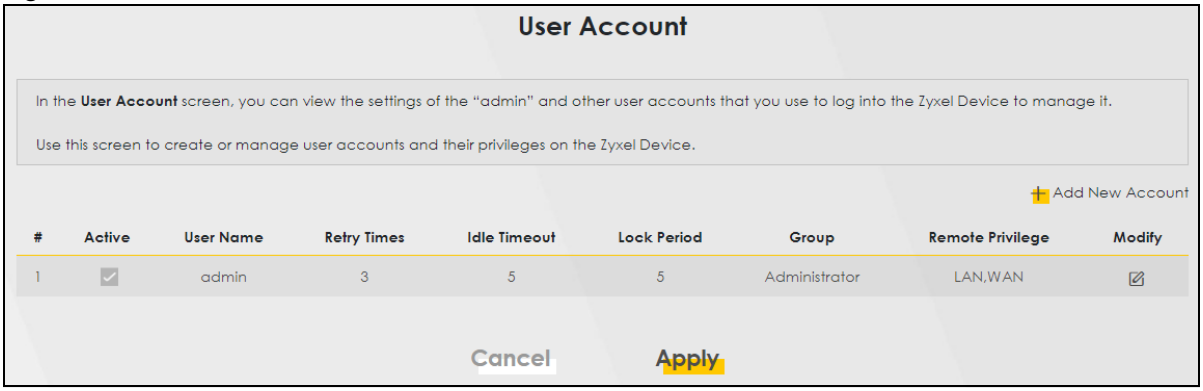
Table 160 Account Privilege Comparison Table - Example (continued)

	ADMINISTRATOR	USER
Traffic Status	YES	YES
ARP Table	YES	YES
Routing Table	YES	YES
Multicast Status	YES	YES
WLAN Station Status	YES	YES
Maintenance		
System	YES	NO
User Account	YES	YES
Remote Management	YES	YES
Time	YES	YES
Email Notification	YES	YES
Log Setting	YES	YES
Firmware Upgrade	YES	YES
Backup/Restore	YES	YES
Reboot	YES	YES
Diagnostic	YES	YES

35.2 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 Zyxel Device.

Figure 248 Maintenance > User Account



The following table describes the labels in this screen.

Table 161 Maintenance > User Account

LABEL	DESCRIPTION
#	This is the index number.
Active	This indicates whether the user account is active or not. The checkbox is selected when the user account is enabled. It is cleared when it is disabled.

Table 161 Maintenance > User Account (continued)

LABEL	DESCRIPTION
User Name	This displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This displays the length of inactive time before the Zyxel 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 this user has **Administrator** privileges.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

35.2.1 User Account Add or Edit

Add or change the name of the user account, set the security password and the retry times, and whether this user will have **Administrator** or **User** privileges. Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance** > **User Account** to open the following screen.

Figure 249 Maintenance > User Account: Add

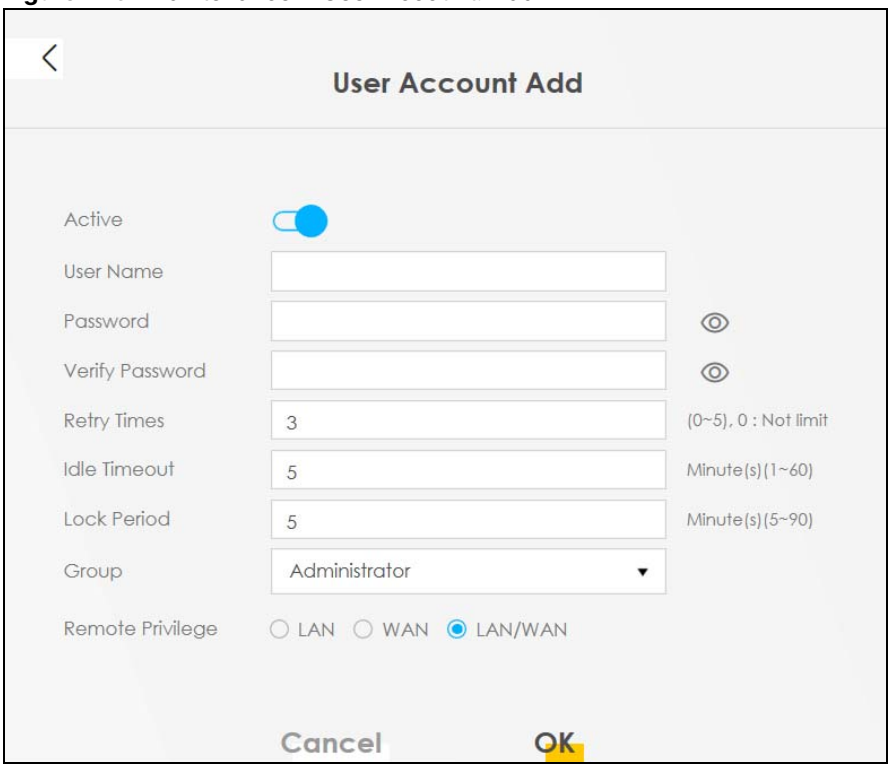
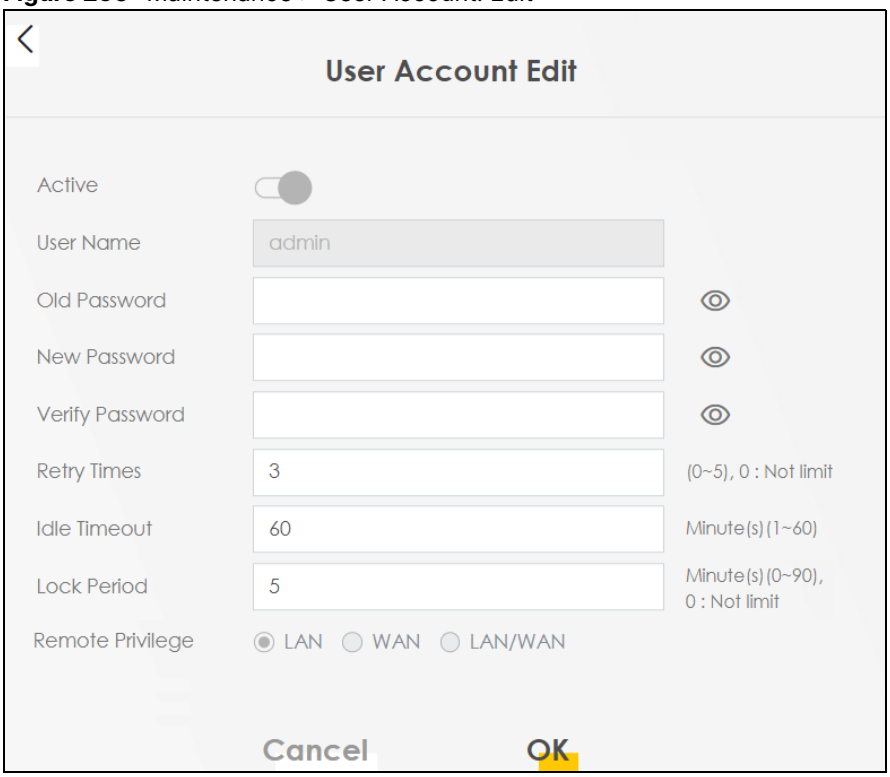


Figure 250 Maintenance > User Account: Edit



The following table describes the labels in this screen.

Table 162 Maintenance > User Account > User Account Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (switch turns blue) or disable (switch turns gray) to activate or deactivate the user account.
User Name	Enter a name for this account. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Verify Password	Enter the new password again for confirmation.
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 Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Cancel	Click **Cancel** to restore your previously saved settings.
OK	Click **OK** to save your changes.

CHAPTER 36
Remote Management

36.1 Remote Management Overview

Use Remote Management to control web services (HTTP, HTTPS, SSH, SNMP, and Ping) can access the Zyxel Device through which interfaces.

Note: Use the Web Configurator (HTTP) to manage the Zyxel Device.

36.1.1 What You Can Do in this Chapter

- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 36.2 on page 399).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 36.3 on page 401).

36.2 MGMT Services

Use this screen to configure the interfaces through which services can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance** > **Remote Management** > **MGMT Services** to open the following screen.

Figure 251 Maintenance > Remote Management > MGMT Services

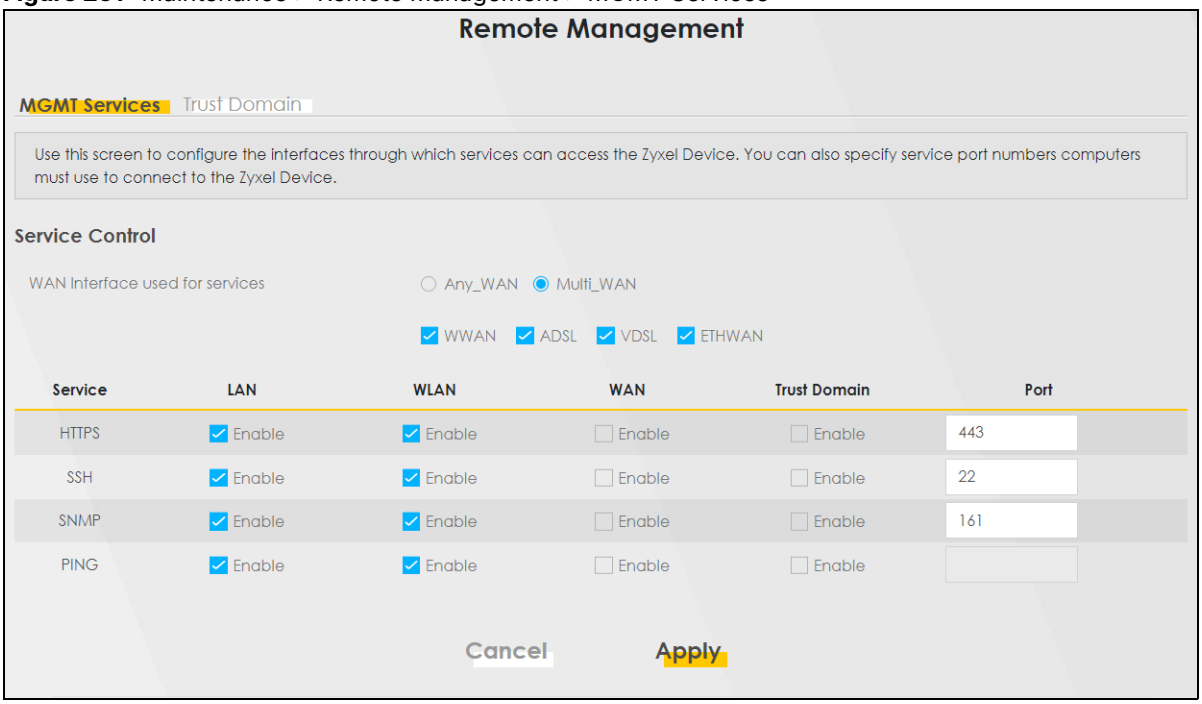
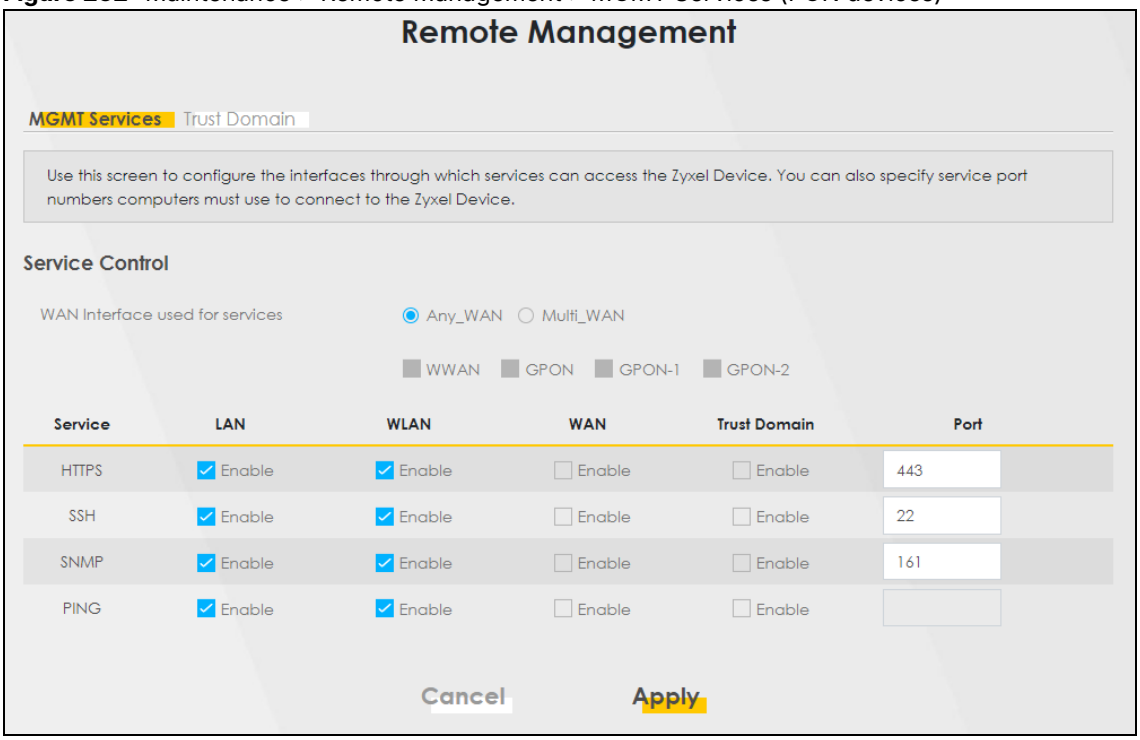


Figure 252 Maintenance > Remote Management > MGMT Services (PON devices)



The following table describes the fields in this screen.

Table 163 Maintenance > Remote Management > MGMT Services

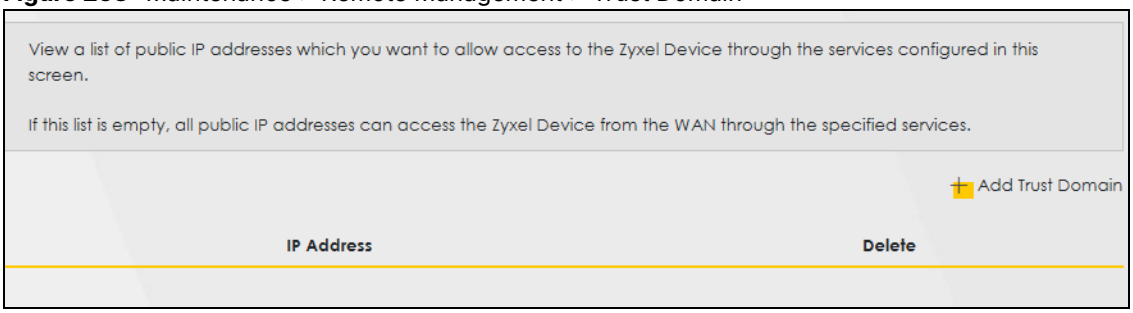
LABEL	DESCRIPTION
Service Control	
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
WWAN	Enable the WWAN (cellular) connection configured in **Network Setting** > **Broadband** > **Cellular Backup** to access the service on the Zyxel Device.
GPON	Enable the Gigabit Ethernet Passive Optical Network WAN connection configured in **Network Setting** > **Broadband** > **Add New WAN Interface** or **Modify** to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the LAN.
WLAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the WLAN.
WAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.
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	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://192.168.1.1 in your browser to access the Web Configurator, then the Zyxel Device will automatically change this to the more secure https://192.168.1.1 for access.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

36.3 Trust Domain

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** > **MGMT Services** screen. Click **Maintenance** > **Remote Management** > **Trust Domain** to open the following screen.

Note: Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Figure 253 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

Table 164 Maintenance > Remote Management > Trust Domain

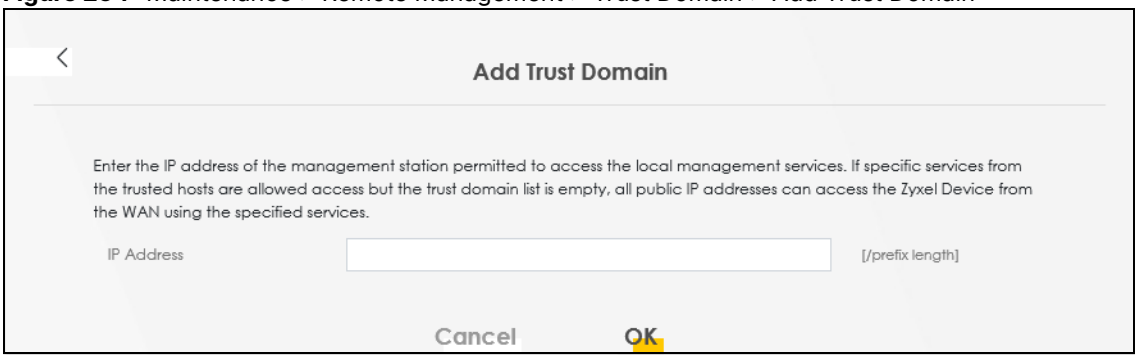
LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon to remove the trusted host IP address.

36.3.1 Add Trust Domain

Use this screen to add a public IP addresses or a complete domain name of a device which is allowed to access the Zyxel Device. Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted-hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Click the **Add Trust Domain** button in the **Maintenance** > **Remote Management** > **Trust Domain** screen to open the following screen.

Figure 254 Maintenance > Remote Management > Trust Domain > Add Trust Domain



The following table describes the fields in this screen.

Table 165 Maintenance > Remote Management > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IPv4/IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 37
Time Settings

37.1 Time Settings Overview

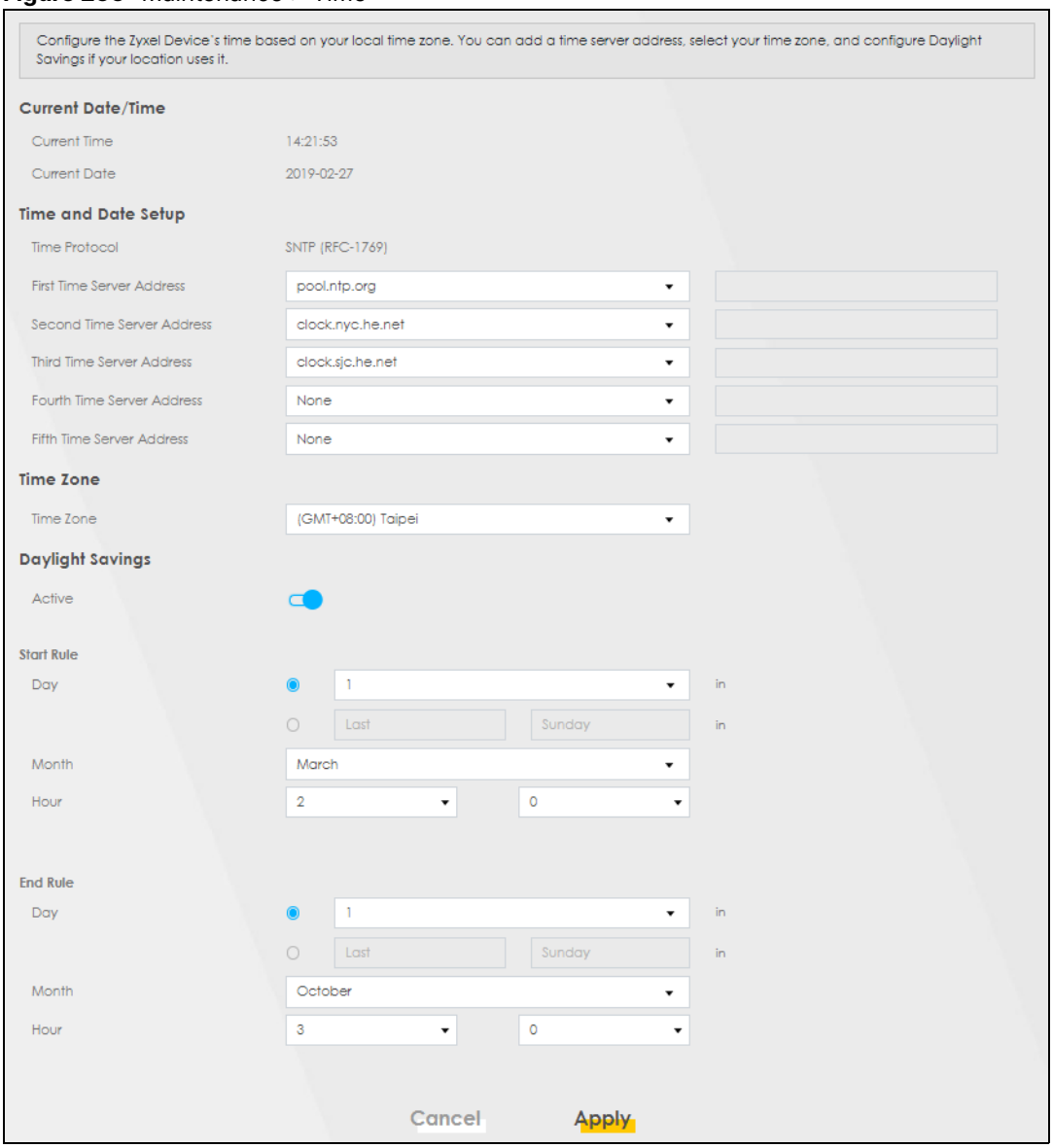
This chapter shows you how to configure system related settings, such as system date and time.

37.2 Time

For effective scheduling and logging, the Zyxel Device system time must be accurate. 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.

To change your Zyxel Device's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 255 Maintenance > Time



The following table describes the fields in this screen.

Table 166 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This displays the time of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the time with the time server.
Current Date	This displays the date of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the date with the time server.
Time and Date Setup	
Time Protocol	This displays the time protocol used by your Zyxel Device.

Table 166 Maintenance > Time (continued)

LABEL	DESCRIPTION
First – Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 printable characters in length) of your time server. Select **None** if you do not want to 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 this switch to enable or disable Daylight Saving Time. When the switch turns blue, the function is enabled. Otherwise, it is not.
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 **Time** 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 in the **o'clock** field 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 **Hour** 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 in the **o'clock** field 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).
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 38
Email Notification

38.1 Email Notification Overview

A mail server is an application or a computer that can receive, forward and deliver email messages.

To have the Zyxel Device send reports, logs or notifications through email, you must specify an email server and the email addresses of the sender and receiver.

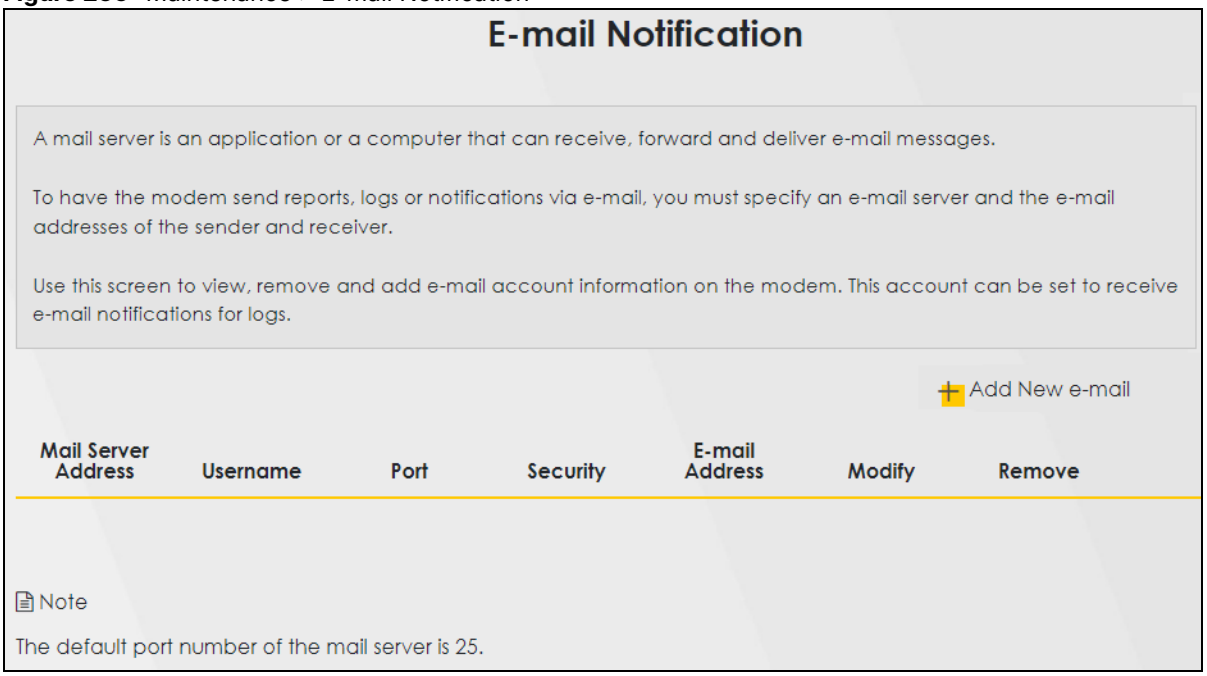
38.2 Email Notification

Use this screen to view, remove and add email account information on the Zyxel Device. This account can be set to send email notifications for logs.

Click **Maintenance** > **E-mail Notification** to open the **E-mail Notification** screen.

Note: The default port number of the mail server is 25.

Figure 256 Maintenance > E-mail Notification



The following table describes the labels in this screen.

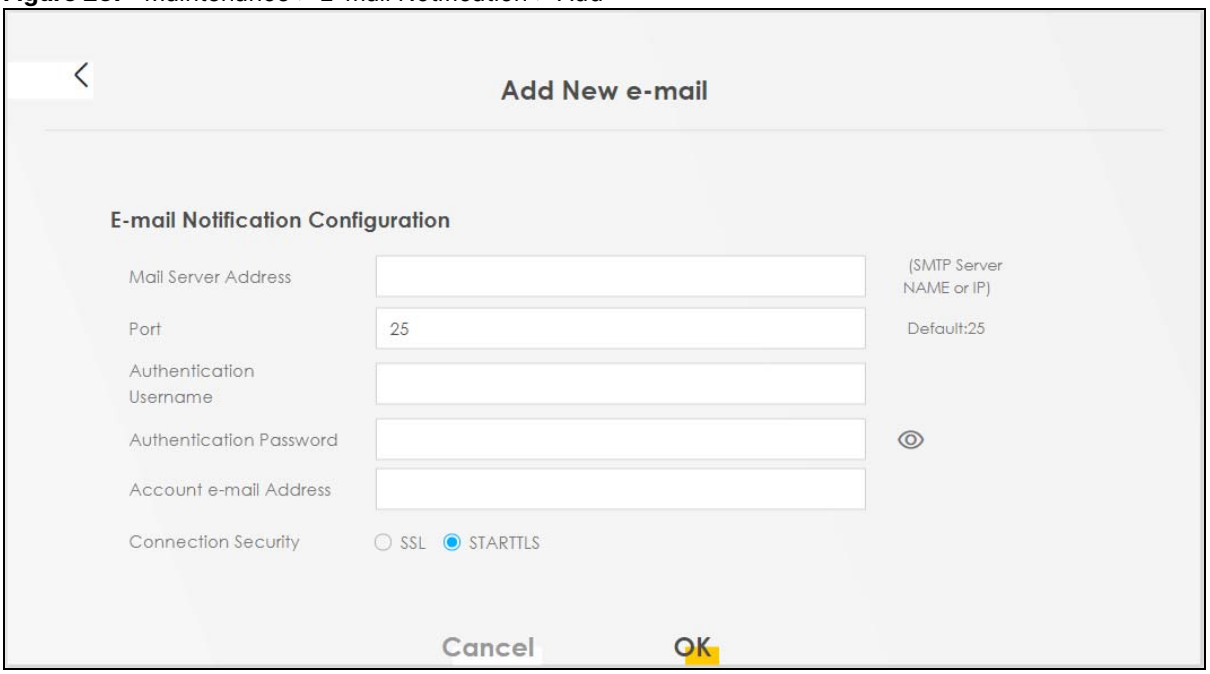
Table 167 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry (up to 32 can be created).
Mail Server Address	This displays the server name or the IP address of the mail server.
Username	This displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the email address that you want to be in the from or sender line of the email that the Zyxel Device sends.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Remove	Click this button to delete the selected entries.

38.2.1 E-mail Notification Edit

Click the **Add** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending email through a mail server.

Figure 257 Maintenance > E-mail Notification > Add



The following table describes the labels in this screen.

Table 168 Maintenance > E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the email address specified in the **Account e-mail Address** field. If this field is left blank, reports, logs or notifications will not be sent through email.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. This is usually the user name of a mail account you specified in the **Account email Address** field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the email address that you want to be in the from or sender line of the email notification that the Zyxel Device sends. If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well.
Cancel	Click this button to begin configuring this screen afresh.
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 39
Log Setting

39.1 Log Setting Overview

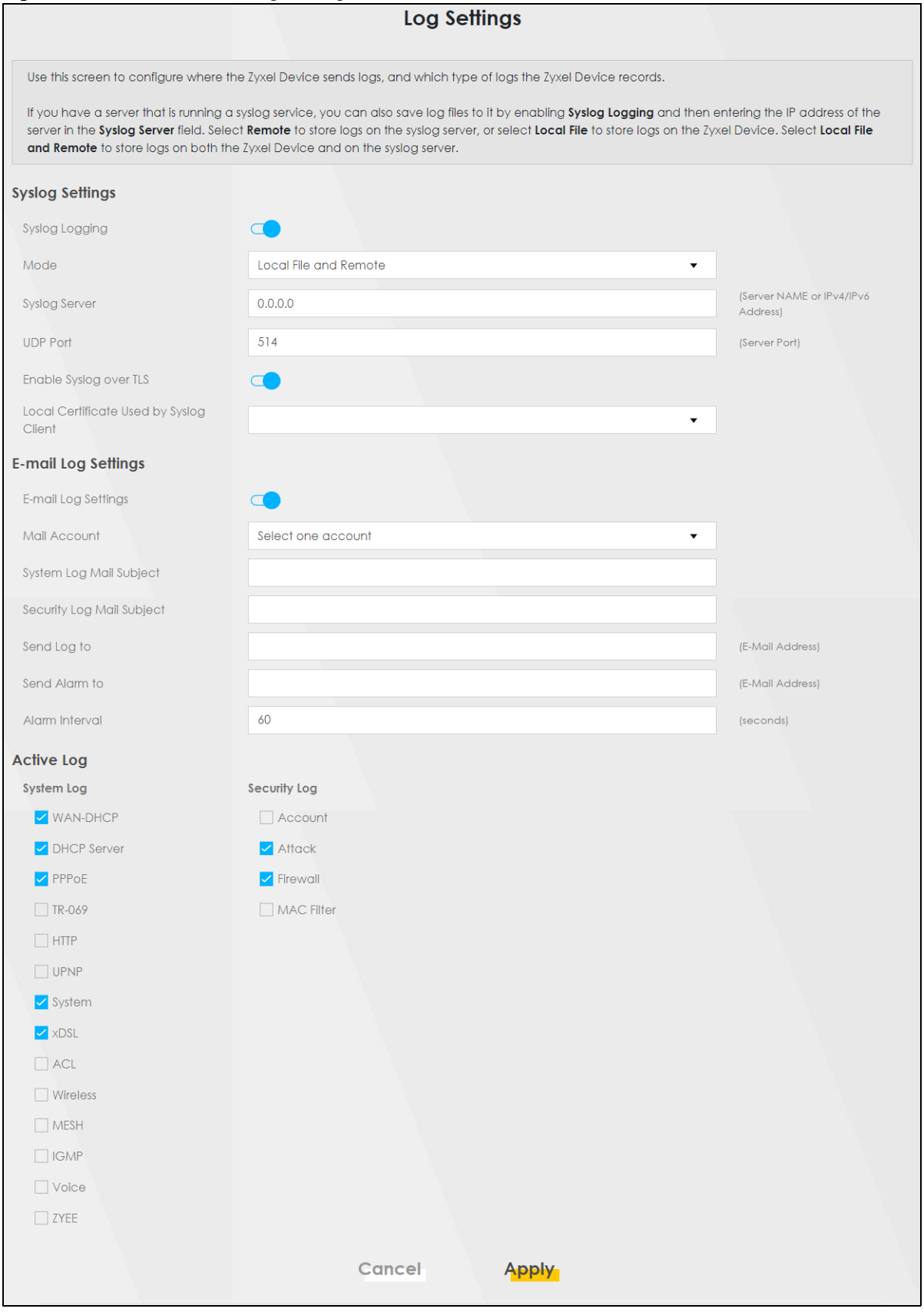
You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the **Logs Setting** screen.

39.2 Log Setting

Use this screen to configure where the Zyxel Device sends logs, and which type of logs the Zyxel Device records.

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging**, and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the Zyxel Device. Select **Local File and Remote** to store logs on both the Zyxel Device and the syslog server. To change your Zyxel Device's log settings, click **Maintenance** > **Log Setting**. The screen appears as shown.

Figure 258 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 169 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Slide the switch to the right to enable syslog logging.
Mode	Select **Remote** to have the Zyxel Device send it to an external syslog server. Select **Local File** to have the Zyxel Device save the log file on the Zyxel Device itself. Select **Local File and Remote** to have the Zyxel Device save the log file on the Zyxel Device itself and send it to an external syslog server. Note: A warning appears upon selecting **Remote** or **Local File and Remote**. Just click **OK** to continue.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
E-mail Log Settings	Slide the switch to the right to allow the sending through email the system and security logs to the email address specified in **Send Log to**. Note: Make sure that the **Mail Server Address** field is not left blank in the **Maintenance** > **E-mail Notifications** screen.
Mail Account	Select a server specified in **Maintenance** > **E-mail Notifications** to send the logs to.
System Log Mail Subject	This field allows you to enter a descriptive name for the system log email (for example Zyxel System Log). Up to 127 printable characters are allowed for the **System Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Security Log Mail Subject	This field allows you to enter a descriptive name for the security log email (for example Zyxel Security Log). Up to 127 printable characters are allowed for the **Security Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Send Log to	This field allows you to enter the log's designated email recipient. The log's format is plain text file sent as an email attachment.
Send Alarm to	This field allows you to enter the alarm's designated e-mail recipient. The alarm's format is plain text file sent as an email attachment.
Alarm Interval	Select the frequency of showing of the alarm.
Active Log	
System Log	Select the categories of **System Log**s that you want to record.
Security Log	Select the categories of **Security Log**s that you want to record.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

39.2.1 Example Email Log

An 'End of Log' message displays for each mail in which a complete log has been sent. The following is an example of a log sent by email.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- 'End of Log' message shows that a complete log has been sent.

Figure 259 Email Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

CHAPTER 40
Firmware Upgrade

40.1 Firmware Upgrade Overview

This chapter explains how to upload new firmware to your Zyxel Device if you get new firmware releases from your service provider.

40.2 Firmware Upgrade

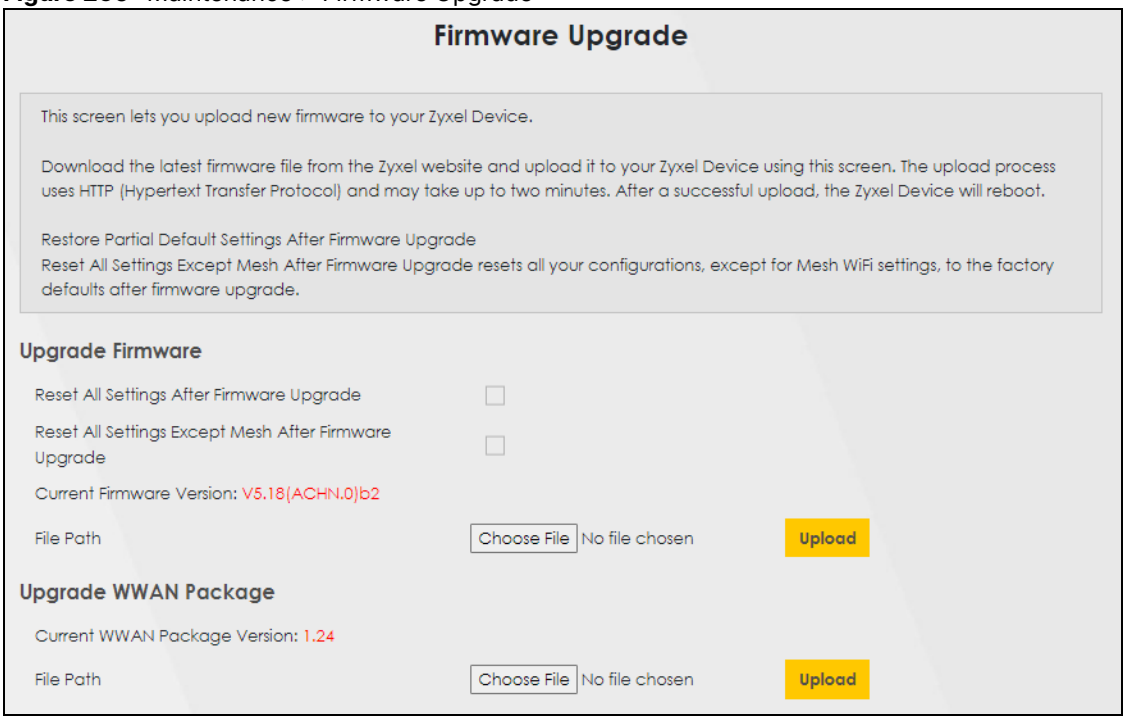
This screen lets you upload new firmware to your Zyxel Device.

Get the latest firmware from your service provider. Then upload the firmware file to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol). The upload may take up to 3 minutes. After a successful upload, the Zyxel Device will reboot.

Click **Maintenance** > **Firmware Upgrade** to open the **following** screen.

Do NOT turn off the Zyxel Device while firmware upload is in progress!

Figure 260 Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

Table 170 Maintenance > Firmware Upgrade

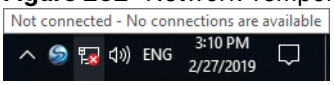
LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select this to reset all your configurations, including Mesh WiFi settings, to the factory defaults after firmware upgrade. Otherwise, make sure this is cleared if you do not want the Zyxel Device to lose all its current configurations and return to the factory defaults. Note: Make sure to back up the Zyxel Device's configuration settings first in case the reset all settings process is not successful.
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 3 minutes. Note: Only use firmware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device. For example, if the Zyxel Device's current firmware version is V5.70(ACDZ.0)B4, you must upload the firmware file containing "ACDZ".

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

Figure 261 Firmware Uploading

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

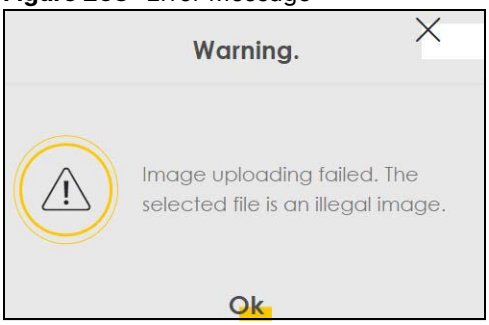
Figure 262 Network Temporarily Disconnected



After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

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

Figure 263 Error Message



40.3 Online Upgrade

This screen lets you check for new firmware for your Zyxel Device by checking online for the latest firmware file now or scheduling when the Zyxel Device will check online for the latest firmware file.

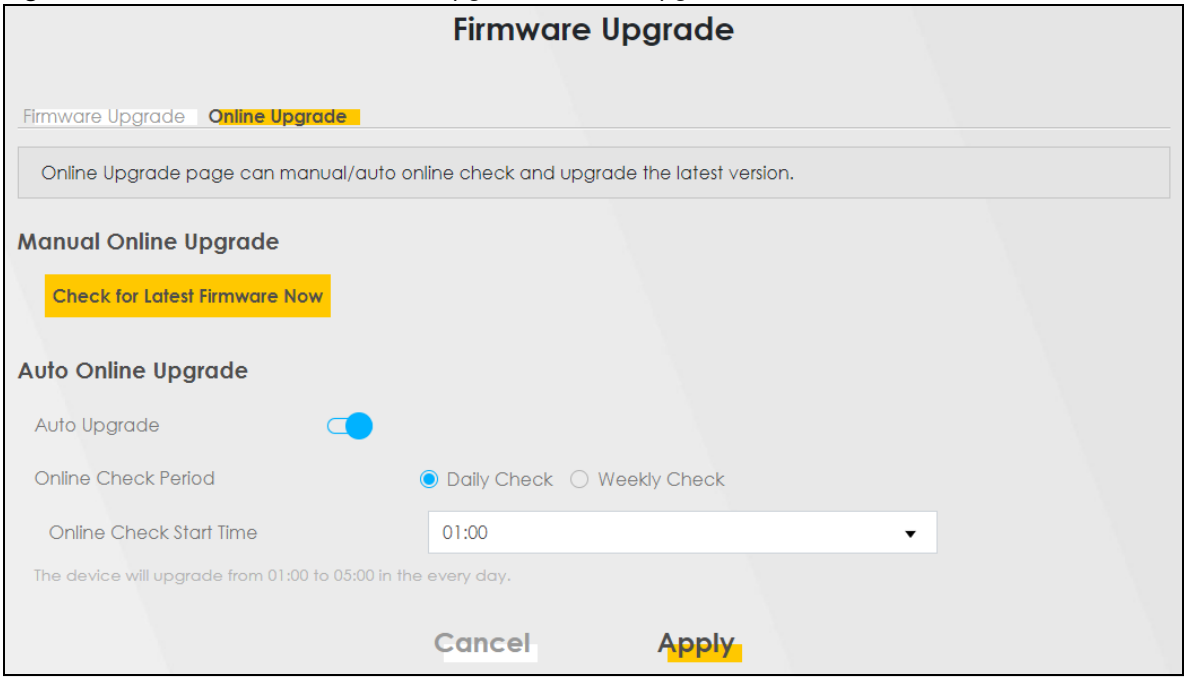
Note: Make sure your Zyxel Device is connected to the Internet.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take more than 3 minutes. After a successful upload, the Zyxel Device will reboot automatically.

Click **Maintenance** > **Firmware Upgrade** > **Online Upgrade** to open the **following** screen.

Do NOT turn off the Zyxel Device while firmware upload is in progress!

Figure 264 Maintenance > Firmware Upgrade > Online Upgrade



The following table describes the labels in this screen.

Table 171 Maintenance > Firmware Upgrade > Online Upgrade

LABEL	DESCRIPTION
Manual Online Upgrade	
Check for Latest Firmware Now	Click this to have the Zyxel Device check for new firmware immediately. If a newer firmware is available, follow the online prompt to upload the new firmware to your Zyxel Device.
Auto Online Upgrade	
Auto Upgrade	Click the switch to the right to activate automatic firmware upgrade. Note: To minimize disruption to your network, the Zyxel Device will upgrade the firmware from 01:00 to 05:00 by default.
Online Check Period	Select **Daily Check** when you want the Zyxel Device to check online for new firmware everyday. Select **Weekly Check** when you want the Zyxel Device to check online for new firmware once a week.
The day of every week	Select the day that you want the Zyxel Device to check for new firmware. Note: This field only appears when you select **Weekly Check** in **Online Check Period**.
Online Check Start Time	Select the hour of the day that you want the Zyxel Device to check for new firmware.
Cancel	Click **Cancel** to close the window with changes unsaved.
Apply	Click **Apply** to save the changes back to the Zyxel Device.

CHAPTER 41
Backup/Restore

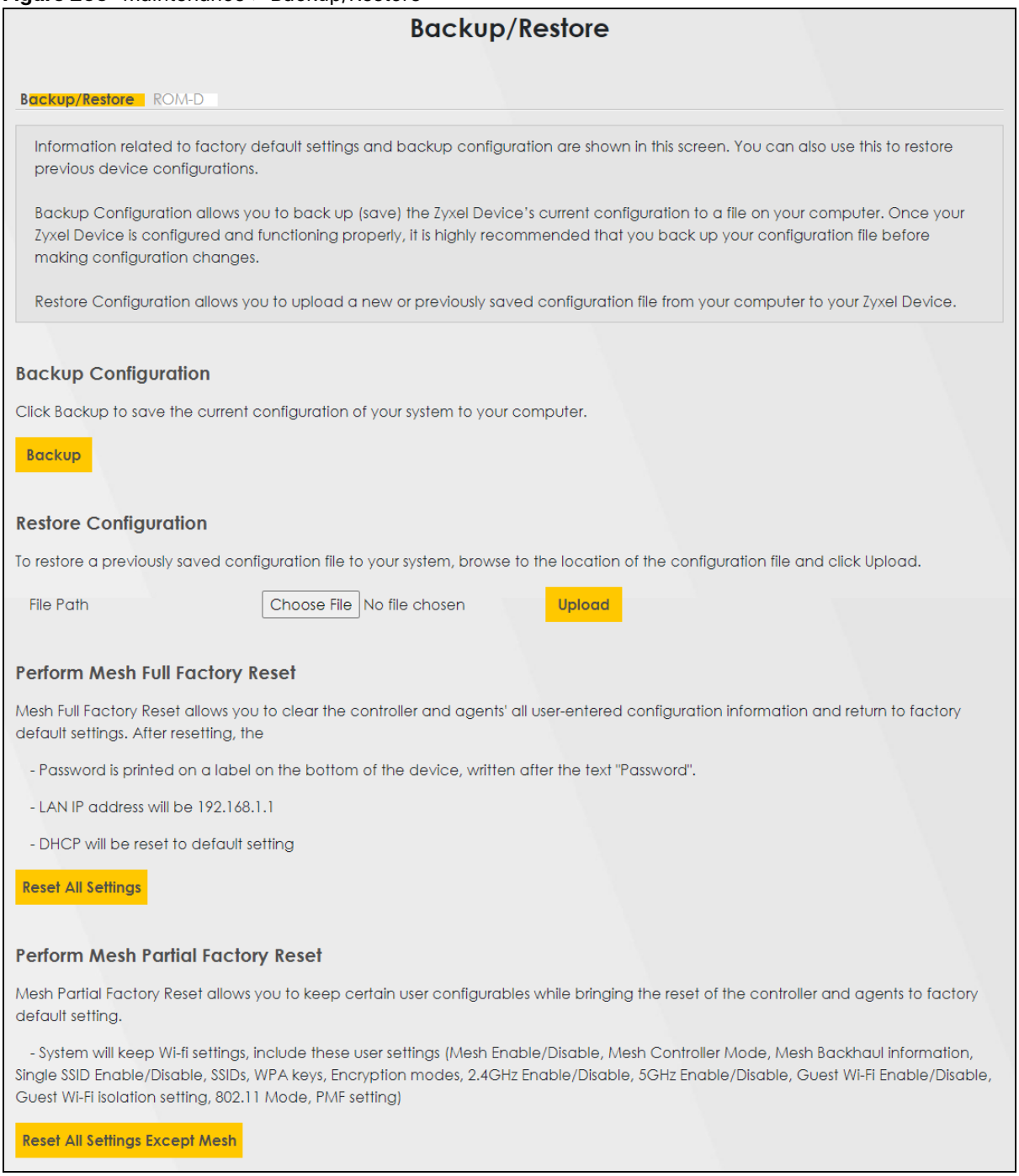
41.1 Backup/Restore Overview

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

41.2 Backup/Restore

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

Figure 265 Maintenance > Backup/Restore



Backup Configuration

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. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Zyxel 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 Zyxel Device.

Table 172 Maintenance > Backup/Restore: Restore Configuration

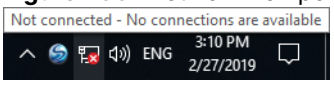
LABEL	DESCRIPTION
File Path	Enter in the location of the file you want to upload in this field or click **Choose File** / **Browse** to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload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

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

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

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

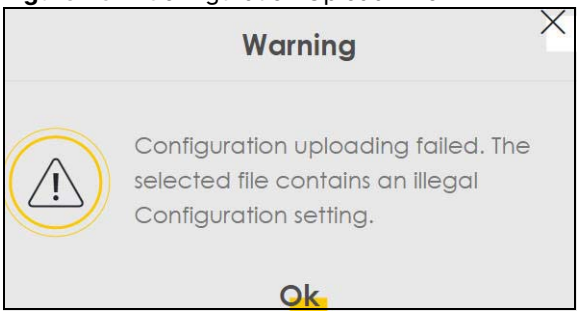
Figure 266 Network Temporarily Disconnected



If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default Zyxel Device IP address (192.168.1.1 – 192.168.225.225).

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

Figure 267 Configuration Upload Error



Back to Factory Default Settings

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

Figure 268 Reset Warning Message

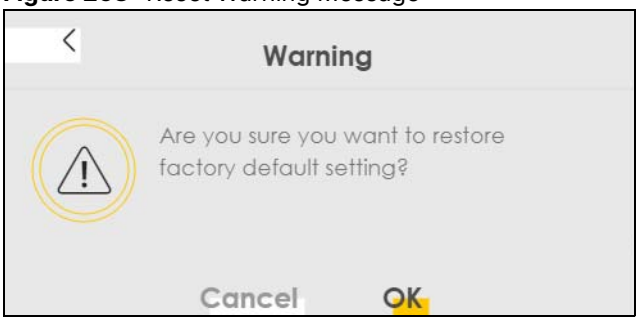
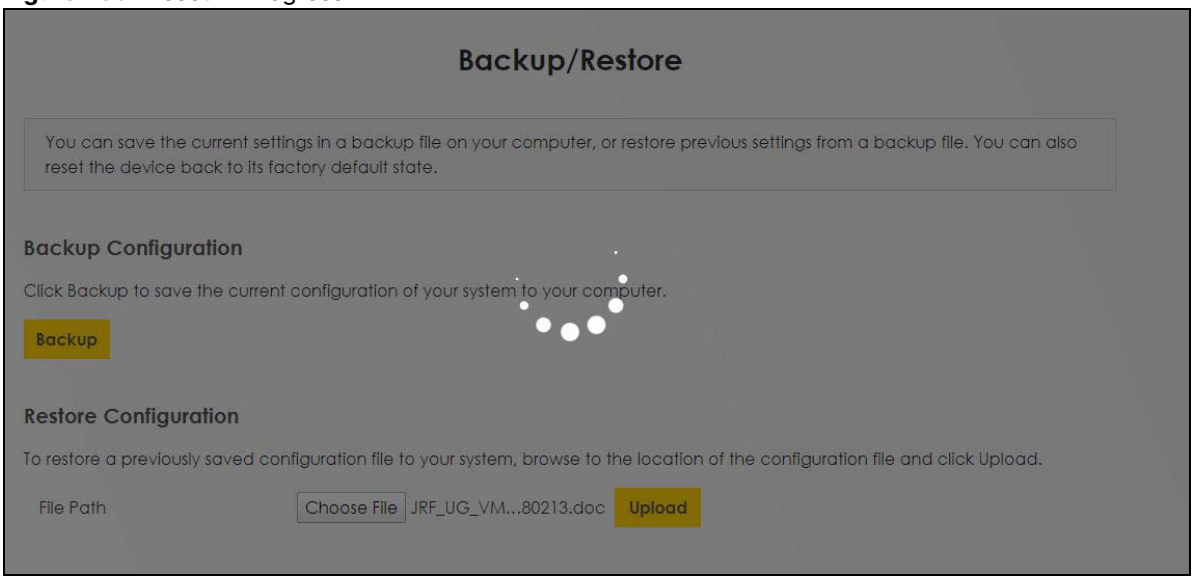


Figure 269 Reset In Progress



You can also press the **RESET** button on the panel to reset the Zyxel Device to the factory defaults.

Perform Partial Factory Reset

Click the **Reset All Settings Except Mesh** button to clear all user-entered configuration information and return the Zyxel Device to its factory defaults except for Mesh WiFi settings. The following warning screen appears.

Figure 270 Reset Warning Message

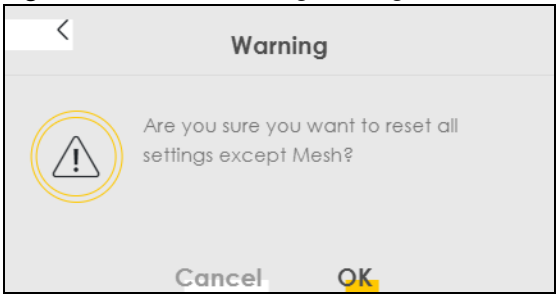
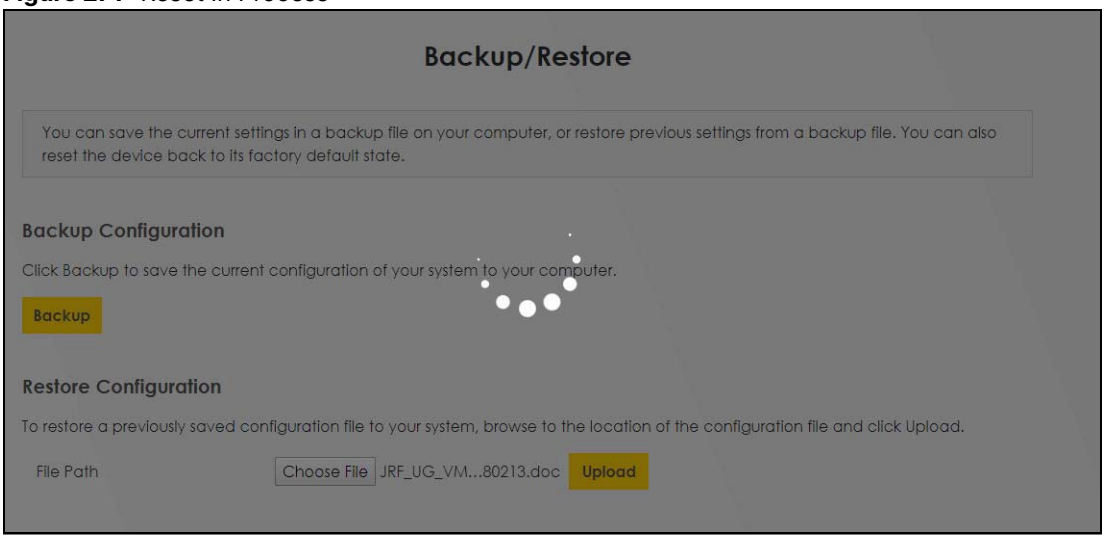


Figure 271 Reset In Process

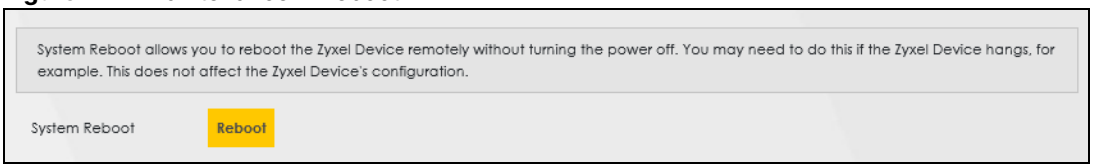


41.3 Reboot

System **Reboot** allows you to restart the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example. This does not affect the Zyxel Device's configuration.

Click **Maintenance** > **Reboot**. Click **Reboot** to have the Zyxel Device restart.

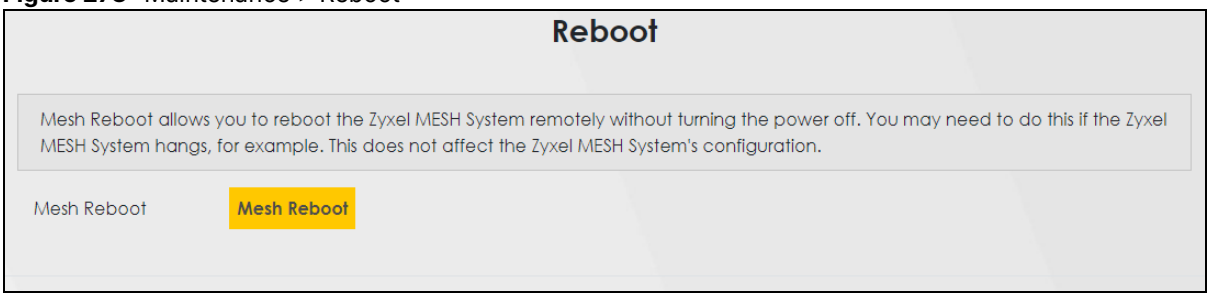
Figure 272 Maintenance > Reboot



Mesh Reboot allows you to reboot the Zyxel Mesh system remotely without turning the power off. You may need to do this if the Mesh system hangs, for example. This does not affect the Zyxel Mesh system's configuration.

Click **Maintenance** > **Reboot**. Click **Mesh Reboot** to have the Zyxel Mesh system reboot.

Figure 273 Maintenance > Reboot



CHAPTER 42
Diagnostic

42.1 Diagnostic Overview

The **Diagnostic** screen displays information to help you identify Internet connection problems with the Zyxel Device.

The route between an Ethernet switch and one of its Customer-Premises Equipment (CPE) may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

42.1.1 What You Can Do in this Chapter

- The **Ping&Traceroute&Nslookup** screen lets you ping an IP address or trace the route packets take to a host (Section 42.3 on page 425).

42.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

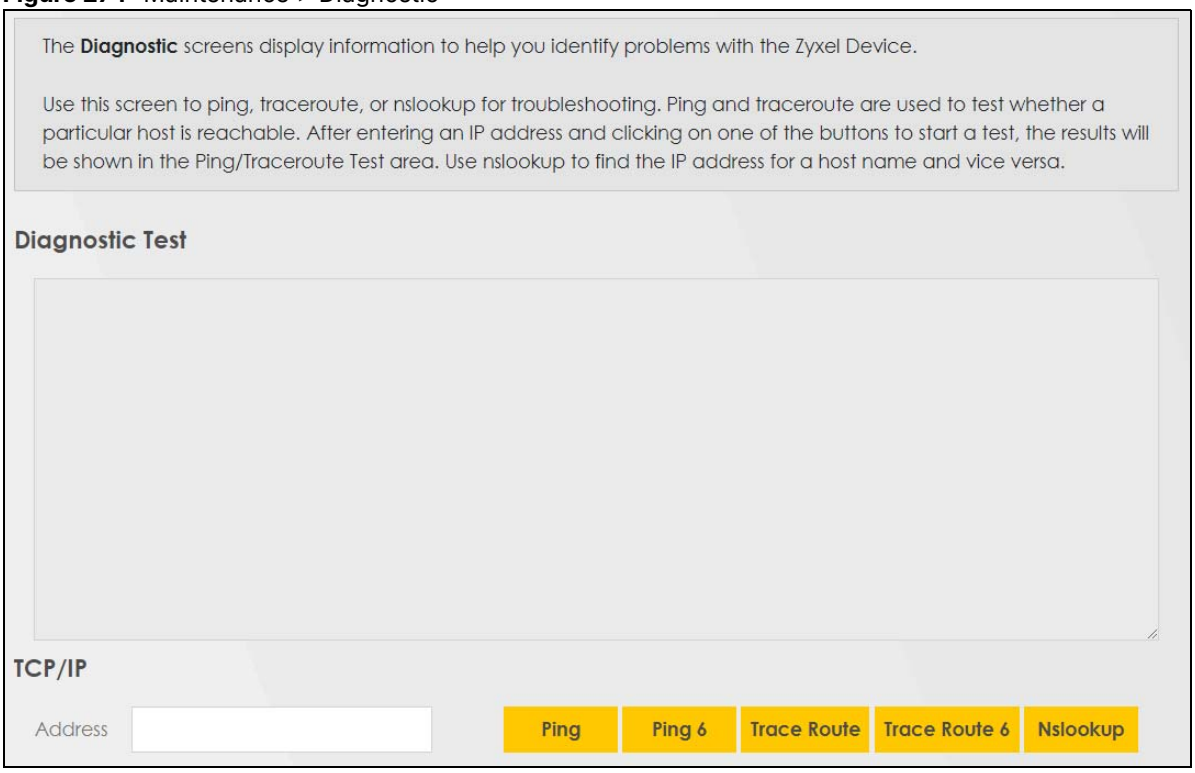
- Loopback test – checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test – provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

42.3 Diagnostic

Use this screen to ping, traceroute or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking one of the buttons to start a test, the results will be shown in the screen. Use nslookup to find the IP address for a host name and the host name for an IP address.

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

Figure 274 Maintenance > Diagnostic



The following table describes the fields in this screen.

Table 173 Maintenance > Diagnostic

LABEL	DESCRIPTION
Ping/TraceRoute Test	The result of tests is shown here in the info area.
Select Test Method	
Ping	Select this to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area.
Ping 6	Select this to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area.
Trace Route	Select this to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Select this to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Select this to perform a DNS lookup on the IP address or host name.
TCP/IP	

Table 173 Maintenance > Diagnostic (continued)

LABEL	DESCRIPTION
Address	Enter the IP address of a computer that you want to perform ping, trace route or nslookup in order to test a connection.
Start Test	Click this to perform the selected test method.

PART III
Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your Zyxel Device.

CHAPTER 43
Troubleshooting

43.1 Troubleshooting Overview

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

43.2 Accessibility and Compatibility Problems

Screen reader not reading content.

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

Web browser not displaying correctly.

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

43.3 Power and Hardware Problems

The Zyxel Device does not turn on.

1. Make sure you are using the power adapter included with the Zyxel Device.
2. Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adapter to the Zyxel Device.
4. Make sure you have pressed the **POWER** button to turn on the Zyxel Device.
5. If the problem continues, contact the vendor.

The LED does not behave as expected.

1. Make sure you understand the normal behavior of the LED.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the Zyxel Device off and on.
5. If the problem continues, contact the vendor.

43.4 Device Access Problems

I do not know the IP address of the Zyxel Device.

1. The default IP address is 192.168.1.1.
2. If you changed the IP address, you might be able to find the IP address of the Zyxel Device by looking up the IP address of your computer's default gateway. To do this in Microsoft Windows, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device, depending on your network environment.
3. If this does not work, reset the Zyxel Device to its factory defaults.
   - Locate a small hole labeled **RESET** on the Zyxel Device.
   - Use a paperclip or a similar tool to press and hold the **RESET** button for more than 5 seconds.

- Release the button, and the Zyxel Device will reset to its default settings, including the default IP address, user name, and password.

Note: Resetting the Zyxel Device will erase all your custom settings, so you need to reconfigure it.

I forgot the admin password.

1 See the Zyxel Device label or this document's cover page for the default admin password.

2 If you changed the password from default and cannot remember the new one, you have to reset the Zyxel Device to its factory default settings.

I cannot access the Web Configurator login screen.

1 Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address, use the new IP address.
   - If you changed the IP address and have forgotten the new address, see the troubleshooting suggestions for I do not know the IP address of the Zyxel Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected.

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

4 Clear the Internet browser cache and try accessing the Web Configurator login screen again. Outdated browser data can cause login issues. If the problem persists, try logging into the web configurator using a different browser. (e.g., Chrome, Firefox, Edge)

5 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance** > **Remote Management**).

6 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.

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

Advanced Suggestions

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

I cannot log into the Zyxel Device.

1 For first-time Zyxel Device logins, after using the label password to access the web configurator, ensure your new password meets the requirements on the screen. For example, some models require the new password to be at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character.

2 Make sure you have entered the user name and password correctly. The default user name is **admin**. These both user name and password are case-sensitive, so make sure [Caps Lock] is not on.

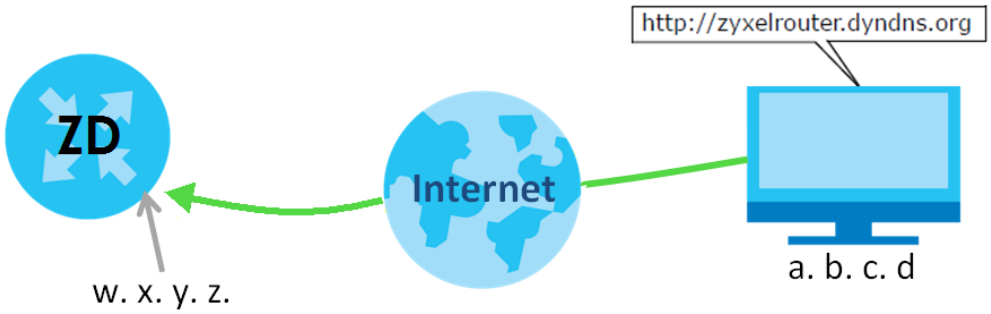
3 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

4 Turn the Zyxel Device off and on.

5 If this does not work, you have to reset the Zyxel Device to its factory default. To reset the Zyxel Device, press the **RESET** button until the POWER LED begins to blink and then release it.

I cannot log into the Zyxel Device using DDNS.

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the Zyxel Device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

Note: If you have a private WAN IP address, then you cannot use DDNS.

Here are the three steps to use a domain name to log in the Web Configurator:

Step 1 Register for a DDNS Account on www.dyndns.org

1 Open a browser and enter **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the Zyxel Device later.

Step 2 Configure DDNS on Your Zyxel Device

Configure the following settings in the **Network Setting** > **DNS** > **Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Enter **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**). Click **Apply**.

Step 3 Test the DDNS Setting

Now you should be able to access the Zyxel Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Enter **http://zyxelrouter.dyndns.org** and press [Enter].

3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

I cannot connect to the Zyxel Device using Telnet, SSH, or Ping.

1 See the Remote Management section for details on allowing web services (such as HTTPS, Telnet, SSH and Ping) to access the Zyxel Device.

2 Check the server **Port** number field for the web service in the **Maintenance** > **Remote Management** screen. You must use the same port number in order to use that web service for remote management.

3 Try the troubleshooting suggestions for I cannot access the Web Configurator login screen. Ignore the suggestions about your browser.

I cannot access the Zyxel Device from outside the network (WAN).

To test if this is due to CGNAT, follow these steps:

1 Log in to your Zyxel Device's Web Configurator using the default IPv4 address (for example, 192.168.1.1).

2 Locate the WAN IP address on the **Dashboard** screen. You can find this information in the Network or WAN settings.

3 Go to a website that can show you the public IP address of your network (for example, https://whatsmyip.com). When you access this site, it will display your public IP address.

4 Compare the WAN IP address displayed on the **Dashboard** screen with the public IP address shown on the https://whatsmyip.com website.

- If both IP addresses are the same, your ISP is not using Carrier-Grade NAT, and you should be able to access your Zyxel Device from the WAN (outside).
- If the IP addresses are different, it indicates that your ISP is using Carrier-Grade NAT, and your Zyxel Device has a shared public IP address. As a result, remote access to your Zyxel Device from the WAN will not be possible.

If you discover that your Zyxel Device is behind a Carrier-Grade NAT and you need remote access, you must contact your ISP and request a public IP address for your SIM card or Zyxel Device.

43.5 Internet Problems

I cannot access the Internet.

1 Check the hardware connections and make sure the LEDs are behaving as expected. See the **Quick Start Guide**.

2 Make sure you entered your ISP account information correctly on the **Network Setting** > **Broadband** screen. Fields on this screen are case-sensitive, so check if [Caps Lock] is on of off.

3 If you are trying to access the Internet wirelessly, make sure that you enabled the WiFi in the Zyxel Device and your WiFi client and that the WiFi settings in the WiFi client are the same as the settings in the Zyxel Device.

4 Disconnect all the cables from your Zyxel Device and reconnect them.

5 If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet connection.

1 Make sure you have the Ethernet WAN port connected to a Modem or Router.

2 Make sure you configured a proper Ethernet WAN interface (**Network Setting** > **Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

3 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting** > **Interface Group**).

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **Network Setting** > **Home Networking** > **LAN Setup** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a Fiber connection.

1 Make sure the Fiber/SFP port has a compatible SFP/SFP+ transceiver installed with a fiber/Ethernet cable connected to it.

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

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 is red if the GPON Device is not receiving an optical signal.

The **LOS** LED blinks red if the GPON Device is receiving a weak optical signal.

3 Disconnect all the cables from your device and reconnect them. Make sure the fiber cable is not curved too much.

4 If that does not work, restart your Zyxel Device.

5 If the problems continues, contact your ISP.

I cannot connect to the Internet using a cellular connection.

1 The DSL and Ethernet connections have priority in that order. If the DSL or Ethernet connection is up, then the cellular connection will be down.

2 Make sure you have connected a compatible cellular dongle to the USB port, if required.

3 Make sure you have configured **Network Setting** > **Broadband** > **Cellular Backup** correctly.

4 Check that the Zyxel Device is within range of a cellular base station.

The Zyxel Device cannot assign individual IP addresses to the connected client devices.

1 Make sure to select **Bridge** in **Network Setting** > **Broadband** > **Add/Edit New WAN Interface**: **Mode**.

2 Make sure to reboot the Zyxel Device after changing to **Bridge** mode.

3 Make sure the Zyxel Device can get an IP address dynamically (DHCP) from the router controller.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 If your Zyxel Device keeps alternating between ISPs, then choose a fixed ISP. Go to the **Network Setting** > **Cellular PLMN** screen, disable **PLMN Auto Selection** and then choose your preferred ISP.

3 Turn the Zyxel Device off and on.

4 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions in I cannot access the Web Configurator login screen.

Note: If your Zyxel Device is an outdoor-type, inclement weather like rain and hot weather may affect cellular signals.

What should I do if my Zyxel Device is under attack?

A slow Internet speed, a web browser that keeps redirecting you, suspicious activity alerts from your ISP, and increased pop-ups on the Zyxel Device; could be signs that your Zyxel Device is under attack. If you suspect that your Zyxel Device is under attack, do the following:

1 Create an ACL (Access Control List) rule to block the ports being targeted. See Section 18.5 on page 310 for more information on using ACL. See also Section 5.6.1 on page 112 for more information on configuring a firewall rule. Go to **System Monitor** > **Log** > **Security Log** to view the security-related logs to determine which ports are being targeted. See Section 25.3 on page 372 for more information on security logs.

2 Contact your ISP to report the attack and seek assistance.

3 When possible, turn off the Zyxel Device for 24 hours, then turn it on again.

4 Request the ISP to change your IP address.

43.6 WiFi Problems

I cannot connect to the Zyxel Device WiFi.

1 Check the WiFi LED status to make sure the Zyxel Device WiFi is on.

2 Make sure your WiFi client is within transmission range of the Zyxel Device.

3 Make sure you entered the correct SSID and password. See the Zyxel Device back label for the default SSID and password.

4 Make sure your WiFi client is using the same WiFi security type (WPA2-PSK, WPA3-SAE, or none) as the Zyxel Device.

5 Make sure the WiFi adapter on your WiFi client is working properly. Right-click your computer's network adapter then select **Properties** to check your network adapter status.

6 Make sure the WiFi adapter on your WiFi client is IEEE 802.11-compatible and supports the same WiFi standard as the Zyxel Device radio.

Note: To check if it is your Zyxel Device that is causing the problem and not your WiFi connection, try using a wired connection.

The WiFi connection is slow and intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your WiFi connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the WiFi client.
- Reduce the number of WiFi clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Place the Zyxel Device where there are minimum obstacles (such as walls and ceilings) between the Zyxel Device and the WiFi client. Avoid placing the Zyxel Device inside any type of box that might block WiFi signals.

I want to allow or block specific devices from connecting to the Zyxel Device’s WiFi network.

MAC authentication allows devices with MAC addresses listed in the Zyxel Device’s MAC address list to connect or block access to its WiFi network.

To set up MAC authentication of your Zyxel Device, follow the steps below:

1 Log into your Zyxel Device's Web Configurator, and go to **Network Setting > Wireless > MAC Authentication**.

2 In the **General** section, select the SSID of the WiFi network for which you want to configure MAC authentication from the dropdown list.

3 There are two ways to configure the MAC authentication:

3a Set the MAC addresses you want to block access to the Zyxel Device's WiFi network.

- In the **MAC Restrict Mode** section, select **Deny**.
- In the **MAC address list** section, click the + icon to add a new MAC address.
- The **Add MAC address to list** screen will appear. In the **MAC Address** field, enter the MAC address you want to block access to the Zyxel Device's WiFi network.

3b Set the MAC addresses you want to allow to connect to the Zyxel Device's WiFi network.

- In the **MAC Restrict Mode** section, select **Allow**.
- In the **MAC address list** section, click the + icon to add a new MAC address.
- The **Add MAC address to list** screen will appear. In the **MAC Address** field, enter the MAC address you want to allow to connect to the Zyxel Device's WiFi network.

43.7 Mesh Problems

I can't build a mesh network between the Zyxel Device and the extender(s).

Different mesh technologies may be incompatible, so make sure the Zyxel Device and the extender(s) use the same mesh technology.

To build a mesh network and ensure the smooth client roaming between the Zyxel Device and the extender(s), please check the following.

1 Make sure the Zyxel Device and the extender(s) have consistent SSID and security settings.

2 Make sure the Zyxel Device and the extender(s) are not too far or too close to each other.

43.8 USB Problems

The Zyxel Device fails to detect my USB device.

1 Disconnect the USB device.

2 Reboot the Zyxel Device.

3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

4 Reconnect your USB device to the Zyxel Device.

43.9 VoIP Problems

I cannot make phone calls through the phone connected to the Zyxel Device.

1 Pick up the phone and check the phone tone. You should hear the dial tone if your configuration on the Zyxel Device is correct, and your phone is successfully connected to the SIP server.

2 Check that the settings from your VoIP service are entered correctly on the Zyxel Device.

3 Make sure your phone is connected to the Zyxel Device phone port through an RJ-11 cable. Check the Zyxel Device phone LED for the corresponding phone status.

4 Make sure the Zyxel Device has an Internet connection. See Section 43.5 on page 433 for more information.

5 Make sure your SIP account is registered and your SIP service plan is valid. Use the **System Monitor** > **VoIP Status** screen to check the account **Registration** status.

6 Make sure your SIP server settings (in the **VoIP** > **SIP** > **SIP Service Provider** and the **VoIP** > **SIP** > **SIP Account** screens) use the correct information from your SIP service provider. For example, your SIP service provider name, SIP account and password.

7 Make sure your phone settings (in the **VoIP** > **Phone** > **Phone Device** screen) are correct.

8 Contact the SIP server administrator and make sure your SIP server is not down.

I am experiencing echoes during calls.

Go to **VoIP > SIP > SIP Account > SIP Account Entry Edit**. Click **Enable G.168 (Echo Cancellation)** to eliminate echo during calls.

43.10 UPnP Problems

My computer cannot detect UPnP settings from the Zyxel Device.

1 Make sure that UPnP is enabled in your computer.

2 On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings** > **Home Networking** > **UPnP** screen.

3 Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.

4 Reconnect the Ethernet cable.

5 Restart your computer.

43.11 Getting More Troubleshooting Help

Search for support information for your model at *https://service-provider.zyxel.com/global/en/tech-support* and *community.zyxel.com* for more troubleshooting suggestions.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the Zyxel Device.

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

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

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

Korea

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

Malaysia

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Belarus

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

Belgium (Netherlands)

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

Bulgaria

- Zyxel Bulgaria

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

Czech Republic

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

Denmark

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Norway

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

Poland

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

Romania

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

Russian Federation

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

Slovakia

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

Spain

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

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

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

South America

Argentina

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

Brazil

- Zyxel Communications Brasil Ltda.

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

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

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

North America

USA

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

APPENDIX B
Wireless LANs

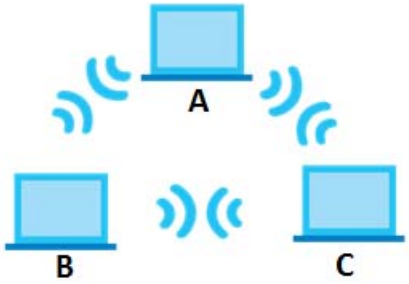
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 275 Peer-to-Peer Communication in an Ad-hoc Network

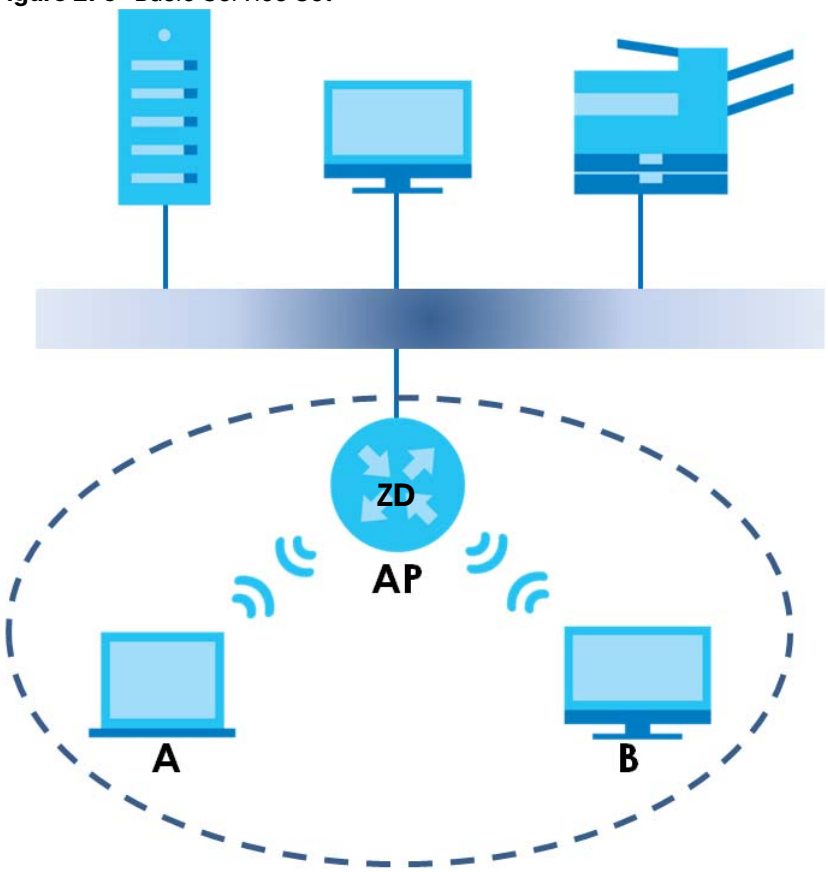


BSS

A Basic Service Set (BSS) exists when all communications between WiFi clients or between a WiFi client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between WiFi clients in the BSS. When Intra-BSS is enabled, WiFi client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, WiFi client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 276 Basic Service Set



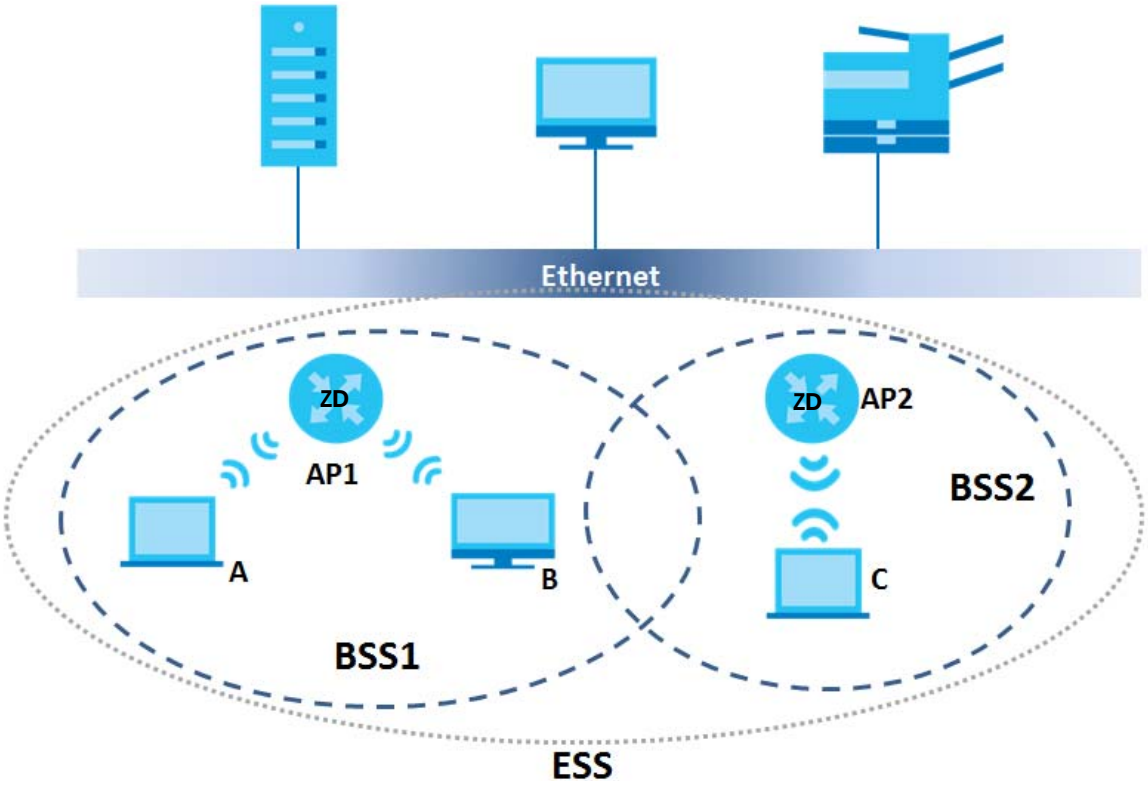
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated WiFi clients within the same ESS must have the same ESSID in order to communicate.

Figure 277 Infrastructure WLAN



Channel

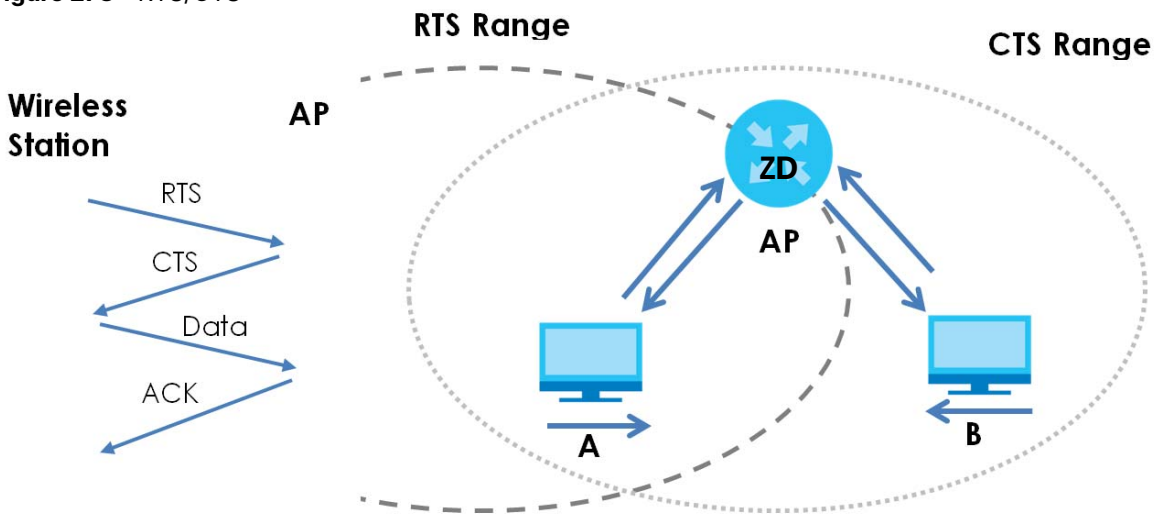
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 278 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 174 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between WiFi clients, access points and the wired network.

Wireless security methods available on the Zyxel Device are data encryption, WiFi client authentication, restricting access by device MAC address and hiding the Zyxel Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Zyxel Device.

Table 175 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	WiFi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the Zyxel Device and on all WiFi clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the WiFi clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the WiFi client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the WiFi client. The WiFi client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the WiFi clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 176 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

WiFi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the WiFi clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and WiFi client. As long as the passwords match, a WiFi client will be granted access to a WLAN.

If the AP or the WiFi clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or WiFi clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a WiFi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP).

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate WiFi clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a WiFi client to store the PMK it derived through a successful authentication with an AP. The WiFi client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the WiFi client (already connected to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WiFi Client WPA Supplicants

A WiFi client supplicant is the software that runs on an operating system instructing the WiFi client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

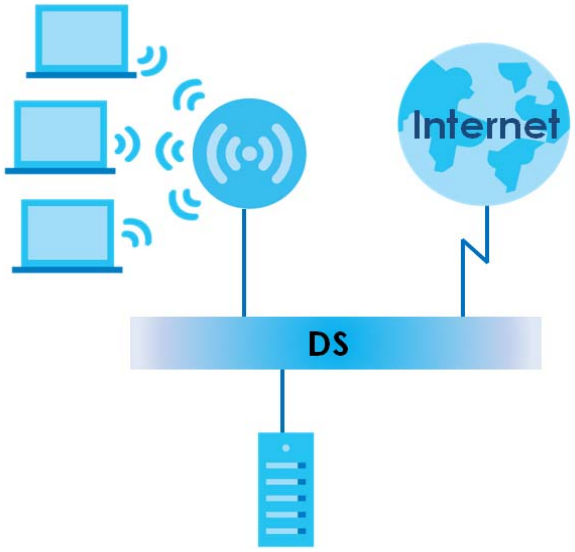
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" WiFi client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the WiFi client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients.

Figure 279 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

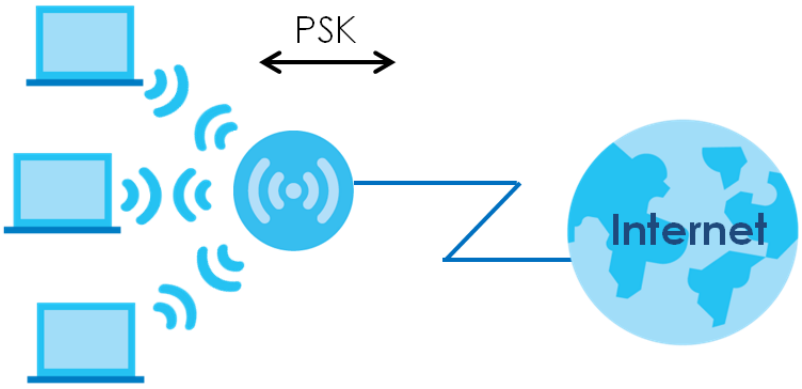
1 First enter identical passwords into the AP and all WiFi clients. The Pre-Shared Key (PSK) must consist of between 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.

2 The AP checks each WiFi client's password and allows it to join the network only if the password matches.

3 The AP and WiFi clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and WiFi clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 280 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 177 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4 GHz (IEEE 802.11b and IEEE 802.11g) or 5 GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WiFi

There are two types of antennas used for WiFi applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

APPENDIX C
IPv6

Overview

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

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

Prefix and Prefix Length

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

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

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

Link-local Address

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

Table 178 Link-local Unicast Address Format

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

Global Address

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

Unspecified Address

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

Loopback Address

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

Multicast Address

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

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

Table 179 Predefined Multicast Address

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

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

Table 180 Reserved Multicast Address

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

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses 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 181

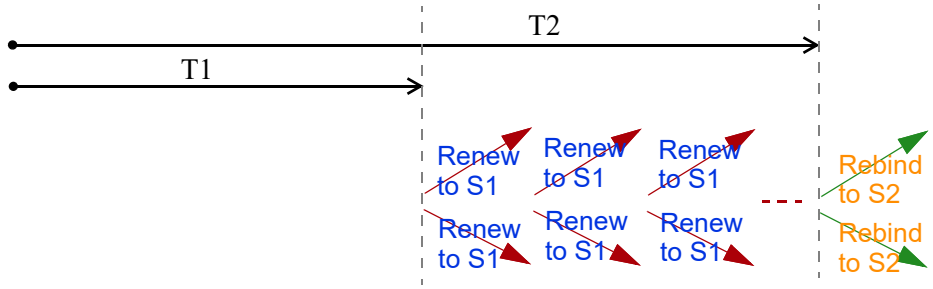
MAC	00	:	13	:	49	:	12	:	34	:	56

Table 182

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 Zyxel 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 Zyxel 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 Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel 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 Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives

a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel 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 Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel 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 Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel 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.

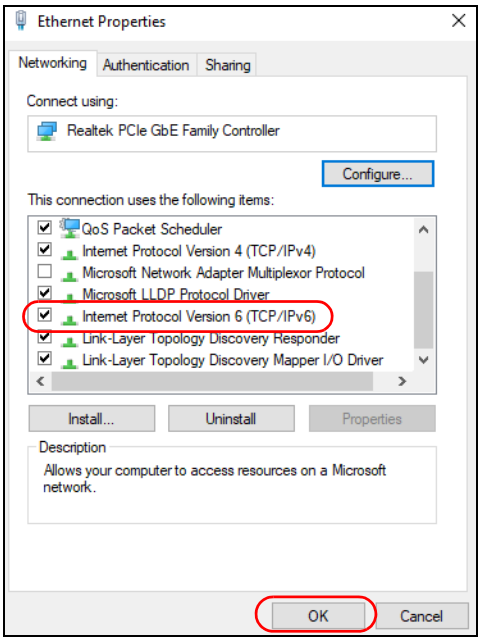
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a Multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected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

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 10 computer.

To enable IPv6 in Windows 10:

1. Click the start icon, **Settings** and then **Network & Internet**.
2. Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
3. Click **OK** to save the change.



4 Click the Search icon ( ) and then enter “cmd” in the search box.

5 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:f
```

APPENDIX D
Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 183 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance *www.zyxel.com*) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for email.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.

Table 183 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get email from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).

Table 183 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

Legal Information

Copyright

Disclaimer

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

Regulatory Notice and Statement

United States of America

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

FCC Statement

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

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

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

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

which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

The following information applies to products with wireless functions.

- For 2.4G WLAN, only channels 1~11 are operational. Selection of other channels is not possible.
- Operation of this device is restricted to indoor use only, unless the relevant user’s manual states that this device can be installed outdoors.

FCC Radiation Exposure Statement

- This device complies with FCC Radio Frequency (RF) radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 50 cm (EE6510-10), 21 cm (EE4410-00), and 20 cm (all other models) from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

The following information applies for products operating in the 5.925-7.125 GHz band.

Low-power Indoor Access Point

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Standard Power Access Point

- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Canada

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

CAN ICES(B) / NMB(B)

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

  (1) this device may not cause interference, and

  (2) this device must accept any interference, including interference that may cause undesired operation of the device.

- L'émetterur/récepteur exempt de licence contenu dans le prés ent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio ex empts de licence.

  L'exploitation est autorisée aux deux condi tions suivantes:

  (1) l'appareil ne doit pas produire de brouillage;

  (2) L'appareil doit accepter tout brouillage radioélectrique su bi, même si le brouillage est susc eptible d'en compromettre le fonctionnement.
- For 2.4 G WLAN, only channels 1-11 are operational. Selection of other channels is NOT possible.
- Pour le WLAN 2,4 G, seuls les canaux 1 à 11 sont opérationnels. La sélection d'autres canaux n'est PAS possible.
- The device operating in the 5150-5250 MHZ band is only for indoor use to reduce the potential for harmful interference to co-channal mobile statellite systems.
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set force in Section 6.2.2.3 of RSS 247 shall be clearly indicated.
- Les dispositifs fonctionnant dans la bande de 5150 à 5250 MHz so nt réservés uniquement pour une utilisation à l'intérieur af in de réduire les risques de brouillage préjudiciable aux systémes de satellites mobiles utilisant les mêmes canaux;
- Lorsq'ily a lieu, les types d'antnnes(s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inc linaison nécessaires pour rester confirme à la limite de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doi vent être clairement indiqués.

Industry Canada radiation exposure statement

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 23 cm (EE6601-00), 29 cm (EE6510-10), 24 cm (EE4410-00), and 20 cm (all other models) between the radiator and your body.

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 23 cm (EE6601-00), 29 cm (EE6510-10), 24 cm (EE4410-00), et 20 cm (tous les autres modèles) de distance entre la source de rayonnement et votre corps.

The following information applies for products operating in the 5.925-7.125 GHz band.

RLAN Devices

- Devices shall not be used for control of or communications with unmanned aircraft systems.

dispositifs RLAN

- Les dispositifs ne doivent pas être utilisés pour commander des systèmes d'aéronef sans pilote ni pour communiquer avec de tels systèmes.

Low-power indoor access points and indoor subordinate devices

- Operation shall be limited to indoor use only.
- Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited except for on large aircraft flying above 3,048 m (10,000 ft).

Points d'accès intérieurs de faible puissance et dispositifs subordonnés intérieurs

- leur utilisation doit être limitée à l'intérieur seulement;
- leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite, sauf à bord d'un gros aéronef volant à plus de 3 048 m (10 000 pi) d'altitude.

Standard-power access points and fixed client devices

- Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited.
- Information for antenna type(s), antenna model(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 4.5.4.c shall be clearly indicated.

Points d'accès de puissance normale et dispositifs clients fixes

- leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite;
- le ou les types d'antennes, le ou les modèles d'antennes et le ou les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la section 4.5.4(c) sur le masque de p.i.r.e par rapport à l'angle de site doivent être clairement indiqués.

Europe and the United Kingdom

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Radio Equipment Regulations 2017

Model List: EE3301-00, EE5301-00, EE6601-00, PE3301-00, PE5301-01

- Compliance information for wireless products relevant to the EU, United Kingdom, and other Countries following the EU Directive 2014/53/EU (RED) and UK Radio Equipment Regulations 2017. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU, United Kingdom, and other European countries, the 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz wireless LANs.
- If this device operates in the 5150 to 5350 MHz band, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF operating power for each band is as follows:
- EE6601-00

  - 83.95 mW for the 2,400 to 2,483.5 MHz band
  - 165.58 mW for the 5,150 to 5,350 MHz band
  - 749.89 mW for the 5,470 to 5,725 MHz band
  - 170.22 mW for the 5,725 to 5,850 MHz band (UK only)
  - 165.96 mW for the 5,945 to 6,425 MHz band
- EE5301-00 / PE5301-01
  - 88.92 mW for the 2,400 to 2,483.5 MHz band
  - 176.20 mW for the 5,150 to 5,350 MHz band
  - 887.16 mW for the 5,470 to 5,725 MHz band
  - 177.42 mW for the 5,725 to 5,850 MHz band (UK only)
- EE3301-00 / PE3301-00
  - 97.95 mW for the 2,400 to 2,483.5 MHz band
  - 197.70 mW for the 5,150 to 5,350 MHz band
  - 988.55 mW for the 5,470 to 5,725 MHz band
  - 196.79 mW for the 5,725 to 5,850 MHz band (UK only)

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

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

Notes:

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

List of national codes

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

Safety Warnings

- Do not put the device in a place that is humid, dusty, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (2) Do not install or service this device during a thunderstorm.
- 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 the device covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connected cables carefully so that no one will step on them or stumble over them.

- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect the power adaptor or cord to the right supply voltage (for example, 120 VAC in North America or 230 VAC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove the damaged power adaptor or cord from the device and the power source. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas.
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

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

  – For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.
- This product is intended to be supplied by a DC power source marked 'L.P.S' or `Limited Power Source'. The rating for each model is as follows:
  - EE6510-10: 12 VDC / 3.5 A / Tma 40 °C
  - EE6601-00: 12 VDC / 3.5 A / Tma 40 °C
  - EE4410-00 / PE5301-01: 12 VDC / 3 A / Tma 40 °C
  - EE5301-00 / EE3301-00 / PE3301-00: 12 VDC / 2.5 A / Tma 40 °C

The following information applies for products with SFP:

- CLASS 1 LASER PRODUCT & “IEC 60825-1:2014”
- CLASS 1 CONSUMER LASER PRODUCT & "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.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.

- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.
- Attention: L'utilisation des commandes ou reglages ou l'execution des procedures autres que celles specifiees dans les presents exigences peuvent etre la cause d'une exposition a un rayonnement dangereux

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market 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 < 8 W, and/or
- Off mode power consumption < 0.5 W, and/or
- Standby mode power consumption < 0.5 W.

(Wireless setting, please refer to the chapter about wireless settings for more detail.)

Disposal and Recycling Information

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

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

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

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

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

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

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 本機限在不干擾合法電台與不被干擾保障條件下於室內使用。本產品使用時建議應距離人體 20 cm 以上。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 – 為了您的安全，請先閱讀以下警告及指示 :

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸 :
  – 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  – 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。

- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 （如：台灣供應電壓 110 伏特）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  – 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  – 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

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

Explanation of the Symbols

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

Viewing Certifications

Go to *http://www.zyxel.com* to view this product's documentation and certifications.

Zyxel Limited Warranty

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

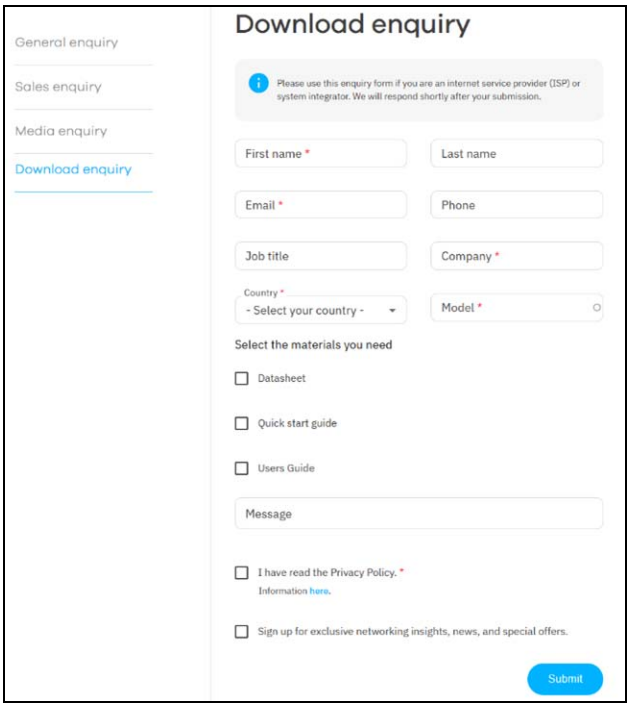
Note

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

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

Enquiries

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



Open Source Licenses

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

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

Index

Numbers

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z