ZYXEL

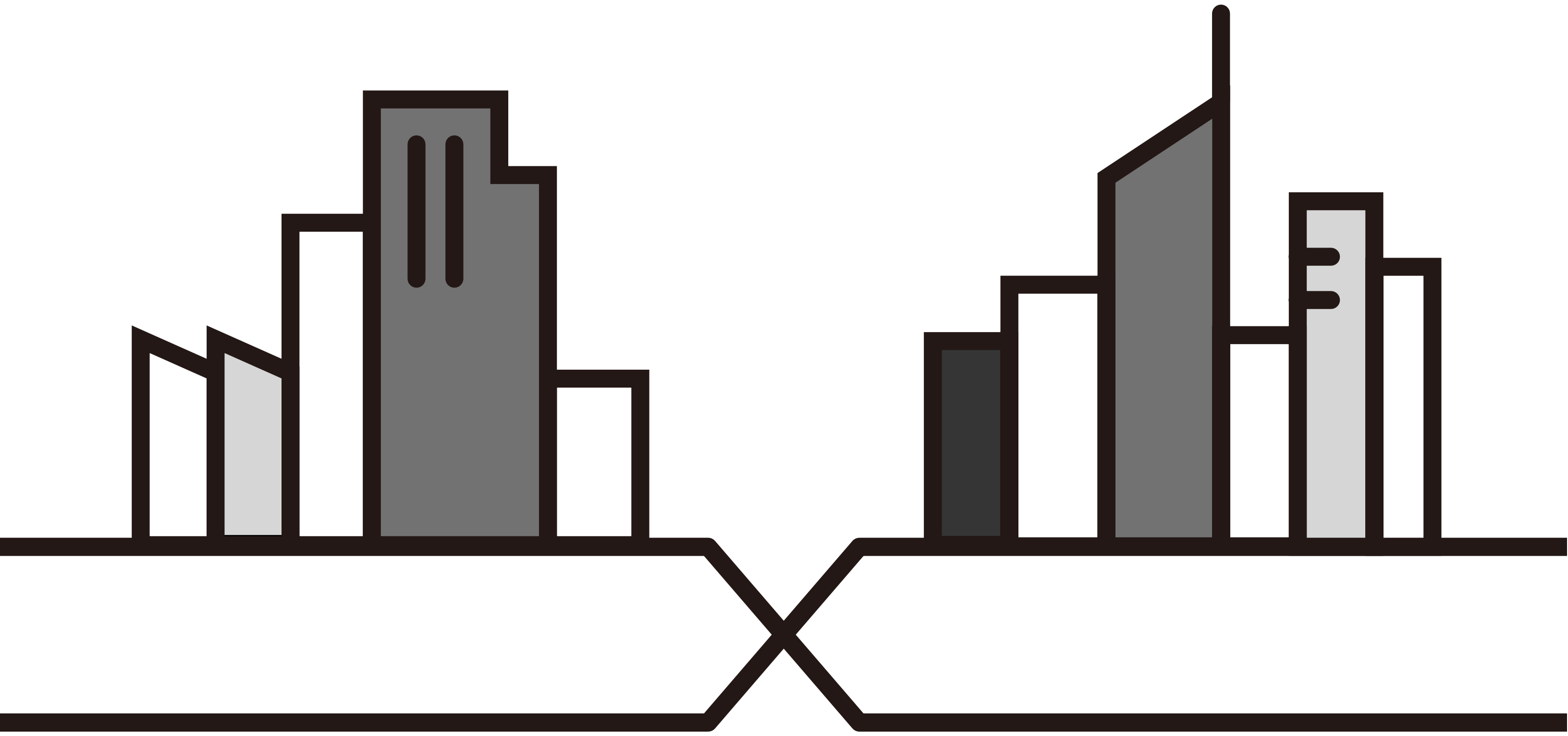
User's Guide

NR Outdoor Series

5G NR Outdoor Router

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

Version 1.00 Ed 1, 12/2021



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Zyxel Device.

- Zyxel Air App HTML Help

  Go to **https://service-provider.zyxel.com/app-help/ZyxelAir/index.html** to find the Zyxel Air App HTML Guide online.

- More Information

  Go to **http://support.zyxel.com** to find other information on the 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

- The NR7101 / NR7102 / NR7103 / NR7123 may be referred to as the “Zyxel Device” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting > Routing > DNS Route** means you first click **Network Setting** in the navigation panel, then the **Routing** submenu and 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 	LTE/5G Base Station 	

Contents Overview

Table of Contents

Chapter 25

Chapter 26

Chapter 27

Chapter 28

Chapter 29

Chapter 30

Chapter 31

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

The Zyxel Device consists of the following models:

- NR7101
- NR7102
- NR7103
- NR7123

1.1.1 Model Feature Differences

The Zyxel Device is a router that supports (but not limited to) the following features.

Note: The rates shown in the **Data Rate** field (in the below table) are the theoretical maximum downlink/uplink rates. The actual speed is affected by network congestion, bandwidth availability, and other factors.

The following table describes the feature differences of the Zyxel Device by model.

Table 1   Model Feature Comparison

FEATURE/MODEL		NR7101	NR7102	NR7103	NR7123
2.4G WiFi		YES	YES	YES	YES
Access Technology (ACT)	5G	YES	YES	YES	YES
	4G	YES	YES	YES	YES
Data Rate (Up to Downlink/Uplink)	5G	5.0 Gbps/900 Mbps	5.0 Gbps/900 Mbps	4.67 Gbps/2.5 Gbps	4.67 Gbps/2.5 Gbps
	4G	2.0 Gbps/200 Mbps	2.0 Gbps/200 Mbps	1.4 Gbps/200 Mbps	1.4 Gbps/200 Mbps
Gigabit Ethernet Port		1G	2.5G	2.5G	2.5 G
USB port		NO	NO	YES	YES
WiFi/WPS Button		YES	NO	NO	NO
WPS Button (on Web Configurator)		YES	YES	YES	YES
LED Indicator		1	2	2	2
PoE Injector		YES	YES	YES	YES
Wall Mounting		YES	YES	YES	YES
Pole Mounting		YES	YES	YES	YES
Sill Mounting		NO	NO	NO	YES
Firmware Version		1.0	1.0	1.0	1.0
Cellular PLMN (Public Land Mobile Network)		YES	YES	YES	YES

Table 1   Model Feature Comparison (continued)

FEATURE/MODEL	NR7101	NR7102	NR7103	NR7123
Cellular Lock	YES	YES	NO	NO
MLD (Multicast Listener Discovery) Proxy	NO	NO	YES	YES
Proxy ARP (Address Resolution Protocol)	YES	YES	NO	NO
FQ_Codel (Fair Queuing with Controlled Delay)	YES	YES	NO	NO
Network Monitoring	YES	YES	NO	NO
DHCP (Dynamic Host Configuration Protocol) server	YES	YES	YES	YES
NAT (Network Address Translation)	YES	YES	YES	YES
DMZ (DeMilitarized Zone)	YES	YES	YES	YES
ALG (Application Layer Gateway)	YES	YES	NO	NO
Port Forwarding	YES	YES	YES	YES
Port Triggering	YES	YES	NO	NO
Embedded Router (default)/IP Passthrough mode	YES	YES	YES	YES
Dynamic DNS (Domain Name System) for the first APN (Access Point Name)	YES	YES	YES	YES
Static Route setting	YES	YES	YES	YES
Dynamic Route setting for RIP (Routing Information Protocol)	YES	YES	NO	NO
VLAN Group	YES	YES	NO	NO
Interface Grouping	YES	YES	NO	NO
Remote Management under Router/IP Passthrough mode	YES	YES	YES	YES
Local and remote device management	YES	YES	YES	YES
ARP (Address Resolution Protocol)	YES	YES	YES	YES
Stateful Packet Inspection (SPI) Firewall	YES	YES	YES	YES
Denial of Service (DoS) Protection	YES	YES	YES	YES
Filter of LAN MAC address, LAN IP address and URLs	YES	YES	YES	YES
Parental Control	NO	NO	YES	YES
Email Notification	YES	YES	NO	NO
Firmware upgrade through TR-069 and Web Configurator	YES	YES	YES	YES
Module upgrade through TR-069 and Web Configurator	YES	YES	NO	NO
XMPP (eXtensible Messaging and Presence Protocol) connection (TR-069)	YES	YES	NO	NO

At the time of writing, the USB port is not available and is for troubleshooting purposes only.

The embedded Web-based Configurator enables straightforward management and maintenance. Just insert the SIM card (with an active data plan) and make the hardware connections. See the Quick Start Guide for how to do the hardware installation, wall, pole or sill mounting, and Internet setup.

1.2 Applications for the Zyxel Device

Wireless WAN

The Zyxel Device can connect to the Internet through a SIM card to access a wireless WAN connection. Just insert a SIM card into the SIM card slot on the Zyxel Device.

Note: You must insert the SIM card into the card slot before turning on the Zyxel Device.

Internet Access

Your Zyxel Device provides shared Internet access by connecting to a cellular network. Connect the **LAN** port of the Zyxel Device to an indoor gateway/router through an RJ45 cable to allow multiple WiFi clients to access the Internet.

A computer can connect (with Ethernet cables and a PoE injector) to the Zyxel Device's **LAN** port for configuration via the Web Configurator.

Wireless LAN (WiFi)

WiFi for an outdoor NR device is mainly for local management. Connect a computer/smartphone to the Zyxel Device's WiFi and use the Web Configurator to configure your Zyxel Device.

Figure 1 Zyxel Device's Internet Access Application

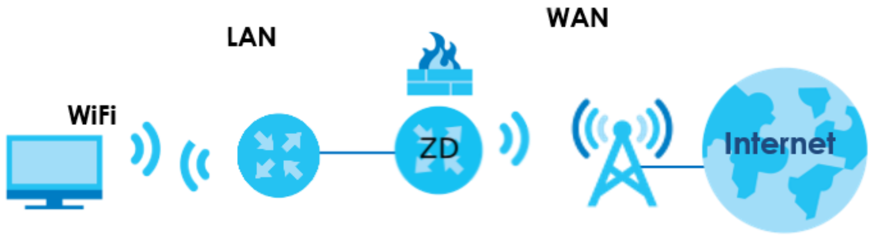


Figure 2 Zyxel Device's Configuration Through WiFi Connection

Carrier Aggregation

Carrier Aggregation (CA) is a technology to deliver high downlink data rates by combining more than one carrier in the same or different bands together.

Figure 3 Zyxel Device's CA Application

1.3 How to Manage your Zyxel Device

You can use the following way to manage your Zyxel Device.

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

• Use the Zyxel Air app (available on the App Store for Apple devices and Google Play for Android devices) for setup and management of the Zyxel Device on your smartphone. You can also use the app for finding the optimal 5G NR signal strength. See the Zyxel Air app QSG for more information. To install the app, scan the QR code on the QSG.

If you are using a computer for web configuration, there are two ways to connect to the Zyxel Device:

- Use the WiFi connection provided by the Zyxel Device.
- Connect the computer's LAN port to the LAN (PoE) on the Zyxel Device. See the QSG for more information.

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 password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

- Back up the configuration (and make sure you know how to restore it). Refer to Section 33.2 on page 233. Restoring an earlier working configuration may be useful if the Zyxel Device becomes unstable or even crashes. If you forget your password to access the Web Configurator, 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. Write down any information your ISP provides you.

CHAPTER 2
Hardware

2.1 Overview

This chapter describes the physical features and their usages of the Zyxel Device.

2.2 Front Panel

The following image shows the front panel of the Zyxel Device.

Figure 4 NR7101/NR7102/NR7103 Front Panel

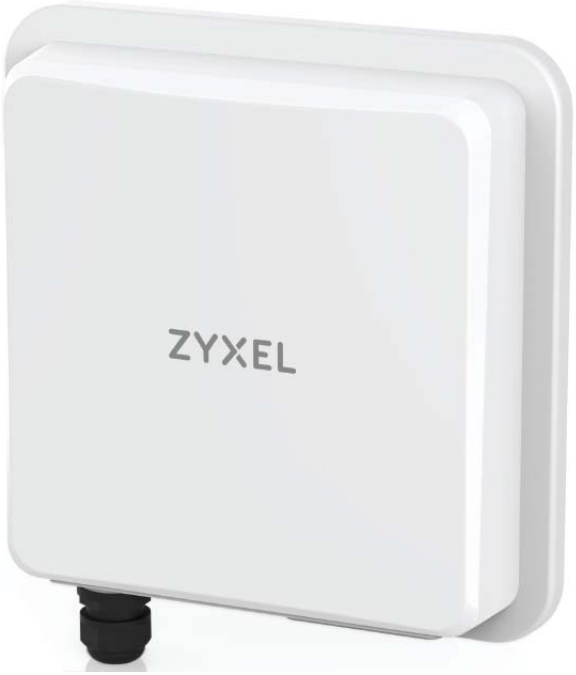
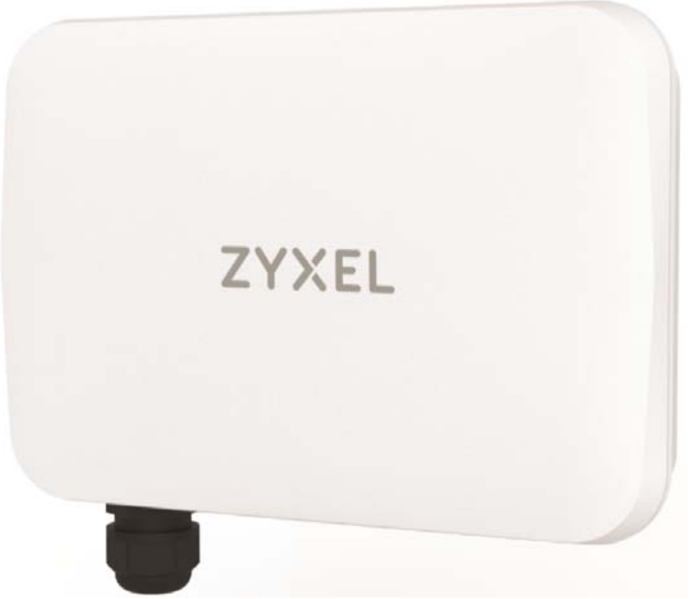


Figure 5 NR7123 Front Panel



2.3 LEDs (Lights)

The LED indicators on your Zyxel Device show current status and/or signal strength of the Zyxel Device.

2.3.1 Zyxel Device Model with Single LED

The following are the Zyxel Device's LED descriptions.

Table 2 NR7101 LED Behavior

COLOR	STATUS	DESCRIPTION
Green	On	The Zyxel Device is connected to the Internet.
	Blinking	The Zyxel Device is trying to connect to the Internet.
Amber	On	The WiFi is activated. The Zyxel Device is connected to the Internet.
	Blinking	The WiFi is activated. The Zyxel Device is not connected to the Internet.
Red	On	The Zyxel Device is not connected to the Internet.
	Blinking	The Zyxel Device is booting or self-testing.
	Off	There is a system failure.
Green/Amber/Red	Looping	Firmware upgrade is in progress.

Note: The LED is off if the Zyxel Device is not receiving power.

2.3.2 Zyxel Device Models With Multiple LEDs

The following are the Zyxel Device's LED descriptions.

Table 3 NR7102/NR7103/NR7123 LED Behavior

LED	COLOR	STATUS	DESCRIPTION
Cellular Signal Strength	Green	On	The signal strength is excellent.
	Amber	On	The signal strength is fair.
	Red	On	The signal strength is weak.
		Blinking	There is no cellular signal, or signal strength is below the weak level.
Status	Green	On	The Zyxel Device is connected to the Internet.
		Blinking	The Zyxel Device is trying to connect to the Internet.
		Off	The Zyxel Device is not receiving power.
	Amber	On	The WiFi is on.
	Red	On	There is a system failure.
		Blinking	The Zyxel Device is booting.
	Green/ Amber/ Red	Looping	Firmware upgrade is in progress.

Note: The LED is off if the Zyxel Device is not receiving power.

2.4 Panel Ports

The connection ports are located on the bottom panel.

Figure 6 NR7101 Panel Port

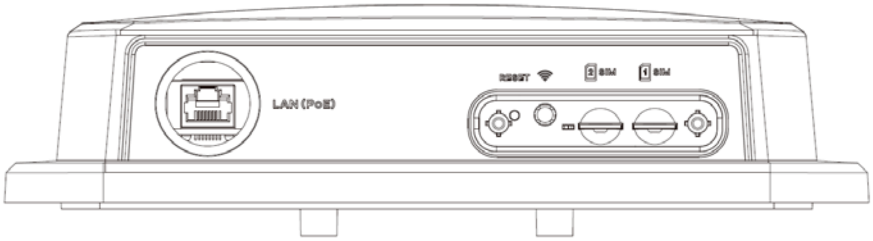


Figure 7 NR7102 Panel Port

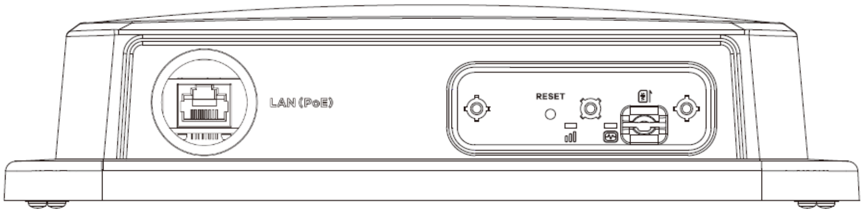


Figure 8 NR7103 Panel Port

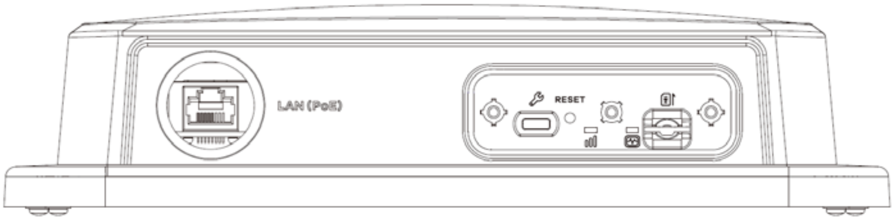
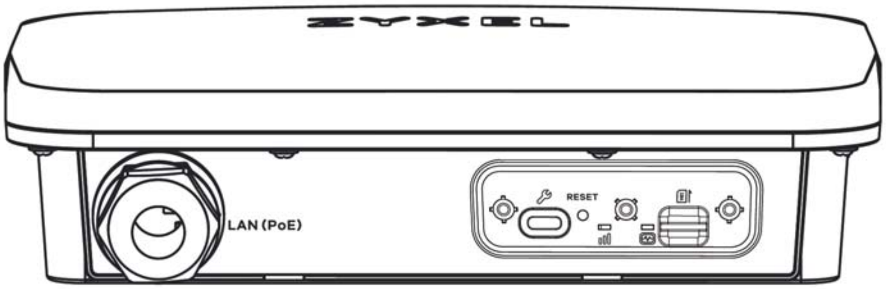


Figure 9 NR7123 Panel Port



The following table describes the items on the bottom panel.

Table 4 Panel Ports

LABELS	DESCRIPTION
USB (Type-C)	The USB port of the Zyxel Device is used for maintenance only. Note: The USB port can only be used by qualified technicians.
LAN (PoE)	Connect the PoE port on the PoE injector to the Zyxel Device's LAN port through an Ethernet cable. Connect the LAN port on the PoE injector to your computer's RJ45 port through another Ethernet cable.
SIM card	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.

2.5 WiFi/WPS Button

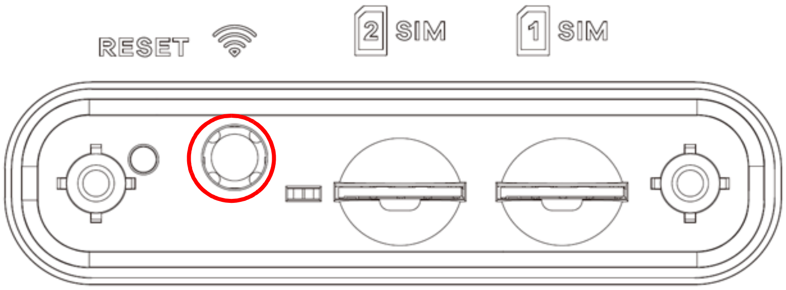
Use the **WiFi/WPS** button on the Zyxel Device to turn on/off the WiFi network or quickly build a WiFi connection with a WiFi client.

Use the WiFi function of the Zyxel Device for configuration (for example, connect to the Zyxel Air app on your mobile device to find the optimal NR/LTE signal strength and manage your Zyxel Device).

See Section 1.1.1 on page 15 to check if your Zyxel Device has a **WiFi/WPS** button.

Note: You can also find a **WPS** button on the Web Configurator. See Section 8.4 on page 90 for more information.

Figure 10 NR7101 WiFi/WPS Button



To turn on WiFi:

1 Make sure the LED is on and not blinking.

2 Press the **WiFi/WPS** button for more than 5 seconds and release it.

Once WiFi is turned on, the LED blinks amber.

To activate WPS (WiFi must be already on):

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

1 Press the **WiFi/WPS** button for more than 1 second but less than 5 seconds and release it (pressing more than 5 seconds will turn off WiFi).

2 Press the WPS button on another WPS-enabled device within range of the Zyxel Device.

Note: If the WPS-enabled device is placed too far, it will not be able to connect to the Zyxel Device.

Once a WiFi connection is ready, the LED blinks amber.

To turn off the WiFi network:

Press the **WiFi/WPS** button for more than 5 seconds.

The amber LED turns off.

2.6 RESET Button

Insert a thin object into the **RESET** hole of the Zyxel Device to restore the factory-default configuration file if you forget your password or IP address, or you cannot access the Web Configurator. This means that you will lose all configurations that you had previously saved. The password will be reset to the default (see the Zyxel Device label) and the IP address will be reset to **192.168.1.1**.

The following table describes the **RESET** button on the bottom panel.

Table 5 Reset/Reboot Button

LABELS	DESCRIPTION
RESET	Press the **RESET** button for more than five seconds to set the Zyxel Device back to the factory defaults.
	Press the **RESET** button for more than two but less than five seconds to restart/reboot the Zyxel Device.

Figure 11 NR7101 Reset Button

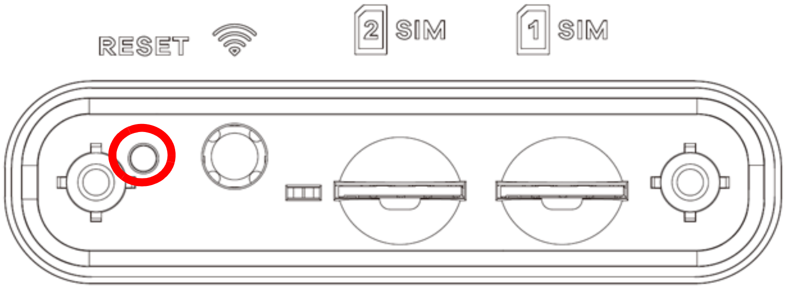


Figure 12 NR7102 Reset Button

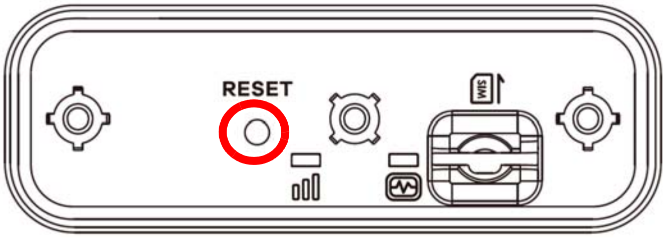
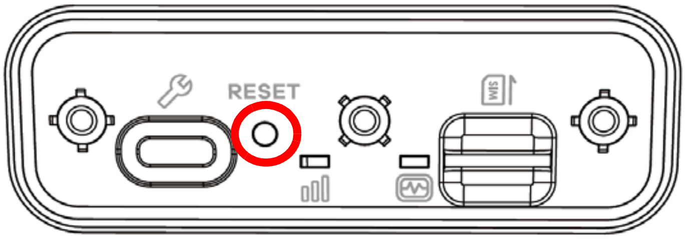


Figure 13 NR7103/NR7123 Reset Button



Note: Make sure the Zyxel Device is connected to power and the Status LED is on.

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, Internet Explorer 11, 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 device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

3.1.1 Access the Web Configurator

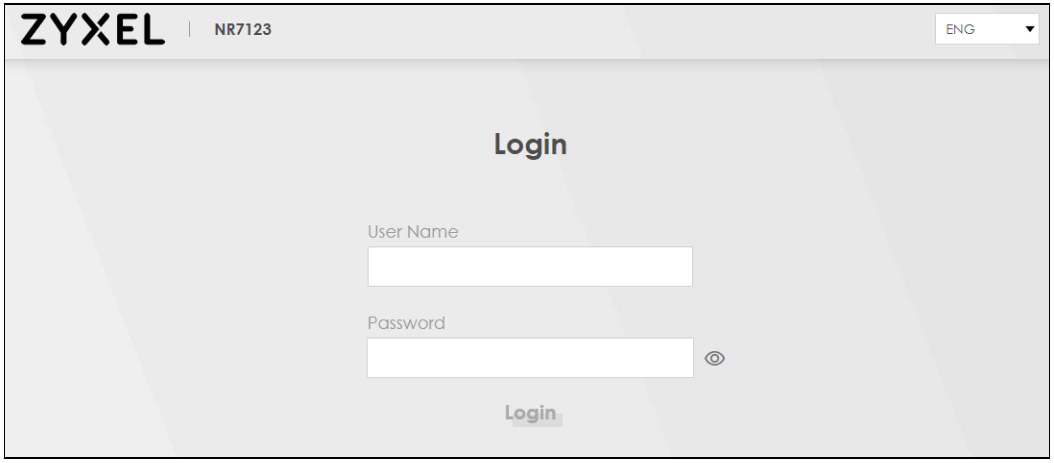
1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to http://192.168.1.1.

3 A password screen displays. Select the language you prefer (upper right).

4 To access the Web Configurator and manage the Zyxel Device, enter the default username **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**.

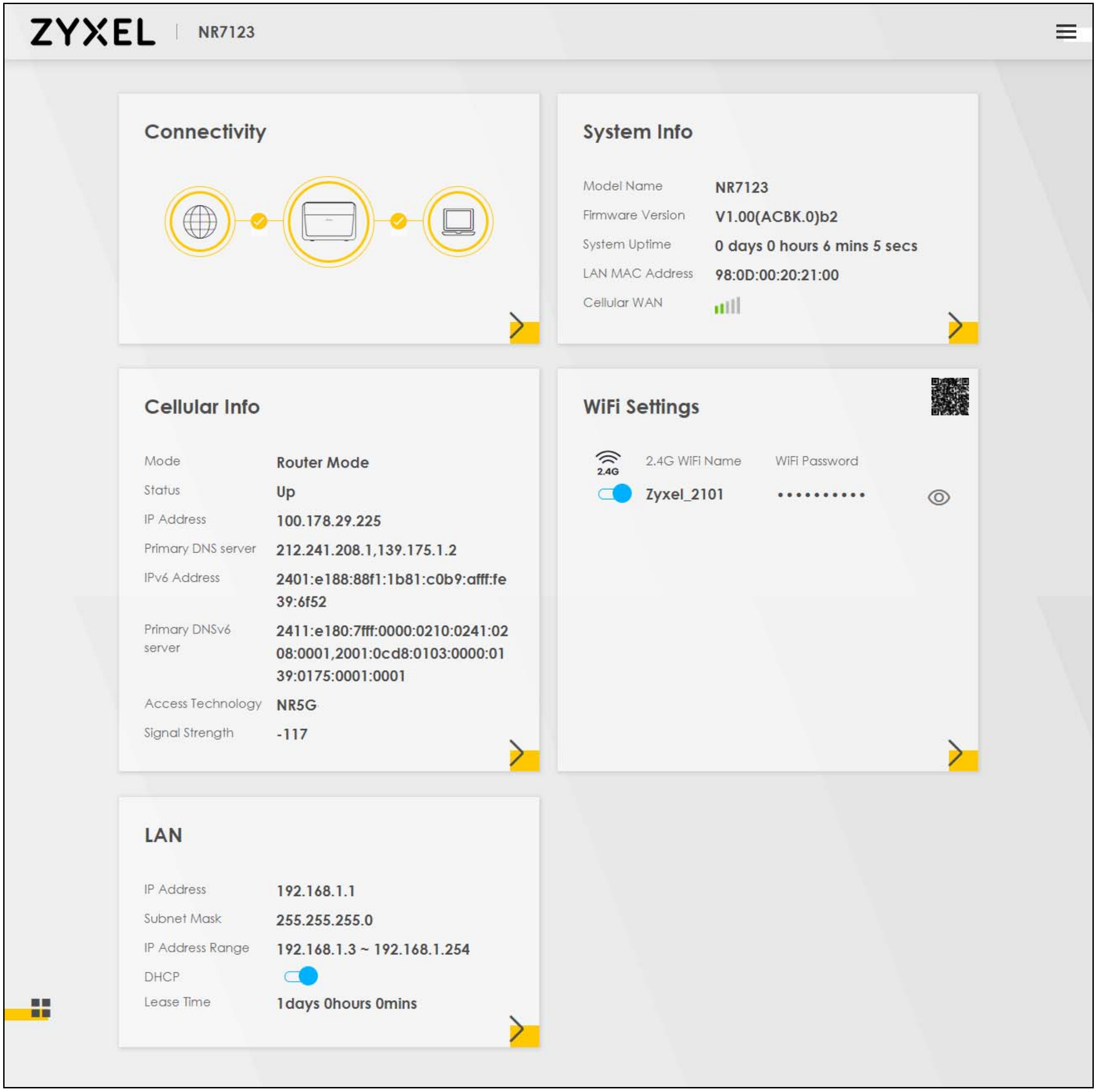
Figure 14 Login Screen



Note: The first time you enter the password, you will be asked to change it. Make sure the new password contains at least one uppercase letter, one lowercase letter and one number. Note that the length of the new password has to be 8-24 characters long, and contain at least one upper case and lower case letter each.

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

Figure 15 Connection Status



Connectivity

System Info

Model Name	NR7123
Firmware Version	V1.00(ACBK.0)b2
System Uptime	0 days 0 hours 6 mins 5 secs
LAN MAC Address	98:0D:00:20:21:00
Cellular WAN	

Cellular Info

Mode	Router Mode
Status	Up
IP Address	100.178.29.225
Primary DNS server	212.241.208.1,139.175.1.2
IPv6 Address	2401:e188:88f1:1b81:c0b9:afff:fe39:6f52
Primary DNSv6 server	2411:e180:7fff:0000:0210:0241:0208:0001,2001:0cd8:0103:0000:0139:0175:0001:0001
Access Technology	NR5G
Signal Strength	-117

WiFi Settings

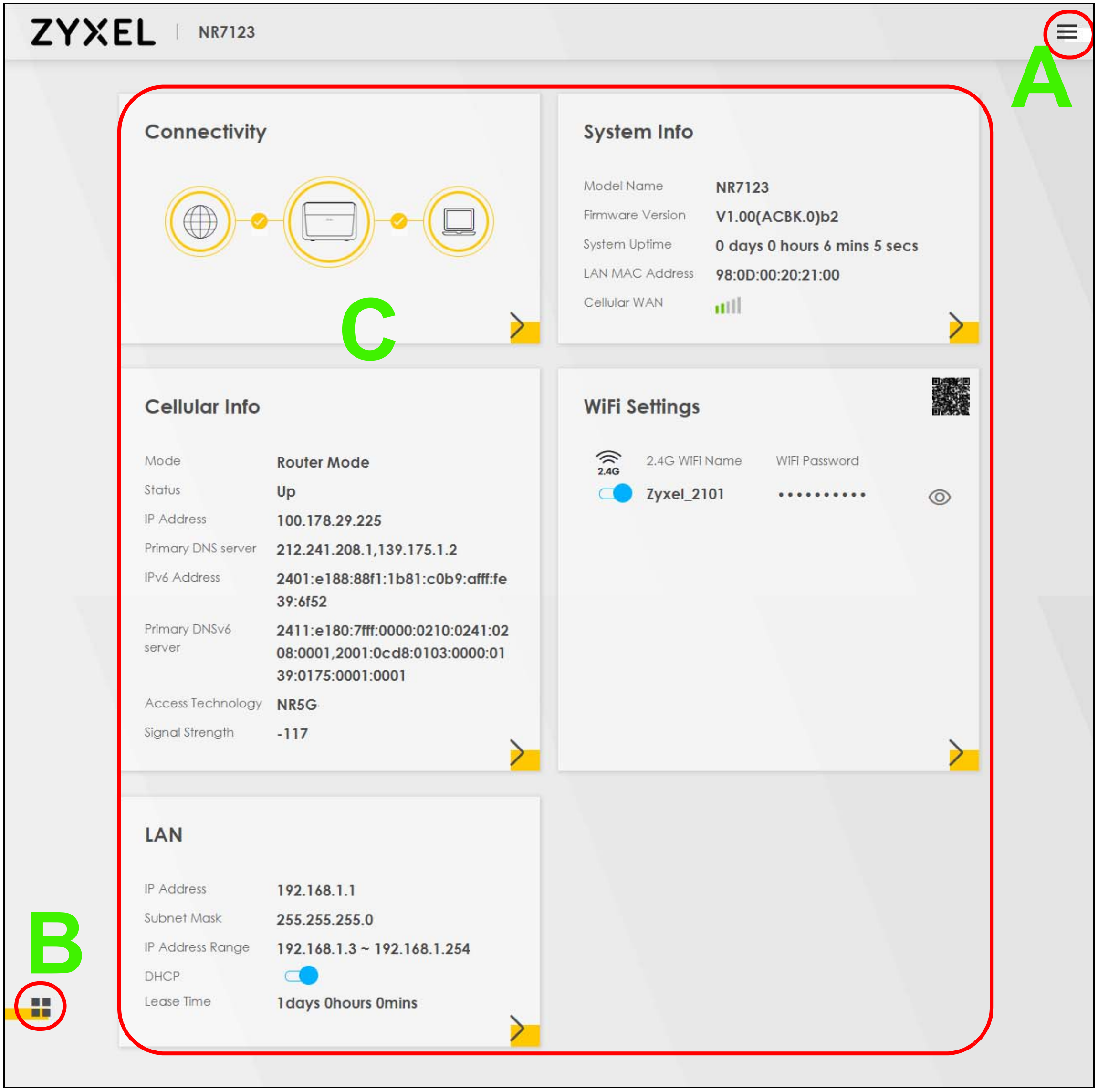
2.4G	2.4G WiFi Name	WiFi Password
	Zyxel_2101	••••••••••

LAN

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IP Address Range	192.168.1.3 ~ 192.168.1.254
DHCP	
Lease Time	1days 0hours 0mins

3.2 Web Configurator Layout

Figure 16 Screen Layout



Connectivity

System Info

Model Name NR7123
Firmware Version V1.00(ACBK.0)b2
System Uptime 0 days 0 hours 6 mins 5 secs
LAN MAC Address 98:0D:00:20:21:00
Cellular WAN

Cellular Info

Mode Router Mode
Status Up
IP Address 100.178.29.225
Primary DNS server 212.241.208.1,139.175.1.2
IPv6 Address 2401:e188:88f1:1b81:c0b9:afff:fe39:6f52
Primary DNSv6 server 2411:e180:7fff:0000:0210:0241:0208:0001,2001:0cd8:0103:0000:0139:0175:0001:0001
Access Technology NR5G
Signal Strength -117

WiFi Settings

2.4G WiFi Name Zyxel_2101
WiFi Password ••••••••••

LAN

IP Address 192.168.1.1
Subnet Mask 255.255.255.0
IP Address Range 192.168.1.3 ~ 192.168.1.254
DHCP
Lease Time 1days 0hours 0mins

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

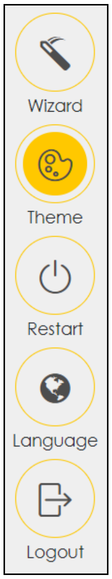
- **A** - Settings Icon (Navigation Panel and Side Bar)
- **B** - Widget Icon
- **C** - Main Window

3.2.1 Settings Icon

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

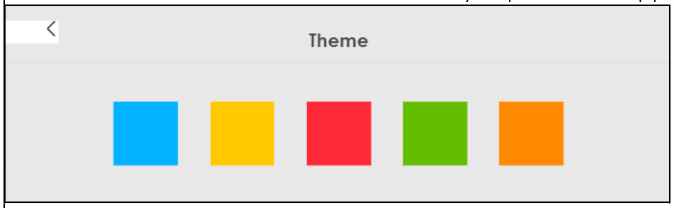
3.2.1.1 Side Bar

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



The icons provide the following functions.

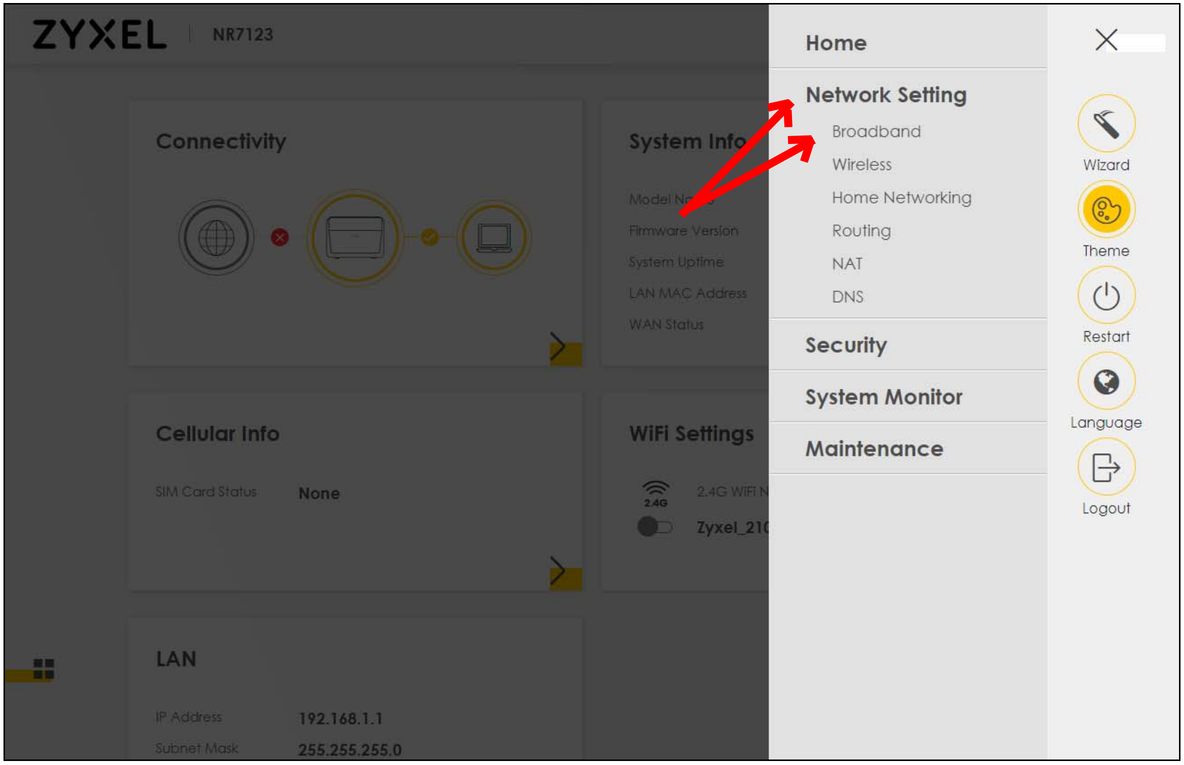
Table 6 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
Wizard	**Wizard**: Click this icon to open scree information about the **Wizard** screens.
Theme	**Theme**: Click this icon to select a color that you prefer and apply it to the Web Configurator.  🟦 🟨 🟥 🟩 🟧
Restart	**Restart**: Click this icon to reboot the Zyxel Device without turning the power off.
Language	**Language**: Select the language you prefer.
Logout	**Logout**: Click this icon to log out of the Web Configurator.

3.2.1.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure Zyxel Device features.

Figure 17 Navigation Panel



The following tables describe each menu item.

Table 7 Navigation Panel Summary

LINK	TAB	FUNCTION
Home		Use this screen to configure basic Internet access and wireless 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.
	Cellular WAN	Use this screen to enable data roaming and network monitoring.
	Cellular APN	Use this screen to configure a cellular WAN connection that includes the Access Point Name (APN) provided by your service provider.
	Cellular SIM	Use this screen to enter a PIN for your SIM card to prevent others from using it.
	Cellular Band	Use this screen to configure the cellular frequency bands that can be used for Internet access as provided by your service provider.
	Cellular PLMN	Use this screen to view available s (PLMNs) and select your preferred network.
	Cellular IP Passthrough (NR7103 / NR7123 Only)	Use this screen to enable IP Passthrough mode (bridge mode).
	Cellular Lock (NR7101 / NR7102 ONLY)	Use this screen to enable or disable Physical Cell Identity (PCI) Lock.

Table 7 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	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.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
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.
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 server(s).
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP (NR7101 / NR7102 ONLY)	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering (NR7101 / NR7102 ONLY)	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 (NR7101 / NR7102 ONLY)	Use this screen to enable or disable ALG.
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.
VLAN Group	VLAN Group (NR7101 / NR7102 ONLY)	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping (NR7101 / NR7102 ONLY)	Use this screen to map a port to create multiple networks on the Zyxel Device.
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.

Table 7 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Parental Control	Parental Control (NR7103 / NR7123 Only)	Use this screen to define time periods and days during which the Zyxel Device performs parental control and/or block web sites with specific URLs.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.
	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.
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.
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.
WLAN Station Status	WLAN Station Status	Use this screen to view the wireless stations that are currently associated with the Zyxel Device.
Cellular WAN Status	Cellular WAN Status	Use this screen to look at the cellular Internet connection status.
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.
	MGMT Services for IP Passthrough	Use this screen to enable various approaches to access this Zyxel Device remotely from a WAN connection.
	Trust Domain for IP Passthrough	Use this screen to enable public IP addresses to access this Zyxel Device remotely from a WAN connection.
TR-069 Client	TR-069 Client	Use this screen to configure your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.
Time	Time	Use this screen to change your Zyxel Device's time and date.
E-mail Notification	E-mail Notification (NR7101 / NR7102 ONLY)	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Settings	Log Setting	Use this screen to change your Zyxel Device's log settings.

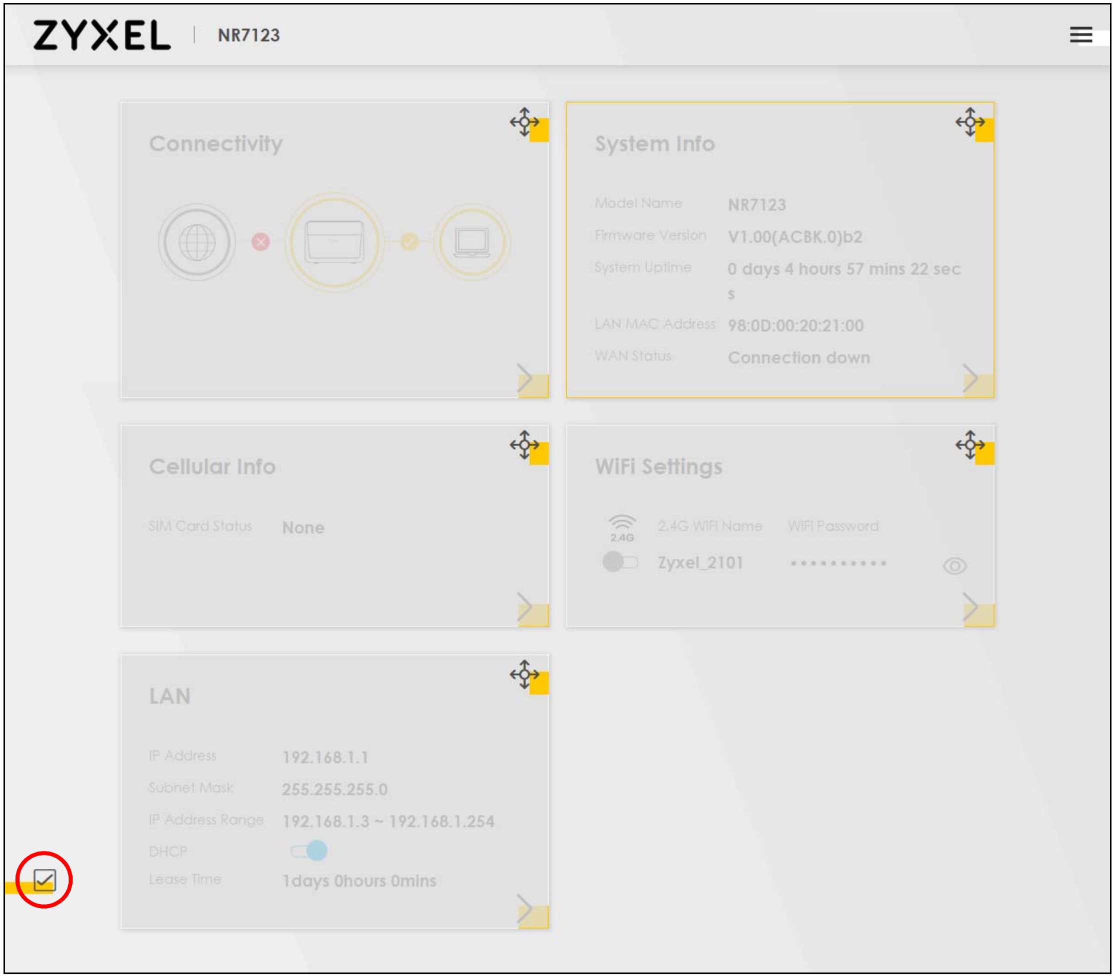
Table 7 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
	Module Upgrade (NR7101 / NR7102 ONLY)	Use this screen to upload new module 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 without turning the power off.
	Schedule Reboot (NR7101 / NR7102 ONLY)	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, TraceRoute, Nslookup, or Speed Test to help you identify problems.

3.2.2 Widget Icon

Click this icon (⊞) in the lower left corner to rearrange the layout.

Figure 18 Widget Icon



System Info

Model Name	NR7123
Firmware Version	V1.00(ACBK.0)b2
System Uptime	0 days 4 hours 57 mins 22 sec s
LAN MAC Address	98:0D:00:20:21:00
WAN Status	Connection down

Cellular Info

SIM Card Status	None

WiFi Settings

2.4G WiFi Name	WiFi Password
Zyxel_2101	••••••••••

LAN

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IP Address Range	192.168.1.3 ~ 192.168.1.254
DHCP	
Lease Time	1days 0hours 0mins

Select a widget and hold it to move around. Click the Check icon (☑) in the lower left corner to save the changes

CHAPTER 4
Quick Start

4.1 Overview

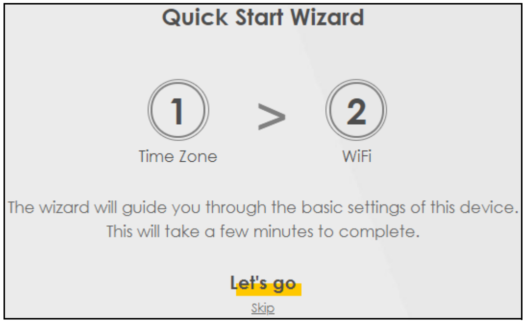
Use the **Wizard** screens to configure the Zyxel Device's time zone and wireless settings.

Note: See the technical reference chapters (starting on Chapter 6 on page 56) 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. See Section 3.2.1.1 on page 29 for more information about the side bar. After you click the **Wizard** icon, the following screen appears. Click **Let's Go** to proceed with settings on time zone and wireless 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 19 Wizard - Home



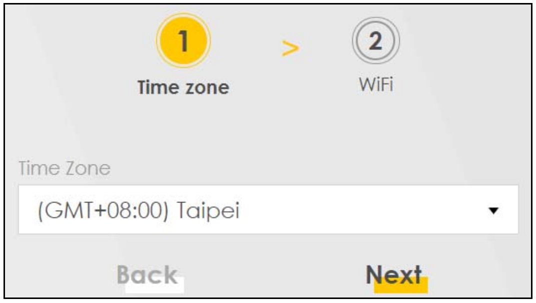
Quick Start Wizard

The wizard will guide you through the basic settings of this device. This will take a few minutes to complete.

4.3 Time Zone

Select the time zone of your location. Click **Next**.

Figure 20 Wizard - Time Zone

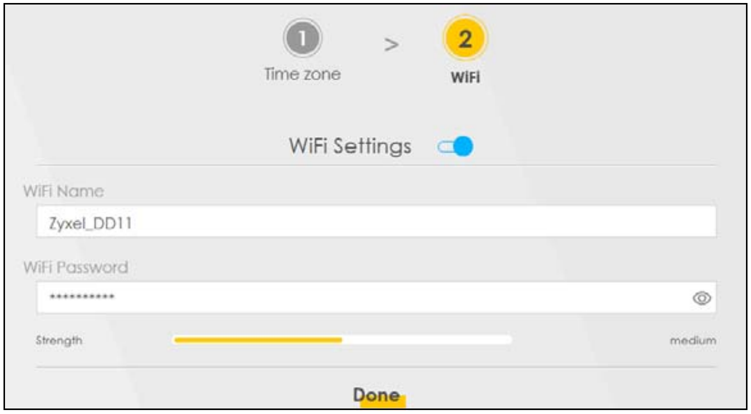


Time Zone: (GMT+08:00) Taipei

4.4 WiFi Setup

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 (👁).
Click **Done**.

Figure 21 Wizard - WiFi



WiFi Settings: ●

WiFi Name: Zyxel_DD11

WiFi Password: ***********

Strength: medium

Note: You can also enable the WiFi using the following methods:

- Click **Network Setting** > **Wireless** to open the **General** screen. Then select **Enable** in the **WiFi** field.
- Under the **Connection Status** screen, select **Enable** in the **WiFi Settings** field.

CHAPTER 5 Tutorials

5.1 Overview

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

- WiFi Network Setup
- Cellular Network Setup
- Network Security
- Device Maintenance

5.2 WiFi Network Setup

In this example, you want to set up a WiFi network so that you can use your notebook or other devices like a smart phone to connect to the Zyxel Device (for configuration). However, the WiFi network is only for configuring the Zyxel Device. Remember to turn it off after all configurations are done.

Figure 22 Zyxel Device's Configuration Through WiFi Connection

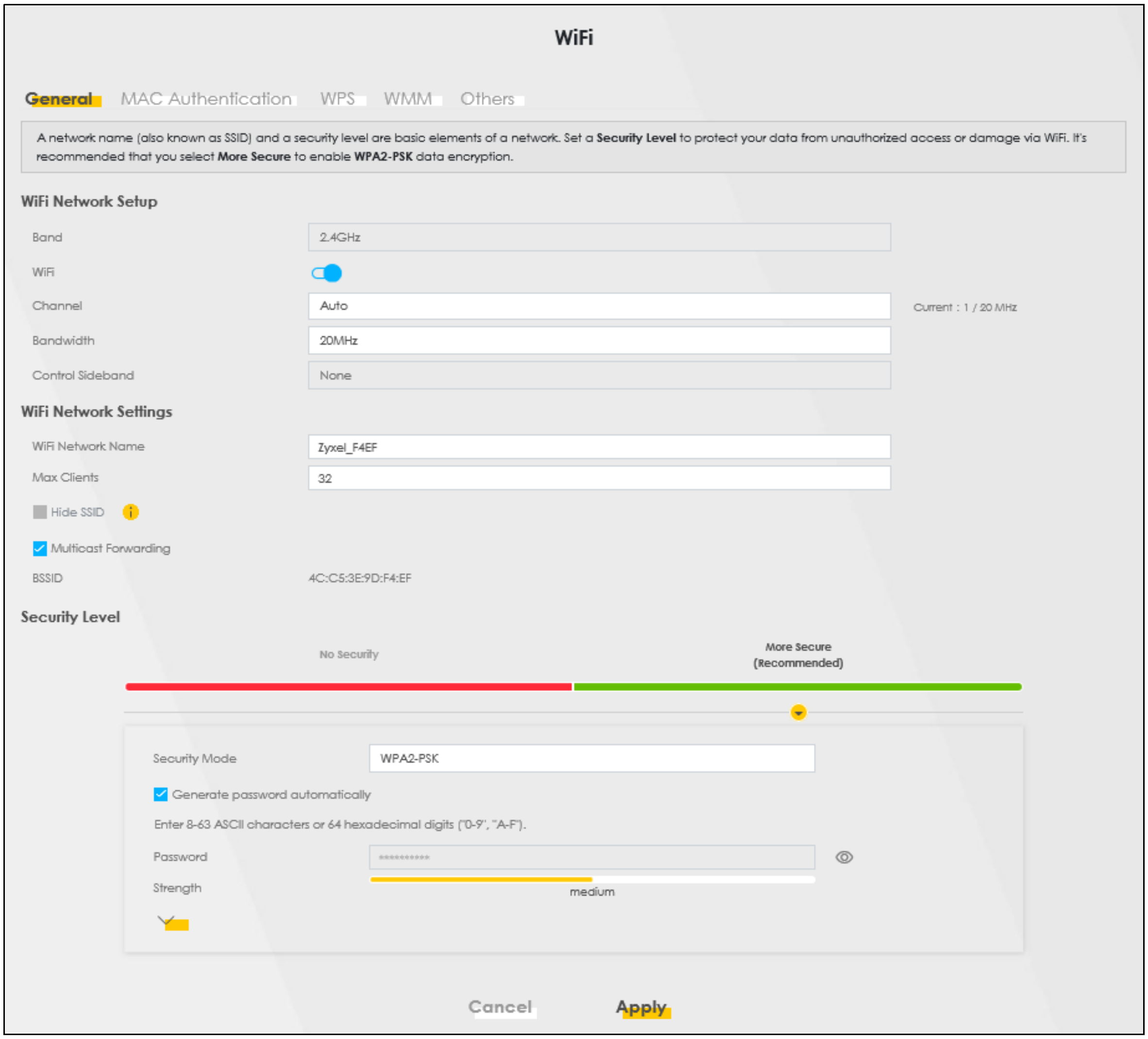
See the label on the Zyxel Device for the WiFi network settings and then connect manually to the Zyxel Device. See Section 5.2.2 on page 39. Alternatively, you can set up a WiFi network using WPS.

5.2.1 Changing Security on a WiFi Network

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

SSID	Example
Security Mode	WPA2-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n Mixed

1 Go to the **Network Setting** > **Wireless** > **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters. Click **Apply**.



WiFi

A network name (also known as SSID) and a security level are basic elements of a network. Set a **Security Level** to protect your data from unauthorized access or damage via WiFi. It's recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

WiFi Network Setup

Band	2.4GHz	
WiFi	●	
Channel	Auto	Current : 1 / 20 MHz
Bandwidth	20MHz	
Control Sideband	None	

WiFi Network Settings

WiFi Network Name	Zyxel_F4EF
Max Clients	32

□ Hide SSID

☑ Multicast Forwarding

BSSID 4C:C5:3E:9D:F4:EF

Security Level

Security Mode WPA2-PSK

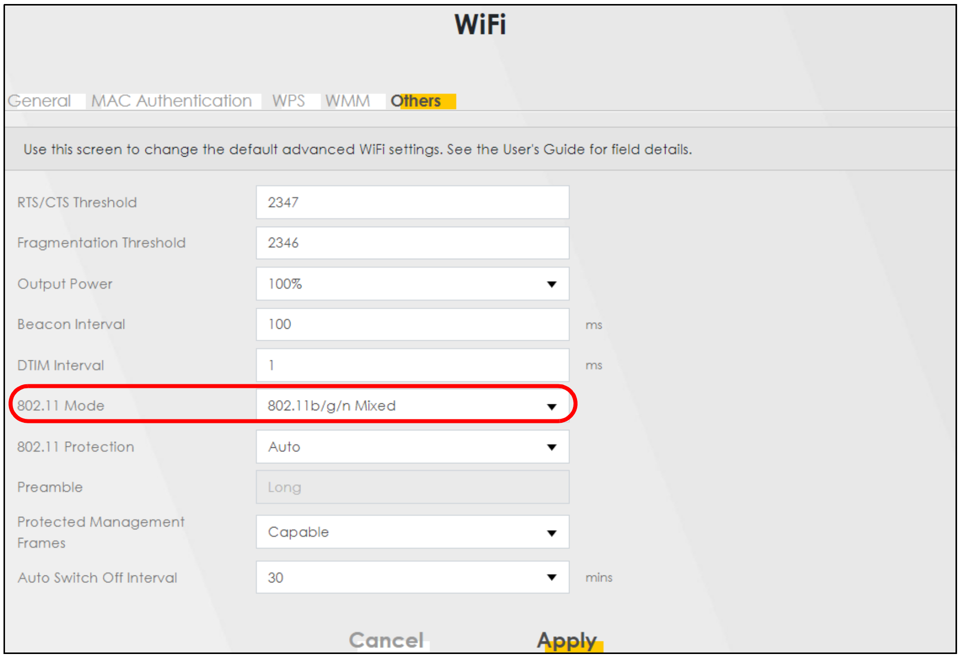
☑ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password ***********

Strength medium

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



Use this screen to change the default advanced WiFi settings. See the User's Guide for field details.

RTS/CTS Threshold	2347	
Fragmentation Threshold	2346	
Output Power	100%	
Beacon Interval	100	ms
DTIM Interval	1	ms
802.11 Mode	802.11b/g/n Mixed	
802.11 Protection	Auto	
Preamble	Long	
Protected Management Frames	Capable	
Auto Switch Off Interval	30	mins

You can now use the WPS feature to establish a WiFi connection between your notebook or other devices and the Zyxel Device (see Section 5.2.2 on page 39).

5.2.2 Connecting 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 are two methods:

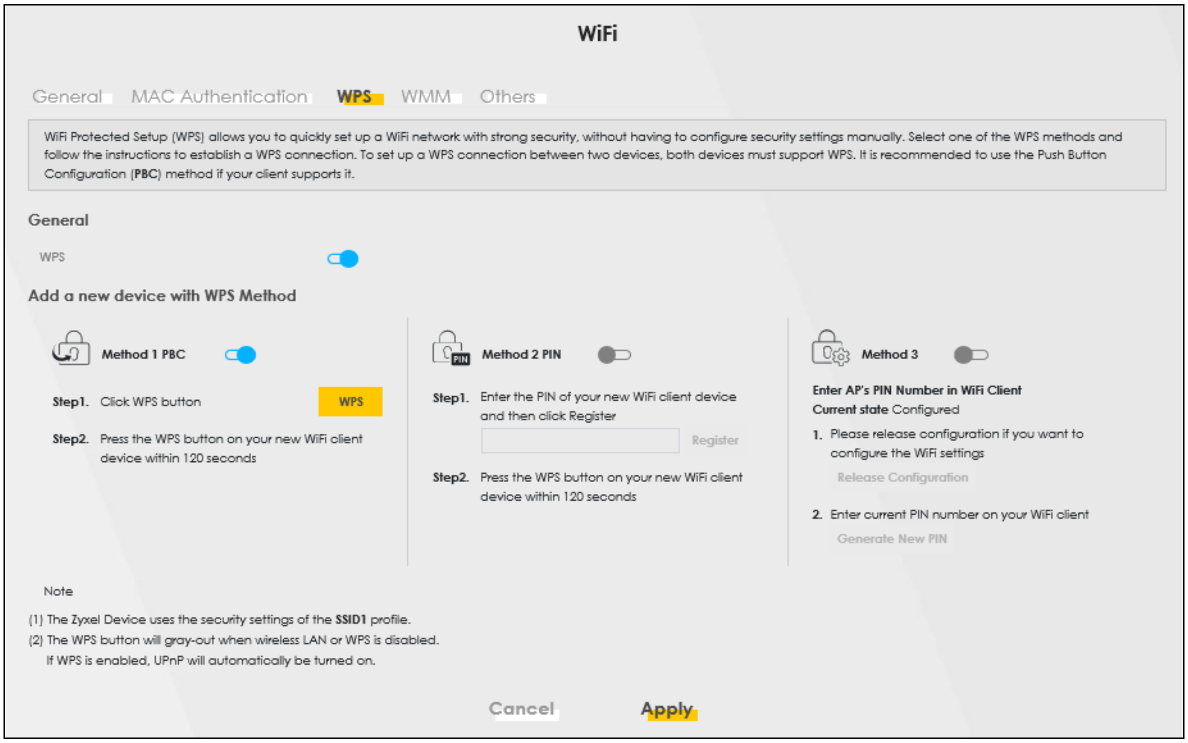
- **Push Button Configuration (PBC)** – Connect to the WiFi network by pressing a button. See Section 5.2.2.1 on page 39. This is the simplest method.
- **PIN Configuration** – Connect to the WiFi network by entering a PIN (Personal Identification Number) from a WiFi-enabled device in the Zyxel Device's Web Configurator. See Section 5.2.2.2 on page 42. This is the more secure method, because one device can authenticate the other.

5.2.2.1 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 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**.



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. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your client supports it.

General

WPS: on

Add a new device with WPS Method

Method 1 PBC: on

Step1. Click WPS button

Step2. Press the WPS button on your new WiFi client device within 120 seconds

Method 2 PIN: off

Step1. Enter the PIN of your new WiFi client device and then click Register

Step2. Press the WPS button on your new WiFi client device within 120 seconds

Method 3: off

Enter AP's PIN Number in WiFi Client

Current state Configured

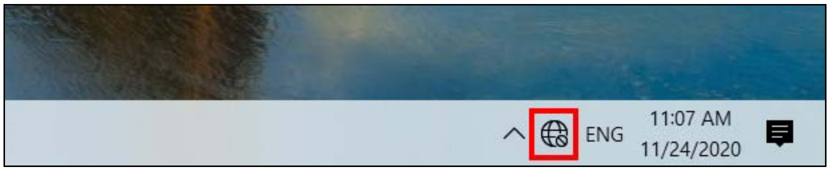
1. Please release configuration if you want to configure the WiFi settings
2. Enter current PIN number on your WiFi client

Note

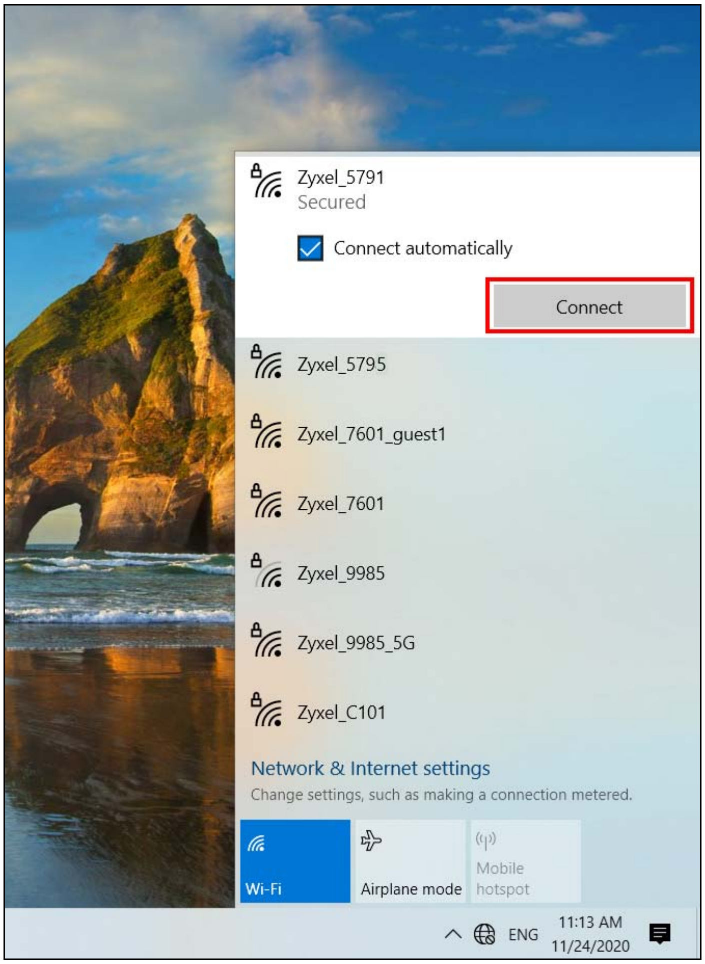
(1) The Zyxel Device uses the security settings of the **SSID1** profile.

(2) The WPS button will gray-out when wireless LAN or WPS is disabled.
If WPS is enabled, UPnP will automatically be turned on.

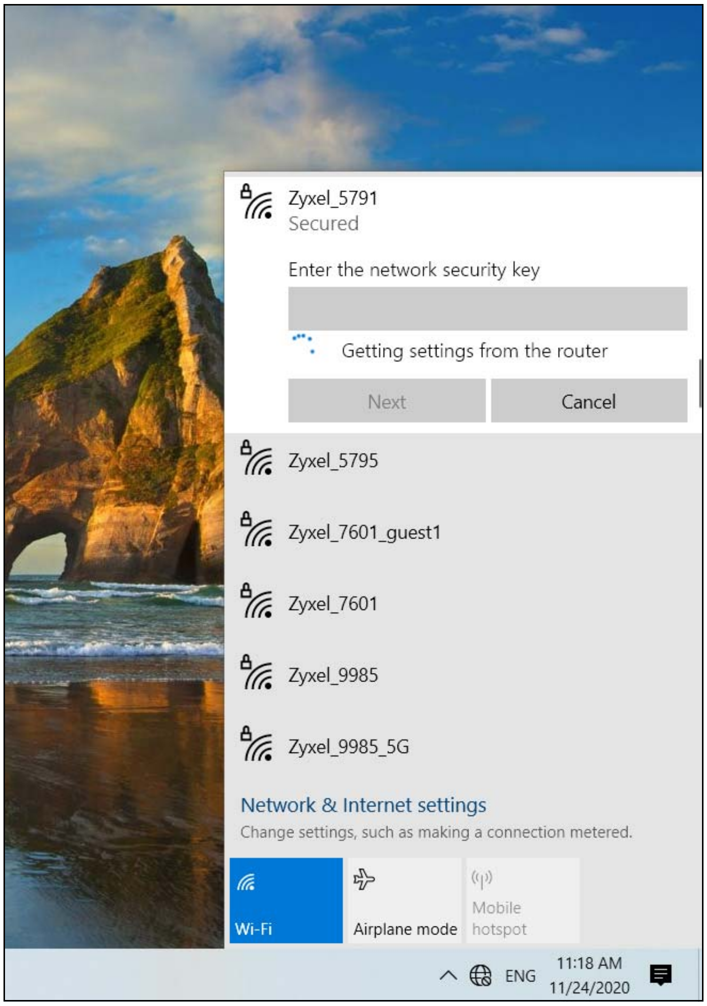
3 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.



4 Locate the WiFi network of the Zyxel Device. The default WiFi network name is “Zyxel_XXXX” (2.4G). Then click **Connect**.



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



Zyxel_5791
Secured

Enter the network security key

Getting settings from the router

Zyxel_5795

Zyxel_7601_guest1

Zyxel_7601

Zyxel_9985

Zyxel_9985_5G

Network & Internet settings
Change settings, such as making a connection metered.

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

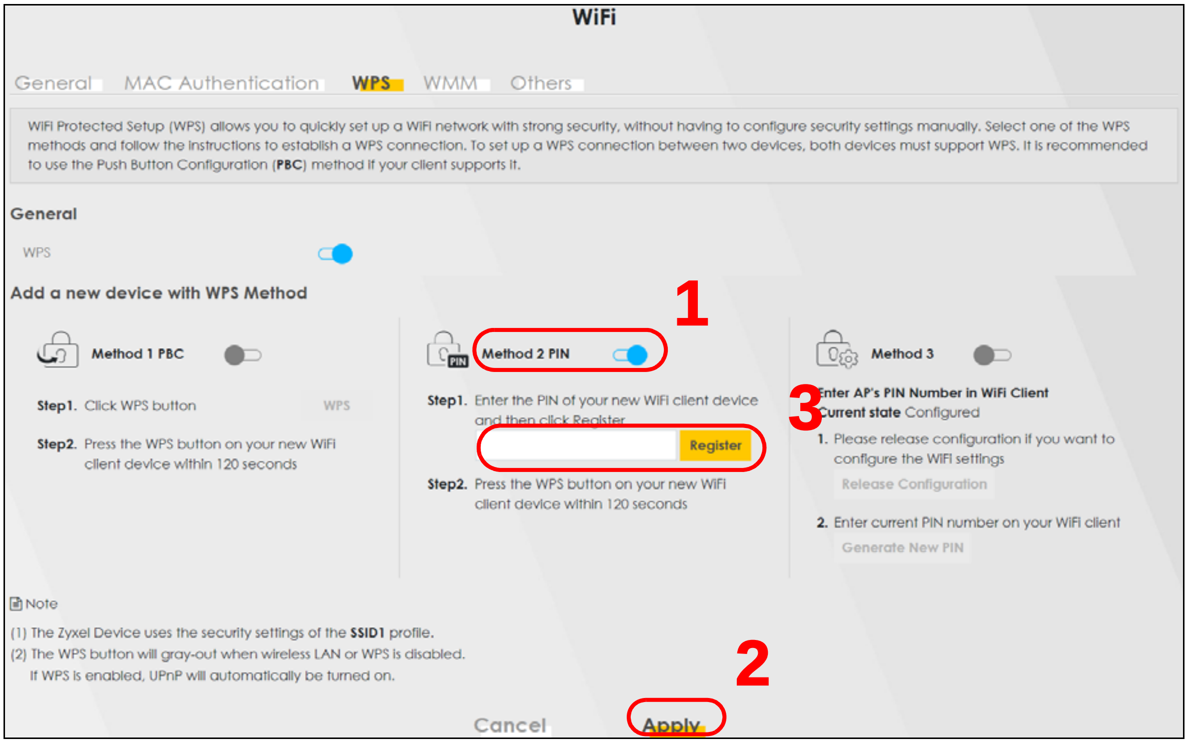
5.2.2.2 WPS PIN Configuration

The WPS PIN (Personal Identification Number) method is a more secure version of WPS, used by WiFi-enabled devices such as printers. To use this connection method, you need to log into the Zyxel Device's Web Configurator.

1 Enable WiFi on the device you want to connect to the WiFi network. Then, note down the WPS PIN in the device's WiFi settings.

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

3 Enable **Method 2 PIN**, and then click **Apply**. Enter the PIN of the WiFi device, and then click **Register**.



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. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your client supports it.

General

WPS

Add a new device with WPS Method

Method 1 PBC

Step1. Click WPS button

Step2. Press the WPS button on your new WiFi client device within 120 seconds

Method 2 PIN

Step1. Enter the PIN of your new WiFi client device and then click Register

Step2. Press the WPS button on your new WiFi client device within 120 seconds

Method 3

Enter AP's PIN Number in WiFi Client

Current state Configured

1. Please release configuration if you want to configure the WiFi settings

2. Enter current PIN number on your WiFi client

Note

(1) The Zyxel Device uses the security settings of the **SSID1** profile.

(2) The WPS button will gray-out when wireless LAN or WPS is disabled. If WPS is enabled, UPnP will automatically be turned on.

4 Within 2 minutes, enable WPS on the WiFi device.

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.

5.3 Cellular Network Setup

This section shows you how to set up a cellular network, from cellular network connection settings to APN settings.

5.3.1 Setting up a Cellular Network Connection

This section gives you an example of how to connect to the Internet using over a cellular connection.

1 Insert a SIM Card into your Zyxel Device SIM slot. Make sure this SIM has an active data plan with your Internet Service Provider (ISP).

2 Connect your Zyxel Device to your computer, and log into the Web Configurator.

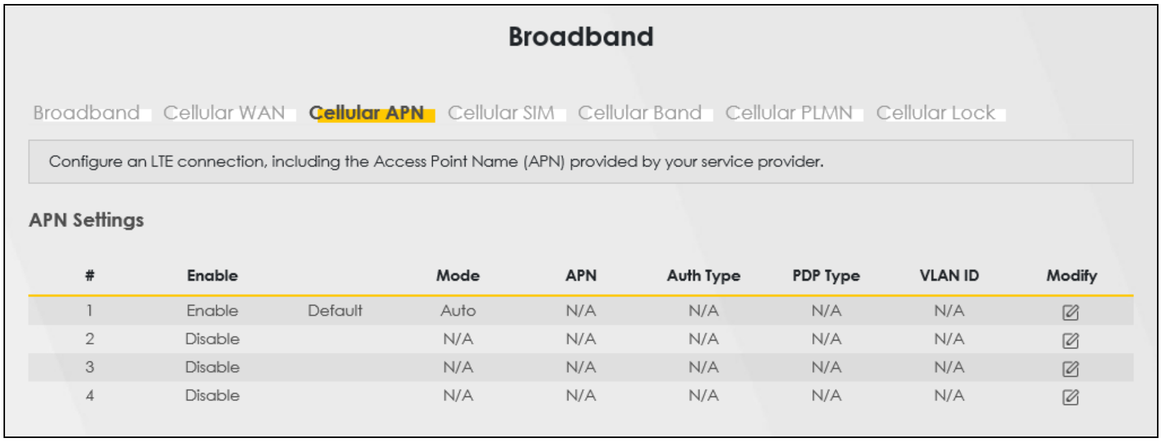
3 If your SIM has a PIN Code, enter this code in the **Broadband** > **Cellular SIM** screen.

Use the Home screen to check the Internet Status (IPv4) or Internet Status (IPv6). If it shows Connected this means your Internet connection is up.

5.3.2 Setting up a Cellular APN setting

You can define an APN (Access Point Name) which is a connection profile with the parameters you need to connect to a cellular network.

Click **Network Setting > Broadband > Cellular APN** to display the following screen.



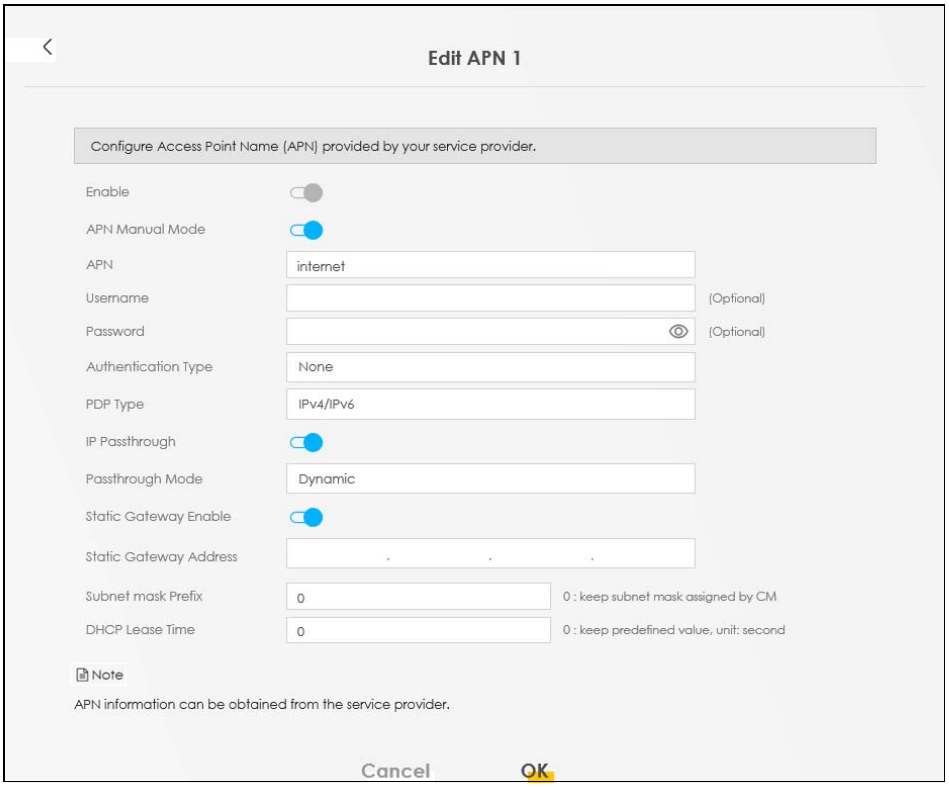
Broadband

Configure an LTE connection, including the Access Point Name (APN) provided by your service provider.

APN Settings

#	Enable		Mode	APN	Auth Type	PDP Type	VLAN ID	Modify
1	Enable	Default	Auto	N/A	N/A	N/A	N/A	✎
2	Disable		N/A	N/A	N/A	N/A	N/A	✎
3	Disable		N/A	N/A	N/A	N/A	N/A	✎
4	Disable		N/A	N/A	N/A	N/A	N/A	✎

Click the **Edit** icon (✎) in the **Cellular APN** screen, the following screen appears.



Edit APN 1

Configure Access Point Name (APN) provided by your service provider.

Enable	○	
APN Manual Mode	●	
APN	internet	
Username		(Optional)
Password		(Optional)
Authentication Type	None	
PDP Type	IPv4/IPv6	
IP Passthrough	●	
Passthrough Mode	Dynamic	
Static Gateway Enable	●	
Static Gateway Address	. . .	
Subnet mask Prefix	0	0 : keep subnet mask assigned by CM
DHCP Lease Time	0	0 : keep predefined value, unit: second

Note

APN information can be obtained from the service provider.

- **APN Manual Mode**: Enable this to configure your APN cellular information manually.
- **APN**: Enter the Access Point Name (APN) provided by your ISP. You can type a name up to 30 printable ASCII characters, including spaces.

- **Username**: Type the username provided by your ISP for authentication. The allowed username is up to 31 printable ASCII characters.
- **Password**: Type the password provided by your ISP for authentication. The allowed password is up to 31 printable ASCII characters.
- **Authentication Type**: Select the authentication type (**PAP**, **CHAP**, **PAP/CHAP**) used by the Zyxel Device.
- **PDP Type**: Select the IP address type (**IPv4**, **IPv6**, **IPv4/IPv6**) the Zyxel Device uses for connection.
- **IP Passthrough**: Enable this to turn off the routing functionality on the Zyxel Device.
- **Passthrough Mode**: Select **Fixed** to specify the MAC address of the computer using the public IP address provided by the ISP. Otherwise, select **Dynamic**.
- **Static Gateway Enable**: Select Enable to use a static IP address for your gateway.
- **Static Gateway Address**: Enter the IP address of your gateway.
- **Subnet mask Prefix**: Enter the subnet address of your gateway.
- **DHCP Lease Time**: Enter the lease time provided by your DHCP server.

5.4 Network Security

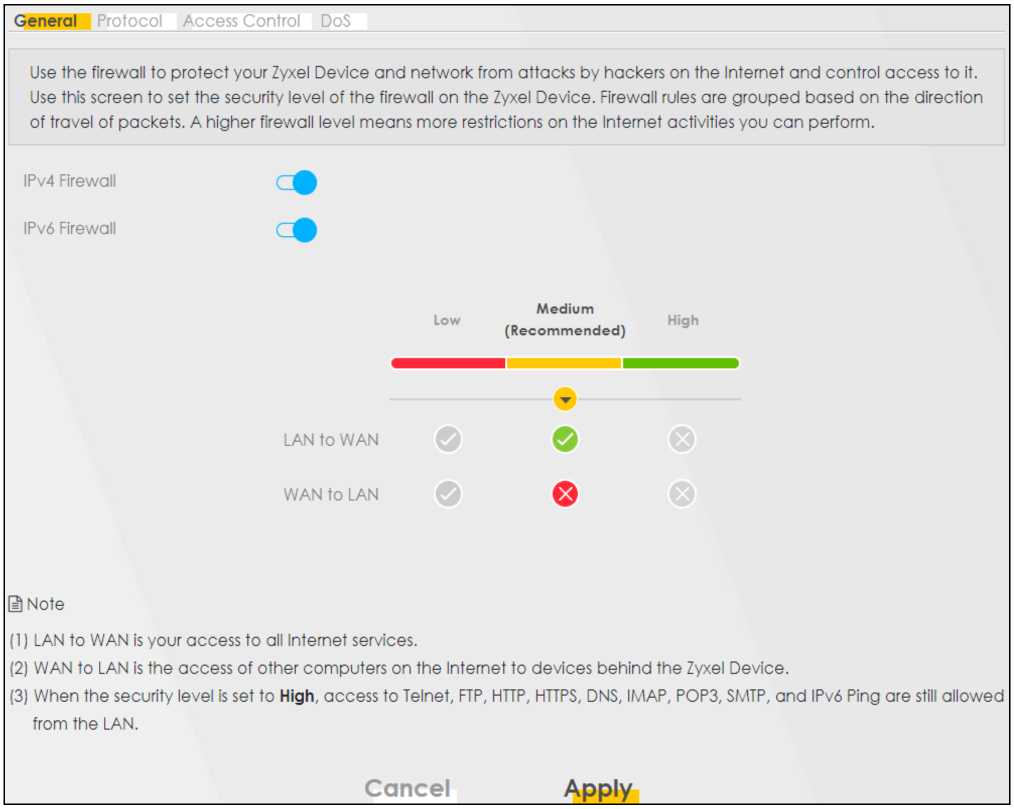
This section shows you how to configure a Firewall rule, Parental Control rule, or MAC Filter rule, and how to access the Zyxel Device using dynamic DNS (DNS).

5.4.1 Configuring 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**.



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.

IPv4 Firewall ●

IPv6 Firewall ●

	Low	Medium (Recommended)	High
LAN to WAN	✓	✓	✗
WAN to LAN	✓	✗	✗

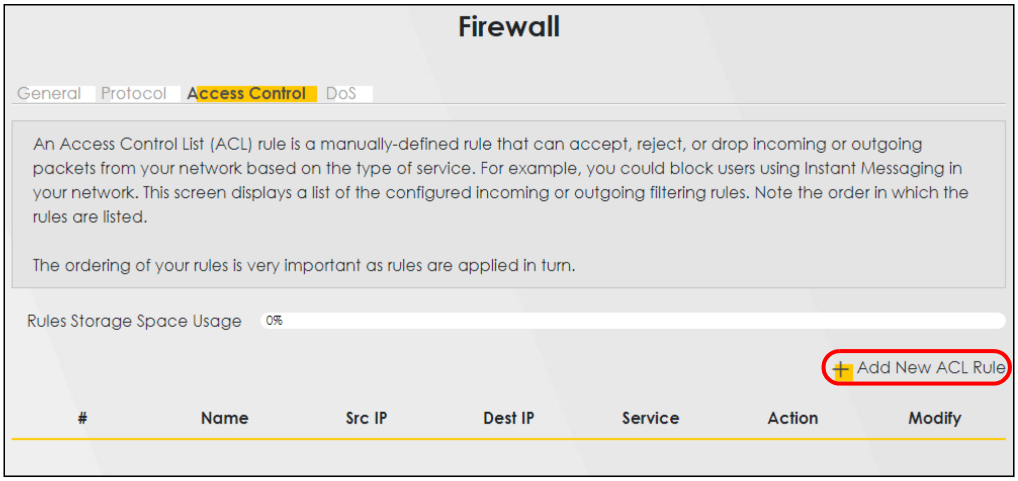
Note

(1) LAN to WAN is your access to all Internet services.

(2) WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

(3) When the security level is set to **High**, access to Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and IPv6 Ping are still allowed from the LAN.

3 Open the **Firewall** > **Access Control** screen.



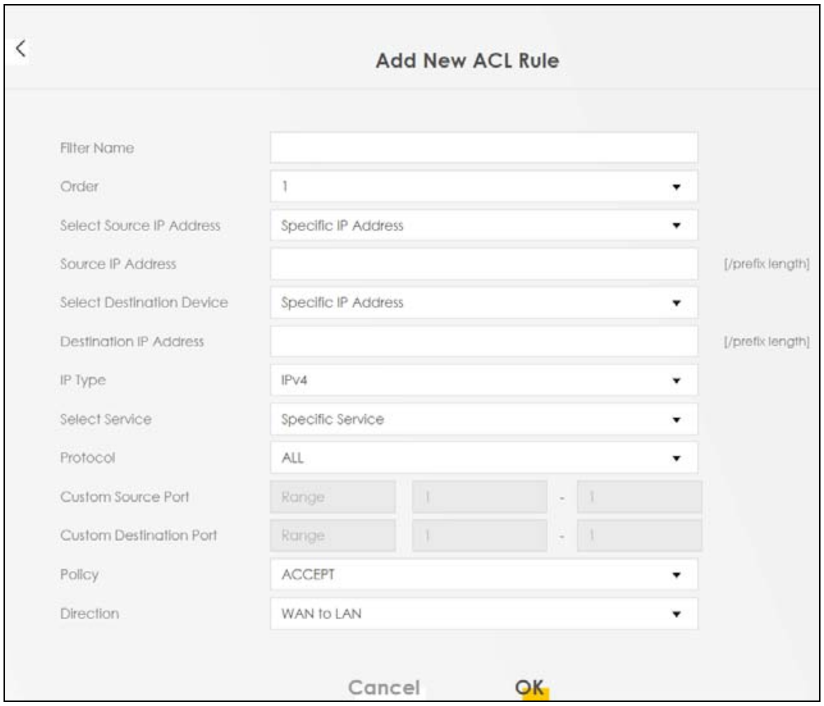
An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network based on the type of service. For example, you could block users using Instant Messaging in your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed.

The ordering of your rules is very important as rules are applied in turn.

Rules Storage Space Usage 0%

#	Name	Src IP	Dest IP	Service	Action	Modify

4 Click **Add New ACL Rule** and use the following fields to configure and apply a new Access Control List (ACL) rule. See Section 15.5 on page 165.



Add New ACL Rule

Filter Name		
Order	1 ▾	
Select Source IP Address	Specific IP Address ▾	
Source IP Address		[/prefix length]
Select Destination Device	Specific IP Address ▾	
Destination IP Address		[/prefix length]
IP Type	IPv4 ▾	
Select Service	Specific Service ▾	
Protocol	ALL ▾	
Custom Source Port	Range 1 - 1	
Custom Destination Port	Range 1 - 1	
Policy	ACCEPT ▾	
Direction	WAN to LAN ▾	

- **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.

5.4.2 Parental Control

This section shows you how to configure rules for accessing the Internet using parental control.
The style and features of your parental control might vary depending on the Zyxel Device you are using.

5.4.2.1 Configuring 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.

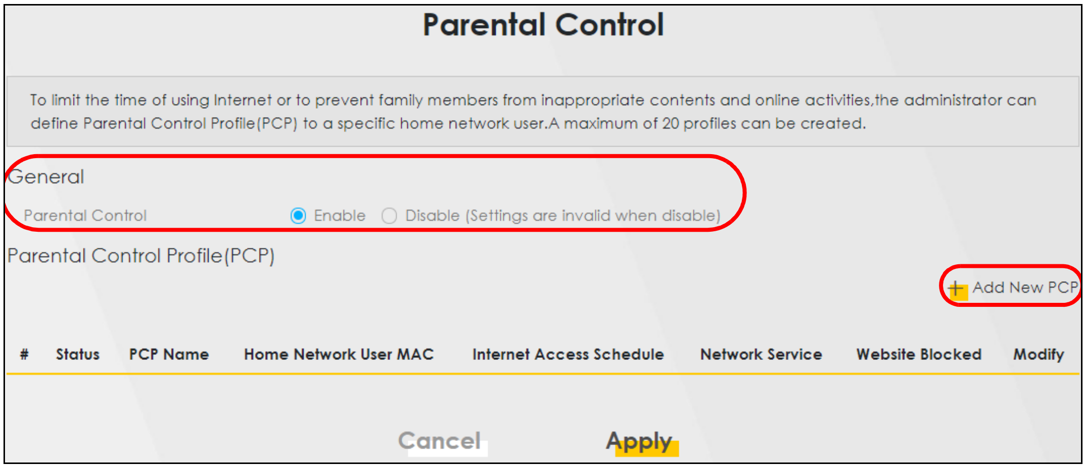
This example shows you how to block a user from accessing the Internet during time for studying. It also shows you how to stop a user from accessing specific websites.

Use the parameter 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	**Network Service Setting**: Block	**Block or Allow the Web Site**: Block the web URLs
	Time: 8:00 to 11:00 13:00 to 17:00	**Service Name**: HTTP	**Website**: gambling
		Protocol: TCP	
		Port: 80	

Open **Security** > **Parental Control** Screen

Select **Enable** under **General** to enable parental control. Then click **Add New PCP** to add a rule.



Parental Control

To limit the time of using Internet or to prevent family members from inappropriate contents and online activities,the administrator can define Parental Control Profile(PCP) to a specific home network user.A maximum of 20 profiles can be created.

General

Parental Control ● Enable ○ Disable (Settings are invalid when disable)

Parental Control Profile(PCP)

#	Status	PCP Name	Home Network User MAC	Internet Access Schedule	Network Service	Website Blocked	Modify

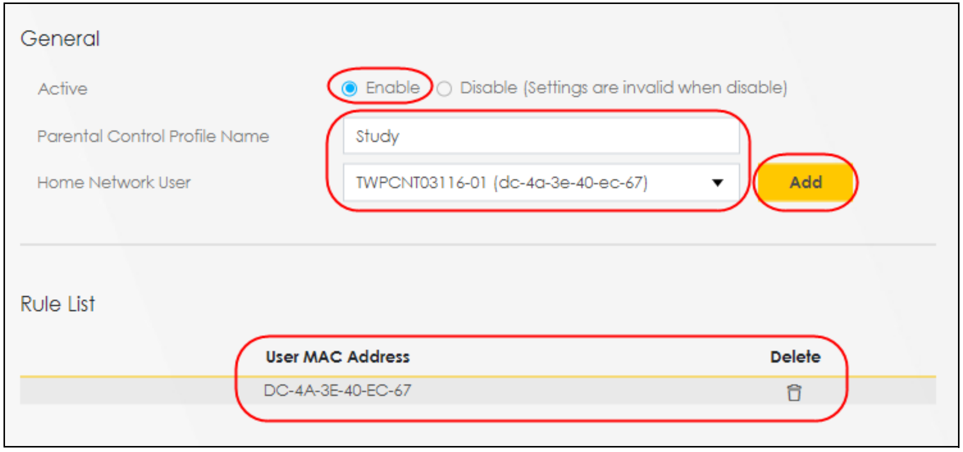
Open **Security** > **Parental Control** > **Add New PCP** Screen

1 Under **General**:

1a Select **Enable** to enable the rule you are configuring.

1b Enter the **Parental Control Profile Name** given in the above parameter.

1c 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**.



General

Active ● Enable ○ Disable (Settings are invalid when disable)

Parental Control Profile Name: Study

Home Network User: TWPCNT03116-01 (dc-4a-3e-40-ec-67) ▾ Add

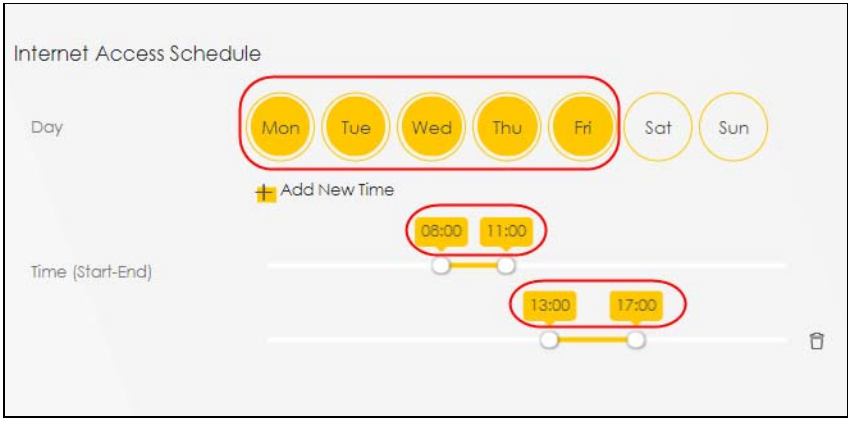
Rule List

User MAC Address	Delete
DC-4A-3E-40-EC-67	🗑

2 Under **Internet Access Schedule**:

2a Click **Add New Time** to add a second schedule.

2b Use the parameter give above to configure the time settings of your schedule.



Internet Access Schedule

Day: Mon Tue Wed Thu Fri Sat Sun

Add New Time

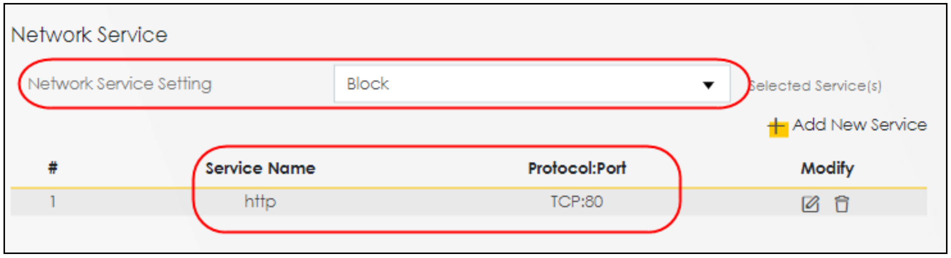
Time (Start-End): 08:00 11:00

13:00 17:00

3 Under **Network Service**:

3a In **Network Service Setting,** select **Block**.

3b Click **Add New Service**, then use the parameter given above to configure settings for the Internet service you are blocking.



Network Service

Network Service Setting: Block ▾ Selected Service(s)

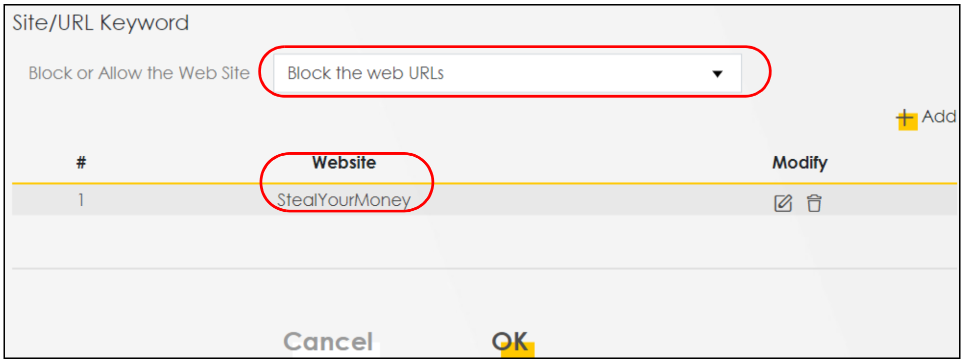
Add New Service

#	Service Name	Protocol:Port	Modify
1	http	TCP:80	✎ 🗑

4 Under **Site** / **URL Keyword**:

4a Select **Block the web URLs** in **Block or Allow the Web Site**.

4b Click **Add**, then use the parameter given above to configure settings for the URL keyword you are blocking.



Site/URL Keyword

Block or Allow the Web Site: Block the web URLs

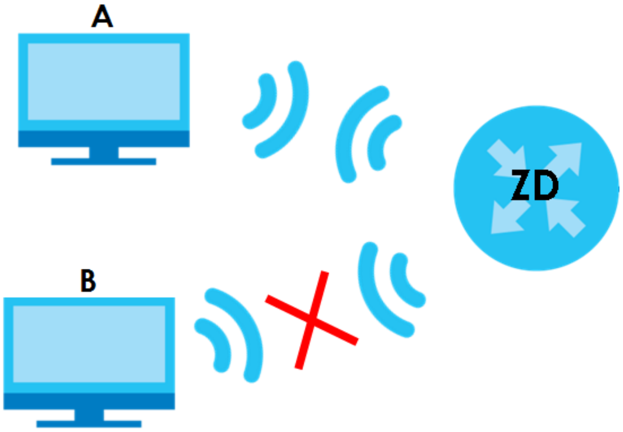
#	Website	Modify
1	StealYourMoney	

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

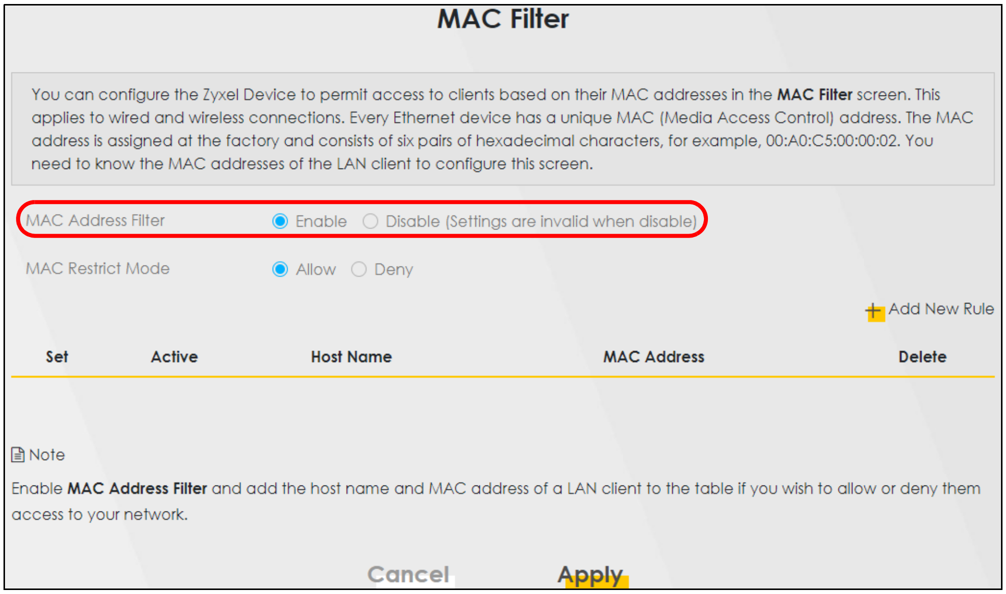
5.4.3 Configuring a MAC Address Filter

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

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



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



MAC Filter

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 and wireless 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 the LAN client to configure this screen.

MAC Address Filter ● Enable ○ Disable (Settings are invalid when disable)

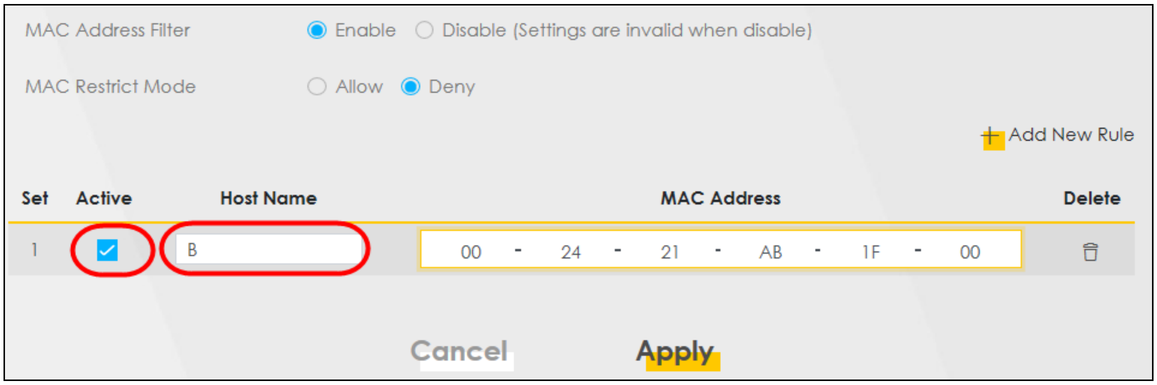
MAC Restrict Mode ● Allow ○ Deny

Set	Active	Host Name	MAC Address	Delete

Note

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network.

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**.



MAC Address Filter ● Enable ○ Disable (Settings are invalid when disable)

MAC Restrict Mode ○ Allow ● Deny

Set	Active	Host Name	MAC Address	Delete
1	☑	B	00 - 24 - 21 - AB - 1F - 00	🗑

5.5 Device Maintenance

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

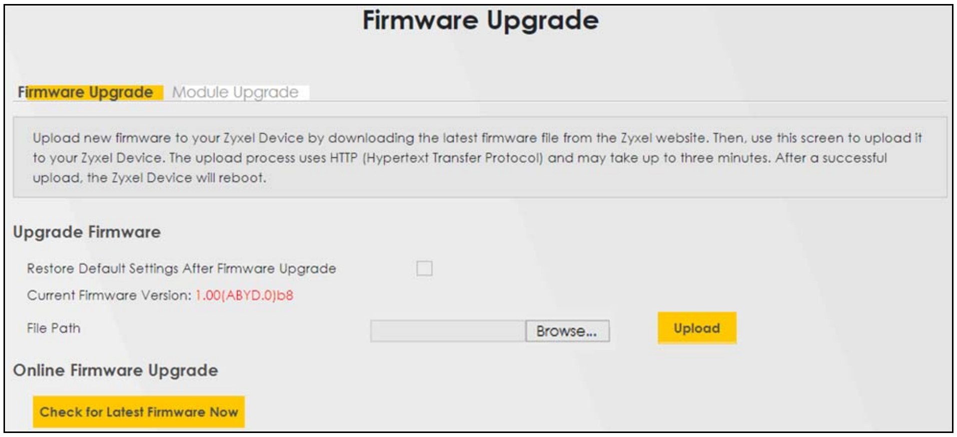
5.5.1 Upgrading the Firmware

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

1 Download the correct firmware file from the download library at the Zyxel website. Note the model code for your device. Unzip the file.

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

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



Firmware Upgrade

Firmware Upgrade | Module Upgrade

Upload new firmware to your Zyxel Device by downloading the latest firmware file from the Zyxel website. Then, use this screen to upload it to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the Zyxel Device will reboot.

Upgrade Firmware

Restore Default Settings After Firmware Upgrade □

Current Firmware Version: 1.00(ABYD.0)b8

File Path [Browse...] [Upload]

Online Firmware Upgrade

[Check for Latest Firmware Now]

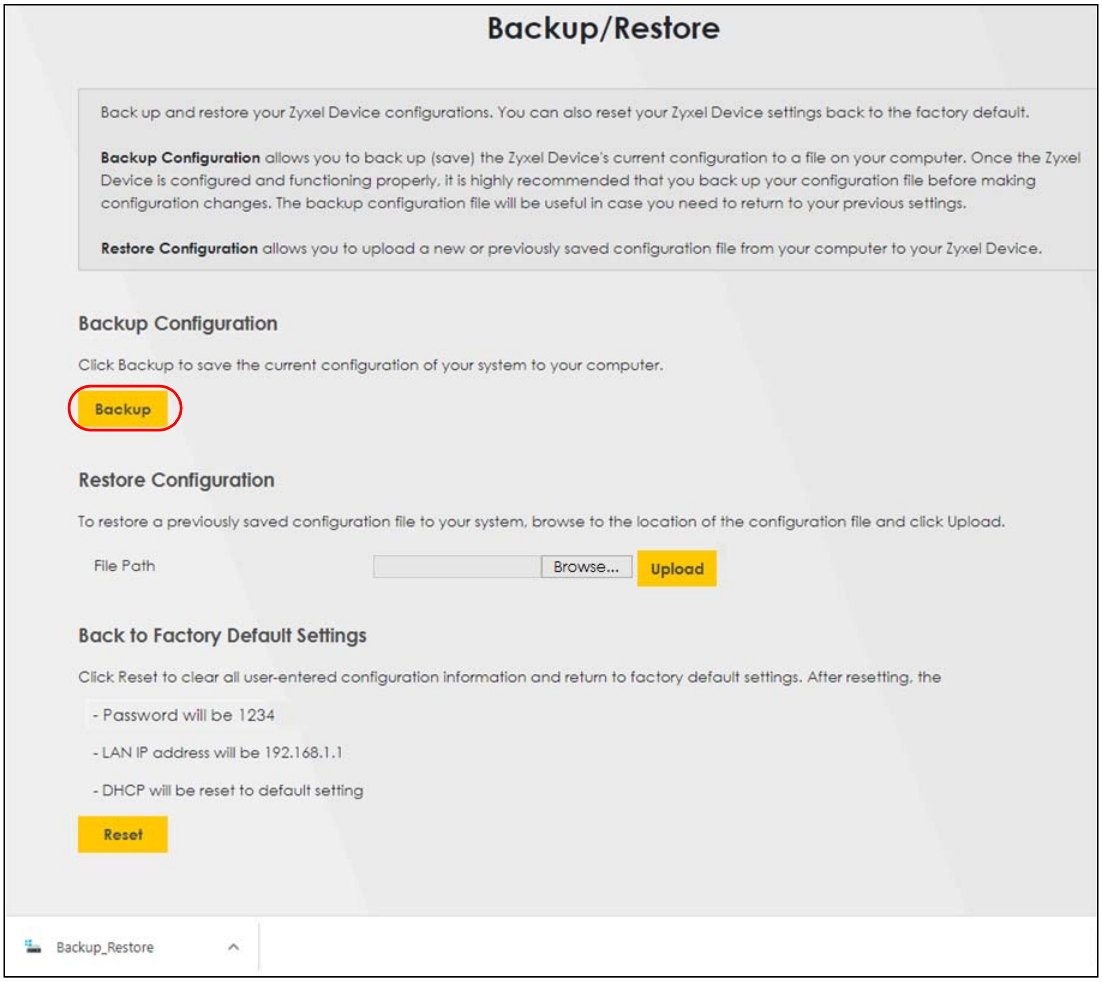
4 This process may take up to 2 minutes to finish. After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

5.5.2 Backing 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.



Backup/Restore

Back up and restore your Zyxel Device configurations. You can also reset your Zyxel Device settings back to the factory default.

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once the 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.

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

Backup Configuration

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

Restore Configuration

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

File Path

Back to Factory Default Settings

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

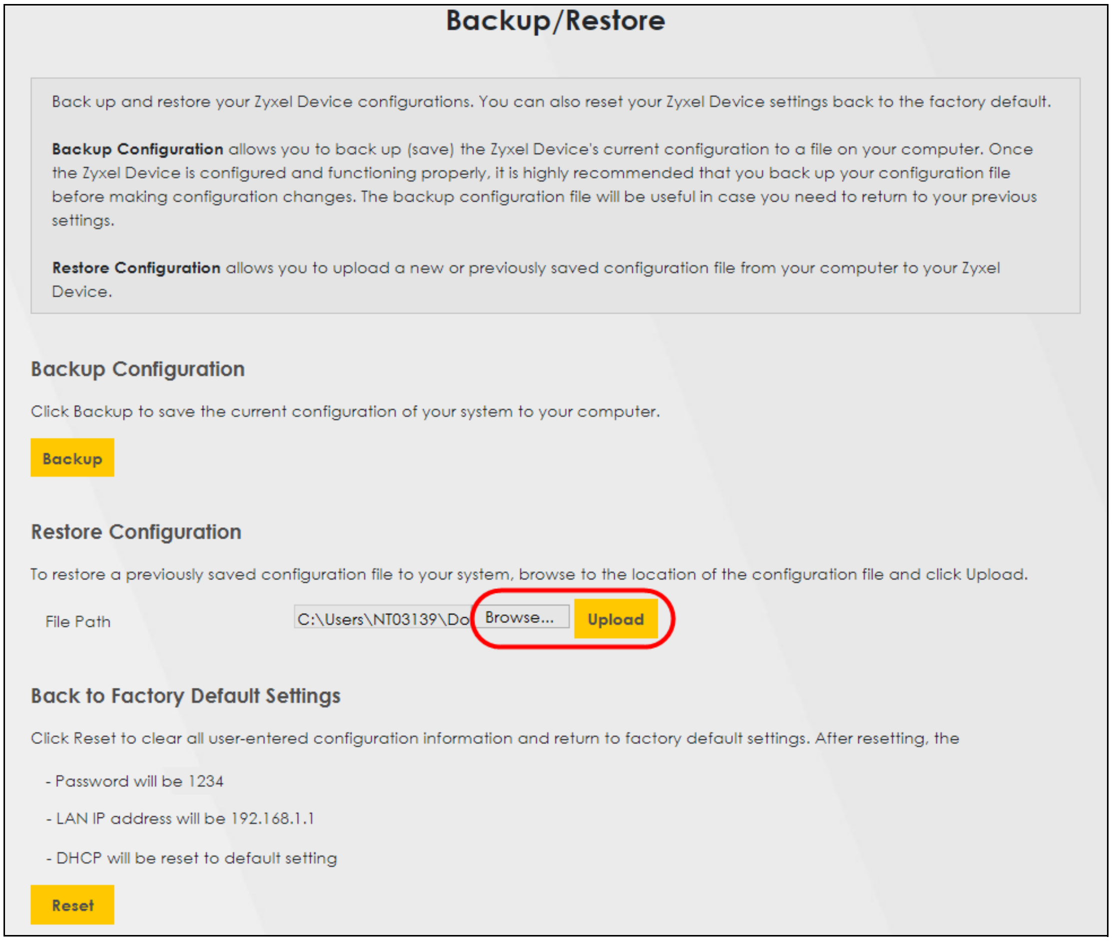
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

5.5.3 Restoring 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**.



Backup/Restore

Back up and restore your Zyxel Device configurations. You can also reset your Zyxel Device settings back to the factory default.

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once the 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.

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

Backup Configuration

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

Restore Configuration

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

File Path C:\Users\NT03139\Do

Back to Factory Default Settings

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

- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

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.

PART II
Technical Reference

CHAPTER 6
Connection Status

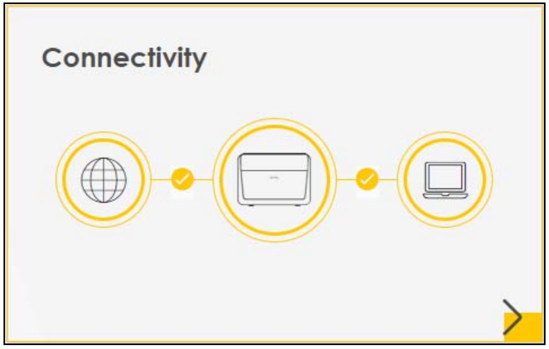
6.1 Connection Status Overview

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

6.1.1 Connectivity

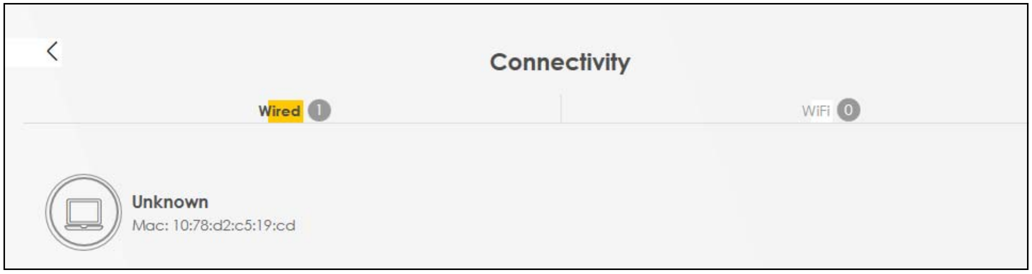
Use this screen to view the network connection status of the Zyxel Device and its clients.

Figure 23 Connectivity



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

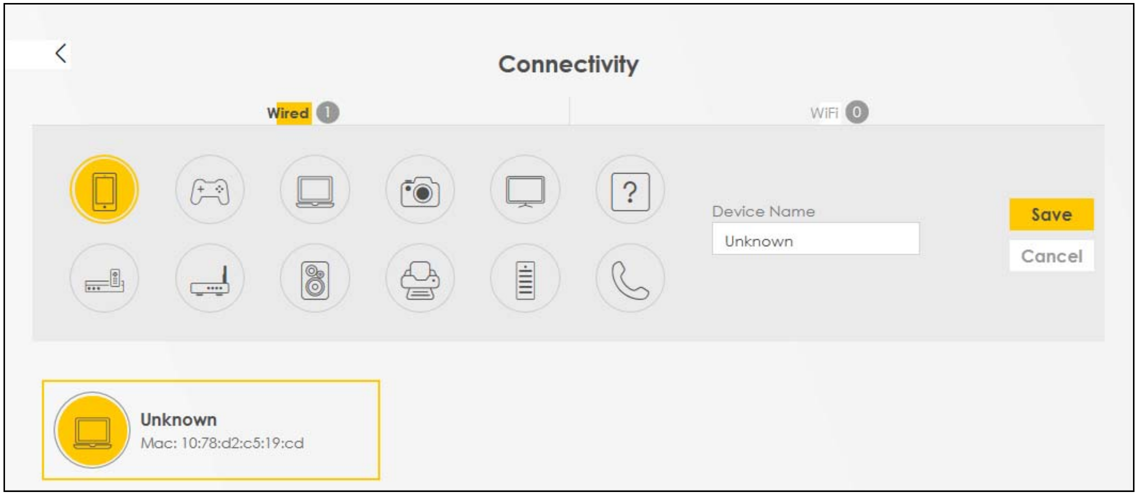
Figure 24 Connectivity: Connected Devices



Unknown
Mac: 10:78:d2:c5:19:cd

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** (**Active**) for a connected device. Click **Save** to save your changes.

Figure 25 Connectivity: Edit



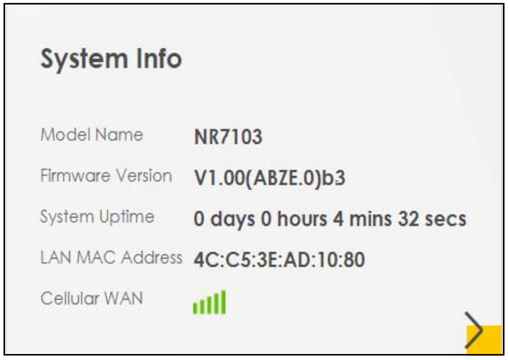
Device Name: Unknown

Unknown
Mac: 10:78:d2:c5:19:cd

6.1.2 System Info

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

Figure 26 System Info

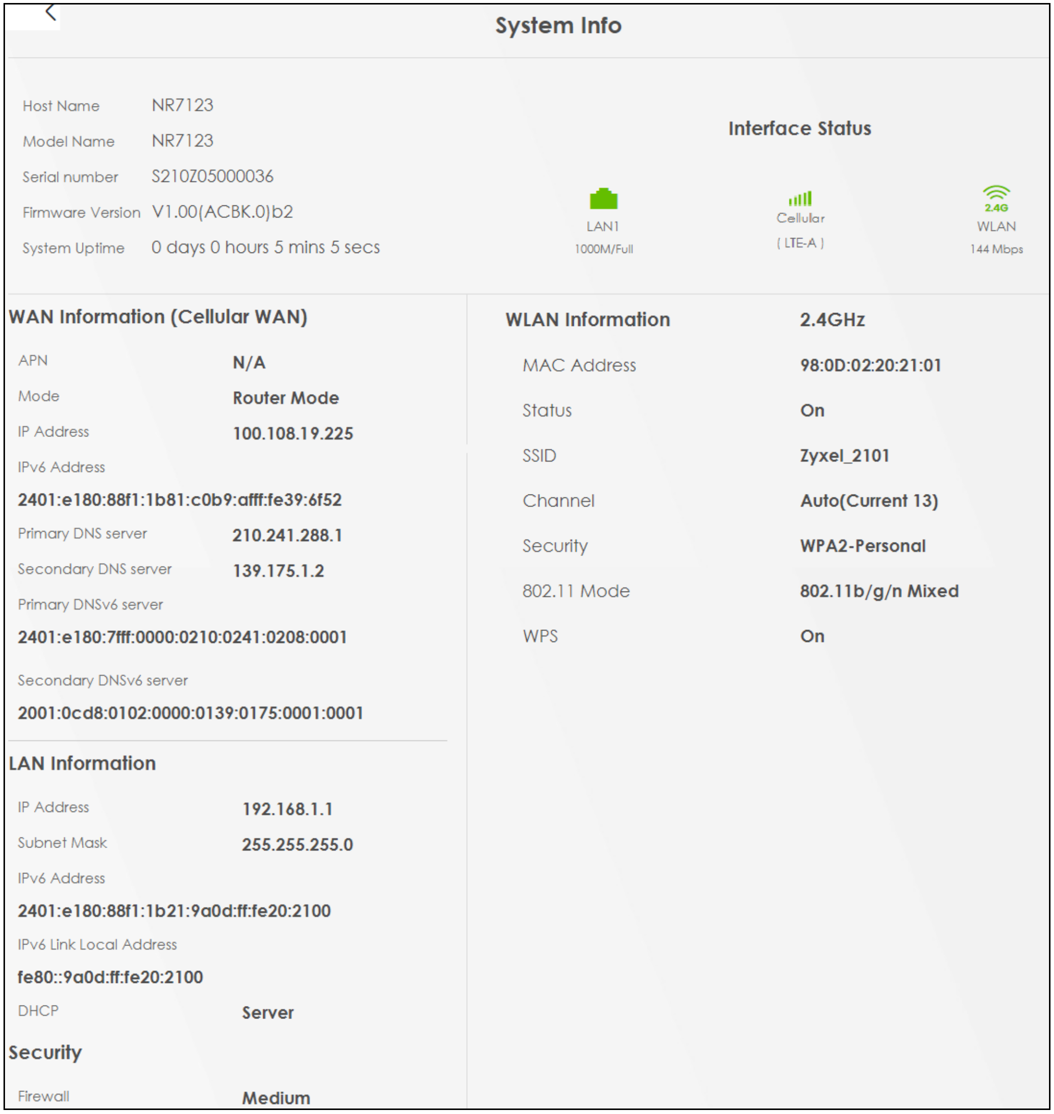


System Info

Model Name	NR7103
Firmware Version	V1.00(ABZE.0)b3
System Uptime	0 days 0 hours 4 mins 32 secs
LAN MAC Address	4C:C5:3E:AD:10:80
Cellular WAN	

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

Figure 27 System Info: Detailed Information



System Info

Host Name NR7123

Model Name NR7123

Serial number S210Z05000036

Firmware Version V1.00(ACBK.0)b2

System Uptime 0 days 0 hours 5 mins 5 secs

Interface Status

WAN Information (Cellular WAN)

APN N/A

Mode Router Mode

IP Address 100.108.19.225

IPv6 Address

2401:e180:88f1:1b81:c0b9:afff:fe39:6f52

Primary DNS server 210.241.288.1

Secondary DNS server 139.175.1.2

Primary DNSv6 server

2401:e180:7fff:0000:0210:0241:0208:0001

Secondary DNSv6 server

2001:0cd8:0102:0000:0139:0175:0001:0001

LAN Information

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

IPv6 Address

2401:e180:88f1:1b21:9a0d:ff:fe20:2100

IPv6 Link Local Address

fe80::9a0d:ff:fe20:2100

DHCP Server

Security

Firewall Medium

WLAN Information 2.4GHz

MAC Address 98:0D:02:20:21:01

Status On

SSID Zyxel_2101

Channel Auto(Current 13)

Security WPA2-Personal

802.11 Mode 802.11b/g/n Mixed

WPS On

Each field is described in the following table.

Table 8 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.
Interface Status Virtual ports are shown here. You can see the ports in use and their transmission rate.	
WAN Information (Cellular WAN) These fields display when you have a WAN connection.	
APN	This field displays the Access Point Name (APN).

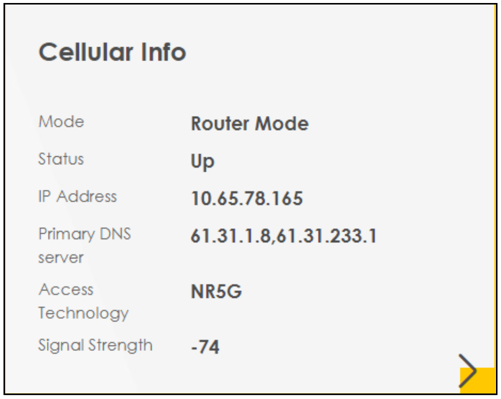
Table 8 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
Mode	This field displays the current mode of your Zyxel Device.The mode is either **Router Mode** or **IP Passthrough Mode**.
Connect Time	This field displays the current WAN connect time.
IP Address	This field displays the current IP address of the Zyxel Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device in the WAN.
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 is the IPv6 address that uniquely identifies a device in the LAN.
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. **None** - The Zyxel Device is not providing any DHCP services to the LAN.
Security	
Firewall	This displays the firewall's current security level.
WLAN Information	
MAC Address	This shows the wireless adapter Media Access Control (MAC Address) of the wireless interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a wireless LAN.
Channel	This is the channel number currently used by the wireless interface.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.

6.1.3 Cellular Info

Use this screen to view the cellular connection details and cellular signal strength value that you can use as reference for positioning the Zyxel Device. SIM card and module information is also shown in the screen.

Figure 28 Cellular Info

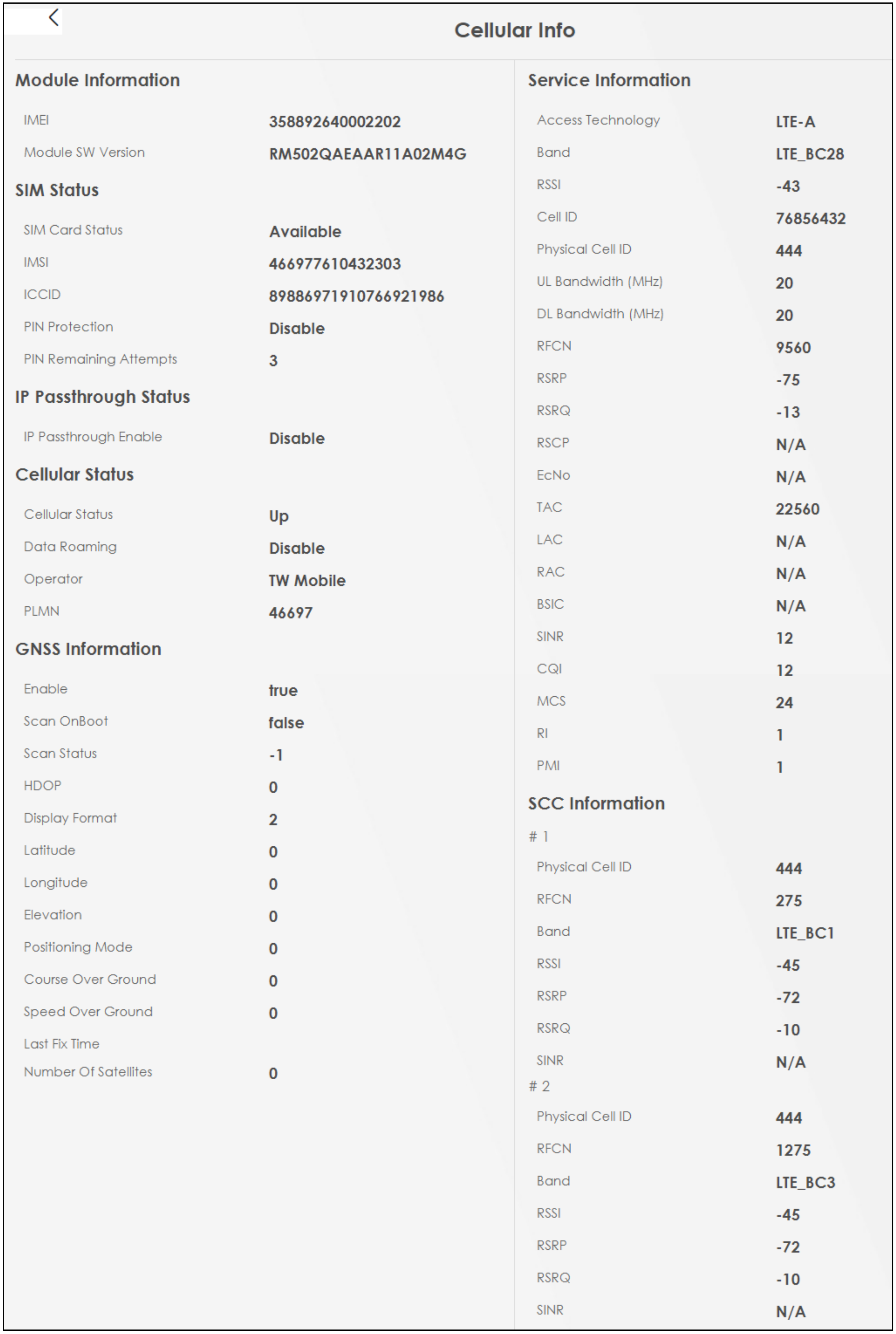


Cellular Info

Mode	Router Mode
Status	Up
IP Address	10.65.78.165
Primary DNS server	61.31.1.8,61.31.233.1
Access Technology	NR5G
Signal Strength	-74

Click the Arrow icon (>) to view the more information on the cellular connection.

Figure 29 Cellular Info: Detailed Information



Cellular Info

Module Information

IMEI	358892640002202
Module SW Version	RM502QAEAAR11A02M4G

SIM Status

SIM Card Status	Available
IMSI	466977610432303
ICCID	89886971910766921986
PIN Protection	Disable
PIN Remaining Attempts	3

IP Passthrough Status

IP Passthrough Enable	Disable

Cellular Status

Cellular Status	Up
Data Roaming	Disable
Operator	TW Mobile
PLMN	46697

GNSS Information

Enable	true
Scan OnBoot	false
Scan Status	-1
HDOP	0
Display Format	2
Latitude	0
Longitude	0
Elevation	0
Positioning Mode	0
Course Over Ground	0
Speed Over Ground	0
Last Fix Time	
Number Of Satellites	0

Service Information

Access Technology	LTE-A
Band	LTE_BC28
RSSI	-43
Cell ID	76856432
Physical Cell ID	444
UL Bandwidth (MHz)	20
DL Bandwidth (MHz)	20
RFCN	9560
RSRP	-75
RSRQ	-13
RSCP	N/A
EcNo	N/A
TAC	22560
LAC	N/A
RAC	N/A
BSIC	N/A
SINR	12
CQI	12
MCS	24
RI	1
PMI	1

SCC Information

1

Physical Cell ID	444
RFCN	275
Band	LTE_BC1
RSSI	-45
RSRP	-72
RSRQ	-10
SINR	N/A

2

Physical Cell ID	444
RFCN	1275
Band	LTE_BC3
RSSI	-45
RSRP	-72
RSRQ	-10
SINR	N/A

Note: The fields in the screen may slightly differ based on the Access Technology your Zyxel Device supports.

Note: The value is ‘0’ (zero) or ‘N/A’ if the Access Technology the Zyxel Device is currently connected to doesn’t have this value in that specific parameter field or there is no network connection.

The following table describes the labels in this screen.

Table 9 Cellular Info: Detailed Information

LABEL	DESCRIPTION
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Module SW Version	This shows the software version of the 5G module.
SIM Status	
SIM Card Status	This displays the SIM card status: **None** - the Zyxel Device does not detect that there is a SIM card inserted. **Waiting SIM Available** - the SIM card is detected but not available yet. **Available** - the SIM card could either have or does not have PIN code security. **Locked** - the SIM card has PIN code security, but you did not enter the PIN code yet. **Blocked** - you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card. **Error** - the Zyxel Device detected that the SIM card has errors.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (**ICCID**). This is the serial number of the SIM card.
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. This field shows **Enable** if **PIN Protection** is enabled. Otherwise, this field shows **Disable**.
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
IP Passthrough Enable	This displays if IP Passthrough is enabled on the Zyxel Device. IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.
Data Roaming	This displays if data roaming is enabled on the Zyxel Device. Data roaming is to use your Zyxel Device in an area which is not covered by your service provider. Enable roaming to ensure that your Zyxel Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Operator	This displays the name of the service provider.

Table 9 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
PLMN	Public Land Mobile Network (PLMN) is a wireless network system that usually contains more than one type of mobile network service. A PLMN code is a unique identifier of a PLMN. A PLMN code identifies a specific operator in a specific country. It consists of Mobile Country Code (MCC) and Mobile Network Code (MNC). This displays the PLMN code.
GNSS Information	Global Navigation Satellite System (GNSS) sends position and timing data from high orbit artificial satellites. It works with GPS navigational satellites to provide better receiver accuracy and reliability than just using GPS alone. This is necessary for 5G networks that require very accurate timing for time and frequency synchronization. With GNSS, your can easily locate the Zyxel Device with accurate information.
Enable	This shows if GNSS is enabled. Note: This can only be configured by a qualified service technician.
Scan OnBoot	This shows Enable if Scan OnBoot is enabled, so that GNSS runs automatically after the Zyxel Device is turned on. Note: This can only be configured by a qualified service technician.
Scan Status	This shows GNSS error codes for debugging by a qualified service technician.
HDOP	Horizontal Dilution of Precision (HDOP) shows how accurate data collected by the Zyxel Device is according to the current satellite configuration. A smaller value of HDOP means a higher precision.
Display Format	This shows the latitude and longitude display modes. There are three modes: 0, 1, and 2. Below are examples for these modes shown in latitude/longitude. 0 - ddmm.mmmmN/S, dddmm.mmmmE/W 1 - ddmm.mmmmmm, N/S, dddmm.mmmmmm, E/W 2 - (-)dd.ddddd, (-)ddd.ddddd N/S/E/W: North/South/East/West “-” : Negative values refer to South latitude/West longitude respectively. Positive values refer to North latitude/East longitude.
Latitude	This shows the latitude coordinate of the Zyxel Device. These positioning values (latitude, longitude, and altitude) help you locate the Zyxel Device accurately.
Longitude	This shows the longitude coordinate of the Zyxel Device.
Elevation	This shows the altitude of the Zyxel Device above sea level in meters.
Positioning Mode	This shows the GNSS positioning mode. 2D (“2”) GNSS positioning mode displays latitude and longitude co-ordinates; 3D (“2”) GNSS positioning mode displays latitude and longitude co-ordinates, and elevation.
Course over ground	This shows the course of the Zyxel Device based on true North. Course Over Ground (COG) is different from the direction an object is headed, but the path derived from its actual motion (considered as Track), since the motion of an object is often with respect to other factors like wind and tides.
Speed Over Ground	This shows the Speed Over Ground (SOG) of the Zyxel Device. SOG is the true object speed over the surface of the Earth.
Last Fix Time	This shows the last time in UTC format that the position of the Zyxel Device was updated.
Number Of Satellites	This shows the number of current active satellites. GNSS requires at least 4 satellites to determine the position of the Zyxel Device.
Service Information /SCC Information	

Table 9 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
#	This is the index number of the Secondary Component Carrier (SCC). The Zyxel Device supports Carrier Aggregation (CA) to use multiple LTE carriers simultaneously for data transmission. CA consists of a Primary Component Carrier (PCC) and secondary component carriers (SCC). The PCC is used for control signaling and the SCC is used for increased data throughput.
Access Technology	This displays the type of mobile network to which your Zyxel Device is currently connected.
Band	This displays the current cellular band of your Zyxel Device. The Zyxel Device supports Carrier Aggregation (CA). There might be more than one band if the Zyxel Device is using multiple carriers for data transmission. See Section on page 17.
RSSI	This displays the strength of the cellular signal between an associated cellular station and the Zyxel Device.
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting. The value depends on the current Access Technology. For LTE/5G, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331.
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Zyxel Device and the mobile network it is connected to.
UL Bandwidth (MHz)	This shows the uplink cellular channel bandwidth from the Zyxel Device to base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
DL Bandwidth (MHz)	This shows the downlink cellular channel bandwidth from base station to the Zyxel Device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting. The value depends on the current Access Technology: • For LTE, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. • For 5G, it is the NR-ARFCN (New Radio Absolute Radio-Frequency Channel Number).
RSRP	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133. An undetectable signal is indicated by the lower limit, example -140 dBm. The normal range is -44 to -140. The signal is better when the value is closer to -44.
RSRQ	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example -240. The normal range is -3 to -20. The signal is better when the value is closer to -3.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device. The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example -120 dBm.
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level. The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example -240 dB.

Table 9 Cellular Info: Detailed Information (continued)

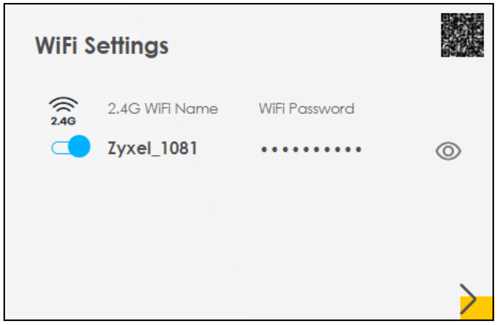
LABEL	DESCRIPTION
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber. The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN. The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003].
RAC	This displays the RAC (Routing Area Code), which is used in mobile network "packet domain service" (PS) to identify a routing area within a location area. In a mobile network, the Zyxel Device uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and uses RAC to identify the location of data service like HSDPA or LTE. The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003].
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good/bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI). PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer). PMI determines how cellular data are encoded for the antennas to improve downlink rate.

6.1.4 WiFi Settings

Use this screen to enable or disable the main 2.4 GHz wireless network. When the switch turns blue (●), the function is enabled. Otherwise, it is not. You can use this screen or the QR code on the upper right corner to check the SSID (WiFi network name) and password of the wireless network. If you want to show or hide your WiFi password, click the Eye icon (👁).

Note: WiFi for an outdoor NR device is only used for configuration.

Figure 30 WiFi Settings



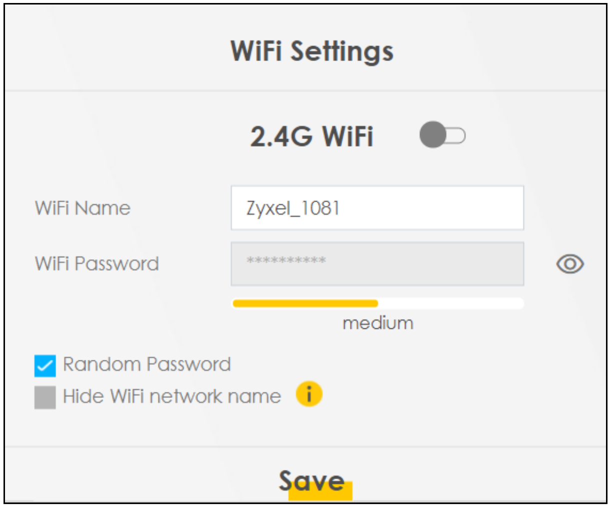
WiFi Settings

2.4G WiFi Name	WiFi Password
Zyxel_1081	••••••••••

Click the Arrow icon (>) to configure the SSID and/or password for the wireless network. Click the Eye icon (◎) to display the characters as you enter the WiFi Password.

Scan the QR code as an alternative way to connect the wireless client to the WiFi network.

Figure 31 WiFi Settings: Configuration



WiFi Settings

2.4G WiFi

WiFi Name: Zyxel_1081

WiFi Password: **********

medium

☑ Random Password

□ Hide WiFi network name

Save

Each field is described in the following table.

Table 10 WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4G WiFi	Click this switch to enable or disable the 2.4 GHz wireless network. When the switch turns blue ●, the function is enabled. Otherwise, it is not.
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 English keyboard characters) for the wireless LAN.
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 type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	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.
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.

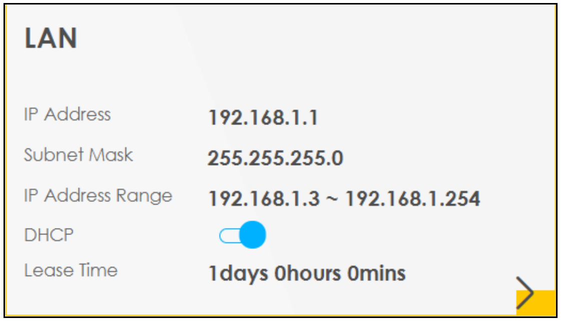
Table 10 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
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.

6.1.5 LAN

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

Figure 32 Status > LAN



LAN

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

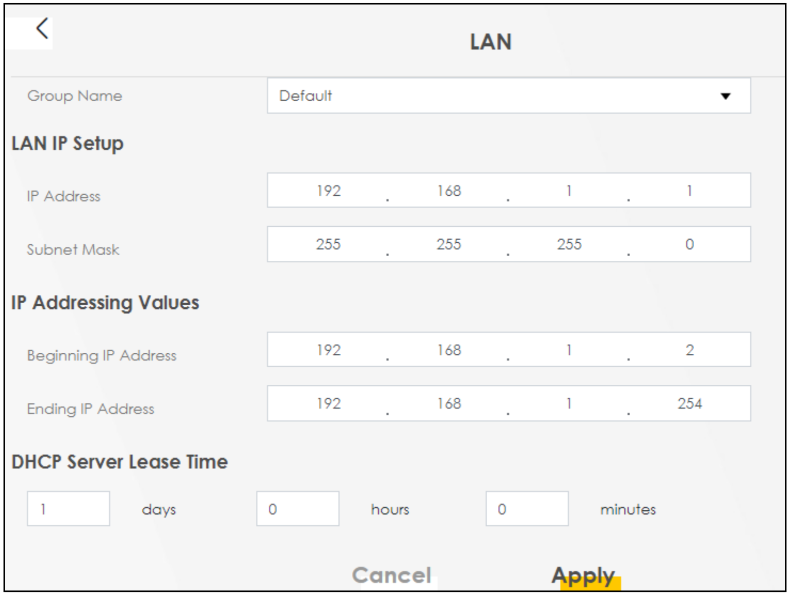
IP Address Range 192.168.1.3 ~ 192.168.1.254

DHCP ●

Lease Time 1days 0hours 0mins

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

Figure 33 LAN Setup



LAN

Group Name: Default

LAN IP Setup

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

IP Addressing Values

Beginning IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 254

DHCP Server Lease Time

1 days 0 hours 0 minutes

Each field is described in the following table.

Table 11 Status > LAN Setup

LABEL	DESCRIPTION
Group Name	Select the interface group you want to use. Usually **Default**.
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, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your 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.
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.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
Save	Click **Save** to save your changes.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

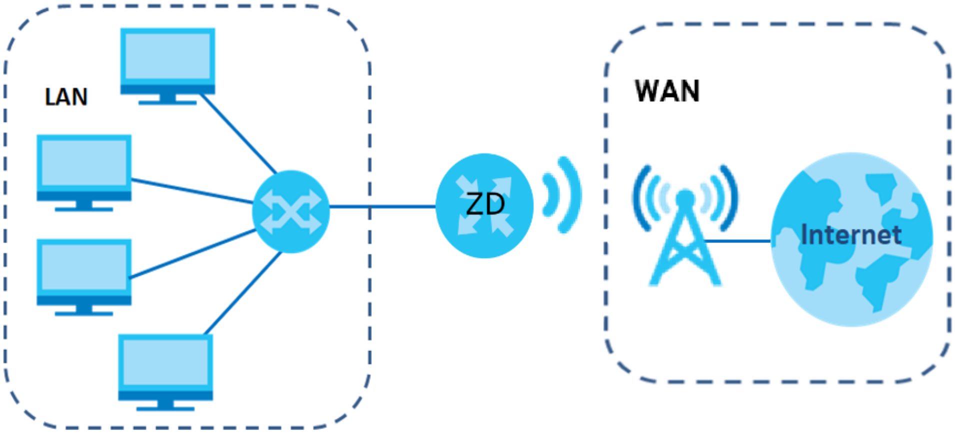
CHAPTER 7
Broadband

7.1 Overview

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

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

Figure 34 LAN and WAN



7.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 7.2 on page 70).
- Use the **Cellular WAN** screen to configure a cellular WAN connection (Section 7.3 on page 72).
- Use the **Cellular APN** screen to configure a WAN connection that includes the Access Point Name (APN) provided by your service provider (Section 7.4 on page 74).
- Use the **Cellular SIM** screen to enter the PIN of your SIM card (Section 7.5 on page 76).
- Use the **Cellular Band** screen to view or edit a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 7.2 on page 70).
- Use the **Cellular PLMN** screen to display available Public Land Mobile Networks (Section 7.7 on page 79).
- Use the **Cellular IP Passthrough** screen to configure a WAN connection (Section 7.8 on page 81).
- Use the **Cellular Lock** screen to configure the base station you choose to connect to (Section 7.9 on page 82).

Table 12 WAN Setup Overview

LAYER-2 INTERFACE		INTERNET CONNECTION		
CONNECTION	DSL LINK TYPE	MODE	ENCAPSULATION	CONNECTION SETTINGS
Ethernet	N/A	Routing	IPoE	WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature.

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. The ISP dynamically assigns it each time the Zyxel Device tries to access the Internet.

APN

Access Point Name (APN) is a unique string which indicates a cellular network. An APN is required for cellular stations to enter the cellular network and then the Internet.

7.1.3 Before You Begin

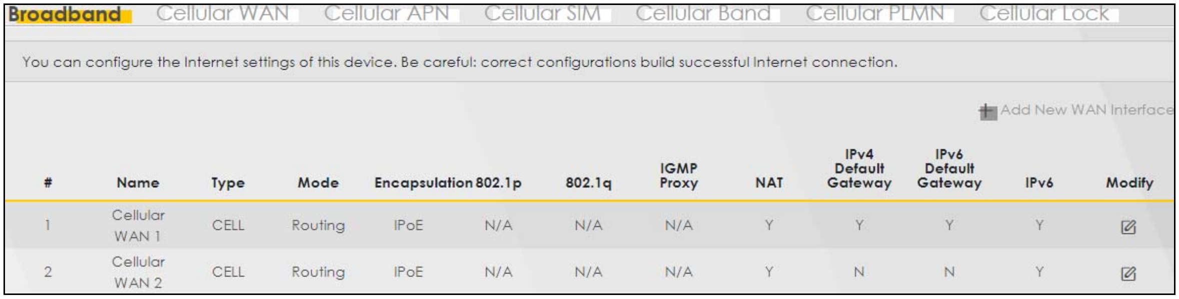
You may need to know your Internet access settings such as cellular APN, WAN IP address and SIM card's PIN code if the Status light on your Zyxel Device shows disconnection of the Internet. Get this information from your service provider.

7.2 Broadband

Use this screen to change your Zyxel Device's Internet access settings. The summary table shows you the configured WAN services (connections) on the Zyxel Device. Use information provided by your ISP to configure WAN settings.

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

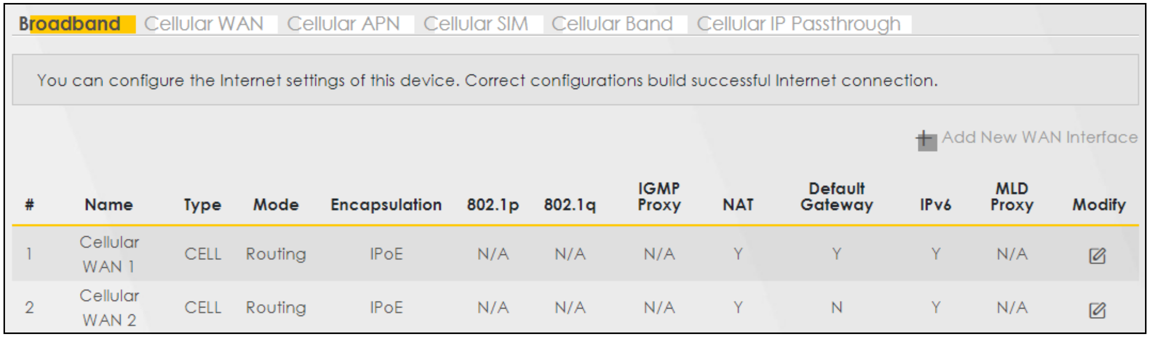
Figure 35 Network Setting > Broadband (with **IPv4** and **IPv6 Default Gateway**)



You can configure the Internet settings of this device. Be careful: correct configurations build successful Internet connection.

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	IPv4 Default Gateway	IPv6 Default Gateway	IPv6	Modify
1	Cellular WAN 1	CELL	Routing	IPoE	N/A	N/A	N/A	Y	Y	Y	Y	✎
2	Cellular WAN 2	CELL	Routing	IPoE	N/A	N/A	N/A	Y	N	N	Y	✎

Figure 36 Network Setting > Broadband (with **MLD Proxy**)



Broadband | Cellular WAN | Cellular APN | Cellular SIM | Cellular Band | Cellular IP Passthrough

You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	Cellular WAN 1	CELL	Routing	IPoE	N/A	N/A	N/A	Y	Y	Y	N/A	✎
2	Cellular WAN 2	CELL	Routing	IPoE	N/A	N/A	N/A	Y	N	Y	N/A	✎

The following table describes the labels in this screen.

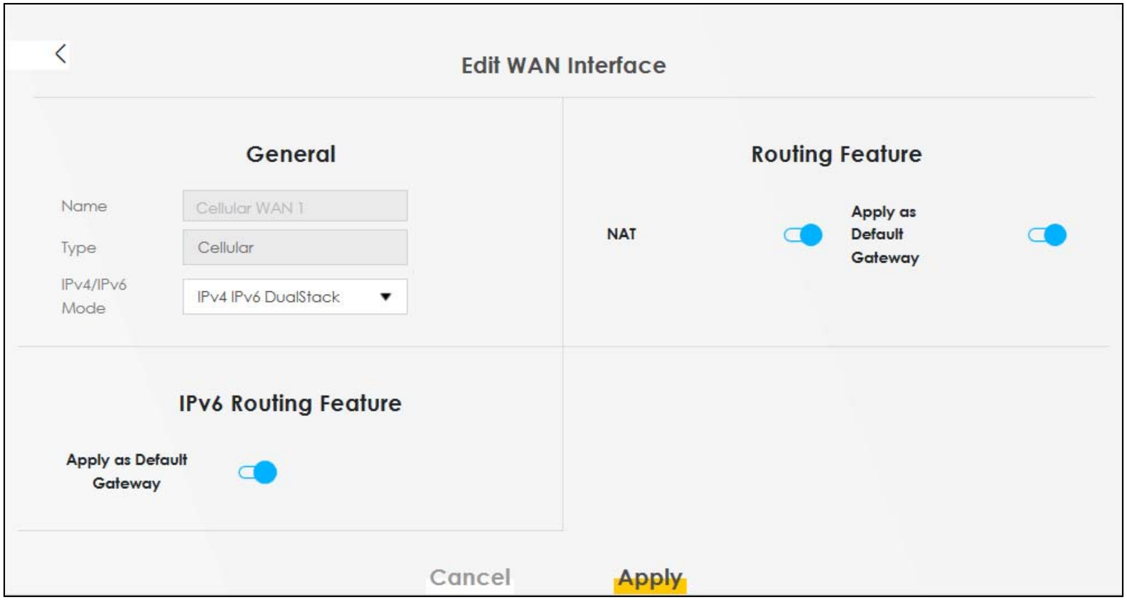
Table 13 Network Setting > Broadband

LABEL	DESCRIPTION
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is a cellular or Ethernet connection.
Mode	This shows the connection is in routing 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 its default gateway.
IPv4 Default Gateway	This shows whether the Zyxel Device use the WAN interface of this connection as its IPv4 default gateway.
IPv6 Default Gateway	This shows whether the Zyxel Device use the WAN interface of this connection as its IPv6 default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the IP Passthrough (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.

7.2.1 Add/Edit Internet Connection

Click the Edit icon (✎) next to an existing WAN interface to open the following screen. Use this screen to configure a WAN connection.

Figure 37 Network Setting > Broadband > Add/Edit New WAN Interface



Edit WAN Interface

General

Name: Cellular WAN 1

Type: Cellular

IPv4/IPv6 Mode: IPv4 IPv6 DualStack

Routing Feature

NAT: enabled

Apply as Default Gateway: enabled

IPv6 Routing Feature

Apply as Default Gateway: enabled

The following table describes the labels in this screen.

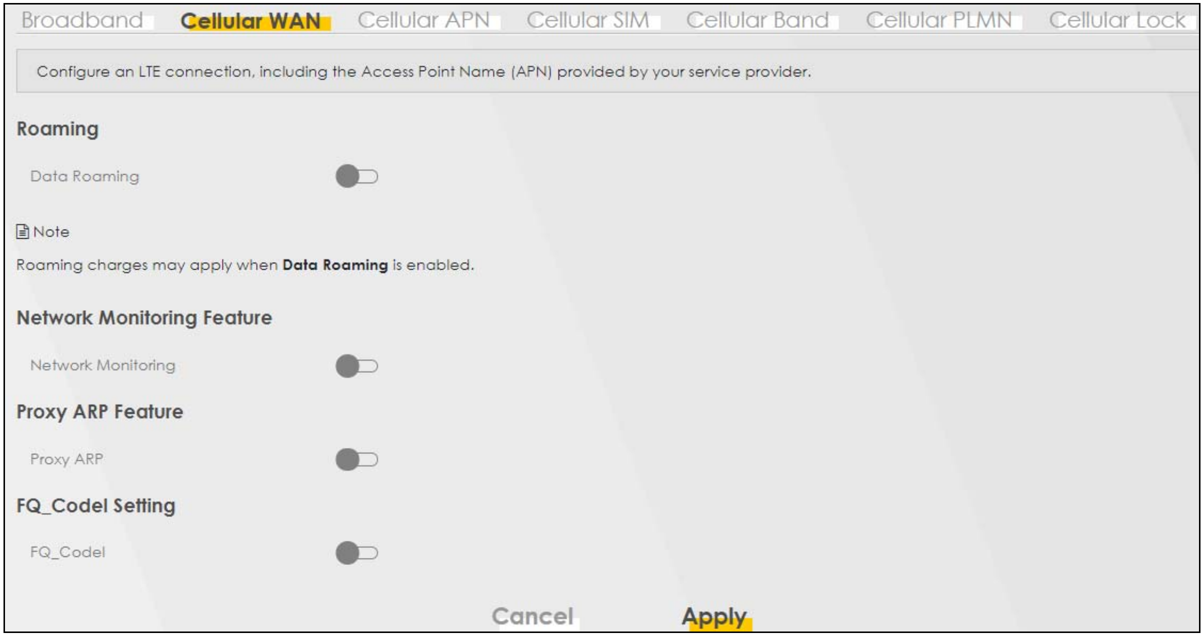
Table 14 Network Setting > Broadband > Add New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Name	This is the service name of the connection.
Type	This shows the connection type.
IPv4/IPv6 Mode	Select **IPv4 Only** if you want the Zyxel Device to run IPv4 only. Select **IPv6 Only** if you want the Zyxel Device to run IPv6 only. Select **IPv4 IPv6 DualStack** to allow the Zyxel Device to run IPv4 and IPv6 at the same time.
Routing Feature	
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.
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.
IPv6 Routing Feature	
Apply as Default Gateway	Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

7.3 Cellular WAN

Click **Network Setting > Broadband > Cellular WAN** to display the following screen. Use this screen to enable data roaming and network monitoring when the Zyxel Device cannot ping a base station.

Figure 38 Network Setting > Broadband > Cellular WAN



Configure an LTE connection, including the Access Point Name (APN) provided by your service provider.

Roaming

Data Roaming

Note

Roaming charges may apply when **Data Roaming** is enabled.

Network Monitoring Feature

Network Monitoring

Proxy ARP Feature

Proxy ARP

FQ_Codel Setting

FQ_Codel

The following table describes the labels in this screen.

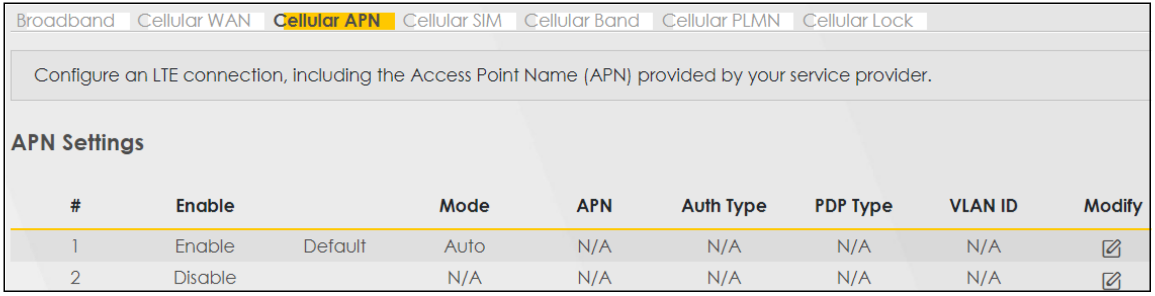
Table 15 Network Setting > Broadband > Cellular WAN

LABEL	DESCRIPTION
Roaming	
Data Roaming	Use this field to enable data roaming on the Zyxel Device. 5G roaming is to use your mobile device in an area which is not covered by your service provider. Enable roaming to ensure that your Zyxel Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Network Monitoring Feature	
Network Monitoring	Use this field to allow the Zyxel Device to try reconnecting to the base station if the cellular connection is lost. After the third try, the Zyxel Device will reboot to try to reconnect with the base station. The LED will blink red to indicate that it is rebooting. Note: This feature only works if there is a previous cellular connection between the Zyxel Device and the base station.
Proxy ARP Feature	
Proxy ARP	Enable this to set your Zyxel Device as a server to handle ARP queries from different subnets. The Zyxel Device will offer Zyxel Device's own MAC address as an reply.
FQ_Codel Setting	
FQ_Codel	Use Fair Queuing with Controlled Delay (FQ_Codel) to reduce delays in traffic that could affect real-time communications, such as video conferencing, live streaming, and Voice over Internet phone calls. FQ_Codel limits traffic throughput, by dropping traffic so as to reduce buffer queuing that causes delays. It does not prioritize traffic by type. Select this field to enable **FQ_Codel** on the Zyxel Device. Clear this field if your network does not have much real-time traffic.
Cancel	Click this to exit this screen without saving.
Apply	Click this to save your changes.

7.4 Cellular APN

Click **Network Setting > Broadband > Cellular APN** to display the following screen. Configure a cellular connection, including the Access Point Name (APN) provided by your service provider.

Figure 39 Network Setting > Broadband > Cellular APN



Configure an LTE connection, including the Access Point Name (APN) provided by your service provider.

APN Settings

#	Enable		Mode	APN	Auth Type	PDP Type	VLAN ID	Modify
1	Enable	Default	Auto	N/A	N/A	N/A	N/A	✎
2	Disable		N/A	N/A	N/A	N/A	N/A	✎

The following table describes the labels in this screen.

Table 16 Network Setting > Broadband > Cellular APN

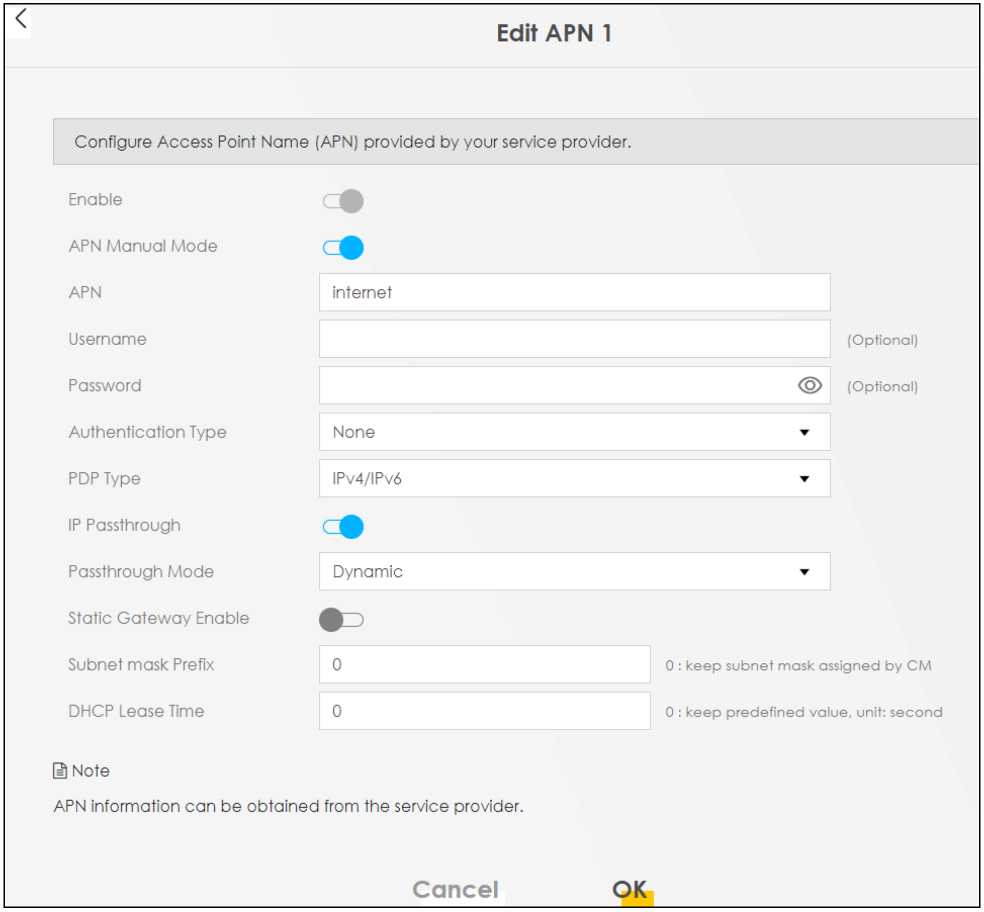
LABEL	DESCRIPTION
APN Settings	
#	This is the number of an individual APN.
Enable	This indicates whether the APN is enabled or disabled.
Mode	This shows **Auto** when the Zyxel Device configures the APN of a cellular network automatically. This shows **Manual** when the APN is entered manually.
APN	This shows the APN.
Auth Type	This shows **PAP** (Password Authentication Protocol) when peers identify themselves with a user name and password. This shows **CHAP** (Challenge Handshake Authentication Protocol) when additionally to a user name and password, the Zyxel Device sends regular challenges to make sure an intruder has not replaced a peer. This shows **PAP/CHAP** when either type of authentication can be used. This shows **None** when no authentication is used.
PDP Type	This shows **IPv4** when the Zyxel Device runs IPv4 (Internet Protocol version 4 addressing system) only. This shows **IPv4/IPv6** when the Zyxel Device runs IPv4 and IPv6 (Internet Protocol version 4 and 6 addressing system) at the same time.
VLAN ID	This shows the VLAN ID for the APN.
Modify	Click the **Edit** icon (✎) to configure cellular.

7.4.1 Edit APN

Click the **Edit** icon (✎) in the **Cellular APN** screen. Use this screen to configure a cellular connection, including the Access Point Name (APN) provided by your service provider.

Note: APN information can be obtained from the service provider.

Figure 40 Network Setting > Broadband > Cellular APN > Edit APN



Edit APN 1

Configure Access Point Name (APN) provided by your service provider.

Enable	○	
APN Manual Mode	●	
APN	internet	
Username		(Optional)
Password		(Optional)
Authentication Type	None	
PDP Type	IPv4/IPv6	
IP Passthrough	●	
Passthrough Mode	Dynamic	
Static Gateway Enable	○	
Subnet mask Prefix	0	0 : keep subnet mask assigned by CM
DHCP Lease Time	0	0 : keep predefined value, unit: second

Note

APN information can be obtained from the service provider.

The following table describes the fields in this screen.

Table 17 Network Setting > Broadband > Cellular APN > Edit APN

LABEL	DESCRIPTION
Enable	Click this to enable (●) the APN on the Zyxel Device.
APN Manual Mode	Disable this to have the Zyxel Device configure the APN of a cellular network automatically. Otherwise, Click this to enable (●) and enter the APN manually in the field below.
APN	This field allows you to display the APN in the profile. Enter the APN provided by your service provider. Connections with different APNs may provide different services (such as Internet access or Multi-Media Messaging Service (MMS)) and charging method. You can enter up to 30 printable ASCII characters. Spaces are allowed.
Username	This field allows you to display the user name in the profile. Type the user name (up to 31 printable ASCII characters) given to you by your service provider.
Password	This field allows you to set the password in the profile. Type the password (up to 31 printable ASCII characters) associated with the user name above.

Table 17 Network Setting > Broadband > Cellular APN > Edit APN (continued)

LABEL	DESCRIPTION
Authentication Type	Select the type of authentication method peers use to connect to the Zyxel Device in cellular connections. In Password Authentication Protocol (**PAP**) peers identify themselves with a user name and password. In Challenge Handshake Authentication Protocol (**CHAP**) additionally to user name and password the Zyxel Device sends regular challenges to make sure an intruder has not replaced a peer. Otherwise select **PAP/CHAP** or **None**.
PDP Type	Select **IPv4** if you want the Zyxel Device to run IPv4 (Internet Protocol version 4 addressing system) only. Select **IPv6** if you want the Zyxel Device to run IPv6 (Internet Protocol version 6 addressing system) only. Select **IPv4/IPv6** if you want the Zyxel Device to run both IPv4 and IPv6 (Internet Protocol version 4 and 6 addressing system) at the same time.
IP Passthrough	Enable this to use the default Router mode. Otherwise, click this to disable (●) to use the IP Passthough mode and enter the below fields.
Passthrough Mode	Select **Dynamic** to allow traffic to be forwarded to the first LAN computer on the local network of the Zyxel Device. Select **Fixed** to specify a LAN computer (for example, Client A) by entering its MAC address. Note: This field will show upon enabling **IP Passthrough** in the previous field.
Static Gateway Enable	Disable this to use static gateway. Otherwise, click this to enable (●) to use the IP Passthough mode and enter the below fields. Note: This field will show upon enabling **IP Passthrough** in the previous field.
Subnet Mask Prefix	Enter the subnet mask prefix of your gateway. A subnet mask prefix is another form to present a subnet mask. Convert a subnet mask address into binary. Count the "1"s in the subnet mask. "/" + the number of "1"s would be the subnet mask prefix. For example, the prefix of the subnet mask 255.255.255.0 is "/24". Note: This field will show upon enabling **IP Passthrough** in the previous field.
DHCP Lease Time	This field allows you to set the DHCP lease time. DHCP server leases an address to a new device for a period of time, called the DHCP lease time. Note: This field will show upon enabling **IP Passthrough** in the previous field.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

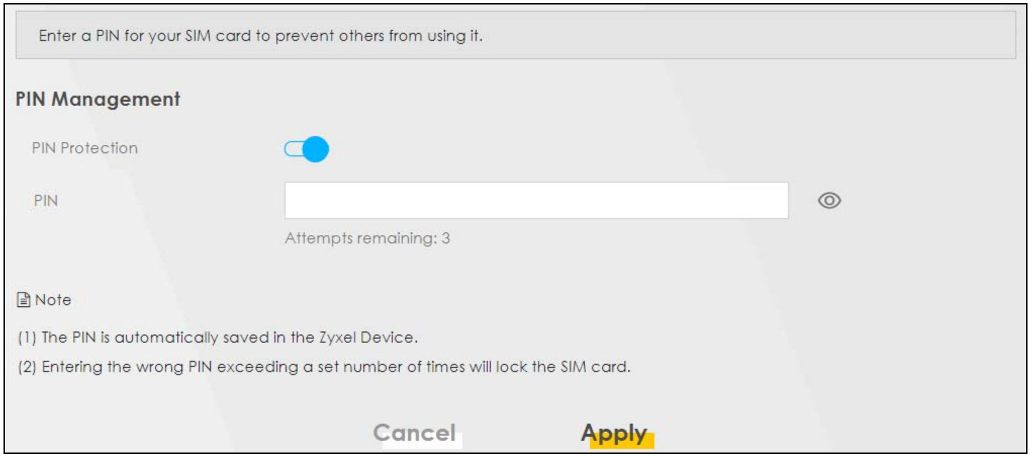
7.5 Cellular SIM Configuration

Enter a Personal Identification Number (PIN) for your SIM card to prevent others from using it.

Entering the wrong PIN code 3 consecutive times locks the SIM card, after which you need a PUK (Personal Unlocking Key) from the service provider to unlock it.

Click **Network Setting > Broadband > Cellular SIM**. The following screen opens.

Figure 41 Network Setting > Broadband > Cellular SIM



Enter a PIN for your SIM card to prevent others from using it.

PIN Management

PIN Protection

PIN

Attempts remaining: 3

Note

(1) The PIN is automatically saved in the Zyxel Device.

(2) Entering the wrong PIN exceeding a set number of times will lock the SIM card.

Note: The PIN is automatically saved in the Zyxel Device.
Entering the wrong PIN exceeding a set number of times will lock the SIM card.

The following table describes the fields in this screen.

Table 18 Network Setting > Broadband > Cellular

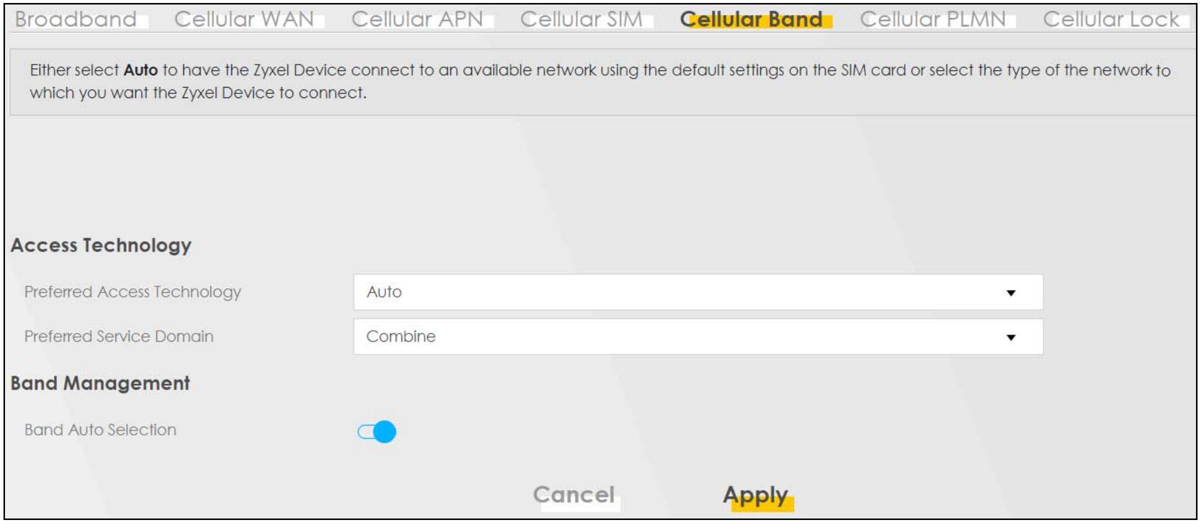
LABEL	DESCRIPTION
PIN Management	
PIN Protection	A PIN code is a key to a SIM card. It is a protection to the SIM card. Some ISPs require you to enter a PIN to use a SIM card. Click to enable (●) if you want the SIM to use a PIN lock. Click to disable if you want to remove the PIN lock on the SIM card. Note: You will be asked to enter a PIN the first time you log into the Web Configurator.
PIN Modification	
more...	Click this ^ to show more fields in this section. Click this ˅ to hide them. Note: **PIN modification** and its following fields will show upon enabling **PIN Protection** in the previous field.
New PIN	Enter a 4-digit code to set as the new PIN code. Note: This field will show upon clicking the ^.
PIN	If you enabled PIN verification, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly too many times, the ISP may block your SIM card and not let you use the account to access the Internet.
Attempts Remaining	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card. If your ISP locks your SIM card, you will need to request a PUK code from them to unlock it.
Cancel	Click **Cancel** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes.

7.6 Cellular Band Configuration

Either select **Auto** to have the Zyxel Device connect to an available network using the default settings on the SIM card or select the type of the mobile network to which you want the Zyxel Device to connect.

Click **Network Setting > Broadband > Cellular Band**. The following screen opens.

Figure 42 Network Setting > Broadband > Cellular Band



Either select **Auto** to have the Zyxel Device connect to an available network using the default settings on the SIM card or select the type of the network to which you want the Zyxel Device to connect.

Access Technology

Preferred Access Technology: Auto

Preferred Service Domain: Combine

Band Management

Band Auto Selection

The following table describes the fields in this screen.

Table 19

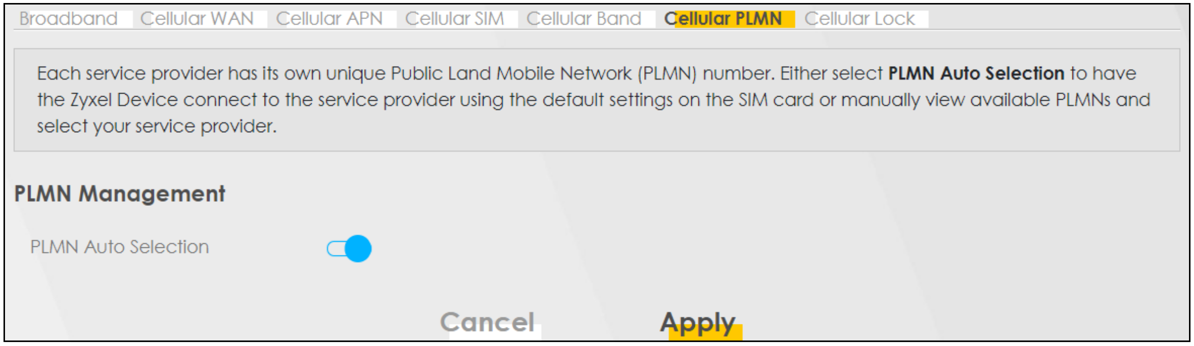
LABEL	DESCRIPTION
Access Technology	
Preferred Access Technology	Select the Access Technology which you want the Zyxel Device to use and click **Apply** to save your settings. Otherwise, select **Auto** to have the Zyxel Device connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the Zyxel Device switches to another available mobile network.
Preferred Service Domain	Choose the service domain you want to use in the mobile network. The CS (Circuit Switching) domain handles voice calls. The PS (Packet Switching) domain handles data sessions. Choose **Combine** to use both PS (Packet Switching) and CS (Circuit Switching) domain. Choose **PS only** to use only the PS domain.
Band Management	
Band Auto Selection	Click to enable (●) automatic frequency band selection as provided by your service provider. Otherwise, click to disable and select the cellular bands to use for the Zyxel Device's WAN connection.
Cancel	Click this to exit this screen without saving.
Apply	Click this to save your changes.

7.7 Cellular PLMN Configuration

Each service provider has its own unique Public Land Mobile Network (PLMN) number. Either select **PLMN Auto Selection** to have the Zyxel Device connect to the service provider using the default settings on the SIM card or manually view available PLMNs and select your service provider.

Click **Network Setting > Broadband > Cellular PLMN**. The screen appears as shown next.

Figure 43 Network Setting > Broadband > Cellular PLMN



Each service provider has its own unique Public Land Mobile Network (PLMN) number. Either select **PLMN Auto Selection** to have the Zyxel Device connect to the service provider using the default settings on the SIM card or manually view available PLMNs and select your service provider.

PLMN Management

PLMN Auto Selection

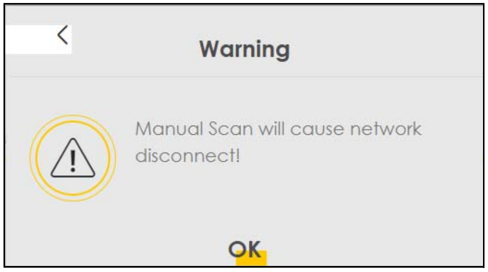
The following table describes the labels in this screen.

Table 20 Network Setting > Broadband > Cellular PLMN

LABEL	DESCRIPTION
PLMN Management	
PLMN Auto Selection	Click to enable (●) and have the Zyxel Device automatically connect to the first available mobile network. Select disabled to display the network list and manually select a preferred network.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

After selecting to disable the following warning appears. Click **OK** to continue.

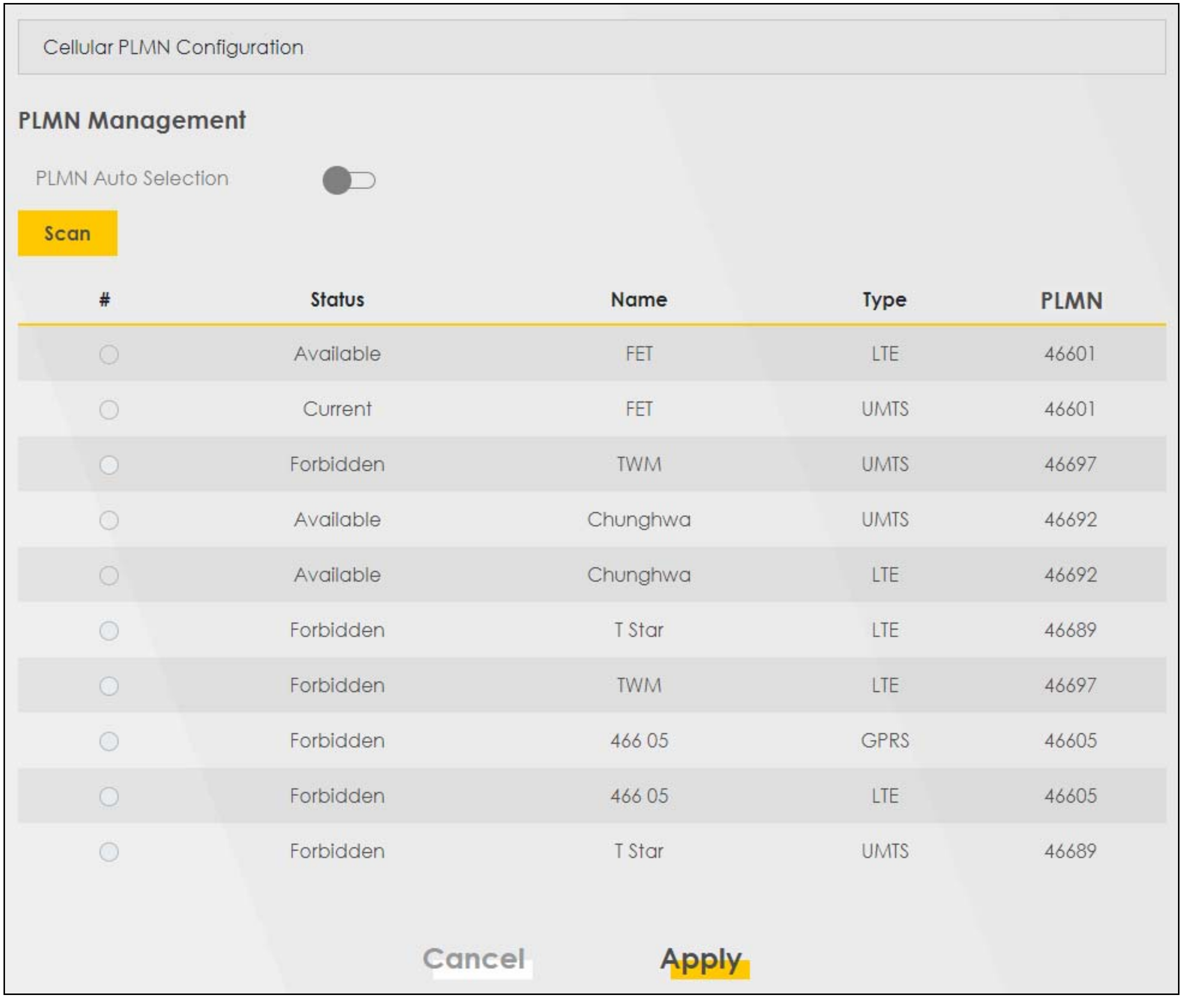
Figure 44 Network Setting > Broadband > Cellular PLMN > Manual Scan Warning



Manual Scan will cause network disconnect!

Click **Scan** to check for available PLMNs in the area surrounding the Zyxel Device, and then display the in the network list. Select from the network list and click **Apply**.

Figure 45 Network Setting > Broadband > Cellular PLMN > Scan



#	Status	Name	Type	PLMN
○	Available	FET	LTE	46601
○	Current	FET	UMTS	46601
○	Forbidden	TWM	UMTS	46697
○	Available	Chunghwa	UMTS	46692
○	Available	Chunghwa	LTE	46692
○	Forbidden	T Star	LTE	46689
○	Forbidden	TWM	LTE	46697
○	Forbidden	466 05	GPRS	46605
○	Forbidden	466 05	LTE	46605
○	Forbidden	T Star	UMTS	46689

The following table describes the labels in this screen.

Table 21 Network Setting > Broadband > Cellular PLMN > Scan

LABEL	DESCRIPTION
#	Click the radio button so the Zyxel Device connects to this ISP.
Status	This shows **Current** to show the ISP the Zyxel Device is currently connected to. This shows **Forbidden** to indicate the Zyxel Device cannot connect to this ISP. This shows **Available** to indicate an available ISP your Zyxel Device can connect to.
Name	This shows the ISP name.
Type	This shows the type of network the ISP provides.
PLMN	This shows the PLMN number.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

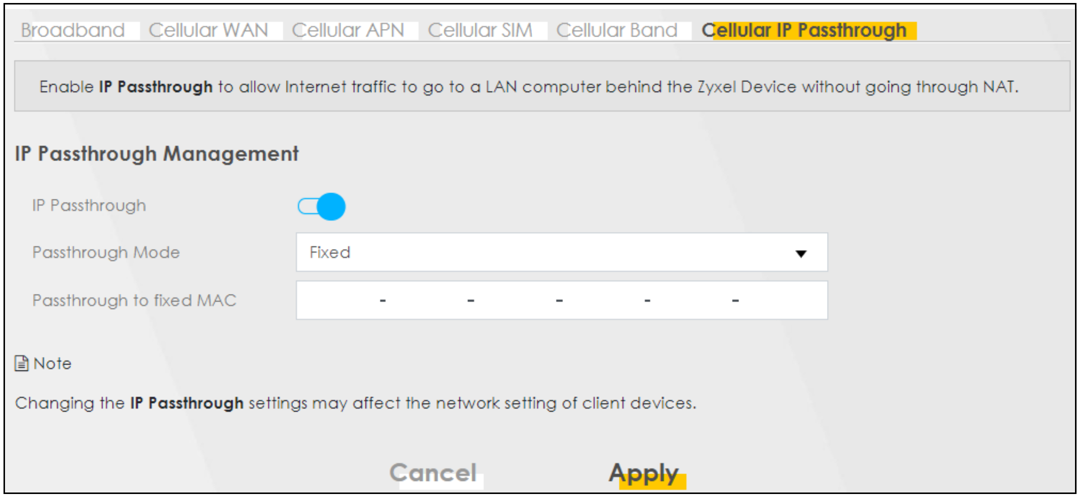
Select from the network list and click **Apply**.

7.8 Cellular IP Passthrough

Enable **IP Passthrough** to allow Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT.

Click **Network Setting > Broadband > Cellular IP Passthrough** to display the following screen.

Figure 46 Network Setting > Broadband > Cellular IP Passthrough



Enable **IP Passthrough** to allow Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT.

IP Passthrough Management

IP Passthrough: On

Passthrough Mode: Fixed

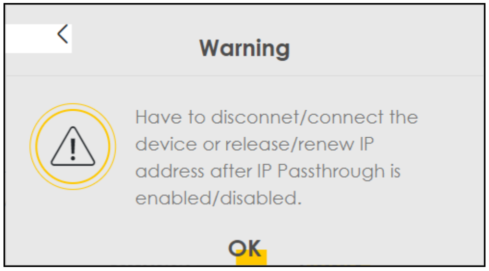
Passthrough to fixed MAC: - - - - -

Note

Changing the **IP Passthrough** settings may affect the network setting of client devices.

Note: Changing the **IP Passthrough** settings may affect the network setting of client devices. After selecting to enable the following warning appears. Click **OK** to continue.

Figure 47 Network Setting > Broadband > Cellular IP Passthrough > Enable Warning



Have to disconnet/connect the device or release/renew IP address after IP Passthrough is enabled/disabled.

The following table describes the fields in this screen.

Table 22 Network Setting > Broadband > IP Passthrough

LABEL	DESCRIPTION
IP Passthrough Management	
IP Passthrough	IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
Passthrough Mode	Select **Dynamic** to allow traffic to be forwarded to the first LAN computer on the local network of the Zyxel Device. Select **Fixed** to specify a computer (for example, Client A) by entering its MAC address. Note: This field will show upon enabling **IP Passthrough** in the previous field.

Table 22 Network Setting > Broadband > IP Passthrough (continued)

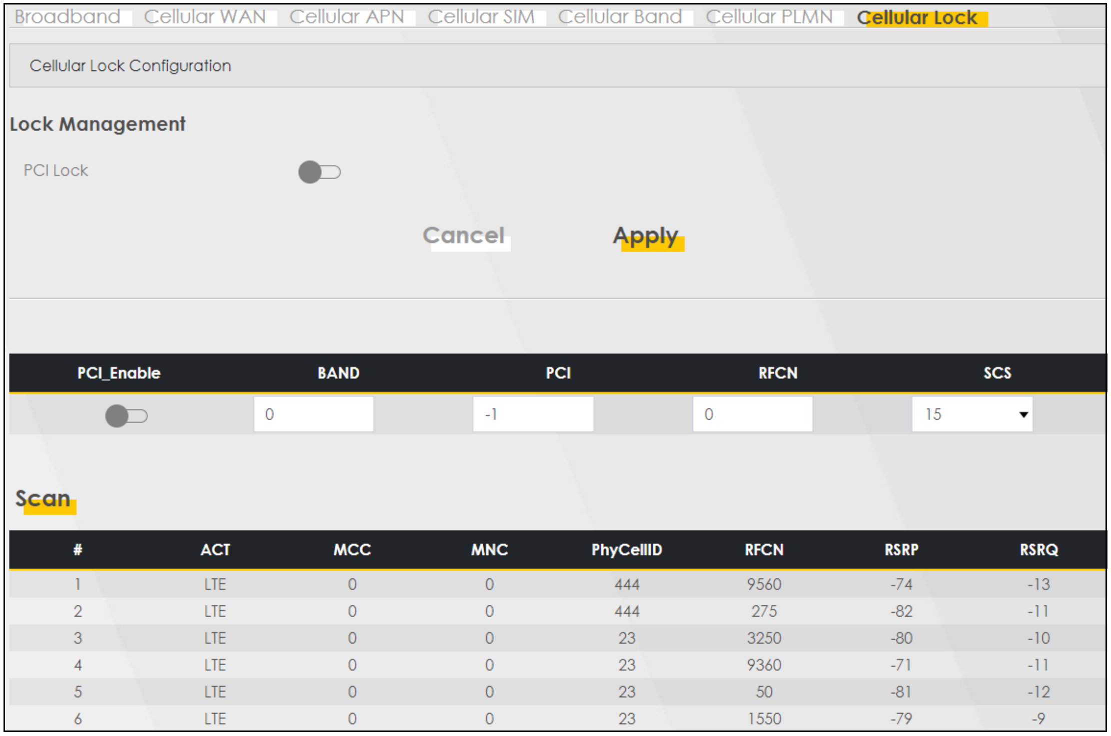
LABEL	DESCRIPTION
Passthrough to fixed MAC	Enter the MAC address of a LAN computer on the local network of the Zyxel Device upon selecting **Fixed** in the previous field. Note: This field will show upon selecting **Fixed** in the previous field.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

7.9 Cellular Lock

Use cellular lock (PCI lock) to not let the Zyxel Device connect to other base stations than the one it is currently connected to. This is useful if the Zyxel Device is within range of multiple base stations, and you would prefer the Zyxel Device to connect to one base station over the others.

Click **Network Setting** > **Broadband** > **Cellular Lock**. The following screen displays.

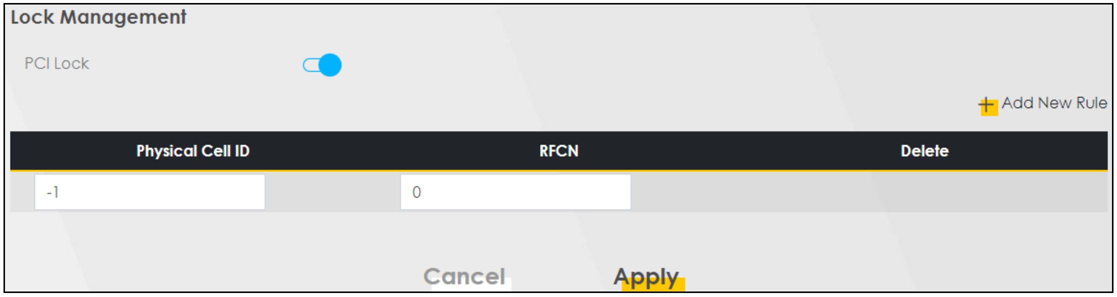
Figure 48 Network Setting > Broadband > Cellular Lock



PCI_Enable	BAND	PCI	RFCN	SCS
	0	-1	0	15

#	ACT	MCC	MNC	PhyCellID	RFCN	RSRP	RSRQ
1	LTE	0	0	444	9560	-74	-13
2	LTE	0	0	444	275	-82	-11
3	LTE	0	0	23	3250	-80	-10
4	LTE	0	0	23	9360	-71	-11
5	LTE	0	0	23	50	-81	-12
6	LTE	0	0	23	1550	-79	-9

Figure 49 Network Setting > Broadband > Cellular Lock > Add New Rule



Lock Management

PCI Lock ●

+ Add New Rule

Physical Cell ID	RFCN	Delete
-1	0	

The following table describes the fields in this screen.

Table 23 Network Setting > Broadband > Cellular Lock

LABEL	DESCRIPTION
Lock Management	
PCI Lock	Select this to enable or disable PCI (Physical Cell Identifier) Lock. Physical Cell ID (PCI) is an identifier for a cell. PCI and Radio Frequency Channel Number (RFCN) are combined to specify a cell. PCI Lock will lock your connection to the selected cell through the cell selection process. CPEs (Customer Premises Equipment) or UEs (User Equipment) do this kind of cell planning to improve users' experience on the connection.
Add New Rule	Select this if you want to add new cellular lock rules.
PCI_Enable	Enable this to set the **PCI Lock** configuration. Enter the value of **BAND, PCI, RFCN, SCS** fields. This can allow you to configure a wider range of PCI Locks.
BAND	Select the band for the PCI Lock.
PCI	Enter the PCI number of the cell signal selected from the scan list below.
RFCN	Enter the RFCN (Radio Frequency Channel Number) of the cell signal selected from the scan list below.
SCS	This shows a Service Capability Server (SCS).
Scan	
ACT	This shows the Access Technology (ACT) of the cell.
MCC	This shows the Mobile Country Code (MCC). MCC is a unique code that identifies the country where a Public Land Mobile Network (PLMN) is at.
MNC	This shows the Mobile Network Code (MNC). MNC is a unique code that identifies a Public Land Mobile Network (PLMN) in a country. MCC and MNC combined together are used to identify a globally unique PLMN.
PhyCellID	This shows the PCI of a cell. Use this to enter the PCI number of the base station you choose to connect to.
RFCN	This shows the RFCN (Radio Frequency Channel Number) of a cell signal. Use this to enter the RFCN of the base station you choose to connect to. See Section on page 64 for more information.
RSRP	This shows the RSRP value of a signal which helps you choose a network with higher quality. See Section on page 64 for more information.
RSRQ	This shows the RSRQ value of a signal which helps you choose a network with higher quality. See Section on page 64 for more information.
Cancel	Select this to not save the changes and return.
Apply	Select this to save and apply the changes.

CHAPTER 8 Wireless

8.1 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 85).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device (Section 8.3 on page 88).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 8.4 on page 90).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 8.5 on page 92).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 8.6 on page 93).

8.1.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there are a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See Section 8.7 on page 95 for advanced technical information on WiFi networks.

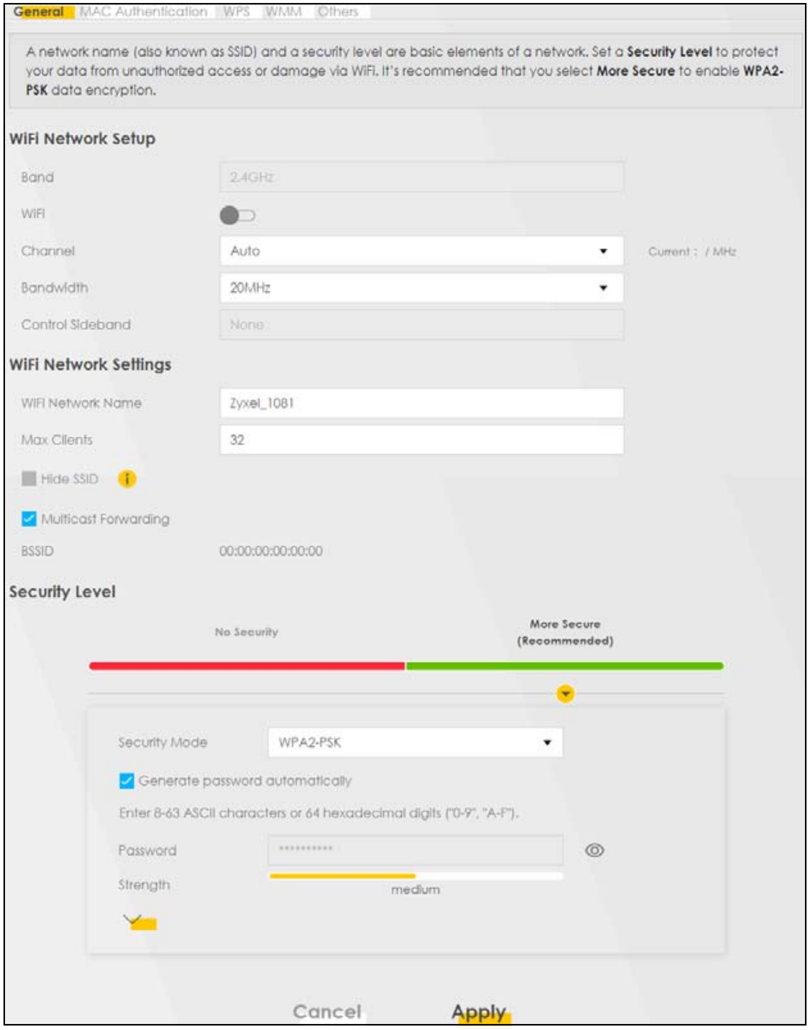
8.2 General Settings

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secured** for **WPA2-PSK** 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 wireless connection when you press **Apply**. You must change the wireless settings of your computer to match the new settings on the Zyxel Device.

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

Figure 50   Network Setting > Wireless > General



A network name (also known as SSID) and a security level are basic elements of a network. Set a **Security Level** to protect your data from unauthorized access or damage via WiFi. It's recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

WiFi Network Setup

Band	2.4GHz
WiFi	○
Channel	Auto ▾ — Current : / MHz
Bandwidth	20MHz ▾
Control Sideband	None

WiFi Network Settings

WiFi Network Name	Zyxel_1081
Max Clients	32

□ Hide SSID

☑ Multicast Forwarding

BSSID 00:00:00:00:00:00

Security Level

Security Mode WPA2-PSK ▾

☑ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password **********

Strength medium

The following table describes the general wireless LAN labels in this screen.

Table 24   Network Setting > Wireless > General

LABEL	DESCRIPTION
WiFi Network Setup	
Band	This shows the band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n clients.

Table 24 Network Setting > Wireless > General (continued)

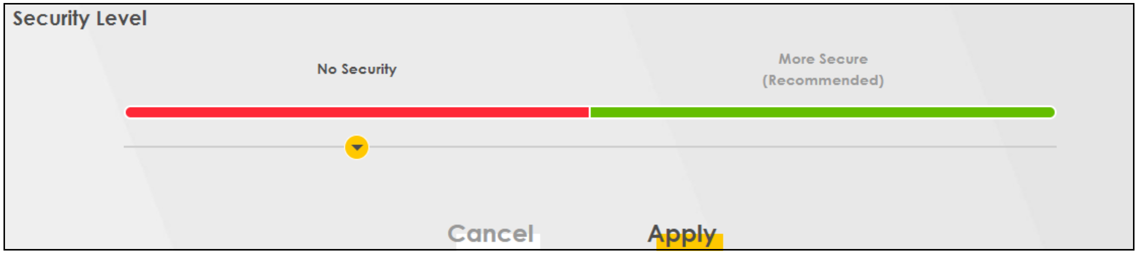
LABEL	DESCRIPTION
WiFi	Click **Enable** to enable the wireless LAN in this field.
Channel	Use **Auto** to have the Zyxel Device automatically determine a channel to use. Otherwise, select a channel you want to use from the drop list.
Bandwidth	Select whether the Zyxel Device uses a WiFi channel width of **20MHz**, **40MHz** or **20/40MHz**. The available options will be shown in the drop list. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40MHz. It is often better to use the 20MHz setting in a location where the environment hinders the WiFi signal. Select **20MHz** if you want to lessen radio interference with other WiFi devices in your neighborhood or the WiFi clients do not support channel bonding.
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
WiFi Network Settings	
WiFi Network Name	The SSID (Service Set IDentity) 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 (up to 32 English keyboard characters) for the wireless LAN.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This check box is grayed out if the WPS function is enabled in the **Network** > **Wireless** > **WPS** screen.
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled.
Security Level	
Security Mode	Select **More Secured (WPA2-PSK)** to add security on this network. The clients which want to associate to this network must have the same 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 with 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 51 Wireless > General: No Security



Note: The following table describes the labels in this screen.

Table 25 Wireless > General: No Security

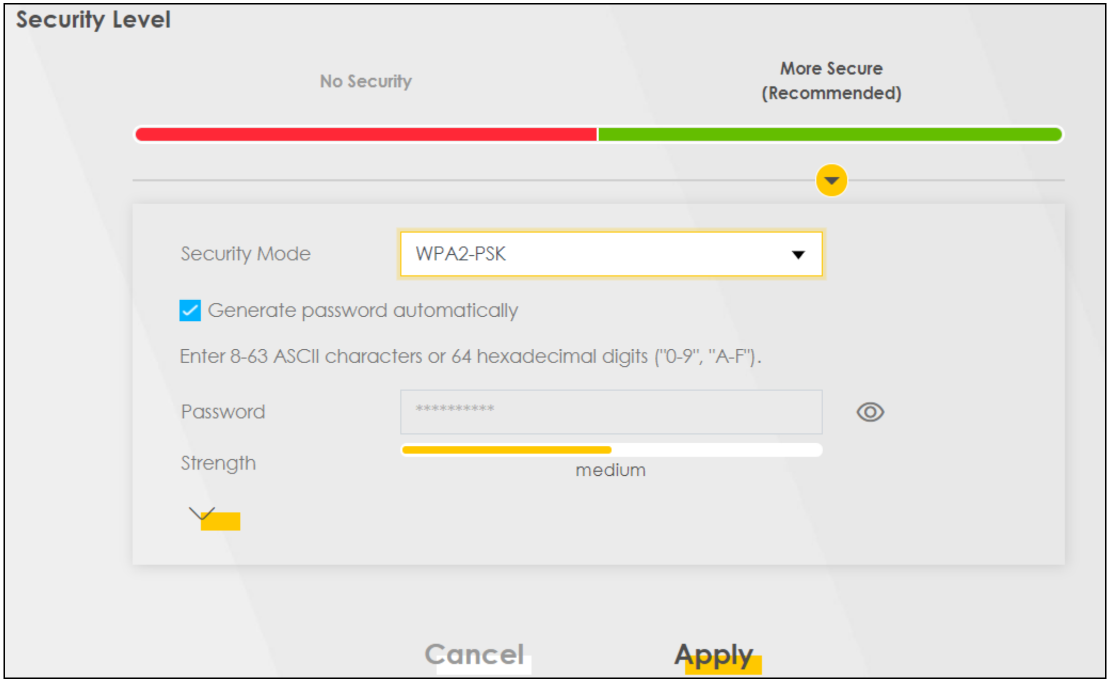
LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all connections without data encryption or authentication.

8.2.2 More Secure (WPA2-PSK)

The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be. Using a Pre-Shared Key (PSK), both the Zyxel Device and the connecting client share a common password in order to validate the connection.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. **WPA2-PSK** is the default **Security Mode**.

Figure 52 Wireless > General: More Secure: WPA2-PSK



Security Mode: WPA2-PSK

☑ Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password: ***********

Strength: medium

The following table describes the labels in this screen.

Table 26 Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA2-PSK data encryption.
Security Mode	**WPA2-PSK** is the default security mode.
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. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: Enter 8-63 ASCII characters only. 64 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.
more...	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.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

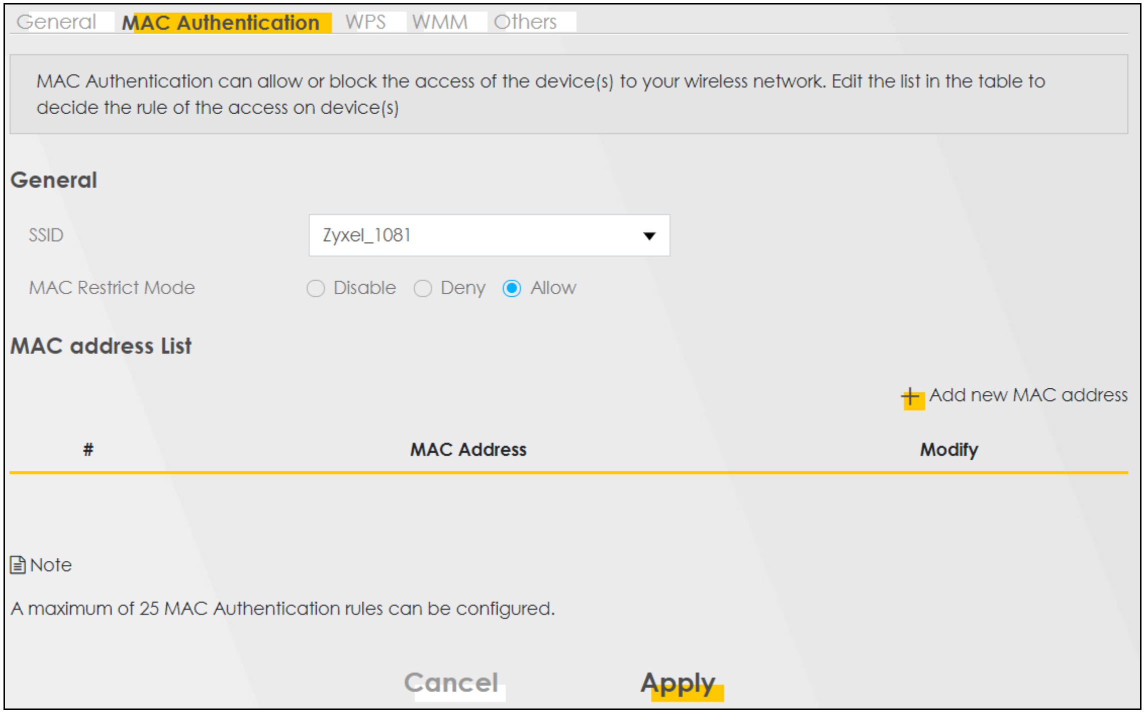
8.3 MAC Authentication

Use this screen to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Zyxel Device (**Deny**) based on the MAC address of each 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 devices you want to allow/deny to configure this 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.

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

Figure 53 Network Setting> Wireless > MAC Authentication



MAC Authentication can allow or block the access of the device(s) to your wireless network. Edit the list in the table to decide the rule of the access on device(s)

General

SSID: Zyxel_1081

MAC Restrict Mode: ○ Disable ○ Deny ● Allow

MAC address List

#	MAC Address	Modify

Note

A maximum of 25 MAC Authentication rules can be configured.

The following table describes the labels in this screen.

Table 27 Network Setting> Wireless > MAC Authentication

LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
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	
Add new MAC address	This field is available when you select **Deny** or **Allow** in the **MAC Restrict Mode** field. Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the devices that are allowed or denied 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. **Figure 54**
#	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.

Table 27 Network Setting> Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
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.

8.4 WPS

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

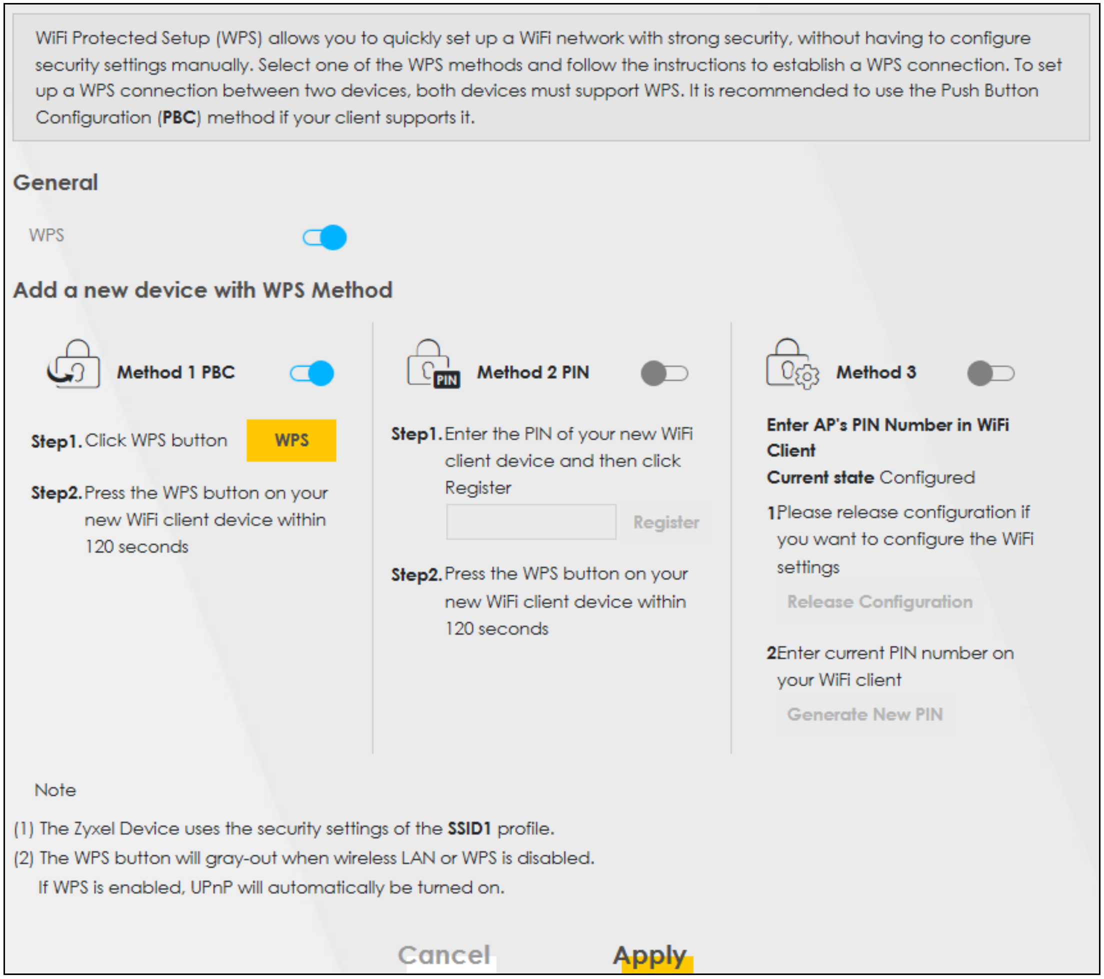
WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection. Your device must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your device supports it. See Section 8.7.7.3 on page 102 for more information about WPS.

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 87). 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 wireless LAN is disabled.

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 55 Network Setting > Wireless > WPS



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. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your client supports it.

General

WPS ●

Add a new device with WPS Method

Method 1 PBC ●

Step1. Click WPS button

Step2. Press the WPS button on your new WiFi client device within 120 seconds

Method 2 PIN ○

Step1. Enter the PIN of your new WiFi client device and then click Register

Step2. Press the WPS button on your new WiFi client device within 120 seconds

Method 3 ○

Enter AP's PIN Number in WiFi Client

Current state Configured

1 Please release configuration if you want to configure the WiFi settings

2 Enter current PIN number on your WiFi client

Note

(1) The Zyxel Device uses the security settings of the **SSID1** profile.

(2) The WPS button will gray-out when wireless LAN or WPS is disabled.
If WPS is enabled, UPnP will automatically be turned on.

The following table describes the labels in this screen.

Table 28 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Click 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 WiFi 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 WiFi device (within WiFi range of the Zyxel Device) to your WiFi network. This button may either be a physical button on the outside of a device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other WiFi device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS WiFi network by entering the PIN of the client into the Zyxel Device. Click this switch to make it turn blue. Click **Apply** to activate WPS method 2 on the Zyxel Device.

Table 28 Network Setting > Wireless > WPS (continued)

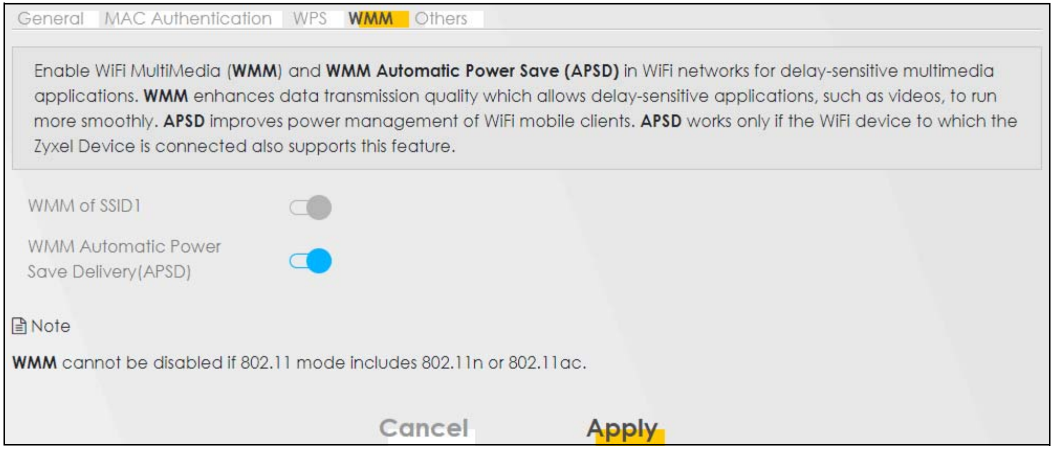
LABEL	DESCRIPTION
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the WiFi device to your WiFi network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Zyxel Device.
Method 3	Use this section to set up a WPS WiFi network by entering the PIN of the Zyxel Device into the client. Click this switch to make it turn blue. Click **Apply** to activate WPS method 3 on the Zyxel Device.
Release Configuration	The default WPS status is configured. Click this button to remove all configured WiFi and WiFi security settings for WPS connections on the Zyxel Device.
Generate New PIN	If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use the WPS push-button method. Click the **Generate New PIN** button to have the Zyxel Device create a new PIN.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.5 WMM

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

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

Figure 56 Network Setting > Wireless > WMM



Enable WiFi MultiMedia (**WMM**) and **WMM Automatic Power Save (APSD)** in WiFi networks for delay-sensitive multimedia applications. **WMM** enhances data transmission quality which allows delay-sensitive applications, such as videos, to run more smoothly. **APSD** improves power management of WiFi mobile clients. **APSD** works only if the WiFi device to which the Zyxel Device is connected also supports this feature.

WMM of SSID1

WMM Automatic Power Save Delivery(APSD)

Note

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

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

The following table describes the labels in this screen.

Table 29 Network Setting > Wireless > WMM

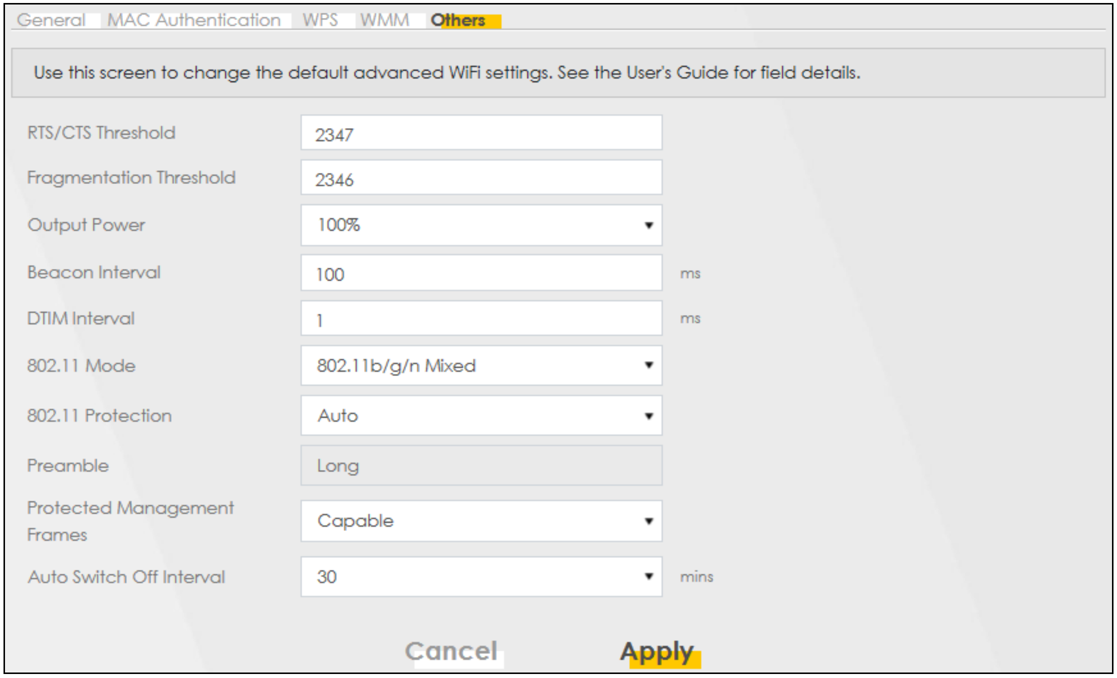
LABEL	DESCRIPTION
WMM of SSID1	Select **On** to have the Zyxel Device automatically give the network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (MultiMedia Quality of Service) gives high priority to video, which makes them run more smoothly. If the **802.11 Mode** in **Network Setting > Wireless > Others** is set to include 802.11n, WMM cannot be disabled.
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.

8.6 Others

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

See Section 8.7.2 on page 96 for detailed definitions of the terms listed here.

Figure 57 Network Setting > Wireless > Others



Use this screen to change the default advanced WiFi settings. See the User's Guide for field details.

RTS/CTS Threshold	2347	
Fragmentation Threshold	2346	
Output Power	100%	
Beacon Interval	100	ms
DTIM Interval	1	ms
802.11 Mode	802.11b/g/n Mixed	
802.11 Protection	Auto	
Preamble	Long	
Protected Management Frames	Capable	
Auto Switch Off Interval	30	mins

The following table describes the labels in this screen.

Table 30 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 50ms to 1000ms. 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.
802.11 Mode	For 2.4GHz frequency WLAN devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Zyxel Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.
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.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 8.7.6 on page 99 for more information.
Protected Management Frames	WiFi with Protected Management Frames (PMF) provides protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging. Select **Capable** if the WiFi client supports PMF, then the management frames will be encrypted. Select **Required** to force the WiFi client to support PMF; otherwise the authentication cannot be performed by the Zyxel Device. Otherwise, select **Disabled**.
Auto Switch Off	Click this to enable **Auto Switch Off** and configure the next field.
Auto Switch Off Interval	Select a time period from the drop list. WiFi will automatically switch off by the time period you selected.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.7 Technical Reference

This section discusses wireless LANs in depth.

8.7.1 WiFi Network Overview

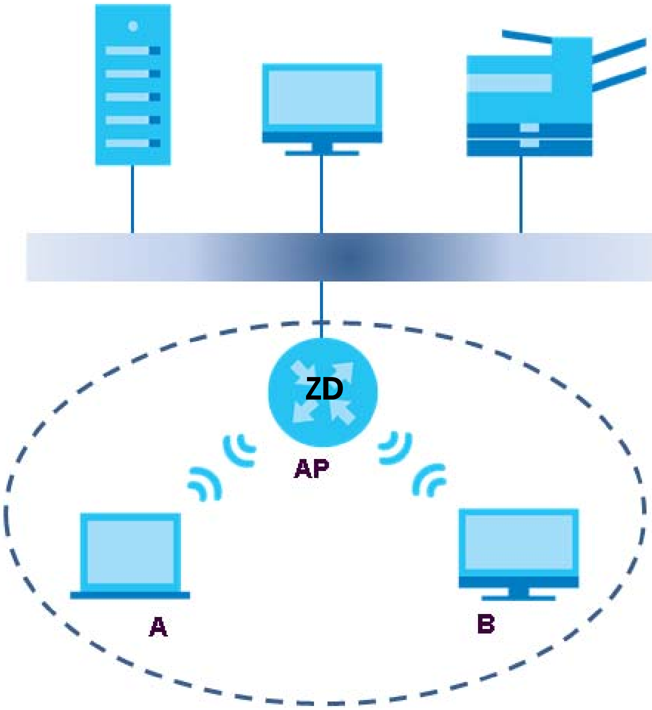
WiFi networks consist of WiFi clients, access points and bridges.

- 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 58 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. Your Zyxel Device is the AP.

Every WiFi network must follow these basic guidelines.

- Every 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 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.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of WiFi networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

8.7.2 Additional Wireless Terms

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

Table 31 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 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.

8.7.3 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's 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.

8.7.3.1 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.

8.7.3.2 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 device in the WiFi network, see the 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 device is allowed to use the WiFi network, it still has to have the correct information (SSID, channel, and security). If a 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 device. Then, they can use that MAC address to use the WiFi network.

[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.

8.7.3.3 User Authentication

Authentication is the process of verifying whether a WiFi device is allowed to use the WiFi network. You can make every user log in to the WiFi network before using it. However, every device in the WiFi network has to support IEEE 802.1x to do this.

For WiFi networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized WiFi devices can still see the information that is sent in the WiFi network, even if they cannot use the WiFi network. Furthermore, there are ways for unauthorized WiFi users to get a valid user name and password. Then, they can use that user name and password to use the WiFi network.

8.7.3.4 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 8.7.3.3 on page 98 for information about this.)

Table 32 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	WPA-PSK	
Strongest	WPA2-PSK	WPA2

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

Note: It is recommended that WiFi networks use **WPA-PSK**, **WPA**, 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.

8.7.4 Signal Problems

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

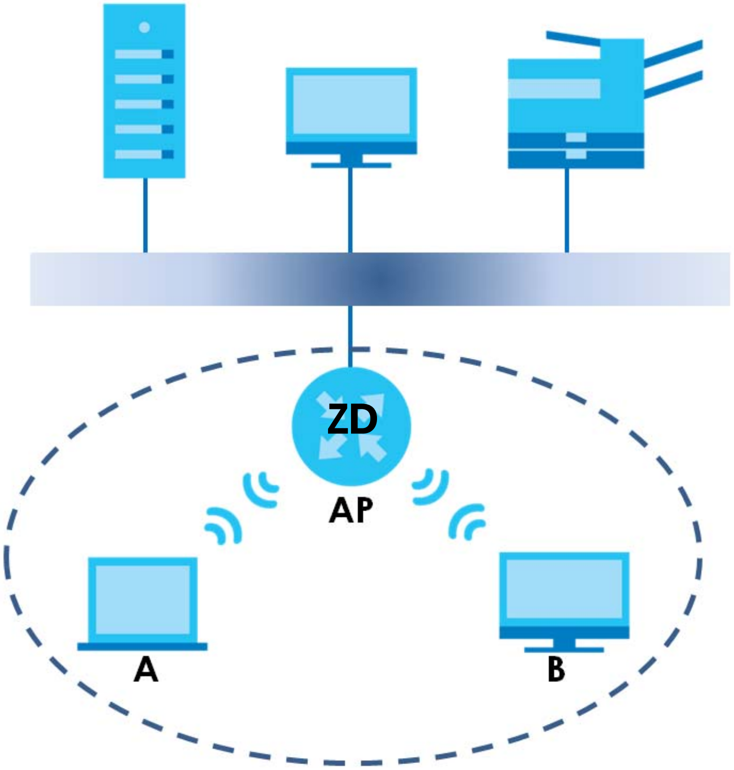
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters 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.

8.7.5 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 59 Basic Service Set



8.7.6 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 wireless 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.

8.7.7 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 two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

8.7.7.1 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 wireless 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, see Section 8.4 on page 90).

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 five seconds.

4 Within two 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.

8.7.7.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the WiFi client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

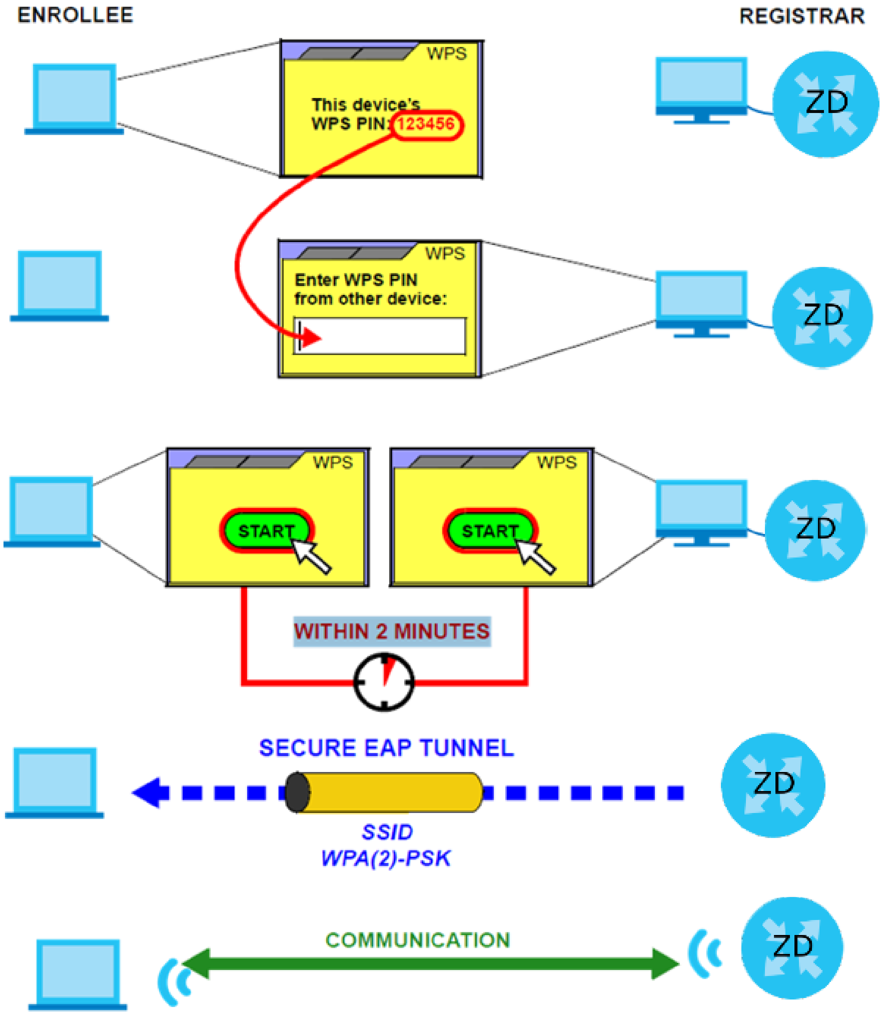
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide on how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide on how to find the WPS PIN - for the Zyxel Device, see Section 8.4 on page 90).
4. Enter the client's PIN in the AP's configuration interface.
5. If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
6. Start WPS on both devices within two minutes.
7. Use the configuration utility to activate WPS.
8. On a computer connected to the WiFi client, try to connect to the Web Configurator. If you can connect, WPS was successful.

   If you cannot connect, 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.

The following figure shows a WPS-enabled WiFi client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 60 Example WPS Process: PIN Method

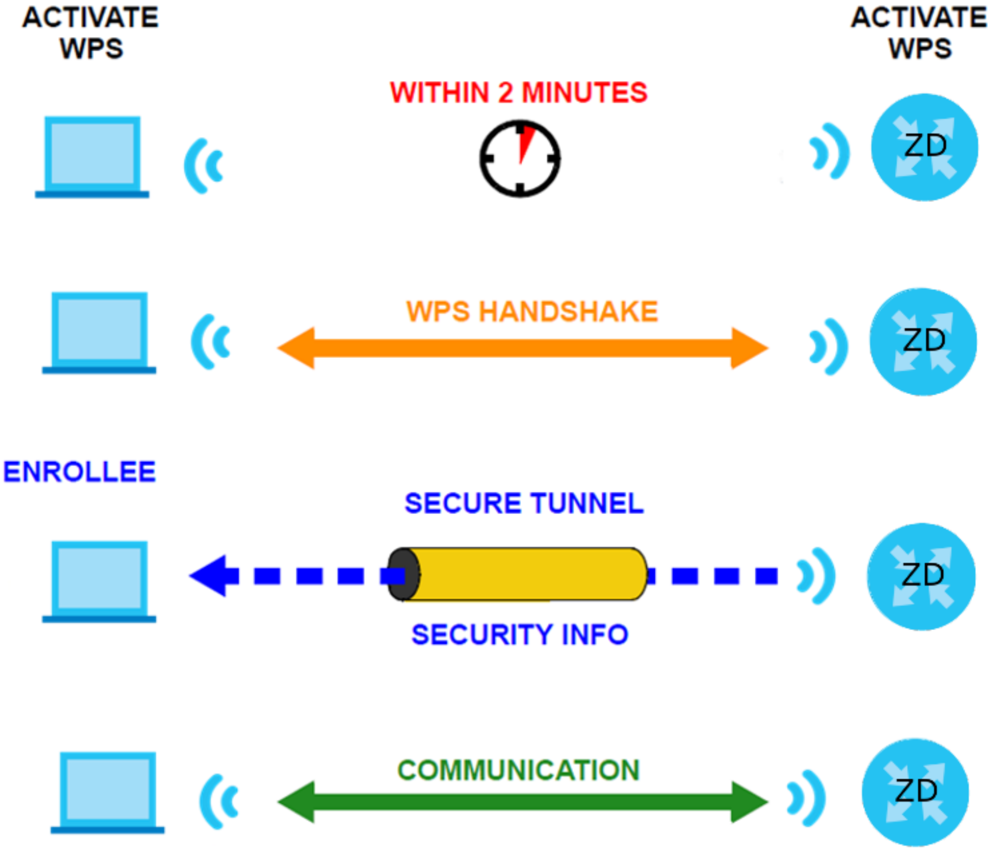


8.7.7.3 How WPS Works

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 WPA(2)-PSK randomly.

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

Figure 61 How WPS Works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two 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.

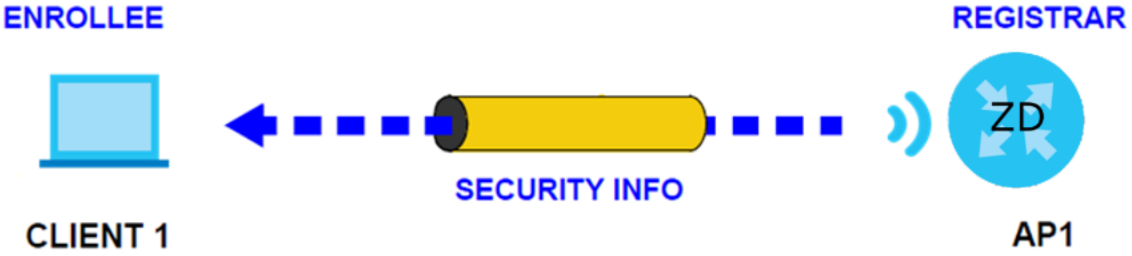
By default, a WPS device is 'unconfigured'. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled 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.

8.7.7.4 Example WPS Network Setup

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

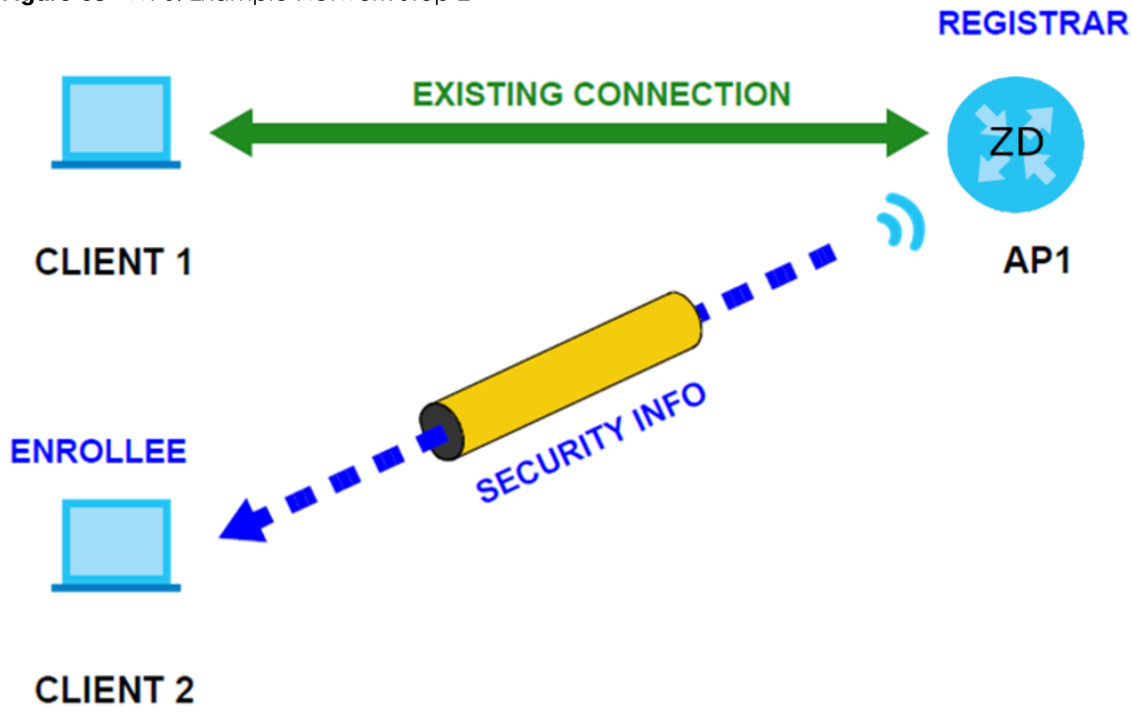
The following figure shows a sample network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 62 WPS: Example Network Step 1



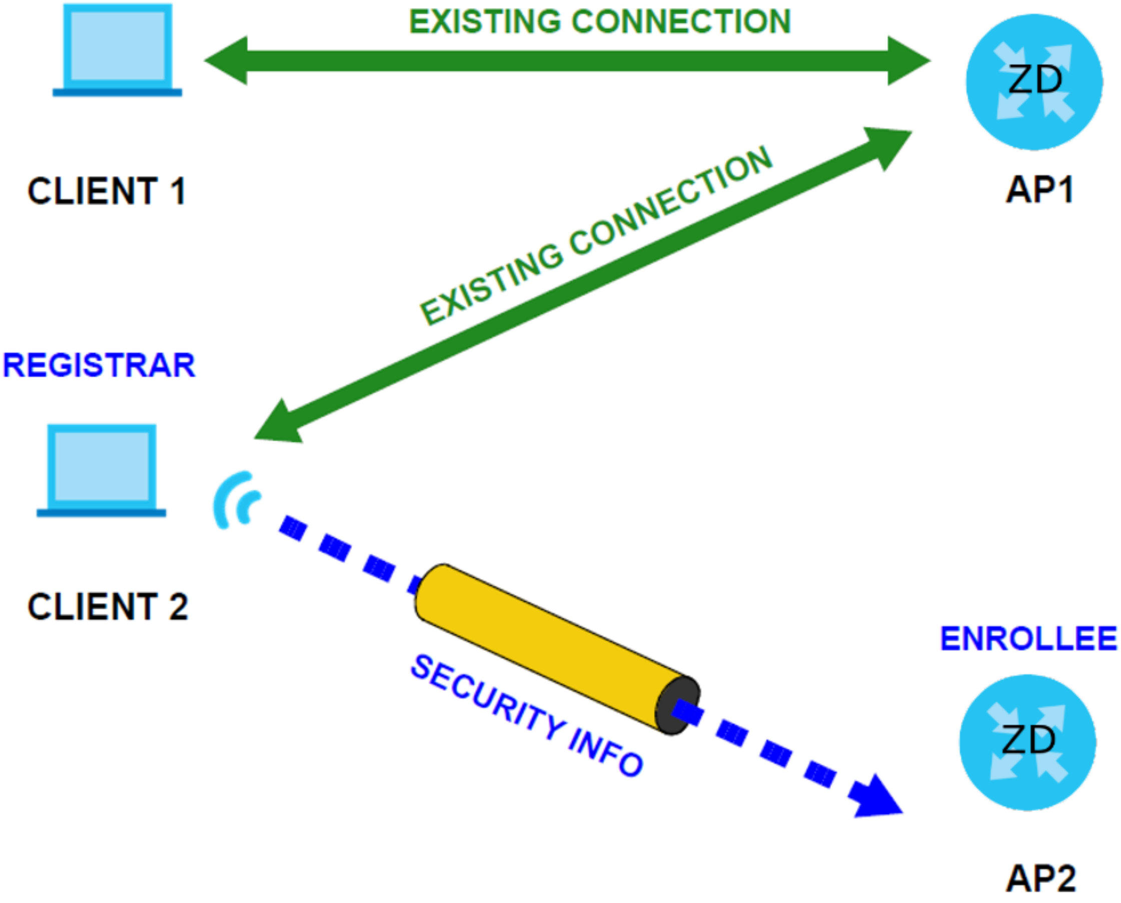
In step **2**, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 63 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 64 WPS: Example Network Step 3



8.7.7.5 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.

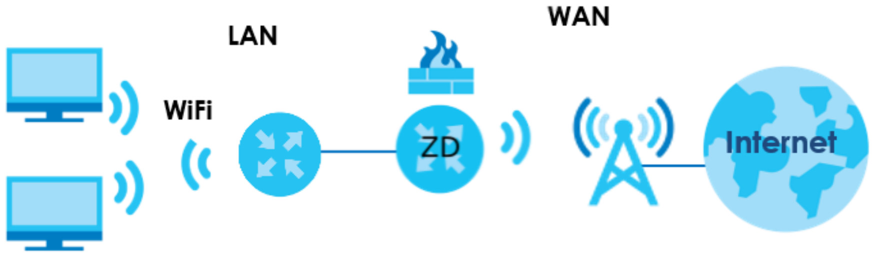
CHAPTER 9
Home Networking

9.1 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 65 Local Area Network of the Zyxel Device



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 108).
- 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 113).
- Use the **UPnP** screen to enable UPnP (Section 9.4 on page 115).

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.

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.

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). Zyxel's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

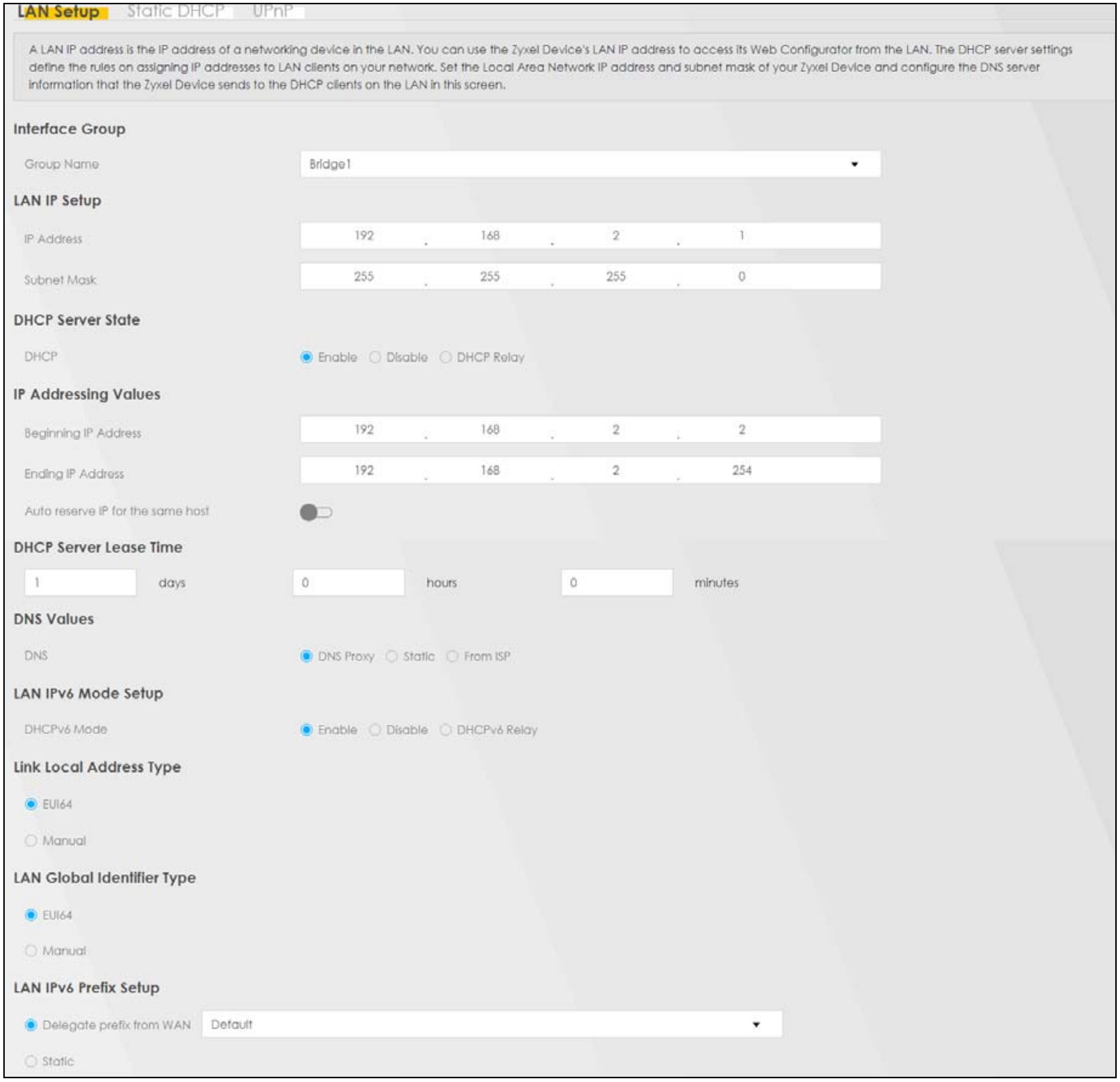
See Section 9.6 on page 117 for examples on installing and using UPnP.

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.

Figure 66 Network Setting > Home Networking > 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. Set the Local Area Network IP address and subnet mask of your Zyxel Device and configure the DNS server information that the Zyxel Device sends to the DHCP clients on the LAN in this screen.

Interface Group

Group Name: Bridge1

LAN IP Setup

IP Address: 192 . 168 . 2 . 1

Subnet Mask: 255 . 255 . 255 . 0

DHCP Server State

DHCP: ● Enable ○ Disable ○ DHCP Relay

IP Addressing Values

Beginning IP Address: 192 . 168 . 2 . 2

Ending IP Address: 192 . 168 . 2 . 254

Auto reserve IP for the same host

DHCP Server Lease Time

1 days 0 hours 0 minutes

DNS Values

DNS: ● DNS Proxy ○ Static ○ From ISP

LAN IPv6 Mode Setup

DHCPv6 Mode: ● Enable ○ Disable ○ DHCPv6 Relay

Link Local Address Type

● EUI64

○ Manual

LAN Global Identifier Type

● EUI64

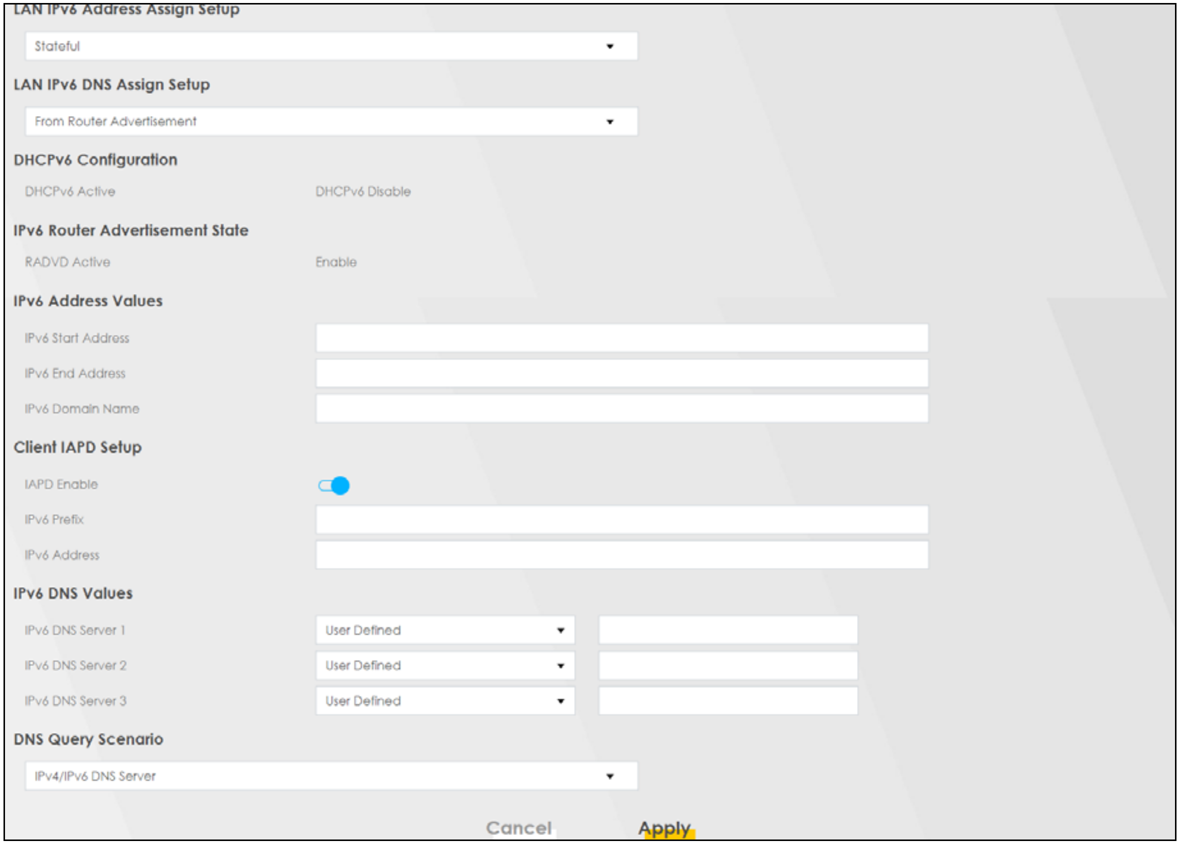
○ Manual

LAN IPv6 Prefix Setup

● Delegate prefix from WAN: Default

○ Static

Figure 67 Network Setting > Home Networking > LAN Setup (continued)



LAN IPv6 Address Assign Setup

Stateful

LAN IPv6 DNS Assign Setup

From Router Advertisement

DHCPv6 Configuration

DHCPv6 Active: DHCPv6 Disable

IPv6 Router Advertisement State

RADVD Active: Enable

IPv6 Address Values

IPv6 Start Address

IPv6 End Address

IPv6 Domain Name

Client IAPD Setup

IAPD Enable

IPv6 Prefix

IPv6 Address

IPv6 DNS Values

IPv6 DNS Server 1: User Defined

IPv6 DNS Server 2: User Defined

IPv6 DNS Server 3: User Defined

DNS Query Scenario

IPv4/IPv6 DNS Server

The following table describes the fields in this screen.

Table 33 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group that you plan to use. Usually default.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your 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. You need to additionally configure the following fields: IP Addressing Values, DHCP Server Lease Time, DNS Values. 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. You need to enter the IP address of the DHCP relay server under the below field: DHCP Relay Server Address.
DHCP Relay Server Address	
IP Address	Enter the IP address of a DHCP relay server.
IP Addressing Values	

Table 33 Network Setting > Home Networking > LAN Setup (continued)

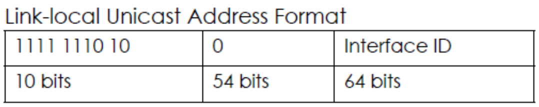
<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></tr>
<tr><td>Beginning IP Address</td><td>This field specifies the first of the contiguous addresses in the IP address pool.</td></tr>
<tr><td>Ending IP Address</td><td>This field specifies the last of the contiguous addresses in the IP address pool.</td></tr>
<tr><td>Auto reserve IP for the same host</td><td>Enable this if you want to reserve the IP address for the same host.</td></tr>
<tr><td colspan="2">DHCP Server Lease Time</td></tr>
<tr><td>Days/Hours/ Minutes</td><td>DHCP server leases an address to a new 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 device.</td></tr>
<tr><td colspan="2">DNS Values</td></tr>
<tr><td>DNS</td><td>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 <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).
Select <b>Static</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field shown upon.
Select <b>DNS Proxy</b> to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.</td></tr>
<tr><td colspan="2">LAN IPv6 Mode Setup</td></tr>
<tr><td>IPv6 Active</td><td>Use this field to <b>Enable</b> or <b>Disable</b> IPv6 activation on the Zyxel Device.
When <b>IPv6 Active</b> is enabled, the following fields show and need to be set:</td></tr>
<tr><td>DHCPv6 Mode</td><td>Select <b>Enable</b> to use the DHCPv6 mode. You will need to configure the fields starting from Link Local Address Type.
Select <b>DHCPv6 Relay</b> to set up DHCPv6 Relay server.
When <b>DHCPv6 Relay</b> is selected, the following fields show and need to be set:</td></tr>
<tr><td colspan="2">DHCPv6 Relay Server Setup</td></tr>
<tr><td>Contact Server from WAN</td><td>Specifies the interface on which messages to servers are sent. Choices are Cellular WAN1 to Cellular WAN 4.</td></tr>
<tr><td>DHCPv6 Server IP Address</td><td>Specifies the DHCPv6 server address to relay packets to.</td></tr>
<tr><td>Link Local Address Type</td><td>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 <b>EUI64</b> 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 <b>Manual</b>.

Link-local Unicast Address Format<table><tr><td>1111 1110 10</td><td>0</td><td>Interface ID</td></tr><tr><td>10 bits</td><td>54 bits</td><td>64 bits</td></tr></table></td></tr>
<tr><td>LAN Global Identifier Type</td><td>Select <b>EUI64</b> to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select <b>Manual</b> to manually enter an interface ID for the LAN interface's global IPv6 address.</td></tr>
</table>

Table 33 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
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.
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. If you select **Stateful**, you need to additionally configure the following fields: IPv6 address values, Client IAPD Setup.
IPv6 address values	
IPv6 Start Address	This field specifies the first of the contiguous addresses in the IPv6 address pool.
IPv6 End Address	This field specifies the last of the contiguous addresses in the IPv6 address pool.
IPv6 Domain Name	The field specifies the domain name of the IPv6 address.
Client IAPD Setup	
IAPD Enable	Identity Association for Prefix Delegation (IAPD) is an IPv6 prefix set assigned to a requesting device. Each IAPD identifies an interface configured by DHCPv6. A device may have more than one IAPD due to multiple interfaces. Click this to enable and configure the following fields.
IPv6 Prefix	Enter the IPv6 prefix assigned by the DHCPv6 server.
IPv6 Address	Enter the IPv6 address assigned by the DHCPv6 server.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: **From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements. **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.
DHCPv6 Configuration	**DHCPv6 Active** shows the status of the DHCPv6. **DHCPv6 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	**RADVD Active** 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.

Table 33 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
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.

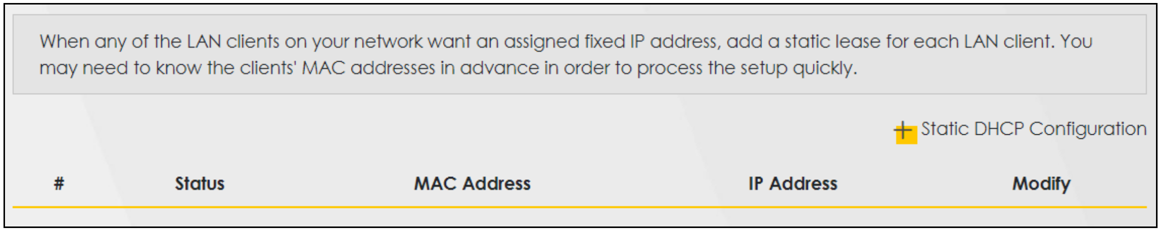
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

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 68 Network Setting > Home Networking > Static DHCP



When any of the LAN clients on your network want an assigned fixed IP address, add a static lease for each LAN client. You may need to know the clients' MAC addresses in advance in order to process the setup quickly.

#	Status	MAC Address	IP Address	Modify

The following table describes the labels in this screen.

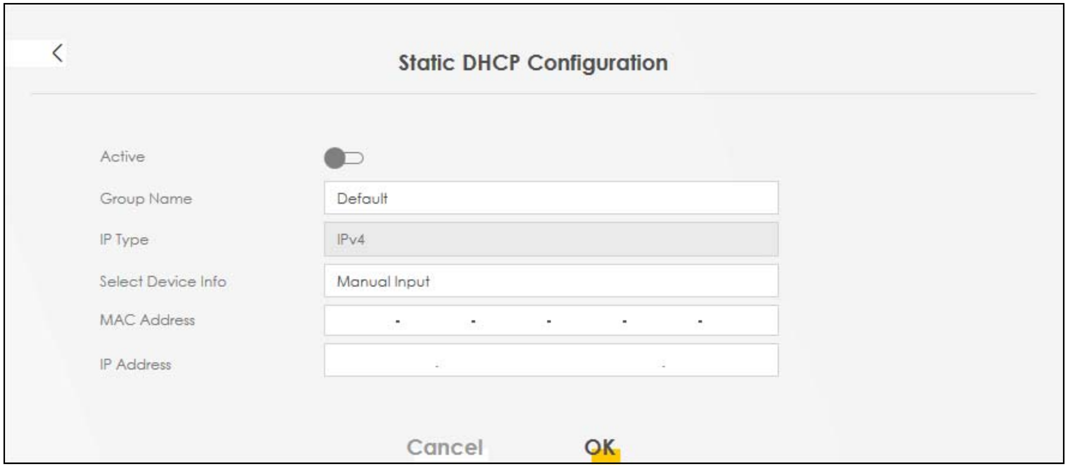
Table 34 Network Setting > Home Networking > Static DHCP

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 delete the fixed IP address assigned.

Using a static DHCP means a client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a device by selecting the interface group of this device and its IP address type and selecting the device/computer from a list or manually entering its MAC address and assigned IP address.

If you click **Static DHCP Configuration** in the **Static DHCP** screen, the following screen displays.

Figure 69 Static DHCP: Static DHCP Configuration



Static DHCP Configuration

Active: ○

Group Name: Default

IP Type: IPv4

Select Device Info: Manual Input

MAC Address: . . . . .

IP Address: . .

The following table describes the labels in this screen.

Table 35 Static DHCP: Configuration

LABEL	DESCRIPTION
Active	Enable static DHCP in your
Group Name	This displays the interface group your want to use, usually **Default**.
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 selecting an existing
MAC Address	Enter the MAC address of a computer on your LAN if you select **Manual Input** in the previous field.

Table 35 Static DHCP: Configuration

LABEL	DESCRIPTION
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

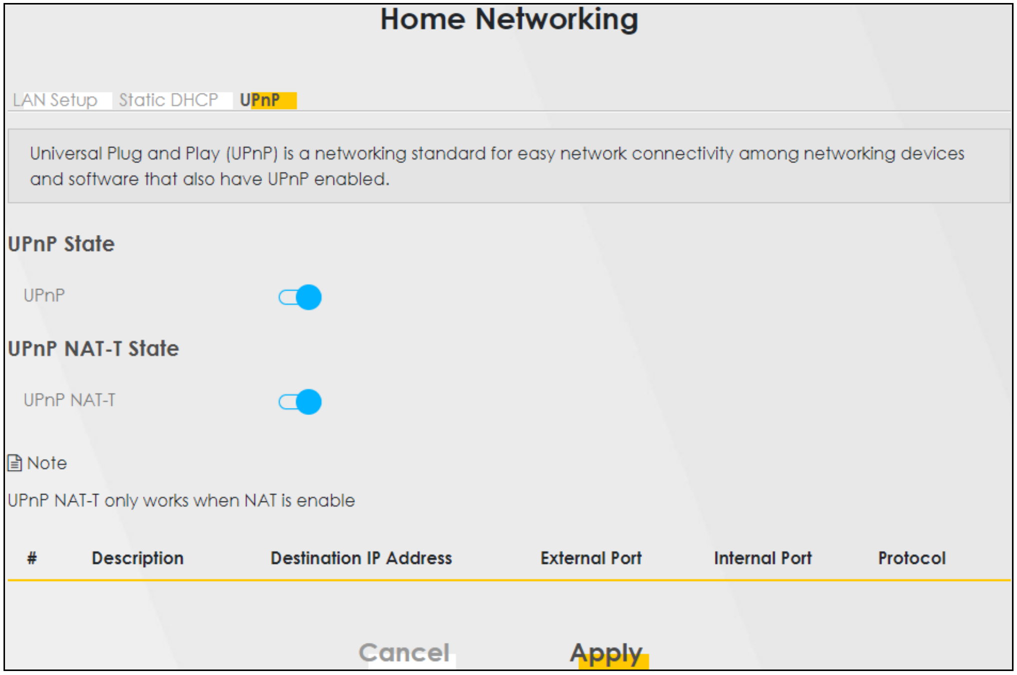
Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn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

See Section 9.6 on page 117 for more information on UPnP.

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.

Note: UPnP NAT-T only works when NAT is enabled.

Figure 70 Network Setting > Home Networking > UPnP



Universal Plug and Play (UPnP) is a networking standard for easy network connectivity among networking devices and software that also have UPnP enabled.

UPnP State

UPnP ●

UPnP NAT-T State

UPnP NAT-T ●

Note

UPnP NAT-T only works when NAT is enable

#	Description	Destination IP Address	External Port	Internal Port	Protocol

The following table describes the labels in this screen.

Table 36 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 (TCP or UDP).
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

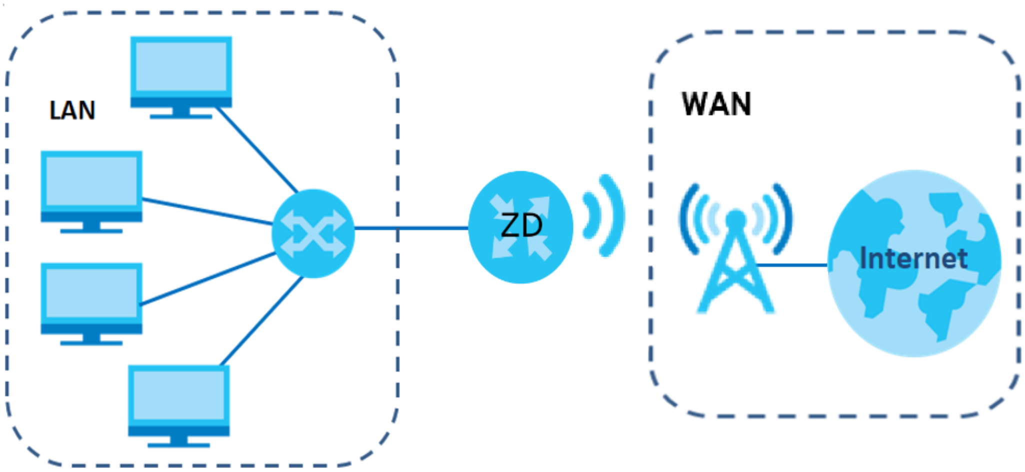
9.5 Technical Reference

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 71 LAN and WAN IP Addresses



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.

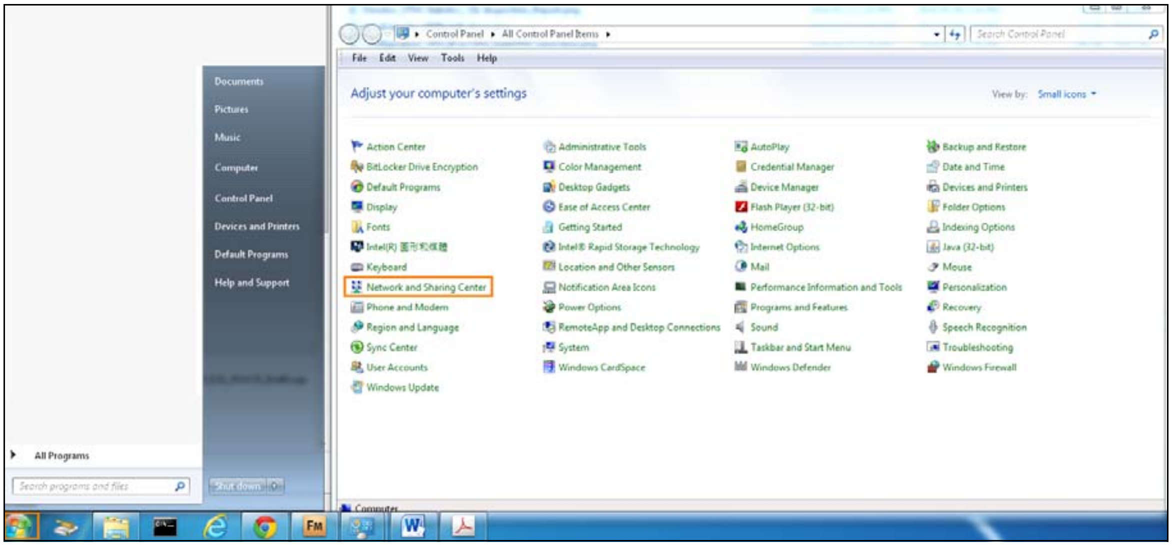
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space."

9.6 Turn on UPnP in Windows 7 Example

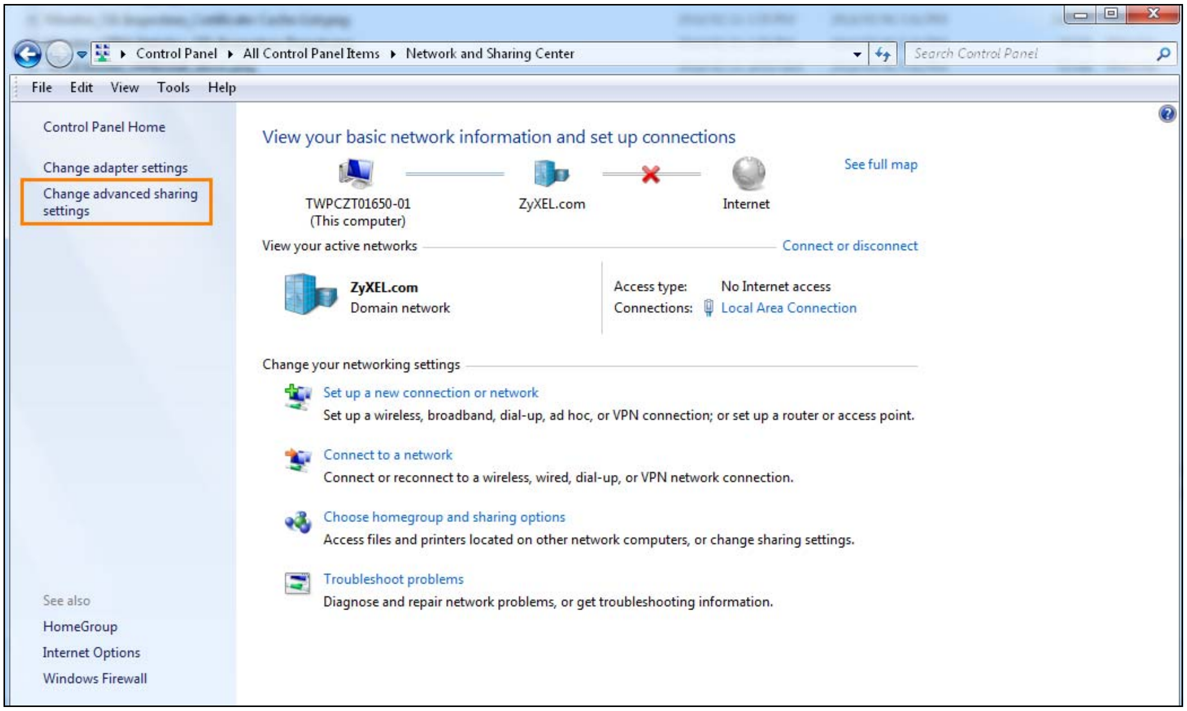
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device by clicking **Network Setting > Home Networking > UPnP**.

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, **Control Panel** and then the **Network and Sharing Center.**



2 Click **Change Advanced Sharing Settings**.



View your basic network information and set up connections

View your active networks

ZyXEL.com
Domain network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

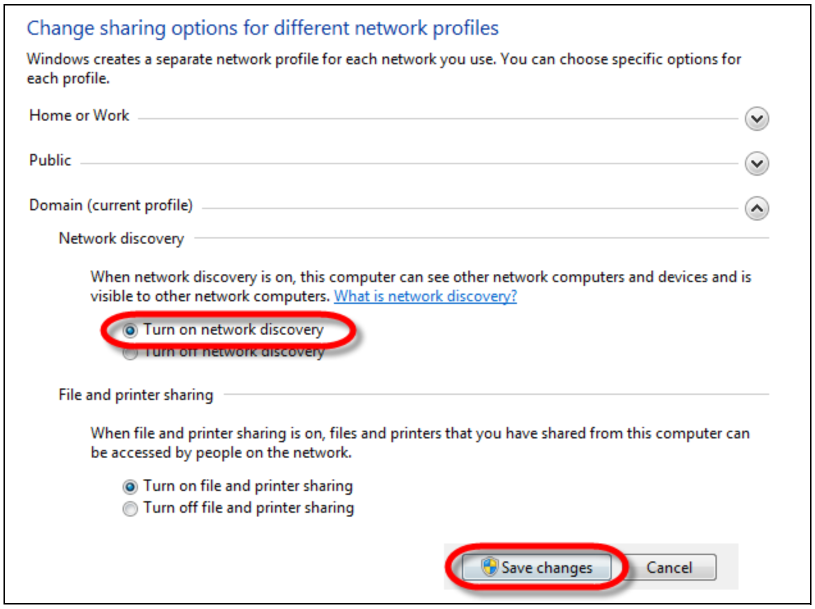
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3 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.



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public

Domain (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

9.6.1 Auto-discover Your UPnP-enabled Network Device

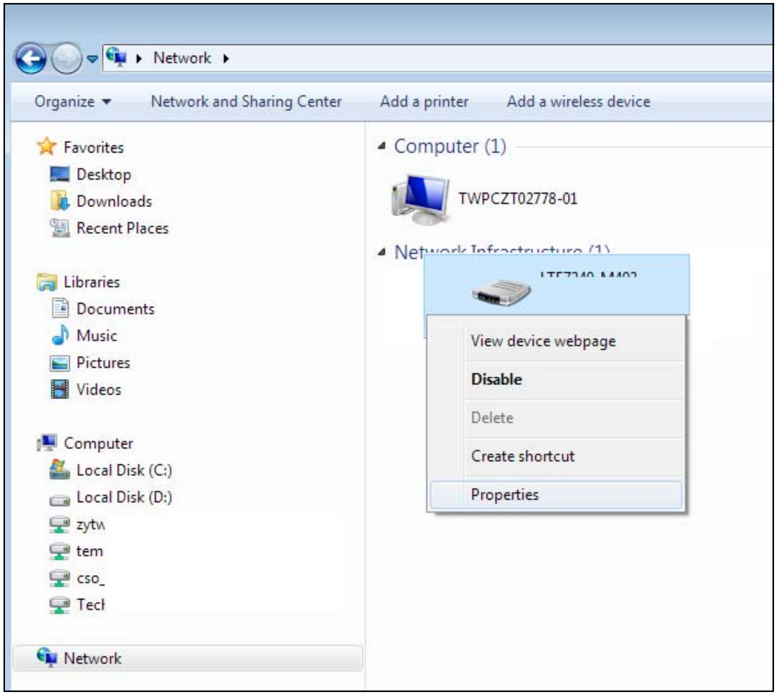
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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

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

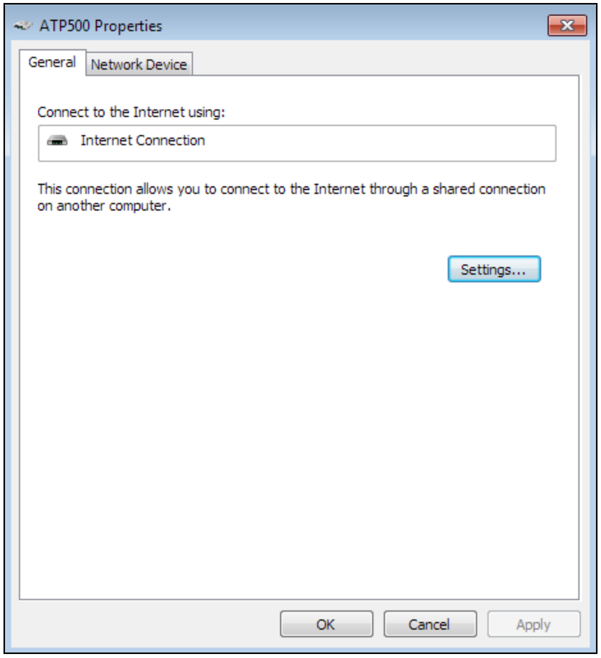
2 Right-click the Zyxel Device icon and select **Properties**.

Figure 72 Network Connections



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

Figure 73 Internet Connection Properties



ATP500 Properties

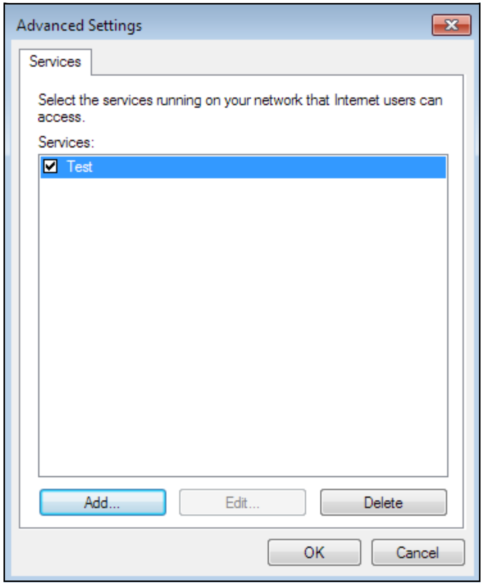
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

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

Figure 74 Internet Connection Properties: Advanced Settings



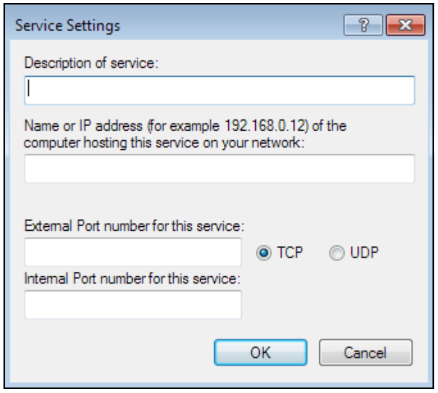
Advanced Settings

Select the services running on your network that Internet users can access.

Services:

☑ Test

Figure 75 Internet Connection Properties: Advanced Settings: Add



Service Settings

Description of service:

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:

External Port number for this service:

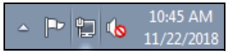
● TCP ○ UDP

Internal Port number for this service:

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

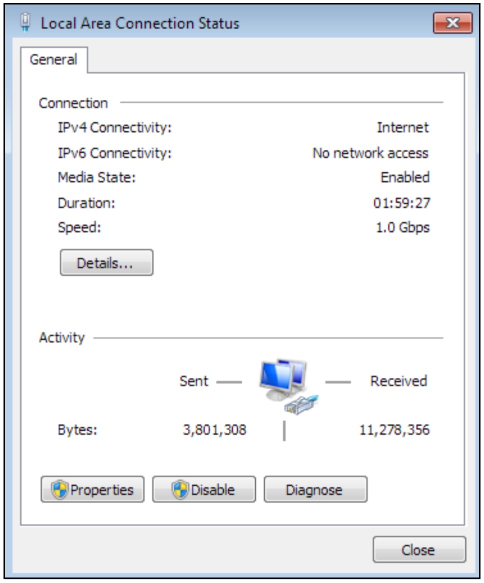
5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 76 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 and Sharing Center**. Click **Local Area Network**.

Figure 77 Internet Connection Status



Local Area Connection Status

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	01:59:27
Speed:	1.0 Gbps

Activity

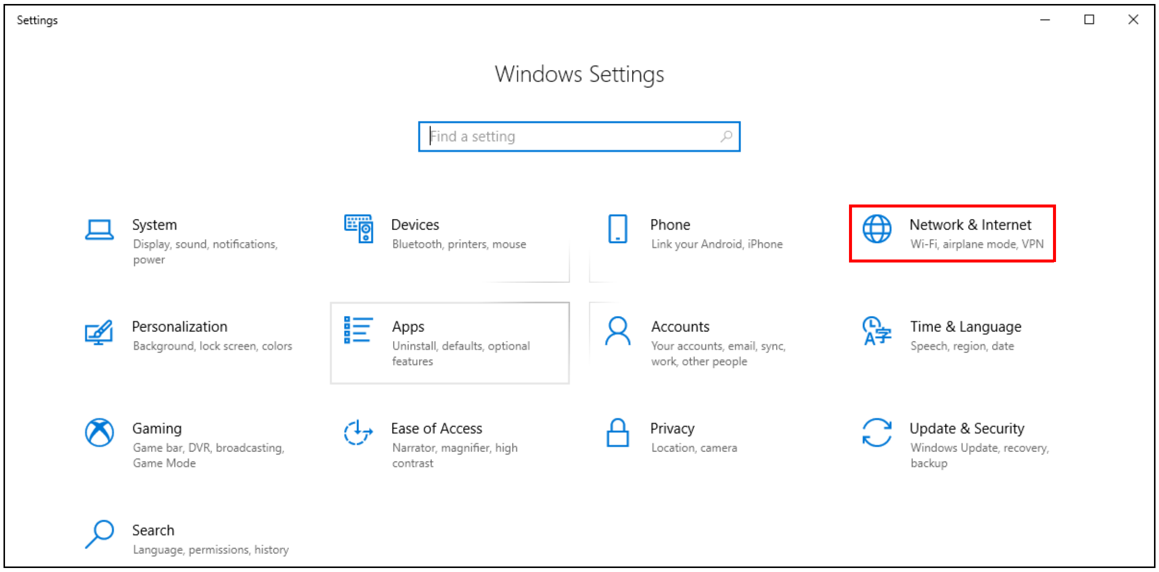
	Sent	Received
Bytes:	3,801,308	11,278,356

9.7 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**.



Settings

Windows Settings

Find a setting

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Phone
Link your Android, iPhone

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, other people

Time & Language
Speech, region, date

Gaming
Game bar, DVR, broadcasting, Game Mode

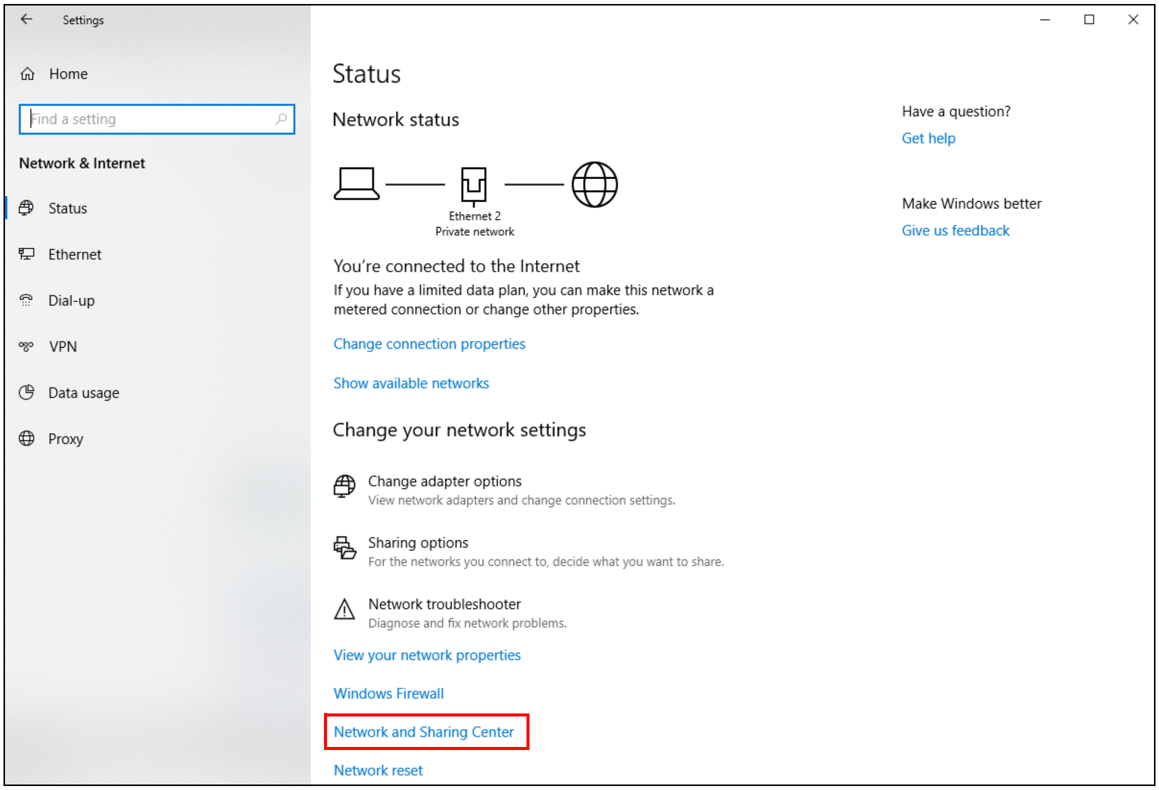
Ease of Access
Narrator, magnifier, high contrast

Privacy
Location, camera

Update & Security
Windows Update, recovery, backup

Search
Language, permissions, history

2 Click **Network and Sharing Center**.



Settings

Home

Find a setting

Network & Internet

Status

Ethernet

Dial-up

VPN

Data usage

Proxy

Status

Network status

You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Change connection properties

Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.

Sharing options
For the networks you connect to, decide what you want to share.

Network troubleshooter
Diagnose and fix network problems.

View your network properties

Windows Firewall

Network and Sharing Center

Network reset

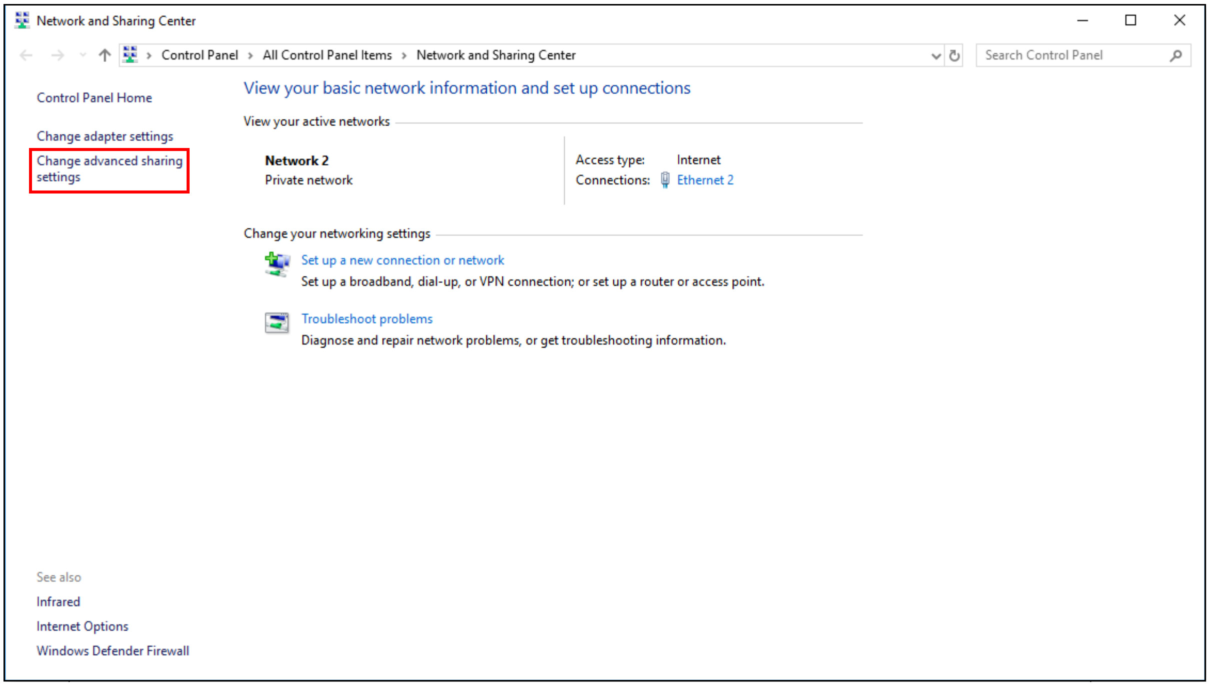
Have a question?

Get help

Make Windows better

Give us feedback

3 Click **Change advanced sharing settings**.


Network and Sharing Center
Control Panel › All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Infrared
Internet Options
Windows Defender Firewall

View your basic network information and set up connections

View your active networks

Network 2
Private network

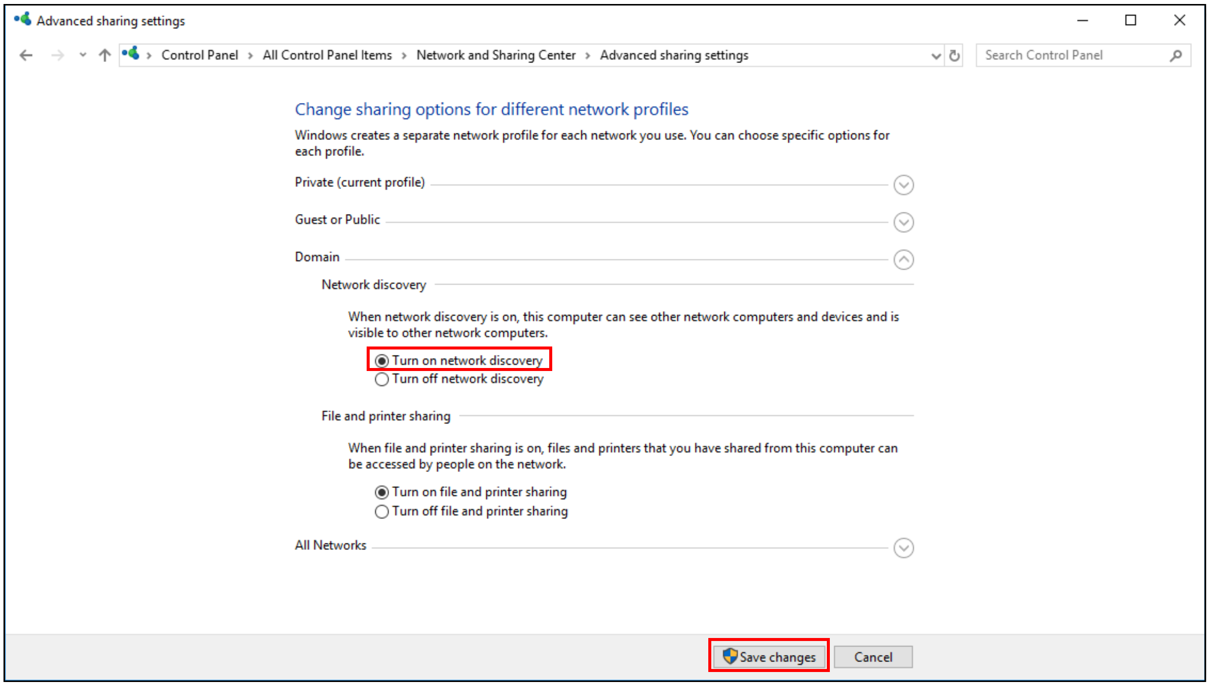
Access type: Internet
Connections: Ethernet 2

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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.


Advanced sharing settings
Control Panel › All Control Panel Items › Network and Sharing Center › Advanced sharing settings
Search Control Panel
Save changes
Cancel

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private (current profile)

Guest or Public

Domain

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

All Networks

9.7.1 Auto-discover Your UPnP-enabled Network Device

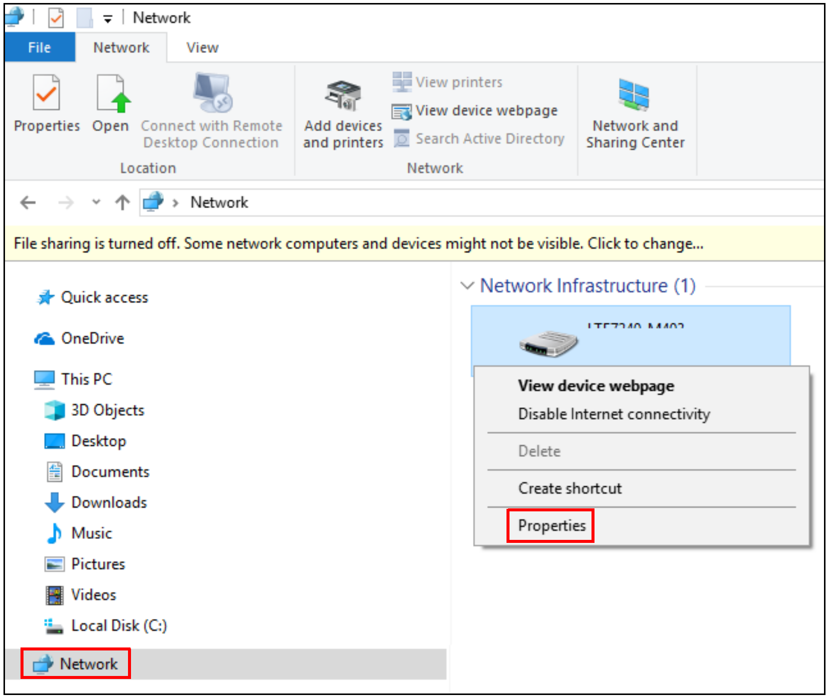
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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

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

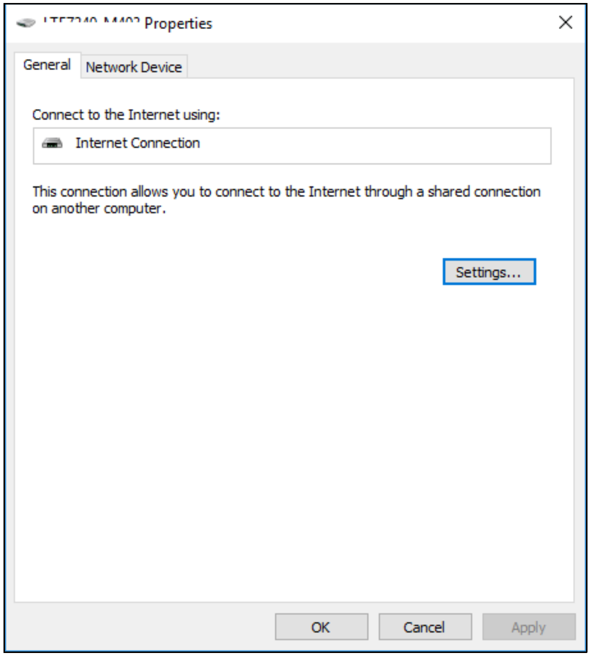
2 Right-click the Zyxel Device icon and select **Properties**.

Figure 78 Network Connections



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

Figure 79 Internet Connection Properties



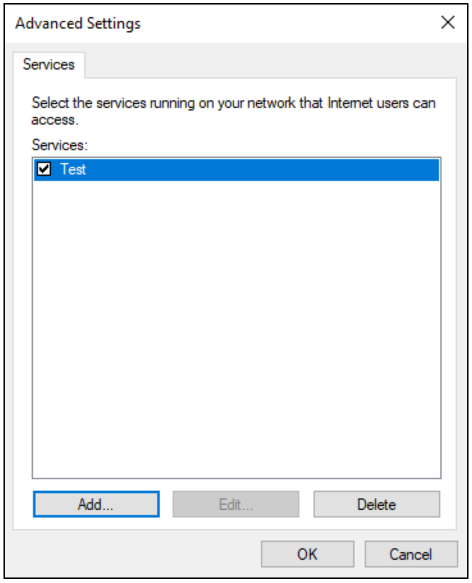
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

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

Figure 80 Internet Connection Properties: Advanced Settings

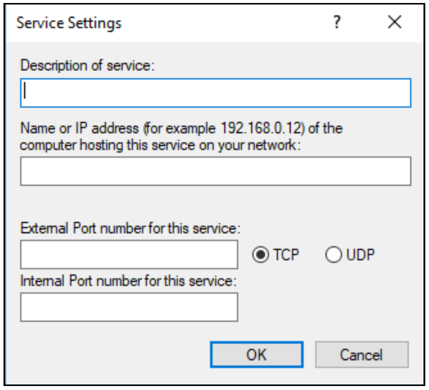


Select the services running on your network that Internet users can access.

Services:

☑ Test

Figure 81 Internet Connection Properties: Advanced Settings: Add



Description of service:

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:

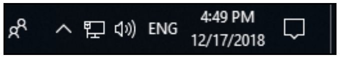
External Port number for this service: ● TCP ○ UDP

Internal Port number for this service:

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

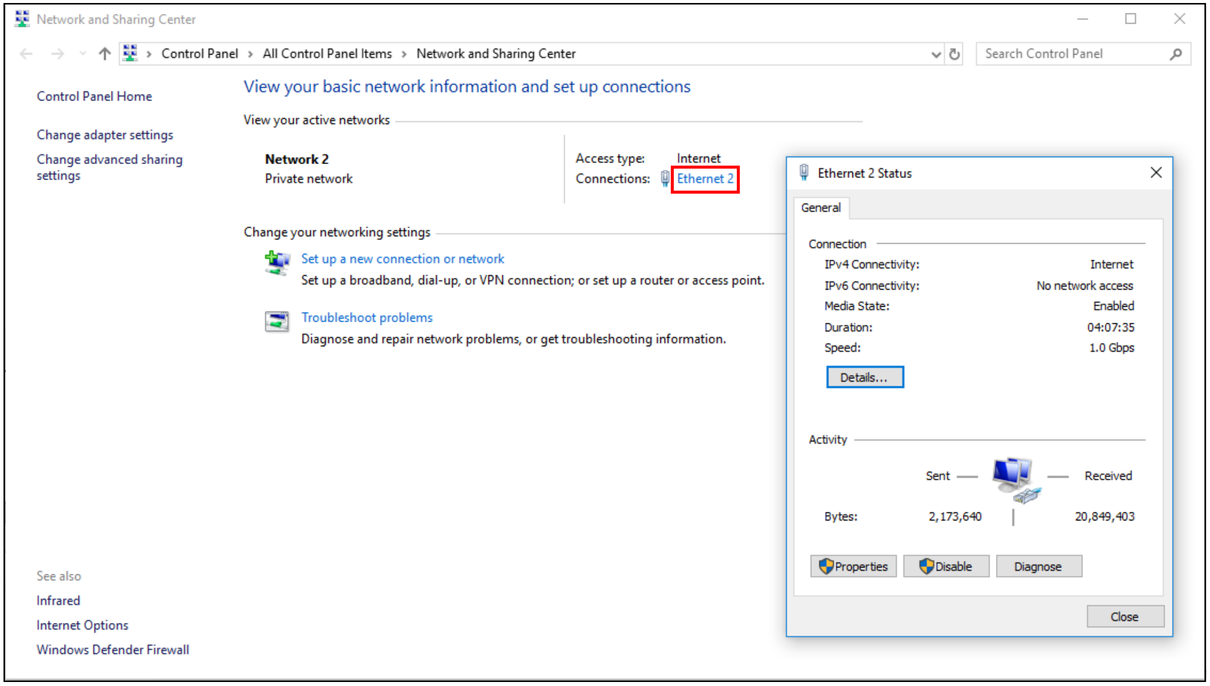
5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 82 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 83 Internet Connection Status



Network and Sharing Center

Control Panel > All Control Panel Items > Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

View your active networks

Network 2
Private network

Access type: Internet
Connections: Ethernet 2

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also
Infrared
Internet Options
Windows Defender Firewall

Ethernet 2 Status

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	04:07:35
Speed:	1.0 Gbps

Details...

Activity

	Sent	Received
Bytes:	2,173,640	20,849,403

Properties Disable Diagnose

Close

9.8 Web Configurator Easy Access in Windows 7

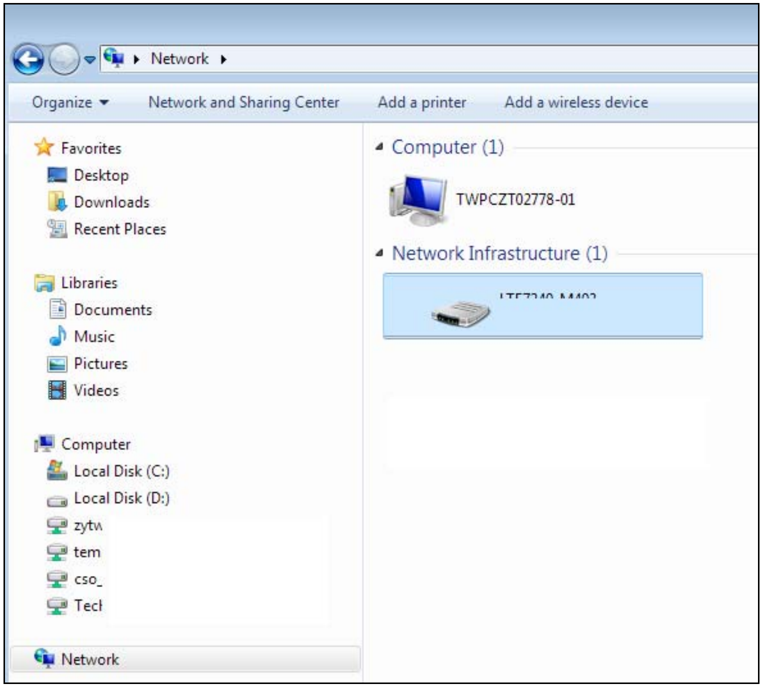
With UPnP, you can access the Web-based Configurator on the Zyxel Device without needing to find out the IP address of the Zyxel Device first. This comes helpful if you do not know the IP address of the Zyxel Device.

Follow the steps below to access the Web Configurator.

1 Open **Windows Explorer**.

2 Click **Network**.

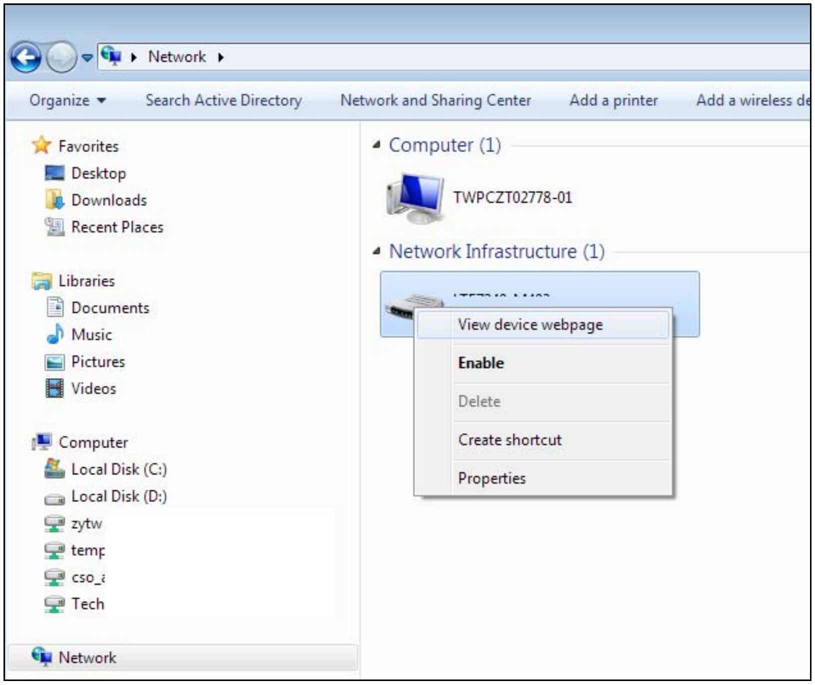
Figure 84 Network Connections



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

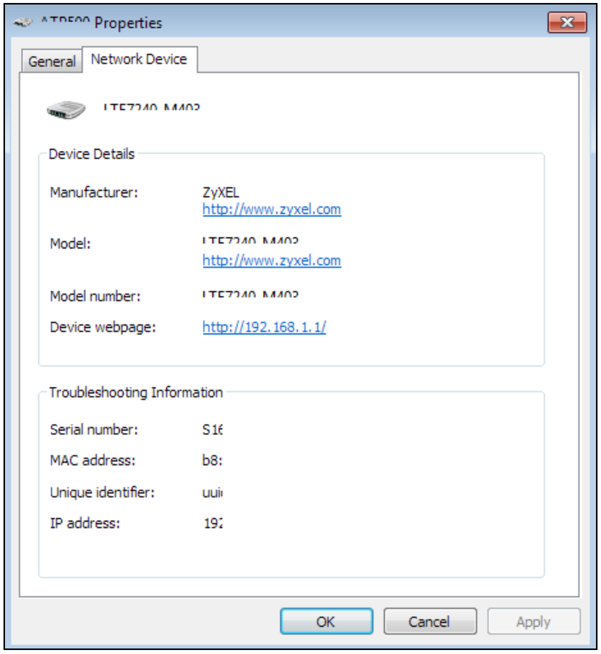
4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

Figure 85 Network Connections: My Network Places



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

Figure 86 Network Connections: My Network Places: Properties: Example



ATP500 Properties

LTE7240-M403

Device Details

Manufacturer: ZyXEL
http://www.zyxel.com

Model: LTE7240-M403
http://www.zyxel.com

Model number: LTE7240-M403

Device webpage: http://192.168.1.1/

Troubleshooting Information

Serial number: S16

MAC address: b8:

Unique identifier: uui

IP address: 192

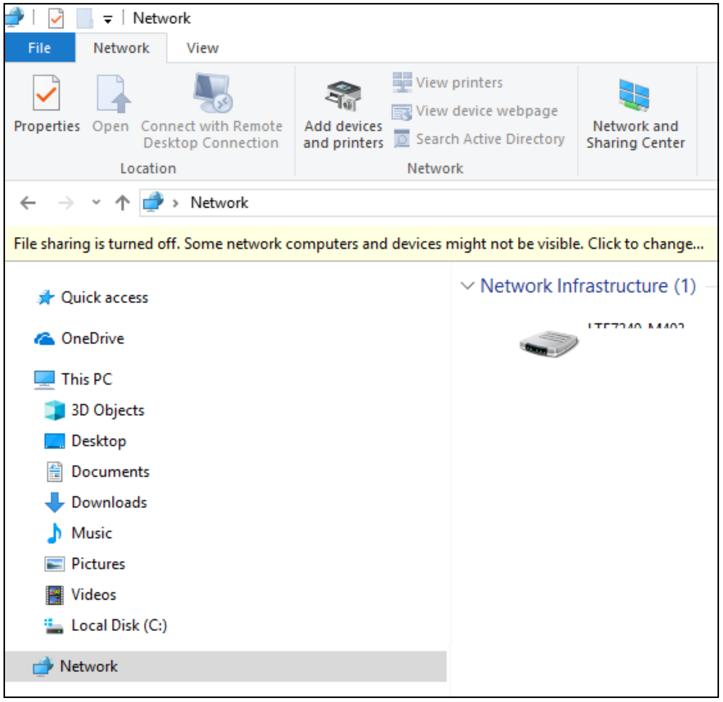
9.9 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

Figure 87 Network Connections

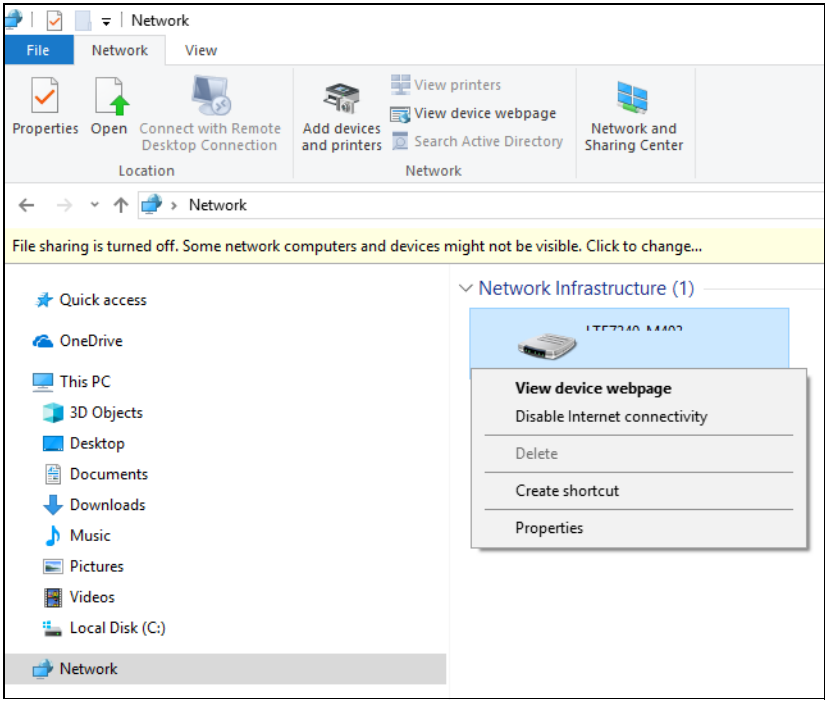


File sharing is turned off. Some network computers and devices might not be visible. Click to change...

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.

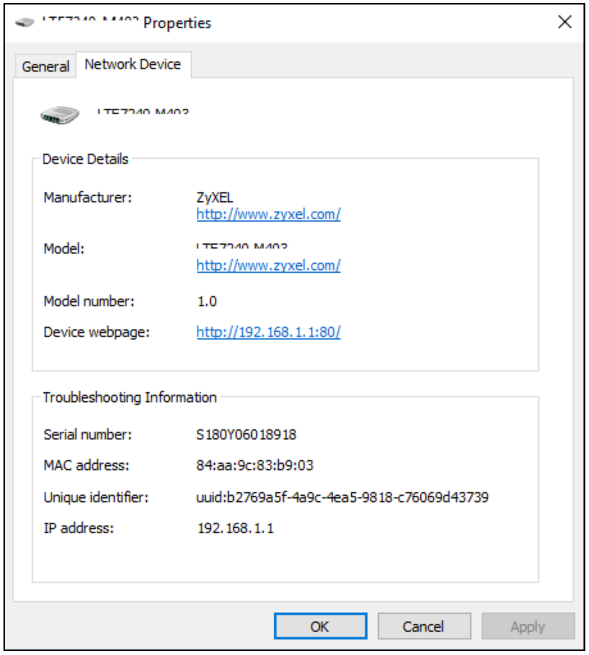
Figure 88 Network Connections: Network Infrastructure



File sharing is turned off. Some network computers and devices might not be visible. Click to change...

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 89 Network Connections: Network Infrastructure: Properties: Example



LTE7240-M403

Device Details

Manufacturer: ZyXEL
http://www.zyxel.com/

Model: LTE7240-M403
http://www.zyxel.com/

Model number: 1.0

Device webpage: http://192.168.1.1:80/

Troubleshooting Information

Serial number: S180Y06018918

MAC address: 84:aa:9c:83:b9:03

Unique identifier: uuid:b2769a5f-4a9c-4ea5-9818-c76069d43739

IP address: 192.168.1.1

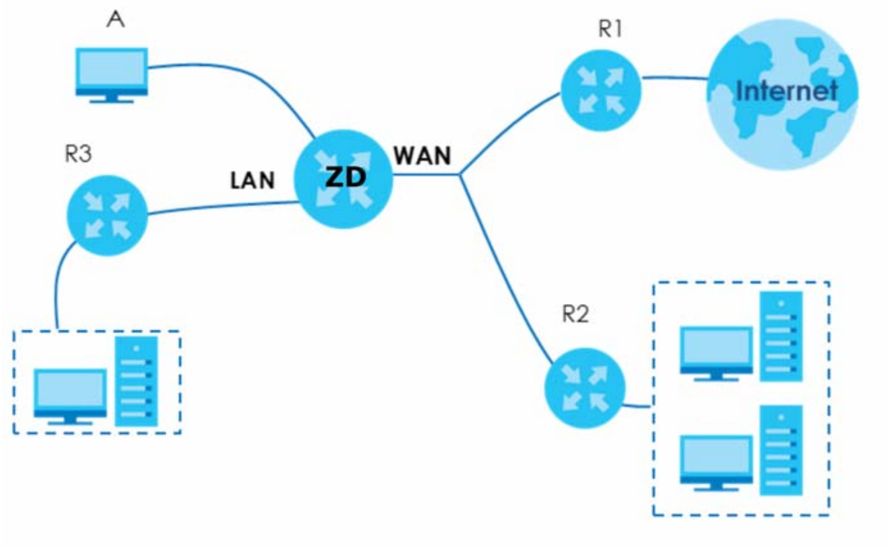
CHAPTER 10 Routing

10.1 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.

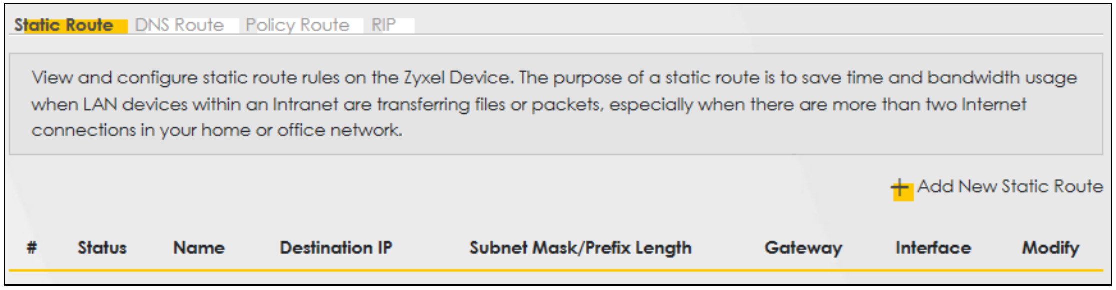
Figure 90 Example of Static Routing Topology



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 91 Network Setting > Routing > Static Route



View and configure static route rules on the Zyxel Device. The purpose of a static route is 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.

#	Status	Name	Destination IP	Subnet Mask/Prefix Length	Gateway	Interface	Modify

The following table describes the labels in this screen.

Table 37 Network Setting > Routing > Static Route

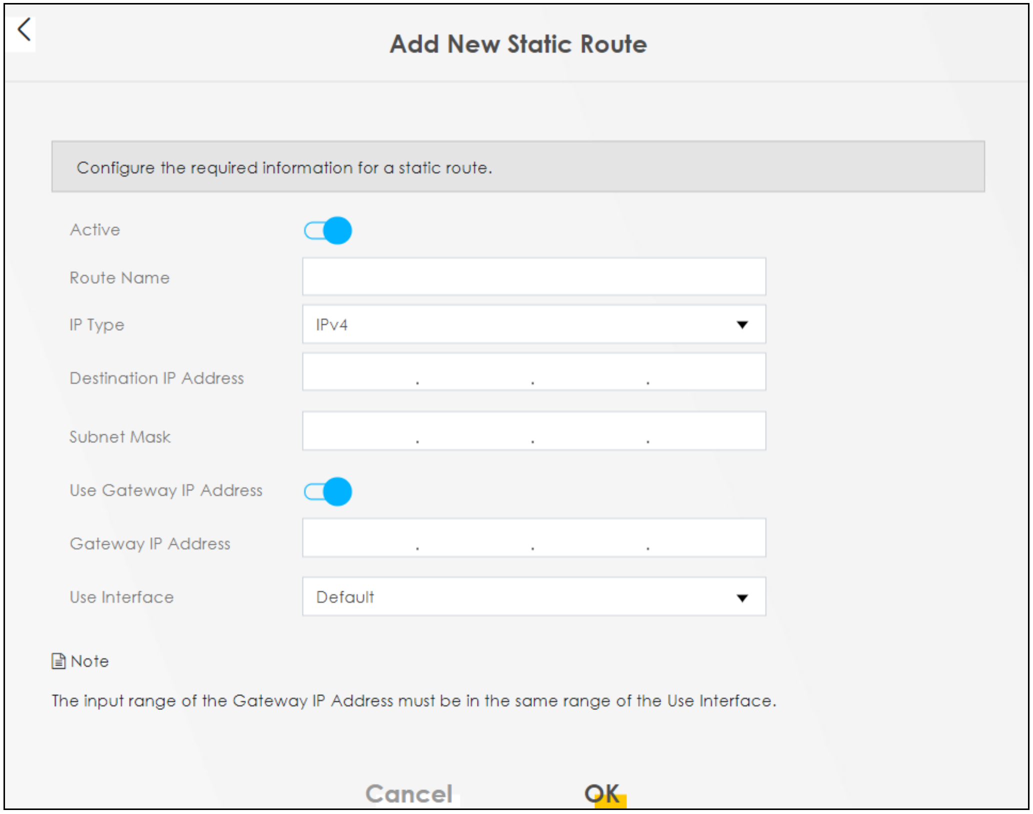
LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Zyxel Device.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This is the name of the static route.
Destination IP	This 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 Zyxel 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/Edit 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 92 Network Setting > Routing > Static Route > Add New Static Route



Add New Static Route

Configure the required information for a static route.

Active	●
Route Name	
IP Type	IPv4 ▼
Destination IP Address	. . .
Subnet Mask	. . .
Use Gateway IP Address	●
Gateway IP Address	. . .
Use Interface	Default ▼

Note

The input range of the Gateway IP Address must be in the same range of the Use Interface.

The following table describes the labels in this screen.

Table 38 Network Setting > Routing > Static Route > Add/Edit

LABEL	DESCRIPTION
Active	Activates static route.
Route Name	Assign a name for your static route (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign ($) vertical bar (|) ampersand (&) semicolon (;)
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.
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.
Prefix Length	If you are using IPv6, enter or set the prefix length in this field.
Use Gateway IP Address	Enables forwarding packets to a gateway IP address or a bound interface.
Gateway IP Address	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Gateway IP Address**, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the Zyxel Device's LAN or WAN port. The gateway helps forward packets to their destinations.

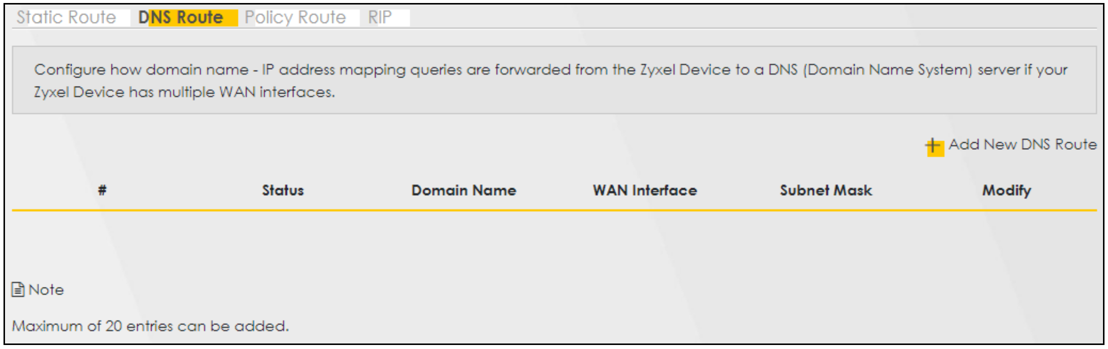
Table 38 Network Setting > Routing > Static Route > Add/Edit (continued)

LABEL	DESCRIPTION
Use Interface	You can decide if you want to forward packets to a gateway IP address (**Default**) or a bound interface (**Cellular WAN**). If you want to configure bound interface, choose an interface through which the traffic is sent. You must have the WAN interfaces already configured in the **Broadband** screen.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

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 93 Network Setting > Routing > DNS Route



Configure how domain name - IP address mapping queries are forwarded from the Zyxel Device to a DNS (Domain Name System) server if your Zyxel Device has multiple WAN interfaces.

#	Status	Domain Name	WAN Interface	Subnet Mask	Modify

Note

Maximum of 20 entries can be added.

The following table describes the labels in this screen.

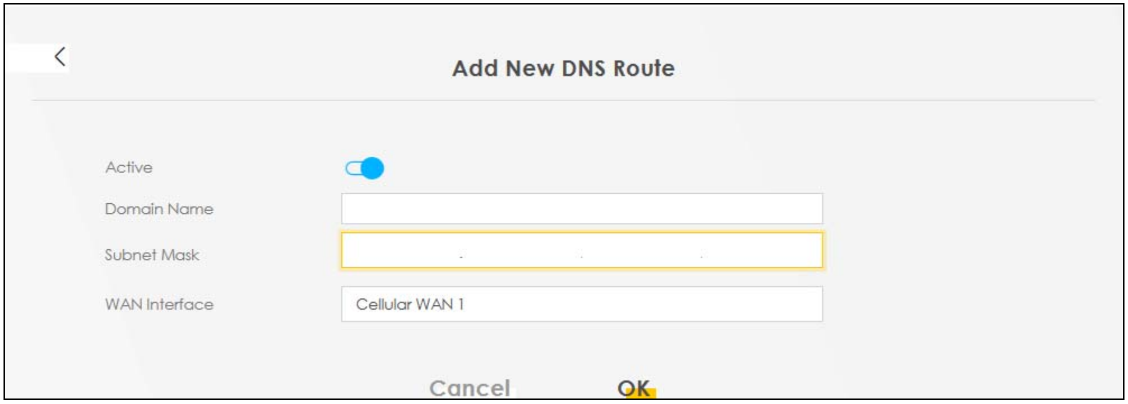
Table 39 Network Setting > Routing > DNS Route

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/Edit DNS Route

Click **Add New DNS Route** in the **DNS Route** screen, use this screen to configure the required information for a DNS route.

Figure 94 Network Setting > Routing > DNS Route > Add New DNS Route



Add New DNS Route

Active	
Domain Name	
Subnet Mask	. . .
WAN Interface	Cellular WAN 1

The following table describes the labels in this screen.

Table 40 Network Setting > Routing > DNS Route > Add/Edit

LABEL	DESCRIPTION
Active	Enable DNS route in your
Domain Name	Enter the domain name you want to resolve. 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	Type 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 interface(s) already configured in the **Broadband** screen.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

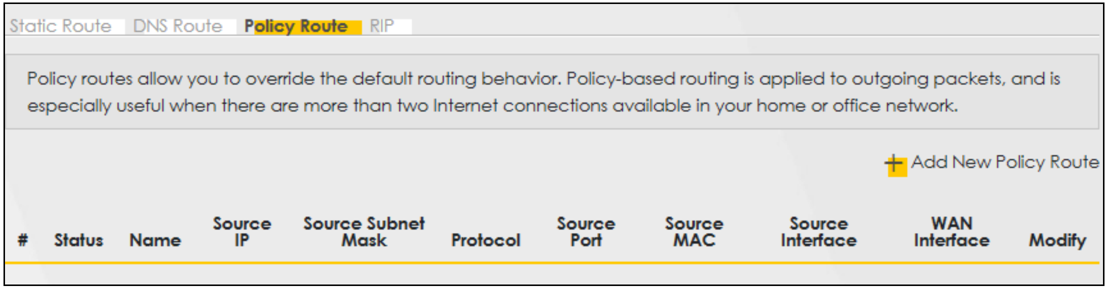
10.4 Policy Route

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 95 Network Setting > Routing > Policy Route



Policy routes allow you to override the default routing behavior. Policy-based routing is applied to outgoing packets, and is especially useful when there are more than two Internet connections available in your home or office network.

#	Status	Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Source Interface	WAN Interface	Modify

The following table describes the labels in this screen.

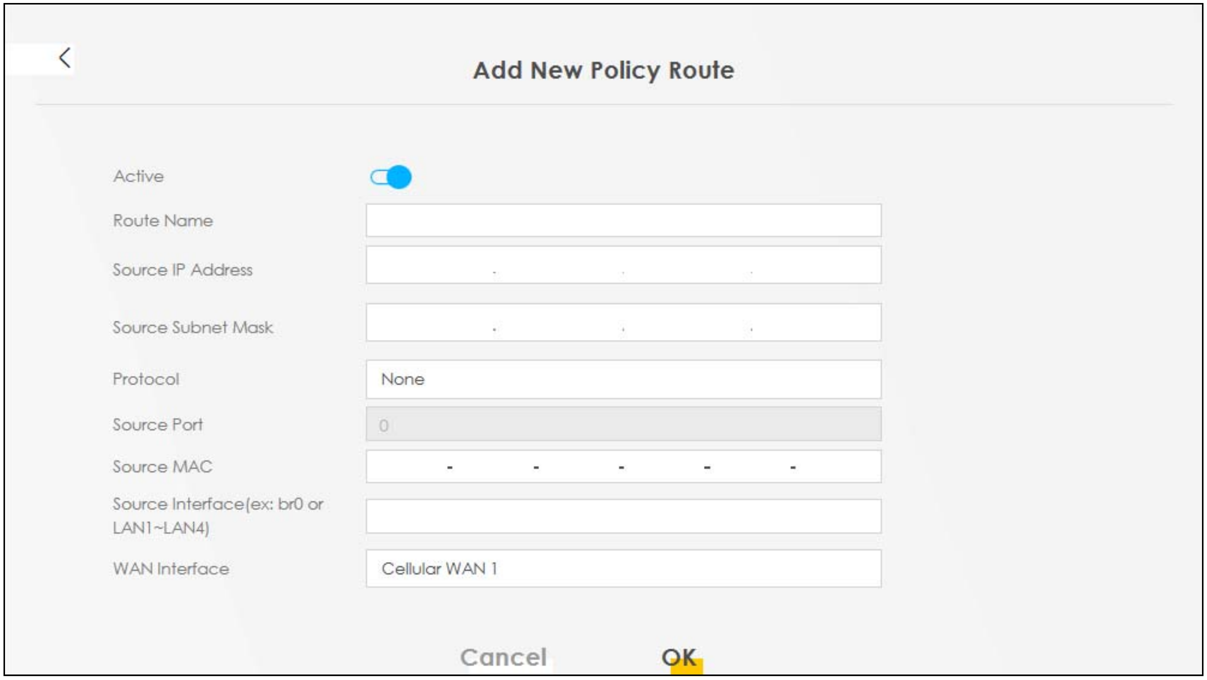
Table 41 Network Setting > Routing > Policy Route

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.
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/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 96 Network Setting > Routing > Policy Route > Add/Edit



Add New Policy Route

Active	●
Route Name	
Source IP Address	. . .
Source Subnet Mask	. . .
Protocol	None
Source Port	0
Source MAC	- - - - -
Source Interface(ex: br0 or LAN1~LAN4)	
WAN Interface	Cellular WAN 1

The following table describes the labels in this screen.

Table 42 Network Setting > Routing > Policy Route > Add/Edit

LABEL	DESCRIPTION
Active	Click this to enable (turns blue) activation of the policy route. Otherwise, click to disable (turns gray).
Route Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (ex: br0 or LAN1~LAN4)	Type 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 interface(s) already configured in the **Broadband** screens.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

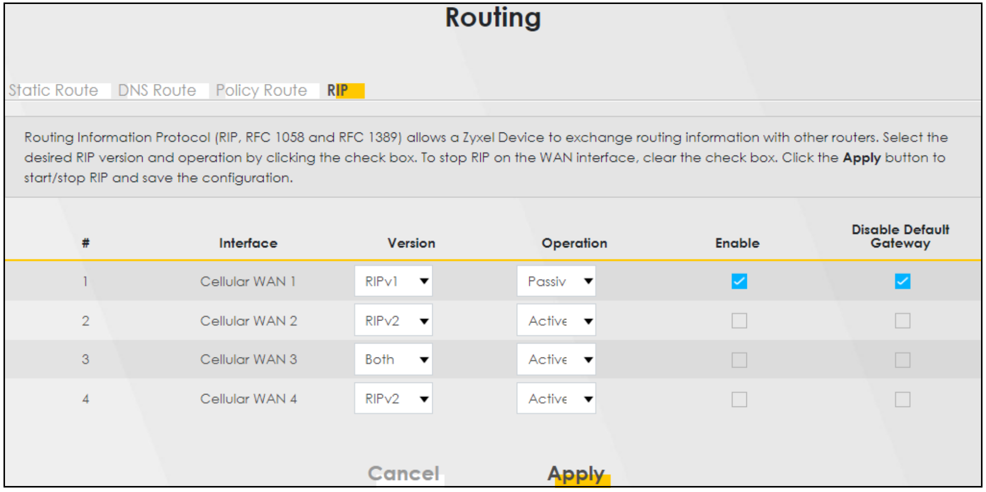
10.5 RIP Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a 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 check box. To stop RIP on the WAN interface, clear the check box. Click the **Apply** button to start/stop RIP and save the configuration.

Figure 97 Network Setting > Routing > RIP



Routing

Static Route | DNS Route | Policy Route | RIP

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a Zyxel Device to exchange routing information with other routers. Select the desired RIP version and operation by clicking the check box. To stop RIP on the WAN interface, clear the check box. Click the **Apply** button to start/stop RIP and save the configuration.

#	Interface	Version	Operation	Enable	Disable Default Gateway
1	Cellular WAN 1	RIPv1	Passiv	☑	☑
2	Cellular WAN 2	RIPv2	Active	□	□
3	Cellular WAN 3	Both	Active	□	□
4	Cellular WAN 4	RIPv2	Active	□	□

Cancel Apply

The following table describes the labels in this screen.

Table 43 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). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
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 check box to activate the settings.
Disable Default Gateway	Select the check box 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
Network Address Translation (NAT)

11.1 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.

11.1.1 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 11.2 on page 140).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings (Section 11.3 on page 143).
- Use the **DMZ** screen to configure a default server (Section 11.4 on page 146).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 11.5 on page 147).

11.1.2 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 or FTP, 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.

11.2 Port Forwarding Overview

Use **Port Forwarding** to forward incoming service requests from the Internet to the server(s) 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.

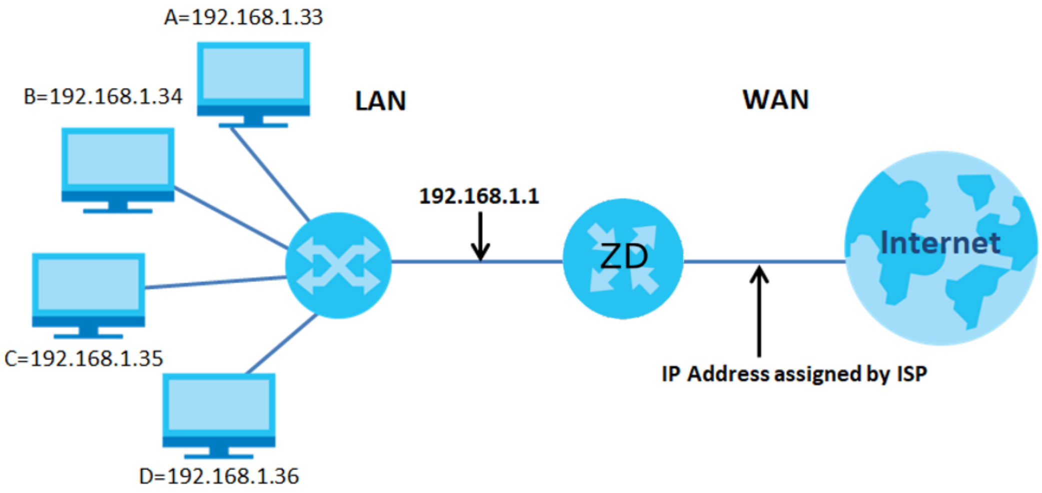
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and 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 or FTP 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 us say you want to assign ports 21-25 to one FTP, 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 98 Multiple Servers Behind NAT Example

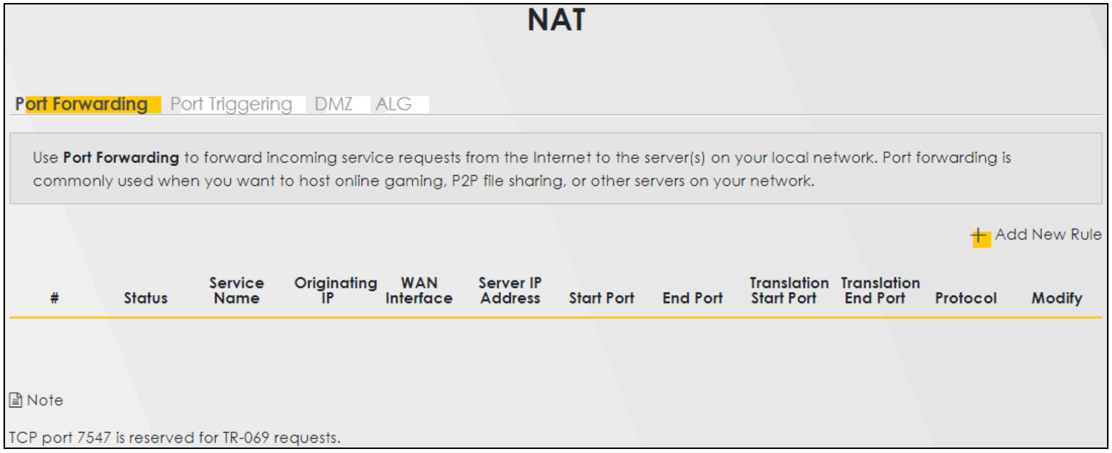


11.2.1 Port Forwarding

Click **Network Setting > NAT** to open the **Port Forwarding** screen.

Note: TCP port 7547 is reserved for system use.

Figure 99 Network Setting > NAT > Port Forwarding



NAT

Use **Port Forwarding** to forward incoming service requests from the Internet to the server(s) 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.

#	Status	Service Name	Originating IP	WAN Interface	Server IP Address	Start Port	End Port	Translation Start Port	Translation End Port	Protocol	Modify

Note

TCP port 7547 is reserved for TR-069 requests.

The following table describes the fields in this screen.

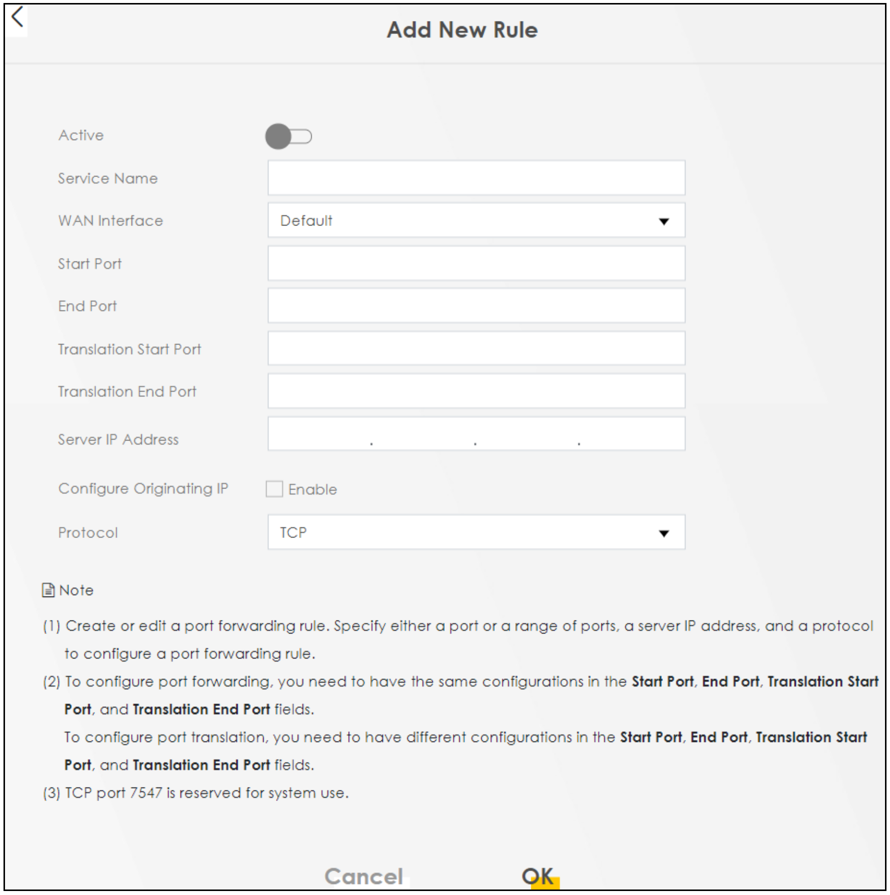
Table 44 Network Setting > NAT > Port Forwarding

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.

11.2.2 Add/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 100 Network Setting > NAT > Port Forwarding > Add/Edit



Add New Rule

Active	○
Service Name	
WAN Interface	Default ▾
Start Port	
End Port	
Translation Start Port	
Translation End Port	
Server IP Address	. . .
Configure Originating IP	□ Enable
Protocol	TCP ▾

Note

(1) 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.

(2) 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.

(3) TCP port 7547 is reserved for system use.

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.

Note: TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 45 Network Setting > NAT > Port Forwarding > Add/Edit

LABEL	DESCRIPTION
Active	Select or clear this field to turn the port forwarding rule on or off.
Service Name	Select a service to forward or select **User Defined** and enter a name in the field to the right.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.

Table 45 Network Setting > NAT > Port Forwarding > Add/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** check box to enter the originating IP in the next field.
Originating IP	Enter the originating IP address here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

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.

11.3 Port Triggering

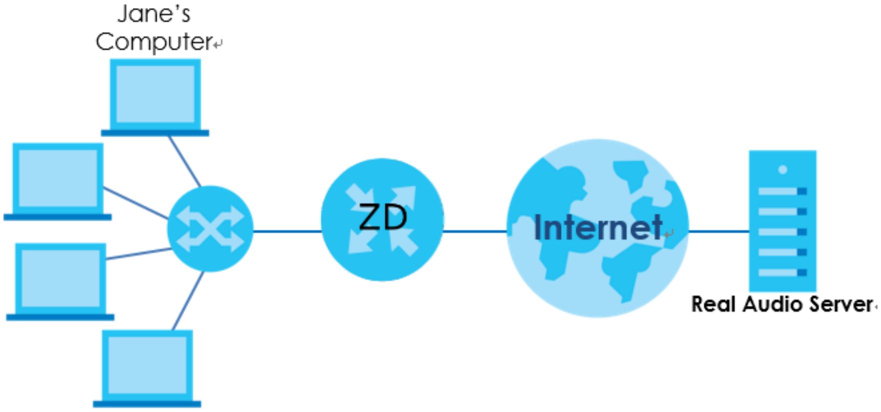
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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.

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 the computer's connection for that service closes, another computer on the LAN can use the service in the same manner.

For example:

Figure 101 Trigger Port Forwarding Process: Example



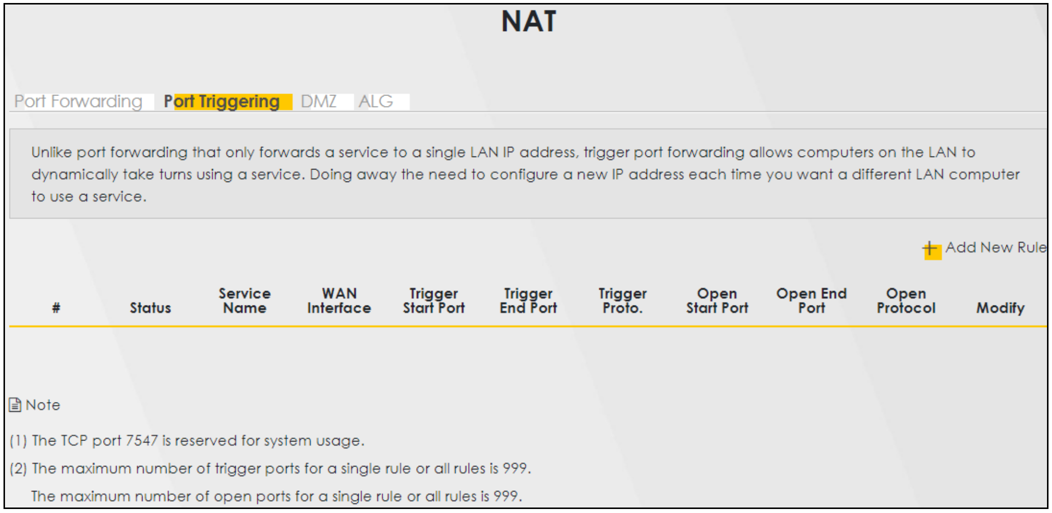
1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970-7170.
3. The Real Audio server responds using a 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 three minutes with UDP (User Datagram Protocol) or two 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 102 Network Setting > NAT > Port Triggering



NAT

Unlike port forwarding that only forwards a service to a single LAN IP address, trigger port forwarding allows computers on the LAN to dynamically take turns using a service. Doing away the need to configure a new IP address each time you want a different LAN computer to use a service.

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Protocol	Modify

Note

(1) The TCP port 7547 is reserved for system usage.

(2) The maximum number of trigger ports for a single rule or all rules is 999.
The maximum number of open ports for a single rule or all rules is 999.

The following table describes the labels in this screen.

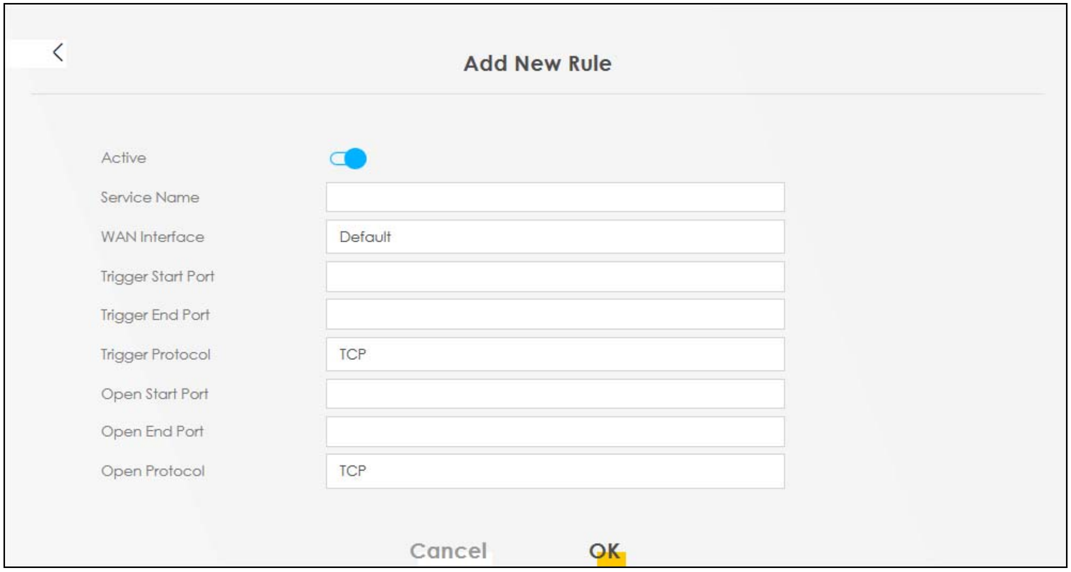
Table 46 Network Setting > NAT > Port Triggering

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.

11.3.1 Add/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 103 Network Setting > NAT > Port Triggering > Add/Edit



Add New Rule

Active

Service Name

WAN Interface: Default

Trigger Start Port

Trigger End Port

Trigger Protocol: TCP

Open Start Port

Open End Port

Open Protocol: TCP

The following table describes the labels in this screen.

Table 47 Network Setting > NAT > Port Triggering > Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (blue switch) or disable (gray switch) to activate or deactivate the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
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. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type 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. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type 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.

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.

11.4 DMZ

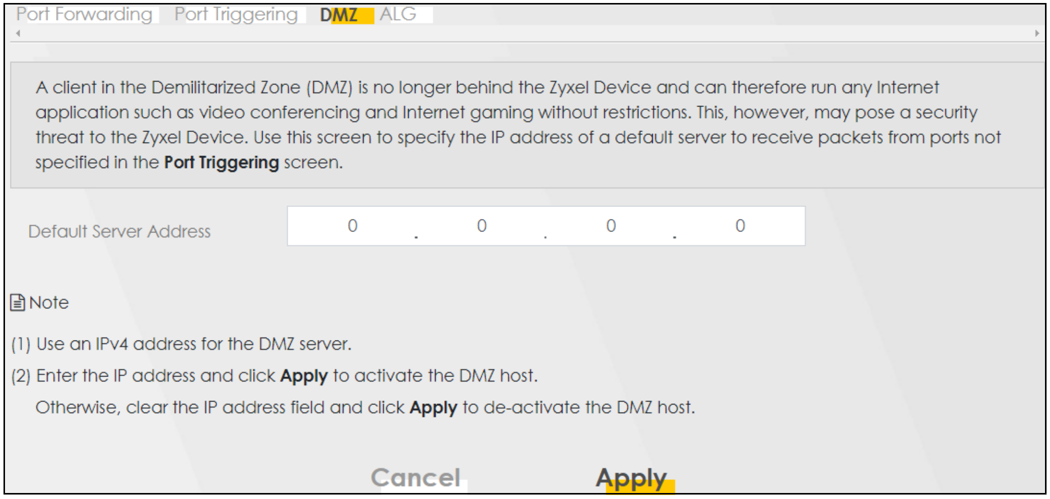
Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (DeMilitarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on 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, web, and FTP 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. Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. 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 104 Network Setting > NAT > DMZ



A client in the Demilitarized Zone (DMZ) is no longer behind the Zyxel Device and can therefore run any Internet application such as video conferencing and Internet gaming without restrictions. This, however, may pose a security threat to the Zyxel Device. Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen.

Default Server Address 0 . 0 . 0 . 0

Note

(1) Use an IPv4 address for the DMZ server.

(2) Enter the IP address and click **Apply** to activate the DMZ host.
Otherwise, clear the IP address field and click **Apply** to de-activate the DMZ host.

The following table describes the fields in this screen.

Table 48 Network Setting > NAT > DMZ

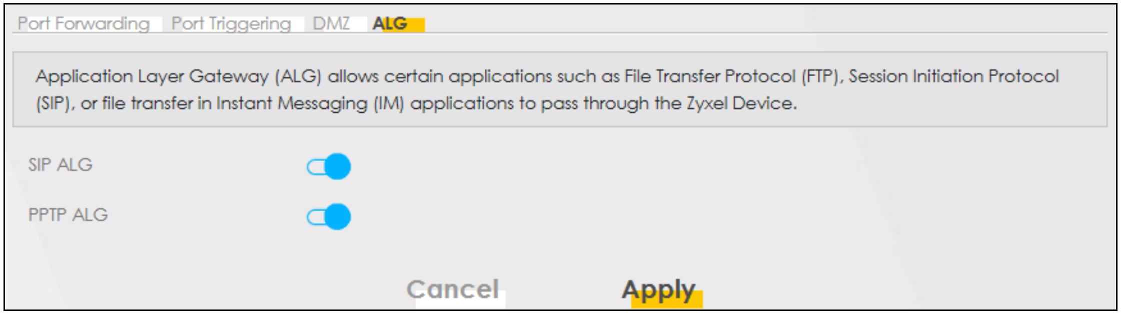
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **Port Forwarding** screen. Note: If you do not assign a default server, the Zyxel Device discards all packets received for ports not specified in the virtual server configuration.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click this to save your changes back to the Zyxel Device.

11.5 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 File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications to pass through the Zyxel Device.

Figure 105 Network Setting > NAT > ALG



Application Layer Gateway (ALG) allows certain applications such as File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications to pass through the Zyxel Device.

SIP ALG

PPTP ALG

The following table describes the fields in this screen.

Table 49 Network Setting > NAT > ALG

LABEL	DESCRIPTION
SIP ALG	Click this (switch turns blue) to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. Otherwise, click this to turn off (switch turns gray) the SIP ALG.
PPTP ALG	Click this to turn on (switch turns blue) the PPTP ALG on the Zyxel Device to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 12
Dynamic DNS Setup

12.1 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 server(s), 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 server(s). 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 FTP server or 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.

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 12.2 on page 150).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device (Section 12.3 on page 151).

12.1.2 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.

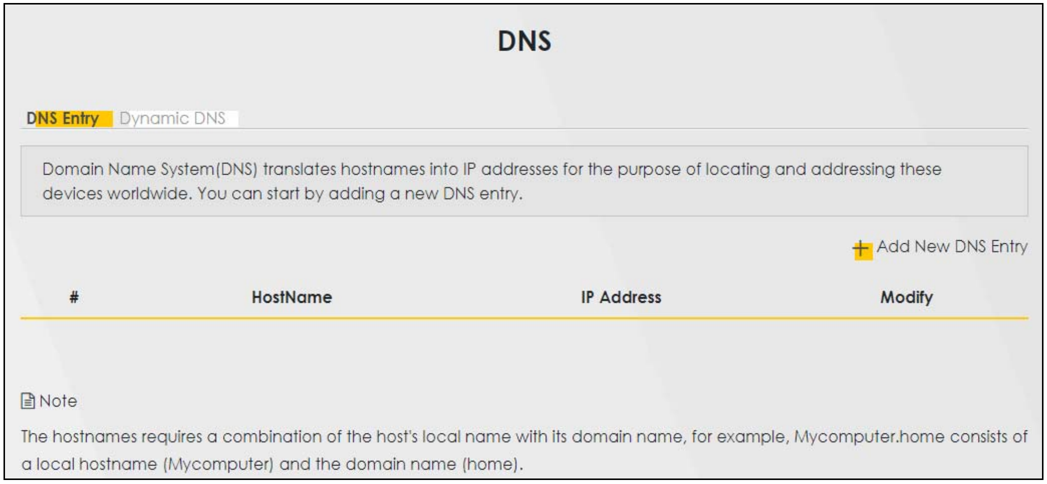
If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 DNS Entry

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 DNS routes 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 106 Network Setting > DNS > DNS Entry



Domain Name System(DNS) translates hostnames into IP addresses for the purpose of locating and addressing these devices worldwide. You can start by adding a new DNS entry.

The hostnames requires a combination of the host's local name with its domain name, for example, Mycomputer.home consists of a local hostname (Mycomputer) and the domain name (home).

The following table describes the fields in this screen.

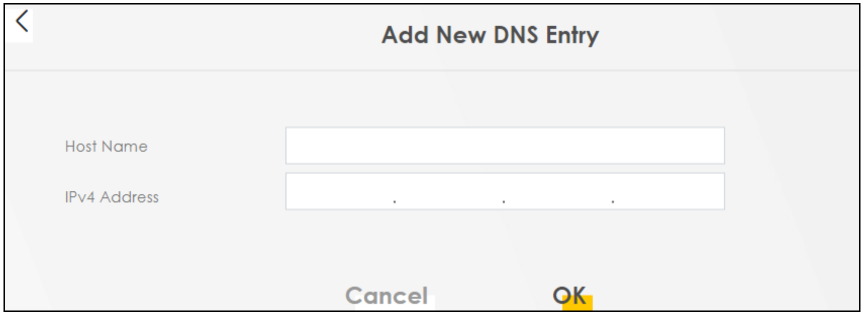
Table 50 Network Setting > DNS > DNS Entry

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.

12.2.1 Add/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 107 Network Setting > DNS > DNS Entry > Add/Edit



Add New DNS Entry

Host Name	
IPv4 Address	. . .

The following table describes the labels in this screen.

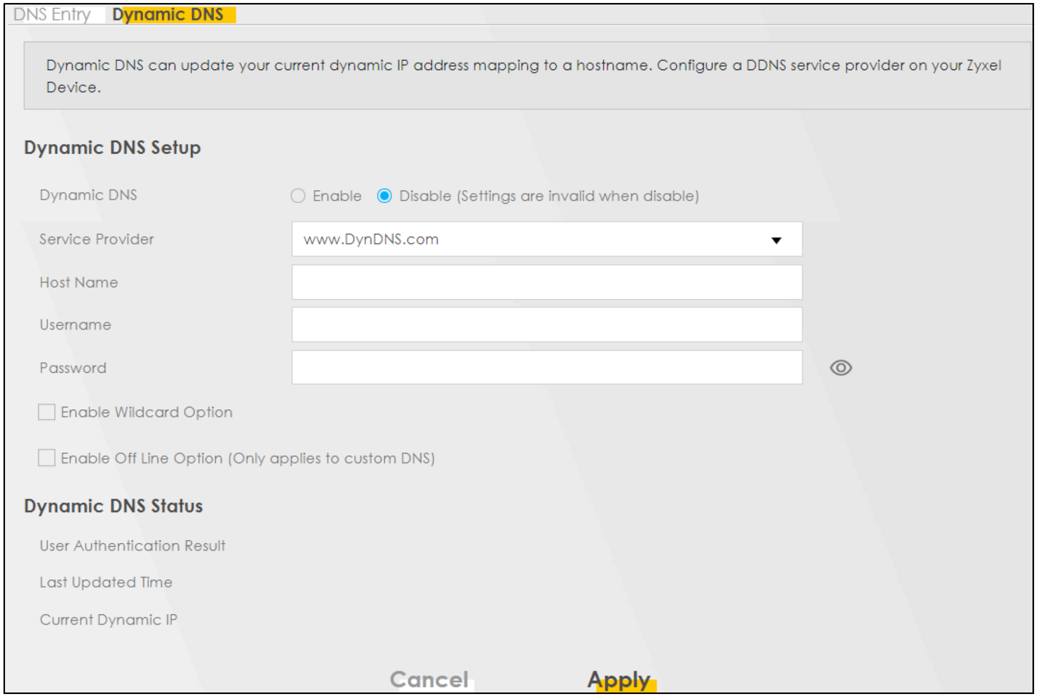
Table 51 Network Setting > DNS > DNS Entry > Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
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.

12.3 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 108 Network Setting > DNS > Dynamic DNS



Dynamic DNS can update your current dynamic IP address mapping to a hostname. Configure a DDNS service provider on your Zyxel Device.

Dynamic DNS Setup

Dynamic DNS	○ Enable ● Disable (Settings are invalid when disable)
Service Provider	www.DynDNS.com ▾
Host Name	
Username	
Password	

□ Enable Wildcard Option

□ Enable Off Line Option (Only applies to custom DNS)

Dynamic DNS Status

User Authentication Result

Last Updated Time

Current Dynamic IP

The following table describes the fields in this screen.

Table 52 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	Type the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box 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.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 13 VLAN Group

13.1 Overview

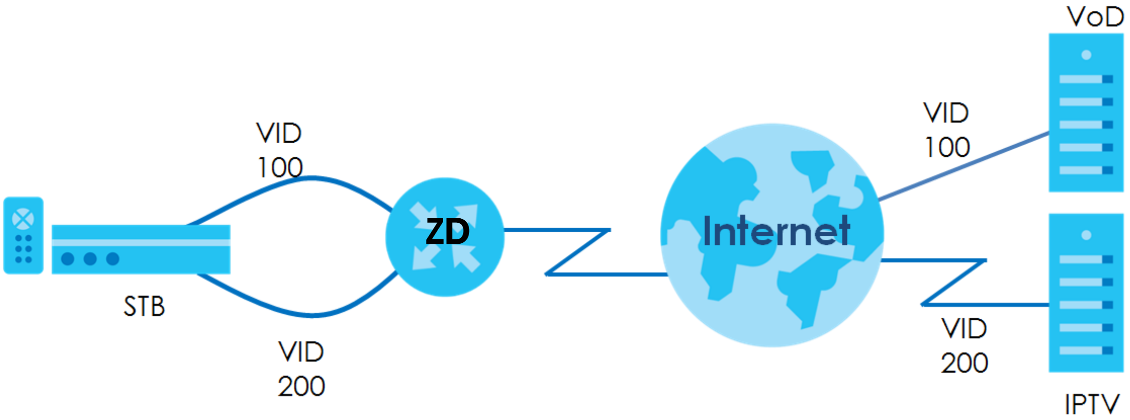
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same groups; 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 109 VLAN Group Example



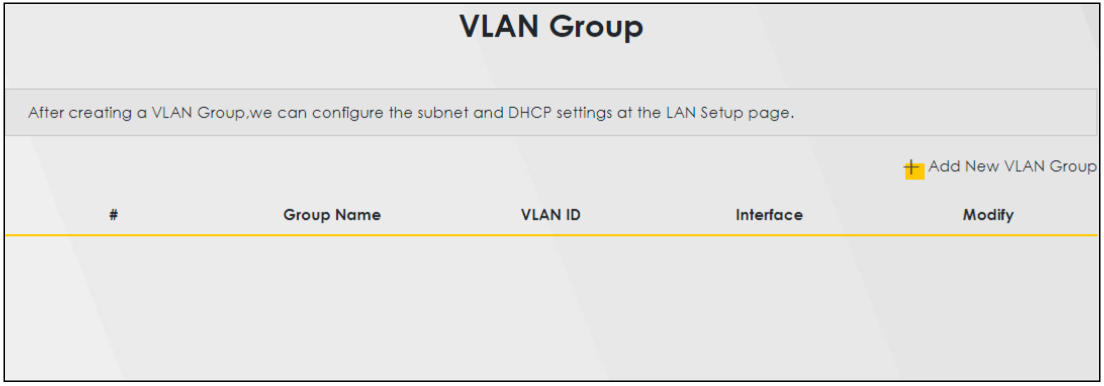
13.1.1 What You Can Do in this Chapter

Use these screens to manage VLAN groups on the Zyxel Device.

13.2 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 110 Network Setting > VLAN Group



VLAN Group

After creating a VLAN Group,we can configure the subnet and DHCP settings at the LAN Setup page.

The following table describes the fields in this screen.

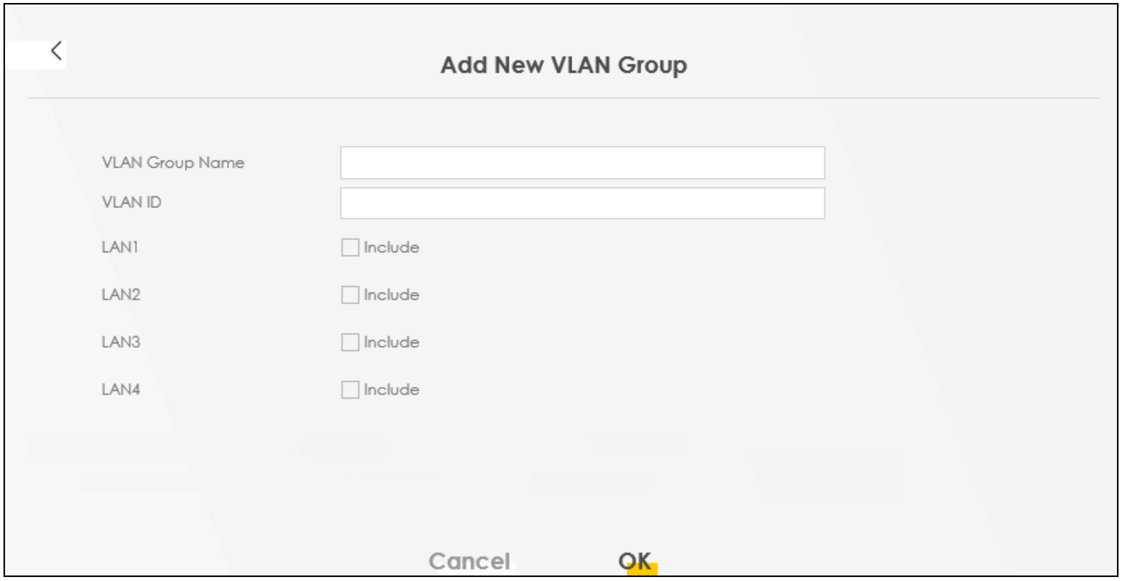
Table 53 Network Setting > VLAN Group

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. Click the **Delete** icon (🗑) to remove the VLAN group.

13.2.1 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 111 Network Setting > VLAN Group > Add/Edit VLAN Group



The following table describes the fields in this screen.

Table 54 Network Setting > VLAN Group > Add/Edit VLAN Group

LABEL	DESCRIPTION
VLAN Group Name	Enter a name to identify this group. You can enter up to 32 characters. You can use letters, numbers, hyphens (–), underscores (_), and spaces.
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify this VLAN group.
LAN	Select **Include** to add the associated LAN interface to this VLAN group.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 14
Interface Grouping

14.1 Interface Grouping Overview

By default, all LAN and WAN interfaces on the Zyxel Device are in the same group and can communicate with each other. Create interface groups to have the Zyxel Device assign IP addresses in different domains to different groups. Each group acts as an independent network on the Zyxel Device. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

14.1.1 What You Can Do in this Chapter

The **Interface Grouping** screen lets you create multiple networks on the Zyxel Device (Section 14.2 on page 156).

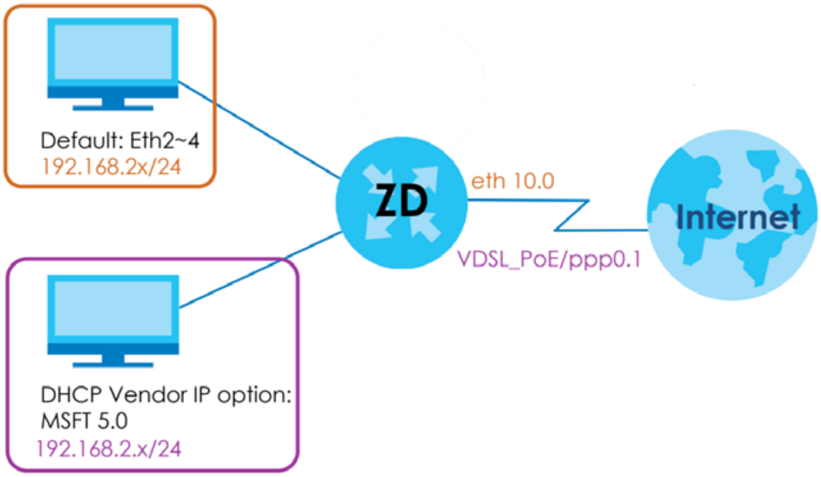
14.2 Interface Grouping

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 Section 9.2 on page 108 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.

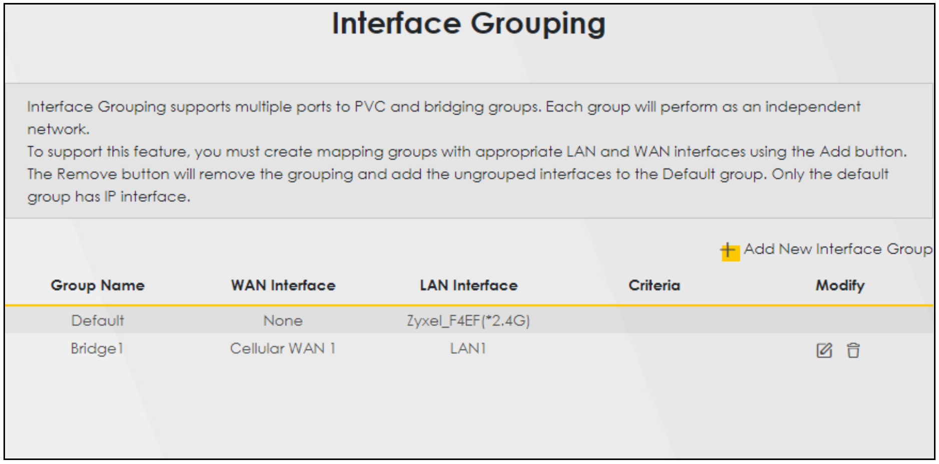
Figure 112 Interface Grouping Application



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 113 Network Setting > Interface Grouping



Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.
To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.
The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	WAN Interface	LAN Interface	Criteria	Modify
Default	None	Zyxel_F4EF(*2.4G)		
Bridge1	Cellular WAN 1	LAN1		✎ 🗑

The following table describes the fields in this screen.

Table 55 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. Click the **Delete** icon(🗑) to remove the Interface group.

14.2.1 Interface Group Configuration

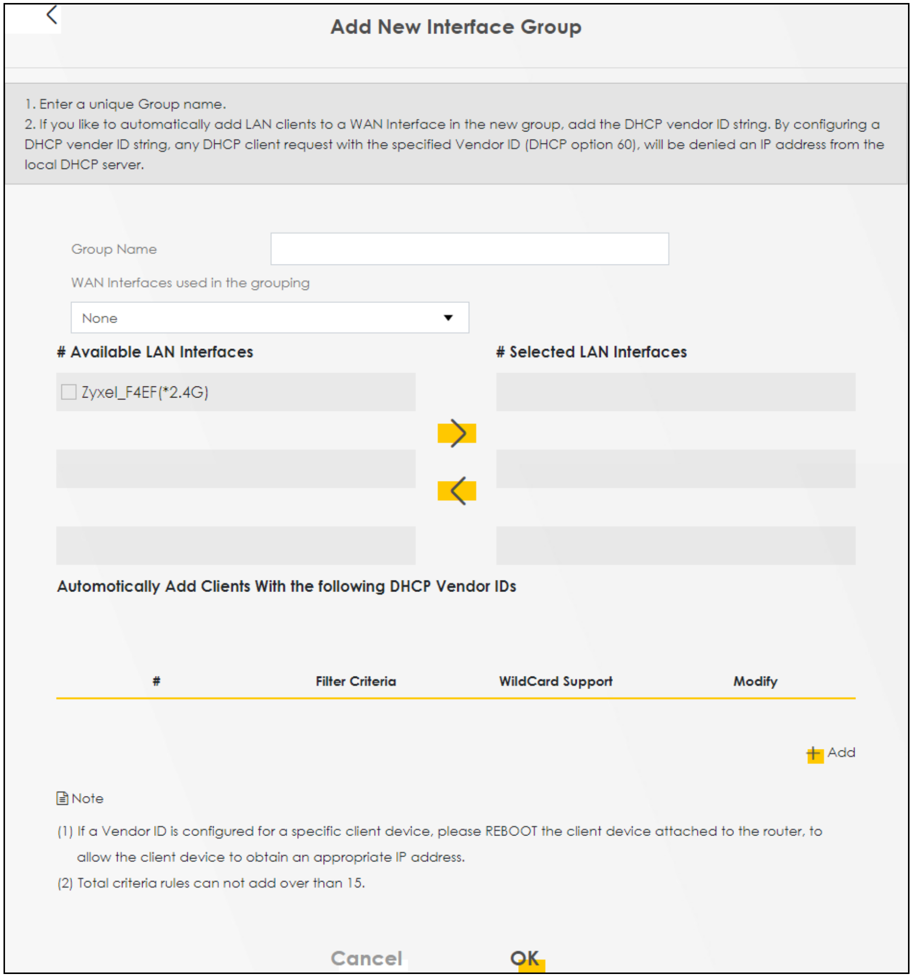
Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group. If you want to automatically add LAN clients to a new group, use filtering criteria.

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.

Note: You can have up to 15 filter criteria.

Figure 114 Network Setting > Interface Grouping > Add/Edit



Add New Interface Group

1. Enter a unique Group name.
2. If you like to automatically add LAN clients to a WAN Interface in the new group, add the DHCP vendor ID string. By configuring a DHCP vender ID string, any DHCP client request with the specified Vendor ID (DHCP option 60), will be denied an IP address from the local DHCP server.

Group Name

WAN Interfaces used in the grouping

None

Available LAN Interfaces

Selected LAN Interfaces

□ Zyxel_F4EF(*2.4G)

Automotically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Modify

Note

(1) If a Vendor ID is configured for a specific client device, please REBOOT the client device attached to the router, to allow the client device to obtain an appropriate IP address.

(2) Total criteria rules can not add over than 15.

The following table describes the fields in this screen.

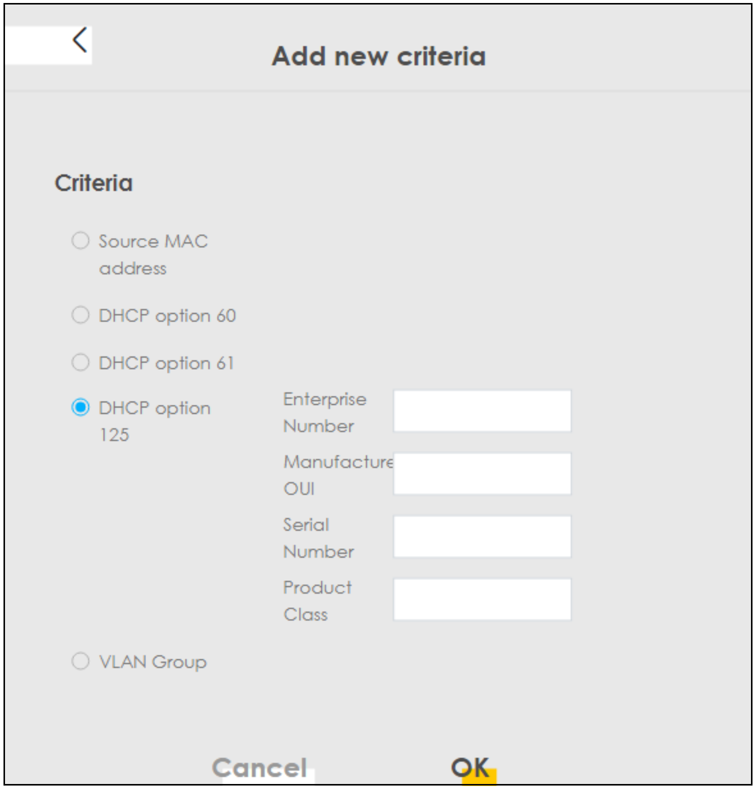
Table 56 Network Setting > Interface Grouping > Add/Edit

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (–) and underscores (_). Spaces are not 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 14.2.2 on page 159 for more information.
Add	Click this to add new criteria.
#	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.

14.2.2 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 115 Network Setting > Interface Grouping > Add/Edit > Add new criteria



Add new criteria

Criteria

○ Source MAC address

○ DHCP option 60

○ DHCP option 61

● DHCP option 125

Enterprise Number

Manufacture OUI

Serial Number

Product Class

○ VLAN Group

The following table describes the fields in this screen.

Table 57 Network Setting > Interface Grouping > Add/Edit > Add new criteria

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
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 15 Firewall

15.1 Overview

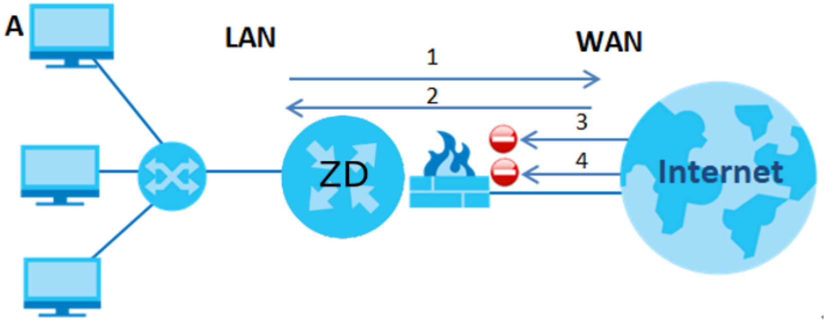
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- 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 116 Default Firewall Action



15.1.1 What You Need to Know About Firewall

DoS

Denials 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.

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.

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.

15.2 Firewall

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it.

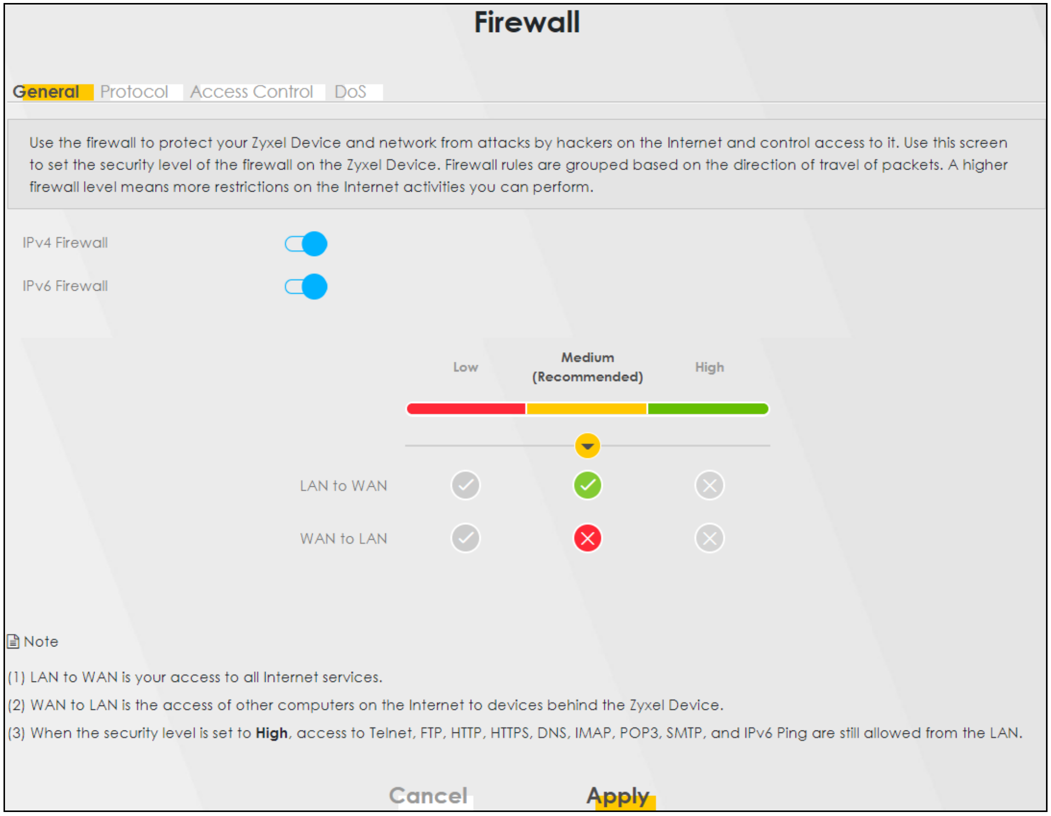
15.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device (Section 15.3 on page 162).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 15.4 on page 164).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 15.5 on page 165).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 15.6 on page 168).

15.3 Firewall General Settings

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 117 Security > Firewall > General



Firewall

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.

IPv4 Firewall ●

IPv6 Firewall ●

	Low	Medium (Recommended)	High
LAN to WAN	✓	✓	✕
WAN to LAN	✓	✕	✕

Note

(1) LAN to WAN is your access to all Internet services.

(2) WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

(3) When the security level is set to **High**, access to Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and IPv6 Ping are still allowed from the LAN.

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, FTP, 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 58 Security > Firewall > General

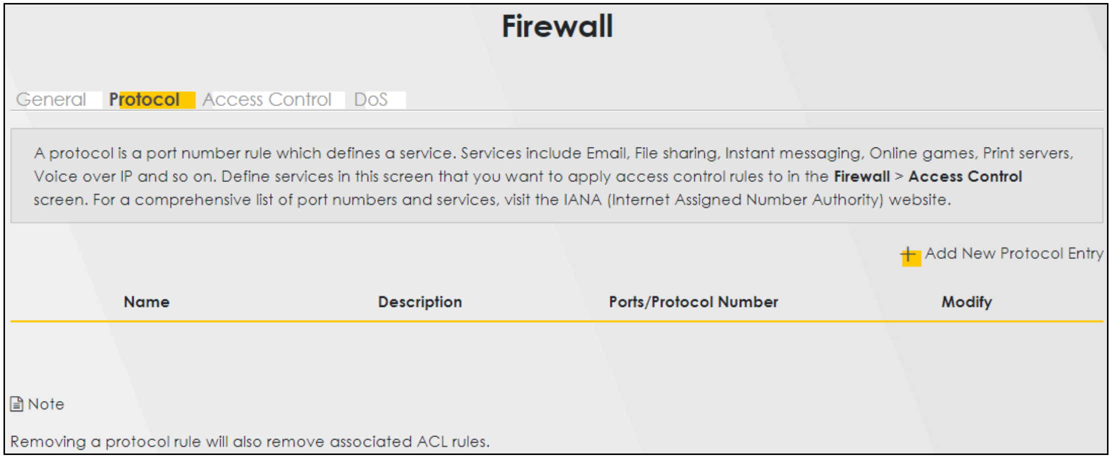
LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using **IPv4** (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using **IPv6** (Internet Protocol version 6).
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and IPv6 Ping) 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.
Cancel	Click this to restore your previously saved settings.
Apply	Click this to save your changes.

15.4 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 118 Security > Firewall > Protocol



Firewall

A protocol is a port number rule which defines a service. Services include Email, File sharing, Instant messaging, Online games, Print servers, Voice over IP and so on. Define services in this screen that you want to apply access control rules to in the **Firewall** > **Access Control** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website.

Name	Description	Ports/Protocol Number	Modify

Note

Removing a protocol rule will also remove associated ACL rules.

The following table describes the labels in this screen.

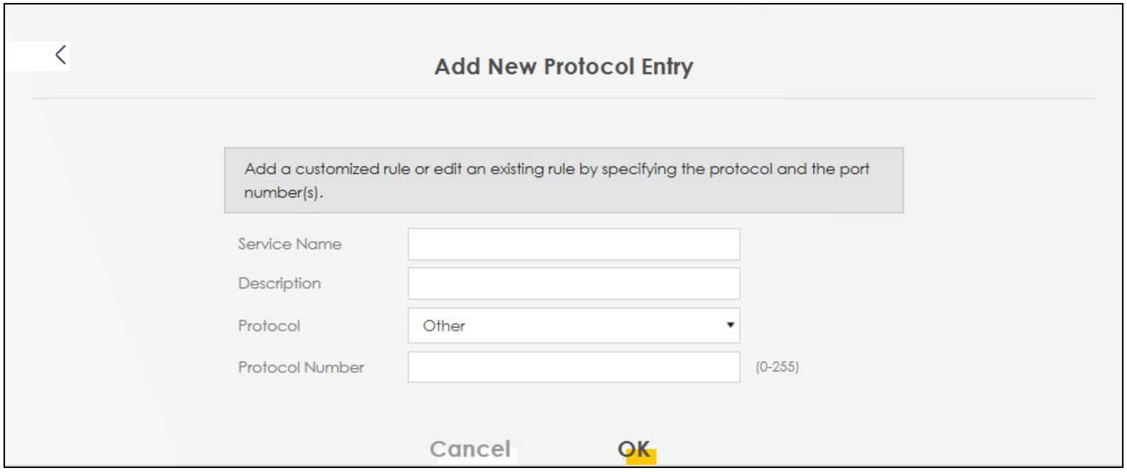
Table 59 Security > Firewall > Protocol

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.
Ports/Protocol Number	This shows the port number or range and the IP protocol (**TCP** or **UDP**) that defines your customized service.
Modify	Click the **Edit** icon (✎) to edit a customized service. Click the **Delete** icon (🗑) to delete an existing customized service.

15.4.1 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 119 Security > Firewall > Protocol: Add New Protocol Entry



Add New Protocol Entry

Add a customized rule or edit an existing rule by specifying the protocol and the port number(s).

Service Name

Description

Protocol: Other

Protocol Number (0-255)

The following table describes the labels in this screen.

Table 60 Security > Firewall > Protocol: Add New Protocol Entry

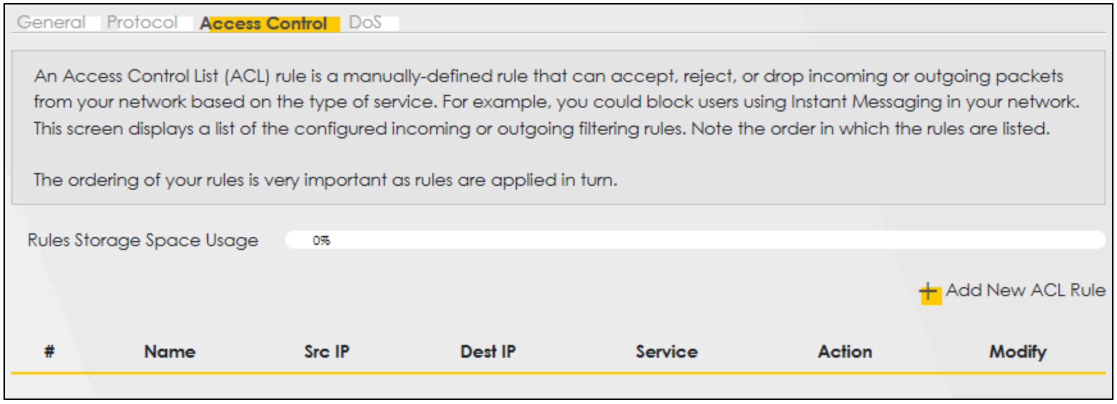
LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Description	Enter a description for your custom port.
Protocol	Choose the protocol (**TCP**, **UDP**, **ICMP**, **ICMPv6**, **Other**) that defines your customized port from the drop down list box.
Protocol Number	Type a single port number or the range of port numbers (**0-255**) that define your customized service.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

15.5 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 120 Security > Firewall > Access Control



An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network based on the type of service. For example, you could block users using Instant Messaging in your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed.

The ordering of your rules is very important as rules are applied in turn.

Rules Storage Space Usage 0%

#	Name	Src IP	Dest IP	Service	Action	Modify

The following table describes the labels in this screen.

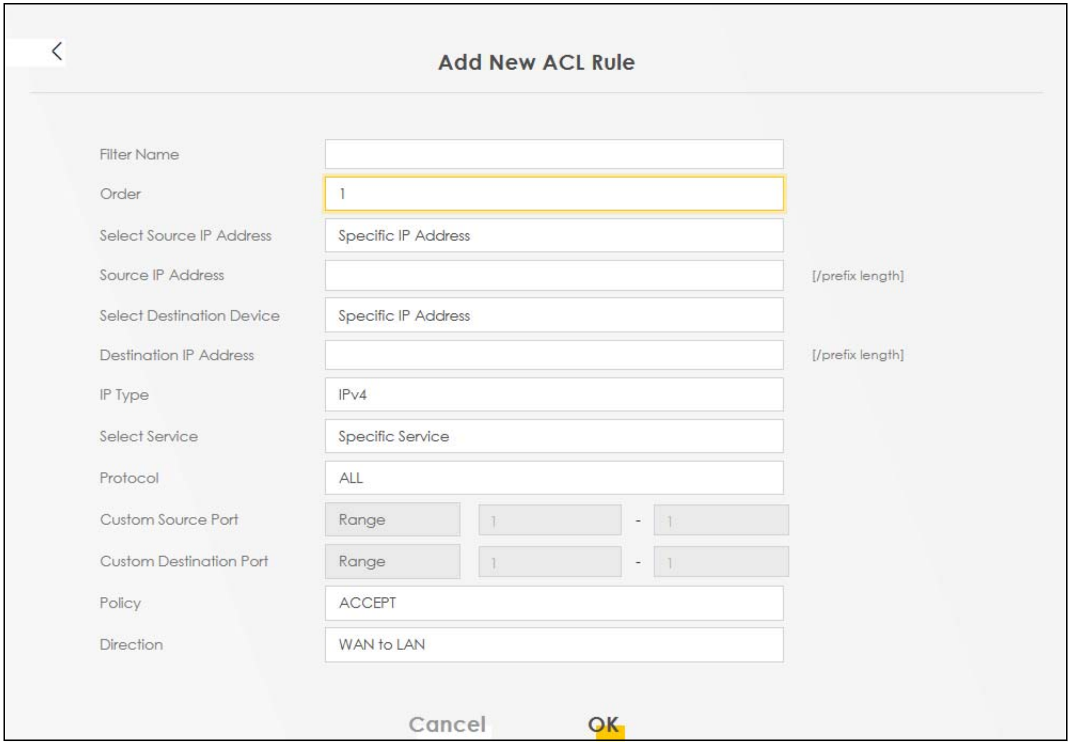
Table 61 Security > Firewall > Access Control

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** 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 (TCP, UDP, TCP/UDP 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.

15.5.1 Add New ACL Rule

Use this screen to configure firewall rules. In the **Access Control** screen, select an index number and click **Add New ACL Rule** or click a rule's **Edit** icon (✎) to display this screen and refer to the following table for information on the labels.

Figure 121 Security > Firewall > Access Control > Add New ACL Rule



Add New ACL Rule

Filter Name		
Order	1	
Select Source IP Address	Specific IP Address	
Source IP Address		[/prefix length]
Select Destination Device	Specific IP Address	
Destination IP Address		[/prefix length]
IP Type	IPv4	
Select Service	Specific Service	
Protocol	ALL	
Custom Source Port	Range	1 - 1
Custom Destination Port	Range	1 - 1
Policy	ACCEPT	
Direction	WAN to LAN	

The following table describes the labels in this screen.

Table 62 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Filter Name	Type a unique name for your filter rule.
Order	Assign the order of your rules as rules are applied in turn.
Select Source IP Address	If you want the source to come from a particular (single) IP, select **Specific IP Address**. If not, select from a detected device.
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).
Select Service	Select a service from the **Select Service** box.
Protocol	Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP**, **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.

Table 62 Security > Firewall > Access Control > Add New ACL Rule (continued)

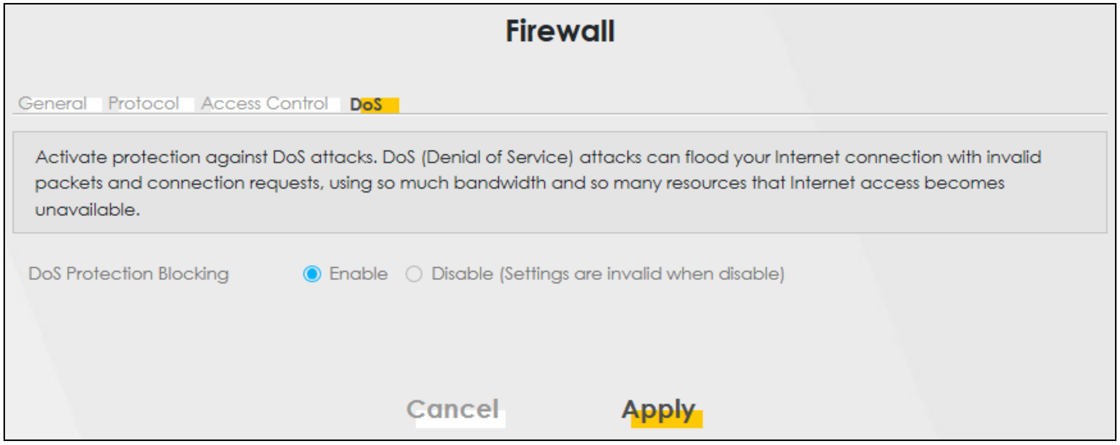
LABEL	DESCRIPTION
Direction	Select **WAN to LAN** to apply the rule to traffic from WAN to LAN. Select **LAN to WAN** to apply the rule to traffic from LAN to WAN. Select **WAN to Router** to apply the rule to traffic from WAN to router. Select **LAN to Router** to apply the rule to traffic from LAN to router.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

15.6 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 122 Security > Firewall > DoS



Firewall

Activate protection against DoS attacks. 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.

DoS Protection Blocking ● Enable ○ Disable (Settings are invalid when disable)

The following table describes the labels in this screen.

Table 63 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.
Cancel	Click this to restore your previously saved settings.
Apply	Click this to save your changes.

15.7 Firewall Technical Reference

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

15.7.1 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.

15.7.2 Guidelines For Security Enhancement With Your Firewall

1. Change the default password via 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 or FTP) that you don't 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.

15.7.3 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 a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. 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 16
MAC Filter

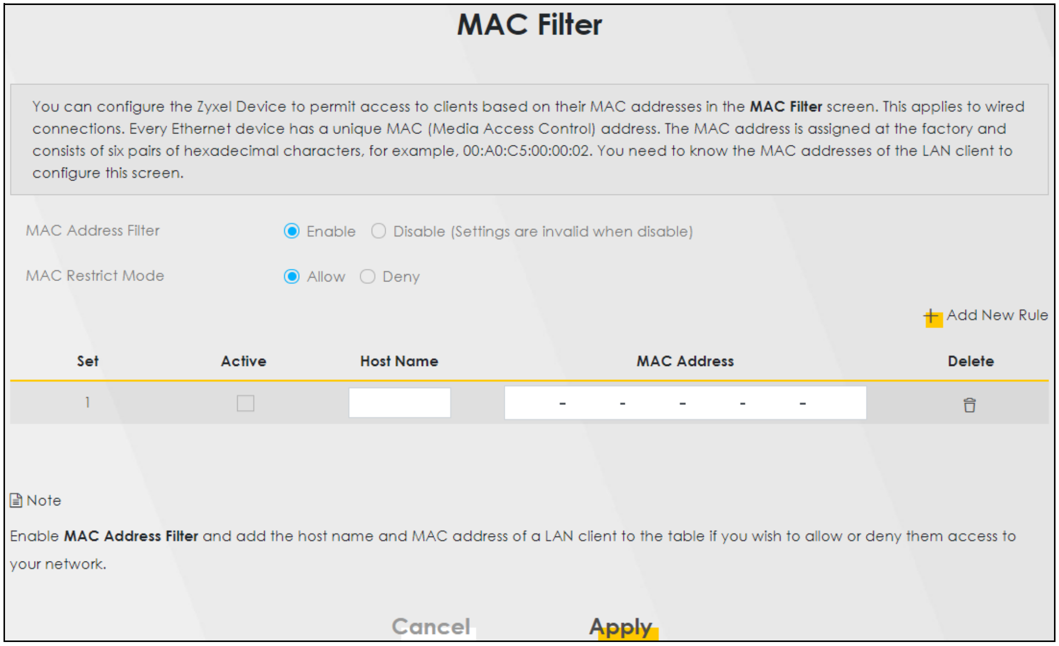
16.1 MAC Filter Overview

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 and wireless 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 the LAN client to configure this screen.

16.2 MAC Filter

Enable **MAC Address Filter** and add the host name and MAC address of a 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 check box under Active is selected if you want to use a filter. Select **Security** > **MAC Filter**. The screen appears as shown.

Figure 123 Security > MAC Filter



MAC Filter

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 the LAN client to configure this screen.

MAC Address Filter ● Enable ○ Disable (Settings are invalid when disable)

MAC Restrict Mode ● Allow ○ Deny

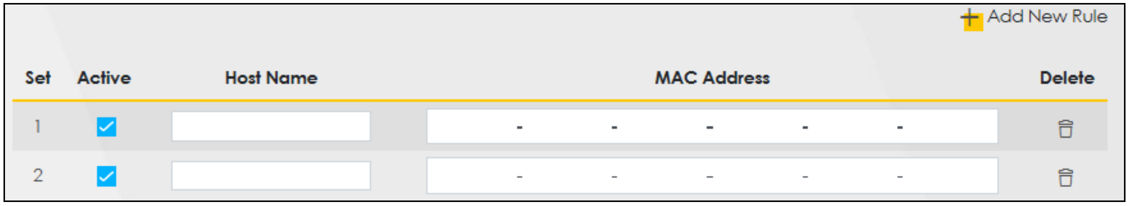
Set	Active	Host Name	MAC Address	Delete
1	□		- - - - -	🗑

Note

Enable **MAC Address Filter** and add the host name and MAC address of a 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 check box under **Active** is selected if you want to use a filter, as shown in the example below.

Figure 124 Security > MAC Filter > Add New Rule



+ Add New Rule

Set	Active	Host Name	MAC Address	Delete
1	☑		- - - - -	🗑
2	☑		- - - - -	🗑

The following table describes the labels in this screen.

Table 64 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.
Add New Rule	Click this button to create a new entry.
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 the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed 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 17
Parental Control

17.1 Parental Control Overview

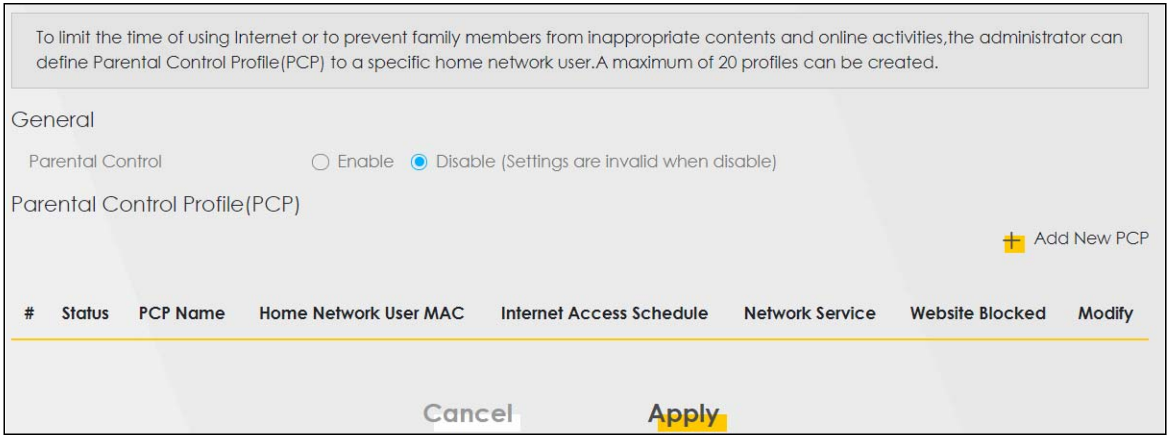
Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

17.2 Parental Control Settings

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 and prevent users from viewing inappropriate content or participating in specified online activities. These rules are defined in a Parental Control Profile (PCP).

Click **Security** > **Parental Control** to open the following screen.

Figure 125 Security > Parental Control



To limit the time of using Internet or to prevent family members from inappropriate contents and online activities,the administrator can define Parental Control Profile(PCP) to a specific home network user.A maximum of 20 profiles can be created.

General

Parental Control ○ Enable ● Disable (Settings are invalid when disable)

Parental Control Profile(PCP)

#	Status	PCP Name	Home Network User MAC	Internet Access Schedule	Network Service	Website Blocked	Modify

The following table describes the fields in this screen.

Table 65 Security > Parental Control

LABEL	DESCRIPTION
General	
Parental Control	Select **Enable** to activate parental control on the Zyxel Device.
Parental Control Profile (PCP)	
Add new PCP	Click this if you want to configure a new Parental Control Profile (PCP).
#	This shows the index number of the rule.
Status	This 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

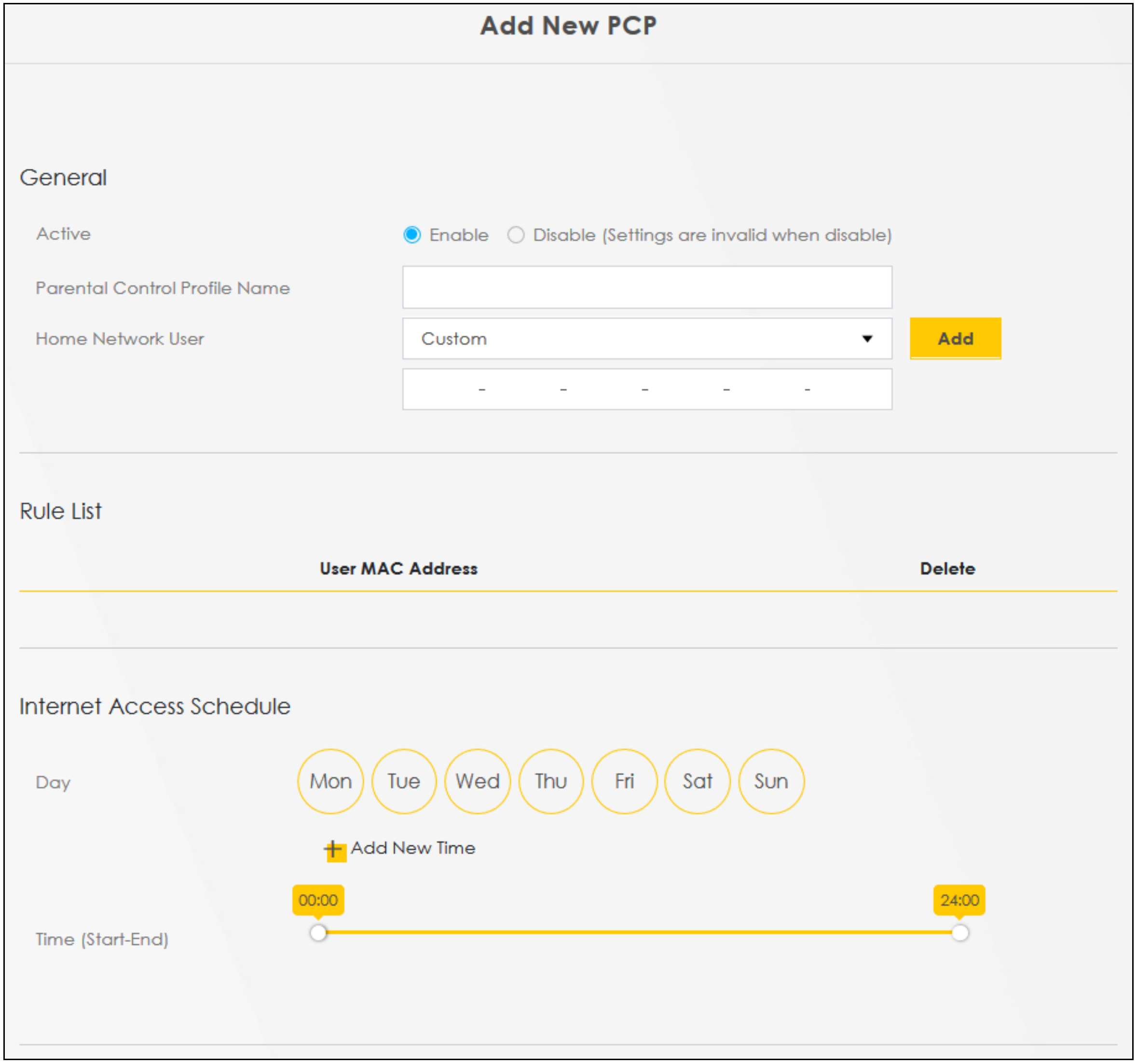
Table 65 Security > Parental Control (continued)

LABEL	DESCRIPTION
PCP Name	This shows the name of the rule.
Home Network User MAC	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the days and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, **None** will be shown.
Website Blocked	This shows whether the website block is configured. If not, **None** will be shown.
Modify	Click the **Edit** icon (✎) to go to the screen where you can edit the rule. 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.

17.2.1 Add or Edit a Parental Control Profile

Click **Add new PCP** 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 and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 126 Security > Parental Control > Add or Edit PCP (General, Rule List & Internet Access Schedule)



Add New PCP

General

Active ● Enable ○ Disable (Settings are invalid when disable)

Parental Control Profile Name

Home Network User: Custom

Rule List

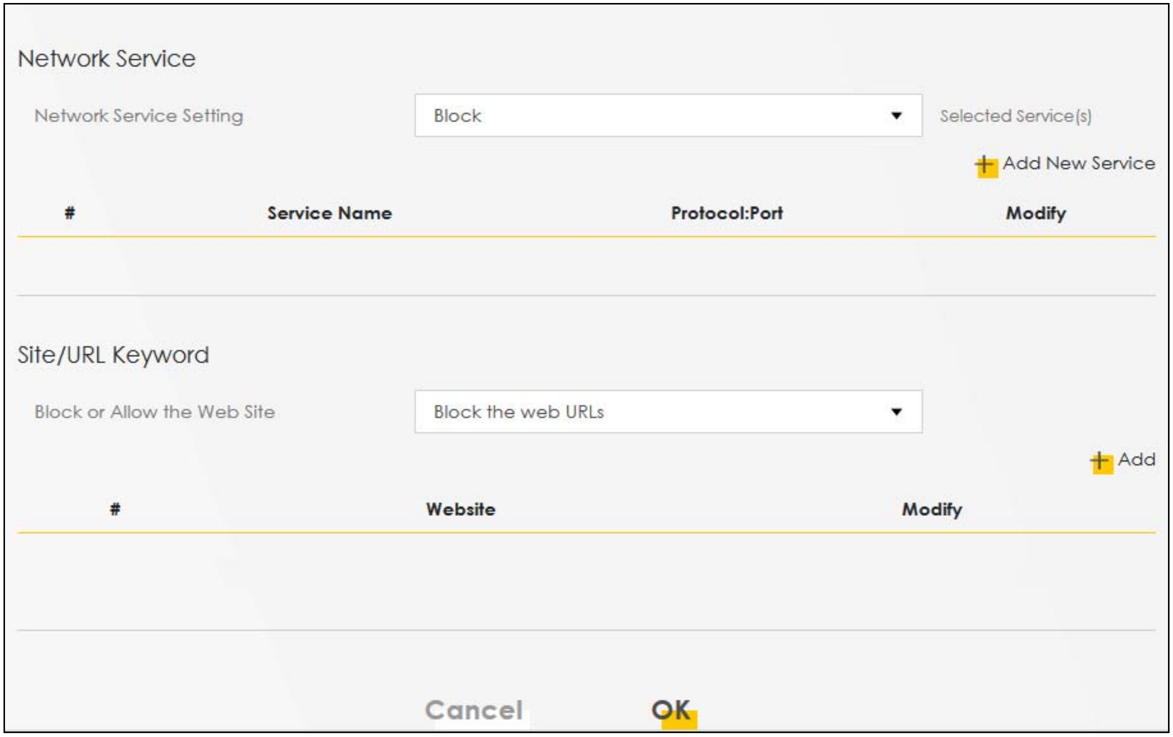
User MAC Address	Delete

Internet Access Schedule

Day: Mon Tue Wed Thu Fri Sat Sun

Time (Start-End): 00:00 – 24:00

Figure 127 Security > Parental Control > Add or Edit PCP (Network Service & Site/URL Keyword)



Network Service

Network Service Setting: Block

Selected Service(s)

#	Service Name	Protocol:Port	Modify

Site/URL Keyword

Block or Allow the Web Site: Block the web URLs

#	Website	Modify

The following table describes the fields in this screen.

Table 66 Security > Parental Control >Add or Edit PCP

LABEL	DESCRIPTION
General	
Active	Select **Enable** or **Disable** to activate or deactivate the parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select **Custom**, enter the LAN user's MAC address. If you select **All**, the rule applies to all LAN users.
Rule List	In **Home Network User**, select **Custom**, enter the LAN user's MAC address, then click the **Add** icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the **Delete** icon (🗑) to remove one.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Zyxel Device to perform parental control.
Time (Start–End)	Drag the time bar to define the time that the LAN user is allowed access (**Authorized access**) or denied access (**No access**).
Add New Time	Click this to add a new time bar. Up to three are allowed.
Network Service	
Network Service Setting	If you select **Block**, the Zyxel Device prohibits the users from viewing the web sites with the URLs listed below. If you select **Allow**, the Zyxel Device blocks access to all URLs except ones listed below.
Add New Service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Port** of the new rule, as shown in Figure 128.

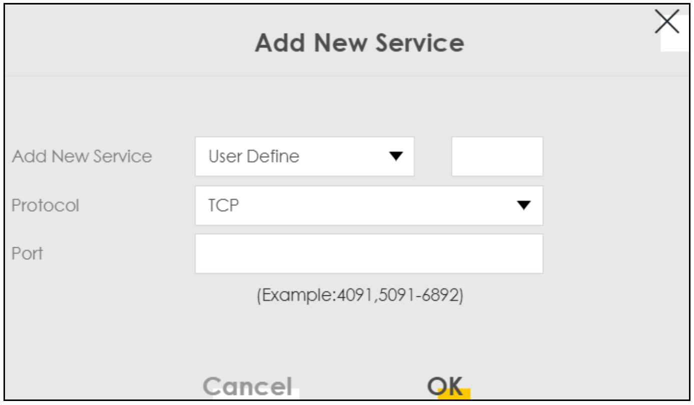
Table 66 Security > Parental Control >Add or Edit PCP (continued)

LABEL	DESCRIPTION
#	This shows the index number of the rule.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the **Edit** icon (✎) to go to the screen where you can edit the rule. Click the **Delete** icon (🗑) to delete an existing rule.
Site/URL Keyword	
Block or Allow the Web Site	If you select **Block the Web URLs**, the Zyxel Device prohibits the users from viewing the Web sites with the URLs listed below. If you select **Allow the Web URLs**, the Zyxel Device blocks access to all URLs except ones listed below.
Add	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
#	This shows the index number of the rule.
Website	This shows the URL of web site or URL keyword to which the Zyxel Device blocks or allows access.
Modify	Click the **Edit** icon (✎) to go to the screen where you can edit the rule. Click the **Delete** icon (🗑) to delete an existing rule.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

Add New Service

Use this screen to add a new service rule.

Figure 128 Security > Parental Control > Add or Edit PCP > Add New Service



Add New Service

Add New Service: User Define

Protocol: TCP

Port:

(Example:4091,5091-6892)

The following table describes the fields in this screen.

Table 67 Security > Parental Control > Add or Edit PCP > Add New Service

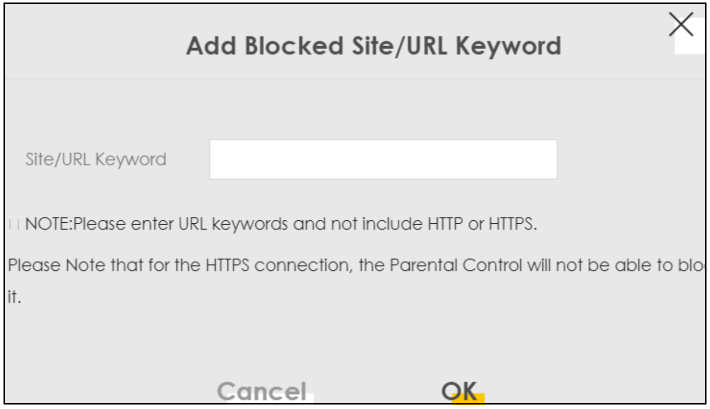
LABEL	DESCRIPTION
Add New Service	Select the name of the service from the drop-down list. Otherwise, select **User Define** and specify the name, protocol, and port of the service. If you have chosen a pre-defined service in the **Service Name** field, this field will not be configurable.
Protocol	Select the transport layer protocol used for the service. Choices are **TCP**, **UDP**, or **TCP&UDP**.
Port	Enter the port of the service. If you have chosen a pre-defined service in the **Service Name** field, this field will not be configurable.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

Add Site/URL Keyword

Click **Add** in the **Site/URL Keyword** section of the **Edit** or **Add new PCP** screen to open the following screen.

Note: Do not include "HTTP" or "HTTPS" in the keyword. HTTPS connections cannot be blocked by Parental Control.

Figure 129 Security > Parental Control > Add or Edit PCP > Add Keyword



Add Blocked Site/URL Keyword

Site/URL Keyword

NOTE:Please enter URL keywords and not include HTTP or HTTPS.

Please Note that for the HTTPS connection, the Parental Control will not be able to blo

it.

The following table describes the fields in this screen.

Table 68 Security > Parental Control > Add or Edit PCP > Add Keyword

LABEL	DESCRIPTION
Site/URL Keyword	Enter a keyword and click **OK** to have the Zyxel Device block access to the website URLs that contain the keyword.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 18 Certificates

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

18.1.1 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 18.3 on page 179).
- 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 18.4 on page 183).

18.2 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.

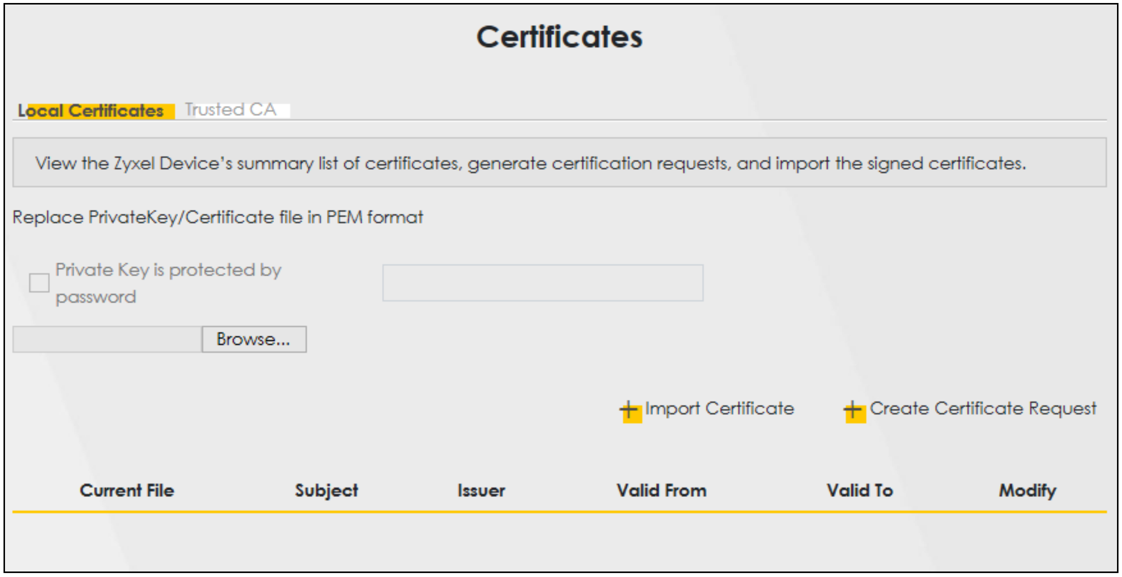
18.3 Local Certificates

View the Zyxel Device's summary list of certificates, generate certification requests, and import the 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 130 Security > Certificates > Local Certificates



Certificates

Local Certificates | Trusted CA

View the Zyxel Device's summary list of certificates, generate certification requests, and import the signed certificates.

Replace PrivateKey/Certificate file in PEM format

□ Private Key is protected by password

Browse...

+ Import Certificate + Create Certificate Request

Current File	Subject	Issuer	Valid From	Valid To	Modify

The following table describes the labels in this screen.

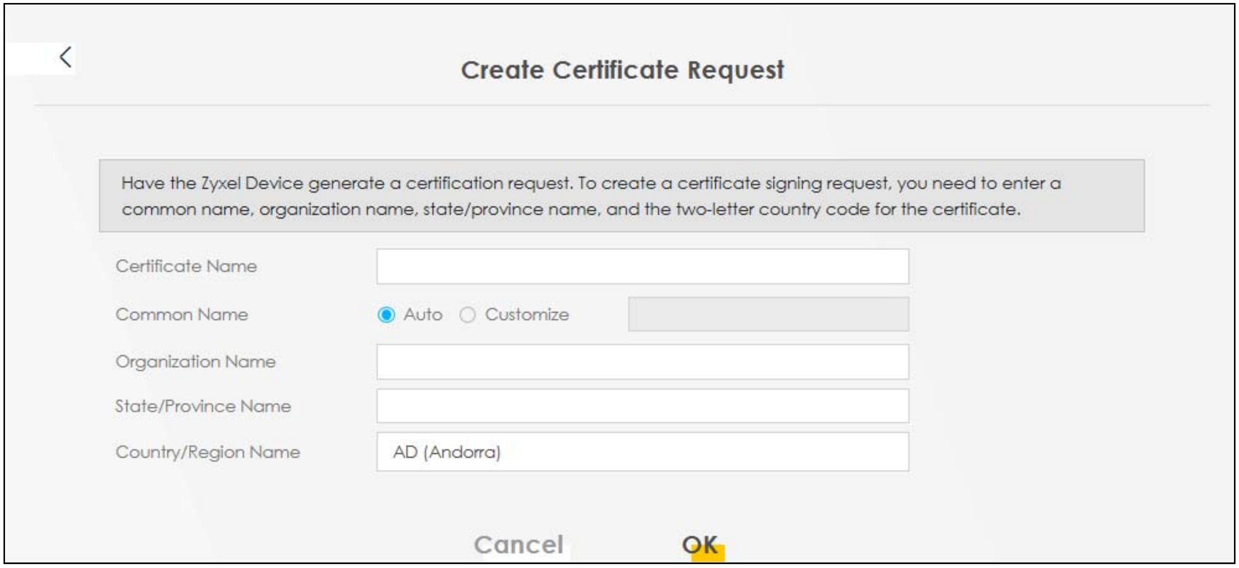
Table 69 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by password	Select the check box and enter the private key into the text box to store it on the Zyxel Device. The private key should not exceed 63 ASCII characters (not including spaces).
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.
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 **Edit** 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 **Delete** 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.

18.3.1 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/province name, and the two-letter country code for the certificate.

Figure 131 Security > Certificates > Local Certificates > Create Certificate Request



Create Certificate Request

Have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Certificate Name	
Common Name	● Auto ○ Customize
Organization Name	
State/Province Name	
Country/Region Name	AD (Andorra)

The following table describes the labels in this screen.

Table 70 Security > Certificates > Local Certificates > Create Certificate Request

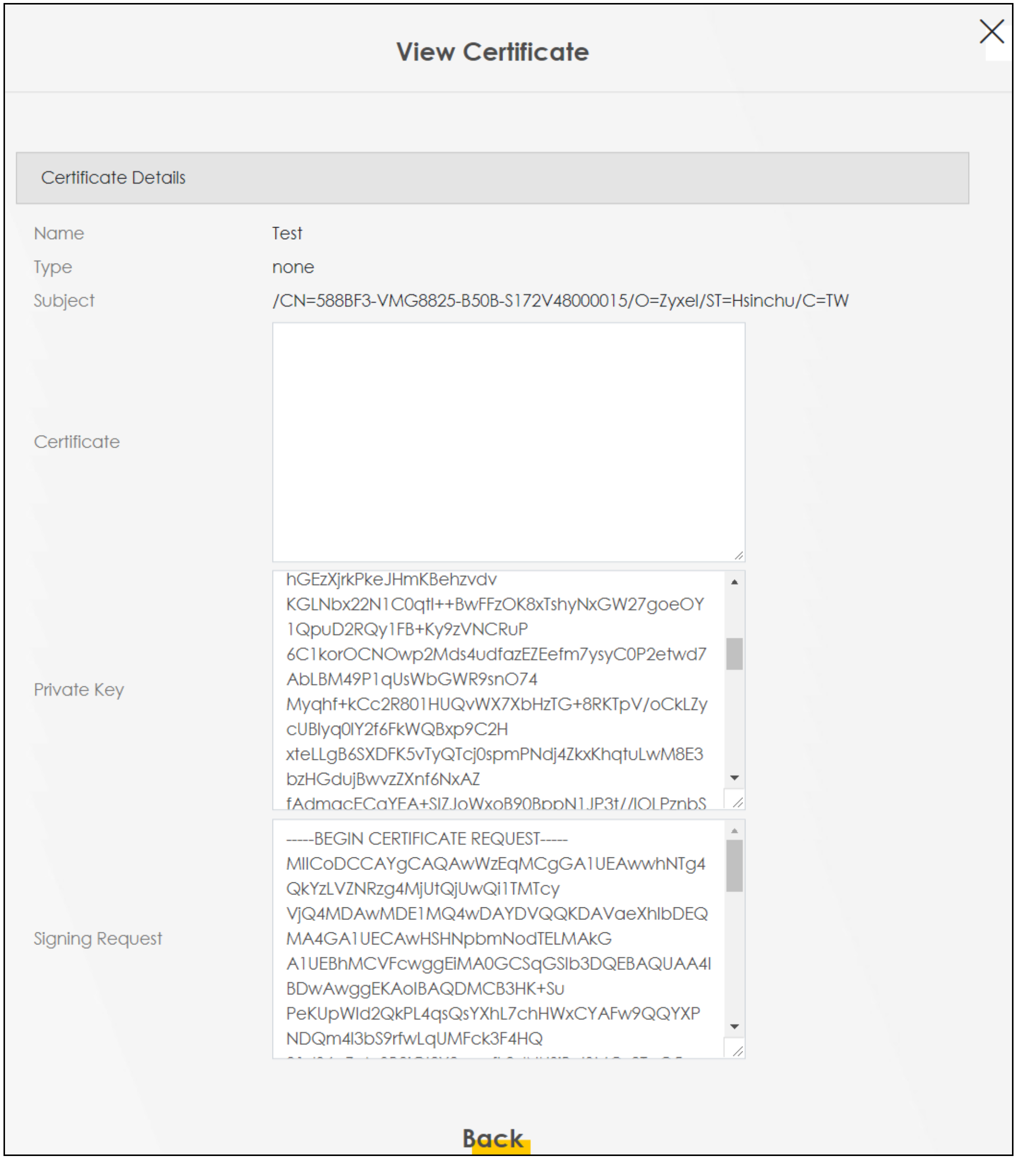
LABEL	DESCRIPTION
Certificate Name	Type up to 32 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the Zyxel Device configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation),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

18.3.2 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 132 Security > Certificates > Local Certificates > View



Certificate Details

Name	Test
Type	none
Subject	/CN=588BF3-VMG8825-B50B-S172V48000015/O=Zyxel/ST=Hsinchu/C=TW
Certificate	

Private Key

```
hGEzXjrkPkeJHmKBehzvdv
KGLNbx22N1C0qtl++BwFFzOK8xTshyNxGW27goeOY
1QpuD2RQy1FB+Ky9zVNCRuP
6C1korOCNOwp2Mds4udfazEZEefm7ysyC0P2etwd7
AbLBM49P1qUsWbGWR9snO74
Myqhf+kCc2R801HUQvWX7XbHzTG+8RKTpV/oCkLZy
cUBlyq0lY2f6FkWQBxp9C2H
xteLLgB6SXDFK5vTyQTcj0spmPNdj4ZkxKhqtuLwM8E3
bzHGdujBwvzZXnf6NxAZ
fAdmacECaYEA+SIZJoWxoB90BppN1JP3t//IOLPznbS
```

Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwWzEqMCgGA1UEAwwhNTg4
QkYzLVZNRzg4MjUtQjUwQi1TMTcy
VjQ4MDAwMDE1MQ4wDAYDVQQKDAVaeXhlbDEQ
MA4GA1UECAwHSHNpbmNodTELMAkG
A1UEBhMCVFcwggEiMA0GCSqGSIb3DQEBAQUAA4I
BDwAwggEKAoIBAQDMCB3HK+Su
PeKUpWld2QkPL4qsQsYXhL7chHWxCYAFw9QQYXP
NDQm4l3bS9rfwLqUMFck3F4HQ
```

The following table describes the fields in this screen.

Table 71 Security > Certificates > Local Certificates > View

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

Table 71 Security > Certificates > Local Certificates > View (continued)

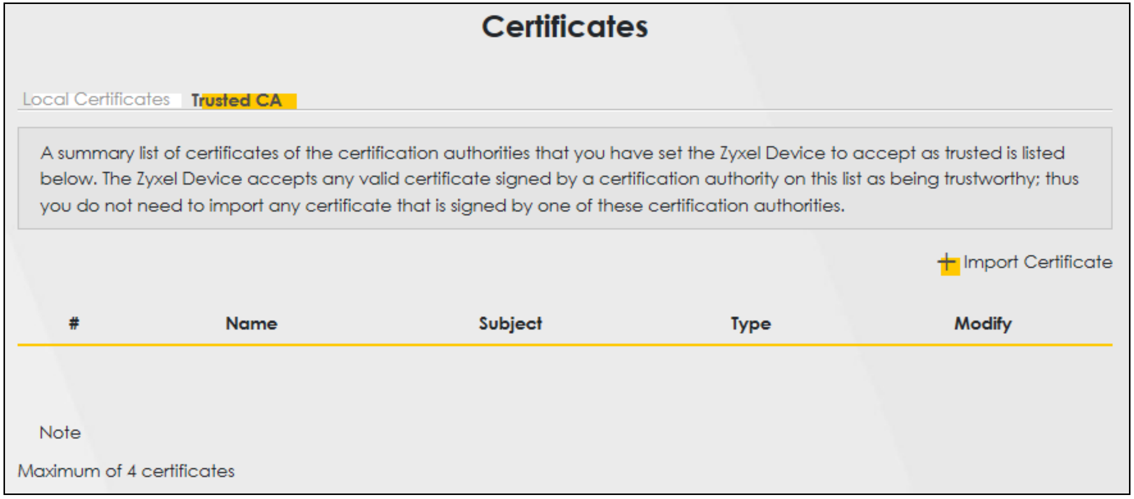
LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste 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.

18.4 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 4 certificates can be added

Figure 133 Security > Certificates > Trusted CA



A summary list of certificates of the certification authorities that you have set the Zyxel Device to accept as trusted is listed below. The Zyxel Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Maximum of 4 certificates

The following table describes the labels in this screen.

Table 72 Security > Certificates > Trusted CA

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

Table 72 Security > Certificates > Trusted CA (continued)

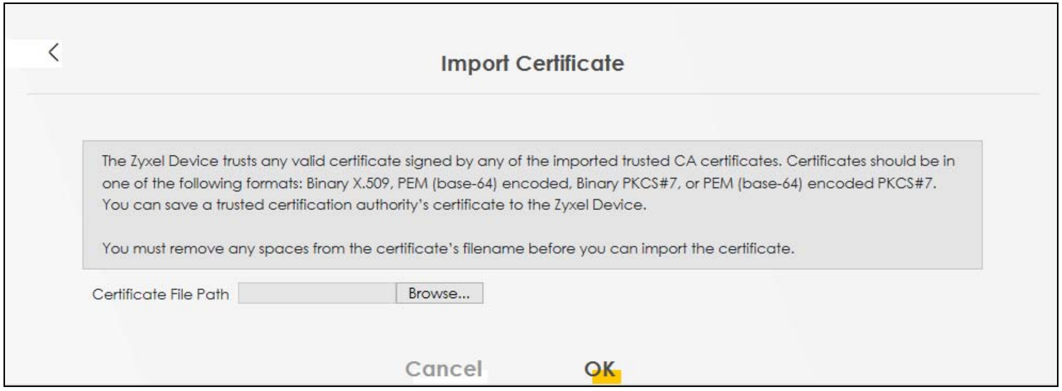
LABEL	DESCRIPTION
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have a unique subject information.
Type	This 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.

18.5 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. You can save a trusted certification authority's certificate to the Zyxel Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 134 Security > Certificate > Trusted CA > Import



Import Certificate

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. You can save a trusted certification authority's certificate to the Zyxel Device.

You must remove any spaces from the certificate's filename before you can import the certificate.

Certificate File Path

The following table describes the labels in this screen.

Table 73 Security > Certificates > Trusted CA > Import

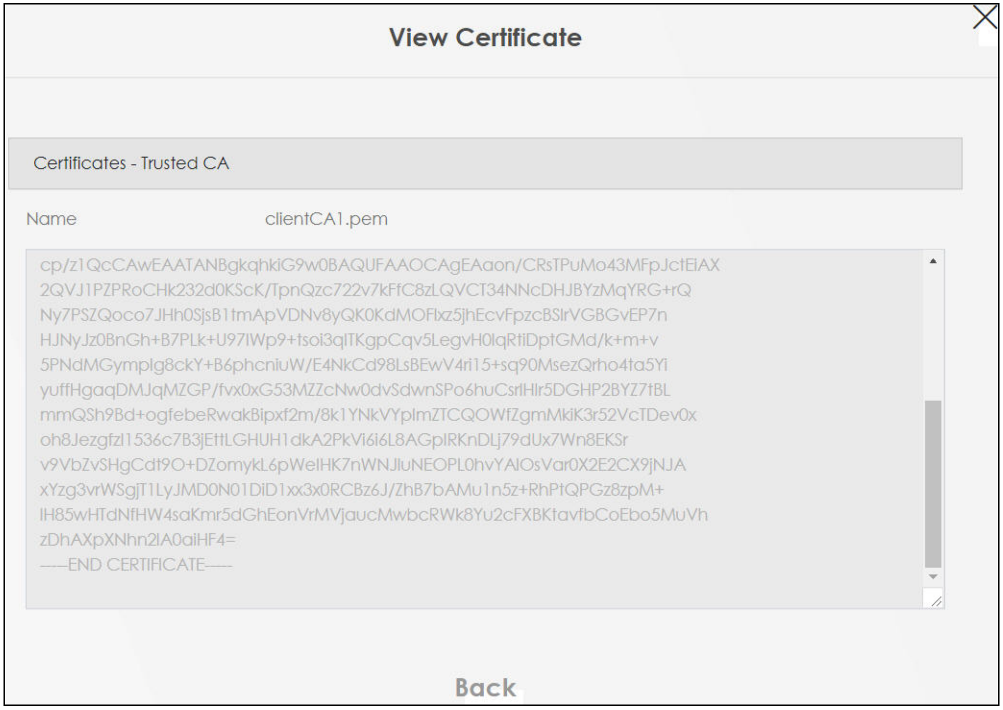
LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click this button to find the certificate file you want to upload.
Cancel	Click this to exit this screen without saving.
OK	Click this to save the certificate on the Zyxel Device.

18.6 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 135 Security > Certificates > Trusted CA > View



Name clientCA1.pem

```
cp/z1QcCAwEAATANBgkqhkiG9w0BAQUFAAOCAgEAaon/CRsTPuMo43MFpJctEiAX
2QVJ1PZPRoCHk232d0KScK/TpnQzc722v7kFfC8zLQVCT34NNcDHJBYzMqYRG+rQ
Ny7PSZQoco7JHh0SjsB1tmApVDNv8yQK0KdMOFlxz5jhEcvFpzcBSlrVGBGvEP7n
HJNyJz0BnGh+B7PLk+U97IWp9+tsoi3qITKgpCqv5LegvH0IqRtiDptGMd/k+m+v
5PNdMGymplg8ckY+B6phcniuW/E4NkCd98LsBEwV4ri15+sq90MsezQrho4ta5Yi
yuffHgaqDMJqMZGP/fvx0xG53MZZcNw0dvSdwnSPo6huCsrlHlr5DGHP2BYZ7tBL
mmQSh9Bd+ogfebeRwakBipxf2m/8k1YNkVYplmZTCQOWfZgmMkiK3r52VcTDev0x
oh8Jezgfzl1536c7B3jEttLGHUH1dkA2PkVi6i6L8AGpIRKnDLj79dUx7Wn8EKSr
v9VbZvSHgCdt9O+DZomykL6pWeIHK7nWNJIuNEOPL0hvYAIOsVar0X2E2CX9jNJA
xYzg3vrWSgjT1LyJMD0N01DiD1xx3x0RCBz6J/ZhB7bAMu1n5z+RhPtQPGz8zpM+
lH85wHTdNfHW4saKmr5dGhEonVrMVjaucMwbcRWk8Yu2cFXBKtavfbCoEbo5MuVh
zDhAXpXNhn2lA0aiHF4=
-----END CERTIFICATE-----
```

The following table describes the labels in this screen.

Table 74 Security > Certificates > Trusted CA > View

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 (via USB thumb drive for example).
Back	Click this to return to the previous screen.

18.7 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.

18.7.1 Verify a Certificate

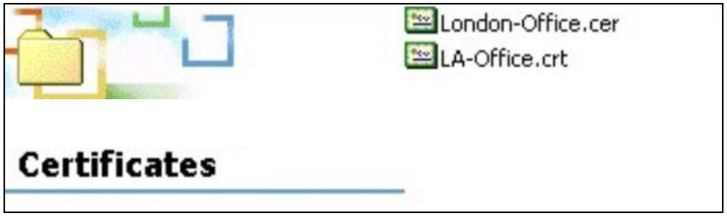
Before you import a trusted CA or trusted remote host certificate into the Zyxel Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the Zyxel Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

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 136 Certificates on Your Computer



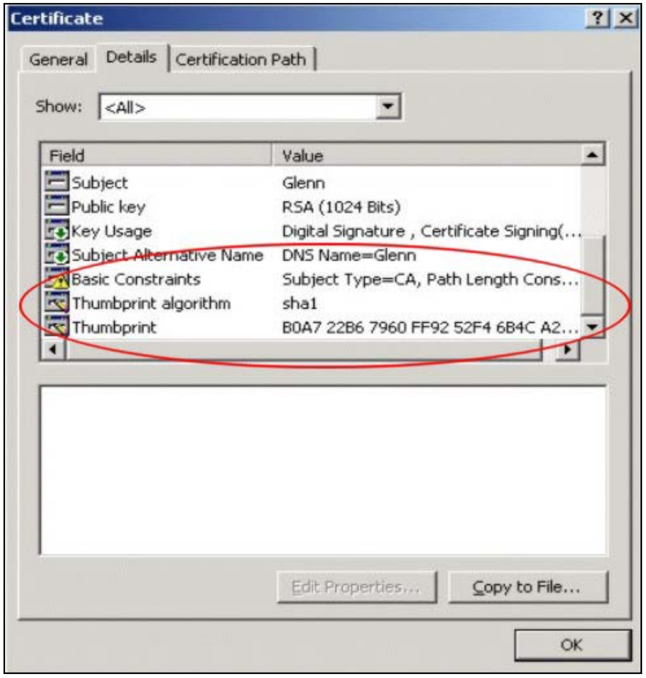
London-Office.cer

LA-Office.crt

Certificates

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 137 Certificate Details



Show: <All>

Field	Value
Subject	Glenn
Public key	RSA (1024 Bits)
Key Usage	Digital Signature , Certificate Signing(...
Subject Alternative Name	DNS Name=Glenn
Basic Constraints	Subject Type=CA, Path Length Cons...
Thumbprint algorithm	sha1
Thumbprint	B0A7 22B6 7960 FF92 52F4 6B4C A2...

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 19
Log

19.1 Log Overview

These screens allow you to determine the categories of events and/or alerts that the Zyxel Device logs and then display these logs or have the Zyxel Device send them to an administrator (through email) or to a syslog server.

19.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 19.2 on page 189).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 19.3 on page 190).

19.1.2 What You Need To Know

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

Alerts and Logs

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

Syslog Overview

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

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

Table 75 Syslog Severity Levels

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

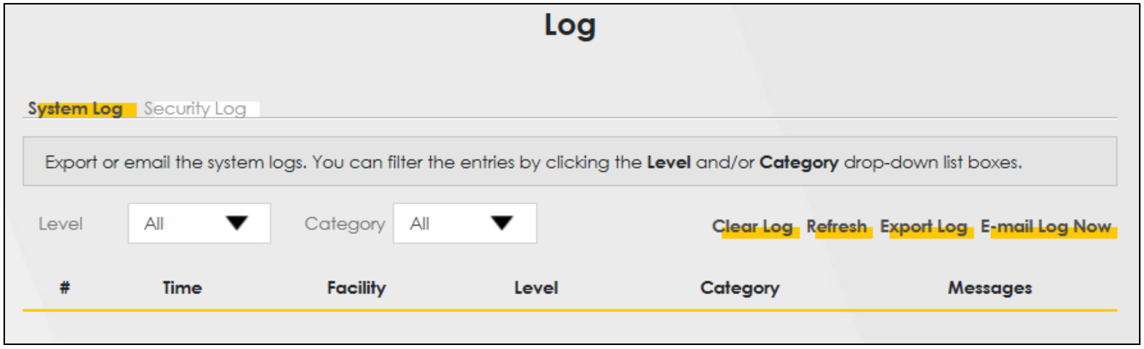
Table 75 Syslog Severity Levels (continued)

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

19.2 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 138 System Monitor > Log > System Log



Export or email the system logs. You can filter the entries by clicking the **Level** and/or **Category** drop-down list boxes.

The following table describes the fields in this screen.

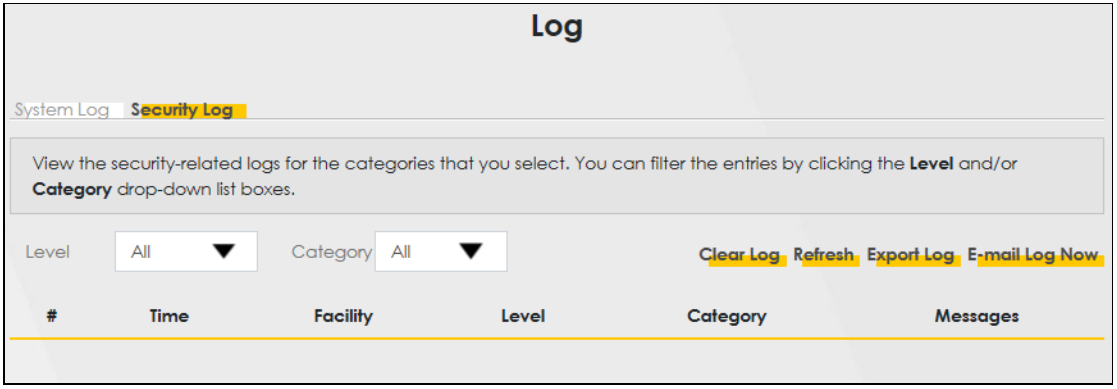
Table 76 System Monitor > Log > System Log

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 log(s).
E-mail Log Now	Click this to send the log file(s) to the e-mail address you specify in the **Maintenance > Logs 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 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.

19.3 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 139 System Monitor > Log > Security Log



Log

View the security-related logs for the categories that you select. You can filter the entries by clicking the **Level** and/or **Category** drop-down list boxes.

Level: All ▼ Category: All ▼

#	Time	Facility	Level	Category	Messages

The following table describes the fields in this screen.

Table 77 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 log(s).
E-mail Log Now	Click this to send the log file(s) to the e-mail address you specify in the **Maintenance > Logs 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 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 20 AS Traffic Status

20.1 Traffic Status Overview

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

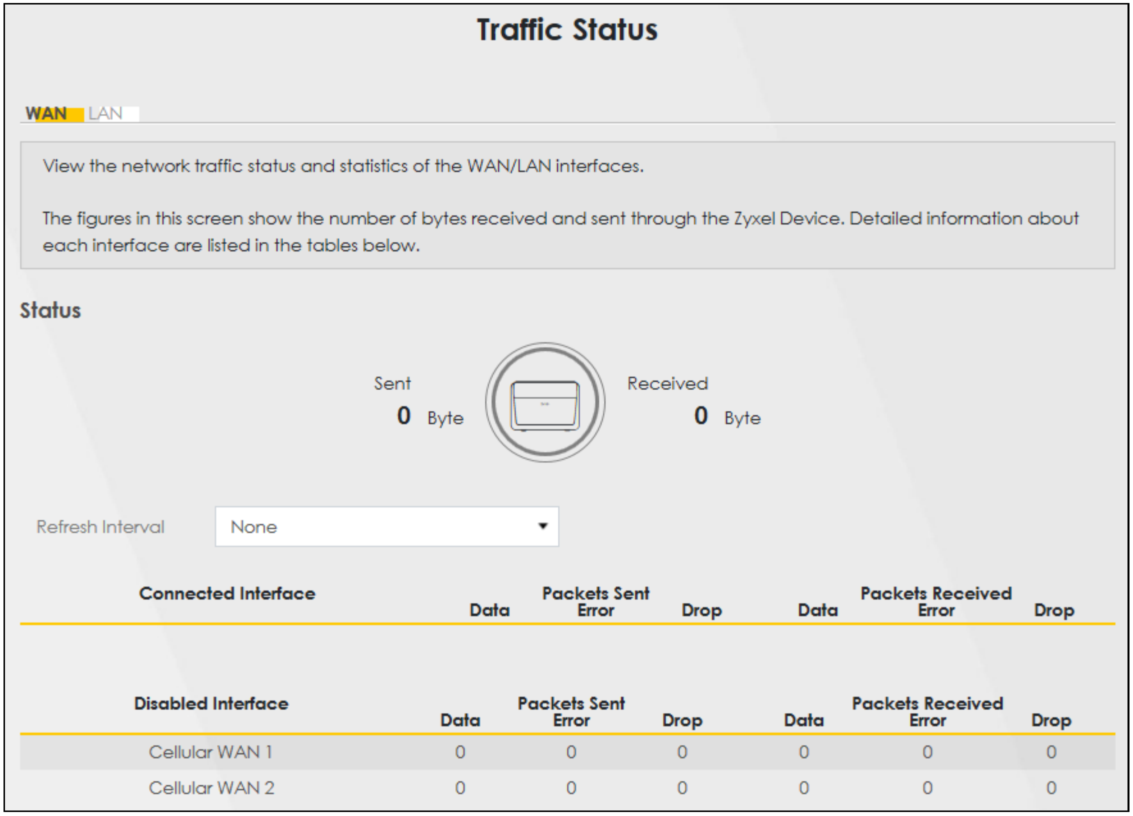
20.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 20.2 on page 191).
- Use the **LAN** screen to view the LAN traffic statistics (Section 20.3 on page 193).

20.2 WAN Status

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figures in this screen show the total number of bytes received and sent through the Zyxel Device's WAN interface. The tables below show packet statistics for each WAN interface.

Figure 140 System Monitor > Traffic Status > WAN



Traffic Status

View the network traffic status and statistics of the WAN/LAN interfaces.

The figures in this screen show the number of bytes received and sent through the Zyxel Device. Detailed information about each interface are listed in the tables below.

Status

Sent 0 Byte

Received 0 Byte

Refresh Interval: None

Connected Interface	Packets Sent Data	Packets Sent Error	Packets Sent Drop	Packets Received Data	Packets Received Error	Packets Received Drop

Disabled Interface	Packets Sent Data	Packets Sent Error	Packets Sent Drop	Packets Received Data	Packets Received Error	Packets Received Drop
Cellular WAN 1	0	0	0	0	0	0
Cellular WAN 2	0	0	0	0	0	0

The following table describes the fields in this screen.

Table 78 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.
Packets Received	
Data	This indicates the number of received packets on this interface.

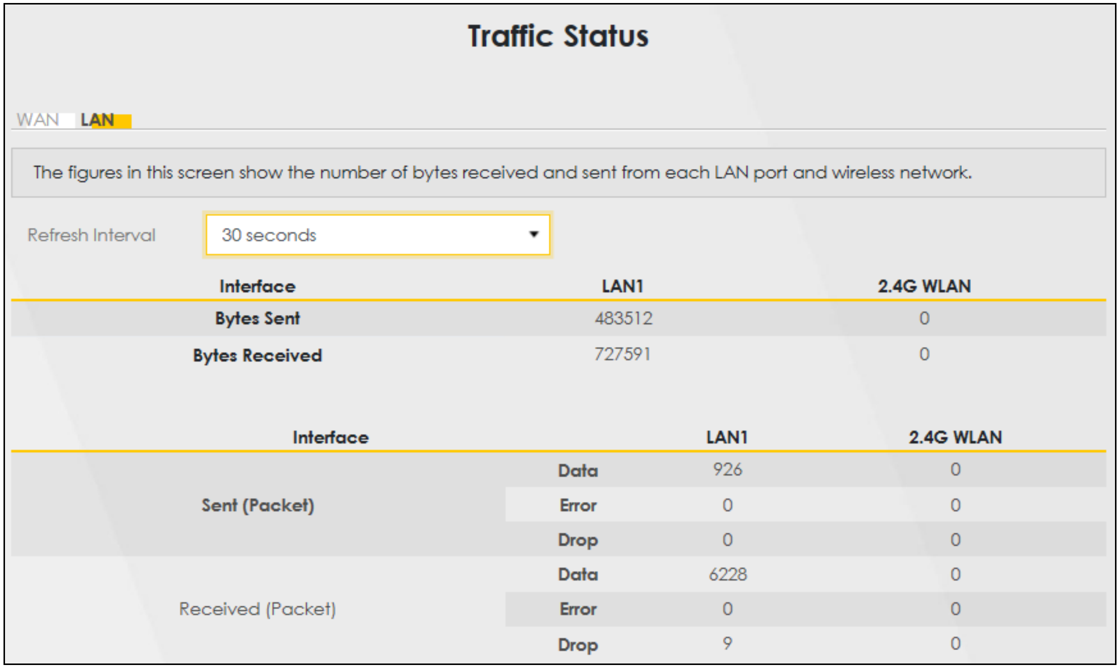
Table 78 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
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.

20.3 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 141 System Monitor > Traffic Status > LAN



Traffic Status

The figures in this screen show the number of bytes received and sent from each LAN port and wireless network.

Refresh Interval: 30 seconds

Interface	LAN1	2.4G WLAN
Bytes Sent	483512	0
Bytes Received	727591	0

Interface		LAN1	2.4G WLAN
Sent (Packet)	Data	926	0
	Error	0	0
	Drop	0	0
Received (Packet)	Data	6228	0
	Error	0	0
	Drop	9	0

The following table describes the fields in this screen.

Table 79 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.

Table 79 System Monitor > Traffic Status > LAN (continued)

LABEL	DESCRIPTION
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

CHAPTER 21 ARP Table

21.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, known as a Media Access Control or 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.

21.1.1 How ARP Works

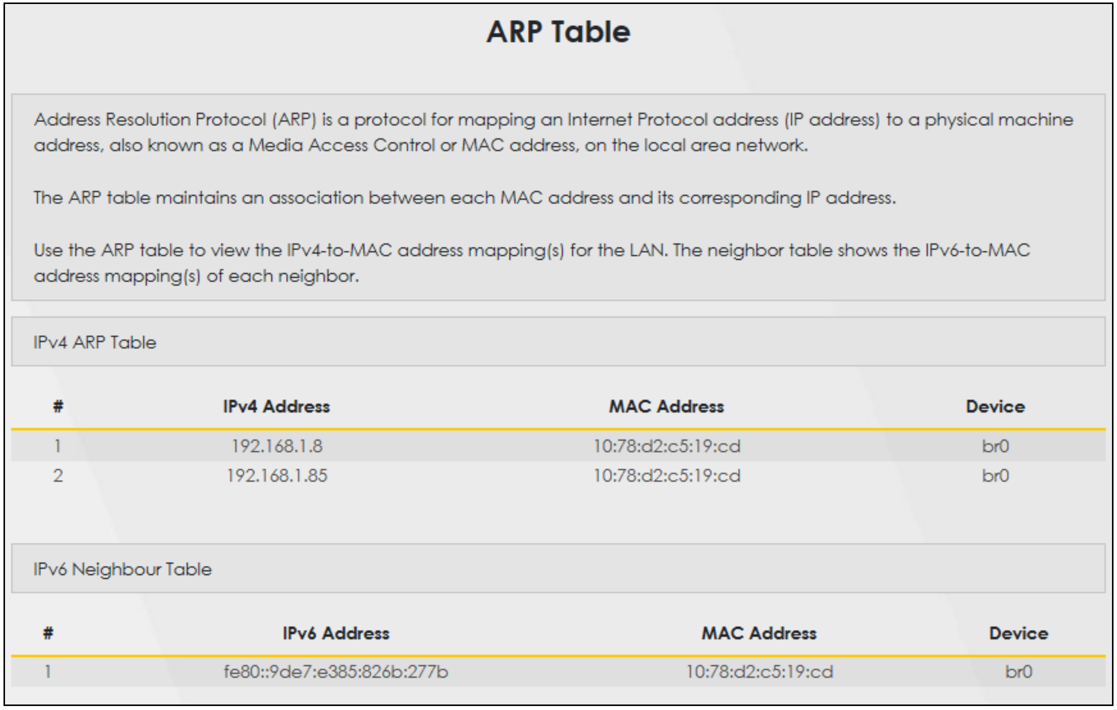
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

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.

21.2 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 142 System Monitor > ARP Table



ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

The ARP table maintains an association between each MAC address and its corresponding IP address.

Use the ARP table to view the IPv4-to-MAC address mapping(s) for the LAN. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor.

IPv4 ARP Table

#	IPv4 Address	MAC Address	Device
1	192.168.1.8	10:78:d2:c5:19:cd	br0
2	192.168.1.85	10:78:d2:c5:19:cd	br0

IPv6 Neighbour Table

#	IPv6 Address	MAC Address	Device
1	fe80::9de7:e385:826b:277b	10:78:d2:c5:19:cd	br0

The following table describes the labels in this screen.

Table 80 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP/Neighbour table entry number.
IPv4/IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click the device type to go to its configuration screen.

CHAPTER 22
Routing Table

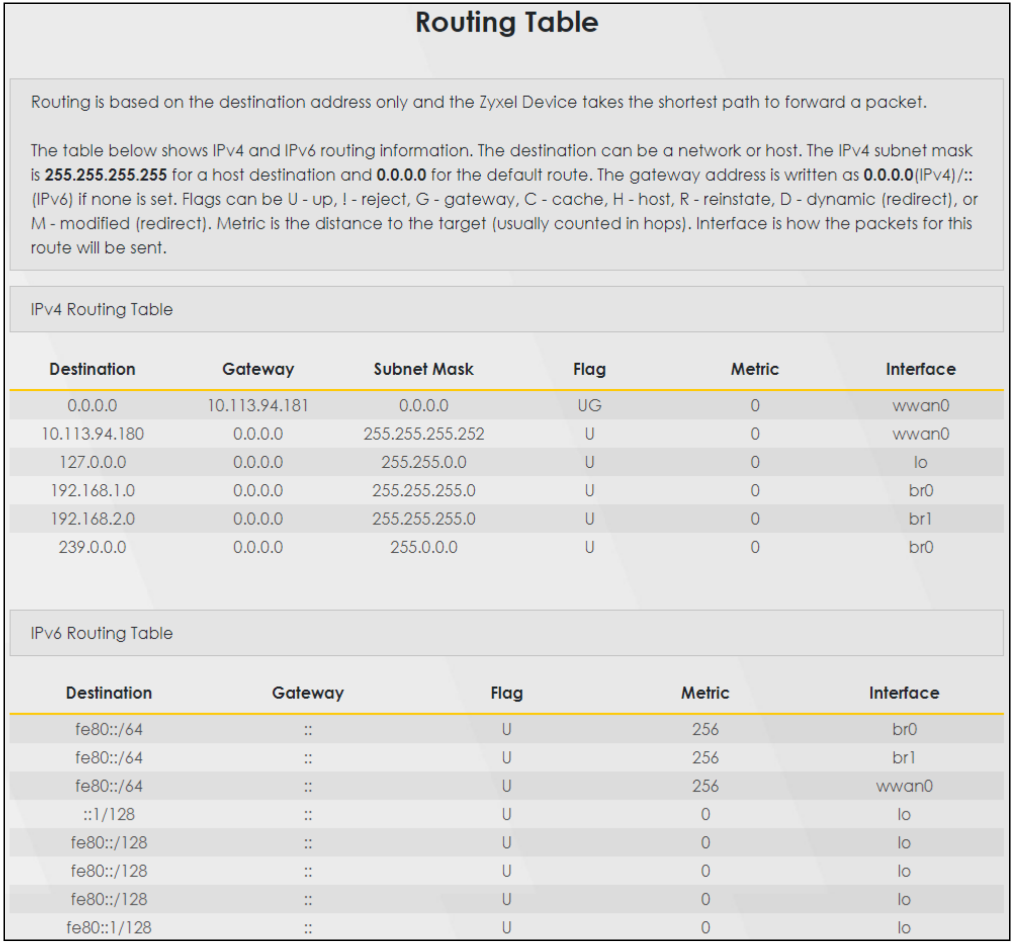
22.1 Routing Table Overview

Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

22.2 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 143 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 destination can be a network or host. 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 **0.0.0.0**(IPv4)/::(IPv6) if none is set. Flags can be U - up, ! - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), or M - modified (redirect). Metric is the distance to the target (usually counted in hops). Interface is how the packets for this route will be sent.

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
0.0.0.0	10.113.94.181	0.0.0.0	UG	0	wwan0
10.113.94.180	0.0.0.0	255.255.255.252	U	0	wwan0
127.0.0.0	0.0.0.0	255.255.0.0	U	0	lo
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	br1
239.0.0.0	0.0.0.0	255.0.0.0	U	0	br0

IPv6 Routing Table

Destination	Gateway	Flag	Metric	Interface
fe80::/64	::	U	256	br0
fe80::/64	::	U	256	br1
fe80::/64	::	U	256	wwan0
::1/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::/128	::	U	0	lo
fe80::1/128	::	U	0	lo

The following table describes the labels in this screen.

Table 81 System Monitor > Routing Table

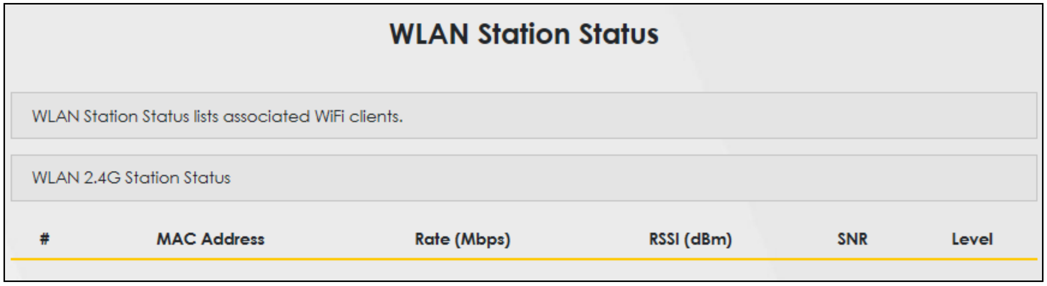
LABEL	DESCRIPTION
IPv4/IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.
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.

CHAPTER 23 WLAN Station Status

23.1 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 wireless stations (wireless clients) that are currently associated with the Zyxel Device. Being associated means that a wireless client (for example, your computer with a wireless network card installed) has connected successfully to an AP (or wireless router) using the same SSID, channel, and WiFi security settings.

Figure 144 System Monitor > WLAN Station Status



WLAN Station Status

WLAN Station Status lists associated WiFi clients.

WLAN 2.4G Station Status

#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level

The following table describes the labels in this screen.

Table 82 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated wireless station and the Zyxel Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's wireless connection. The normal range is -30dBm to -79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.

Table 82 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The normal range is 15 to 40. If the value drops below 15, try moving the associated wireless station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated wireless 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.

CHAPTER 24
Cellular WAN Status

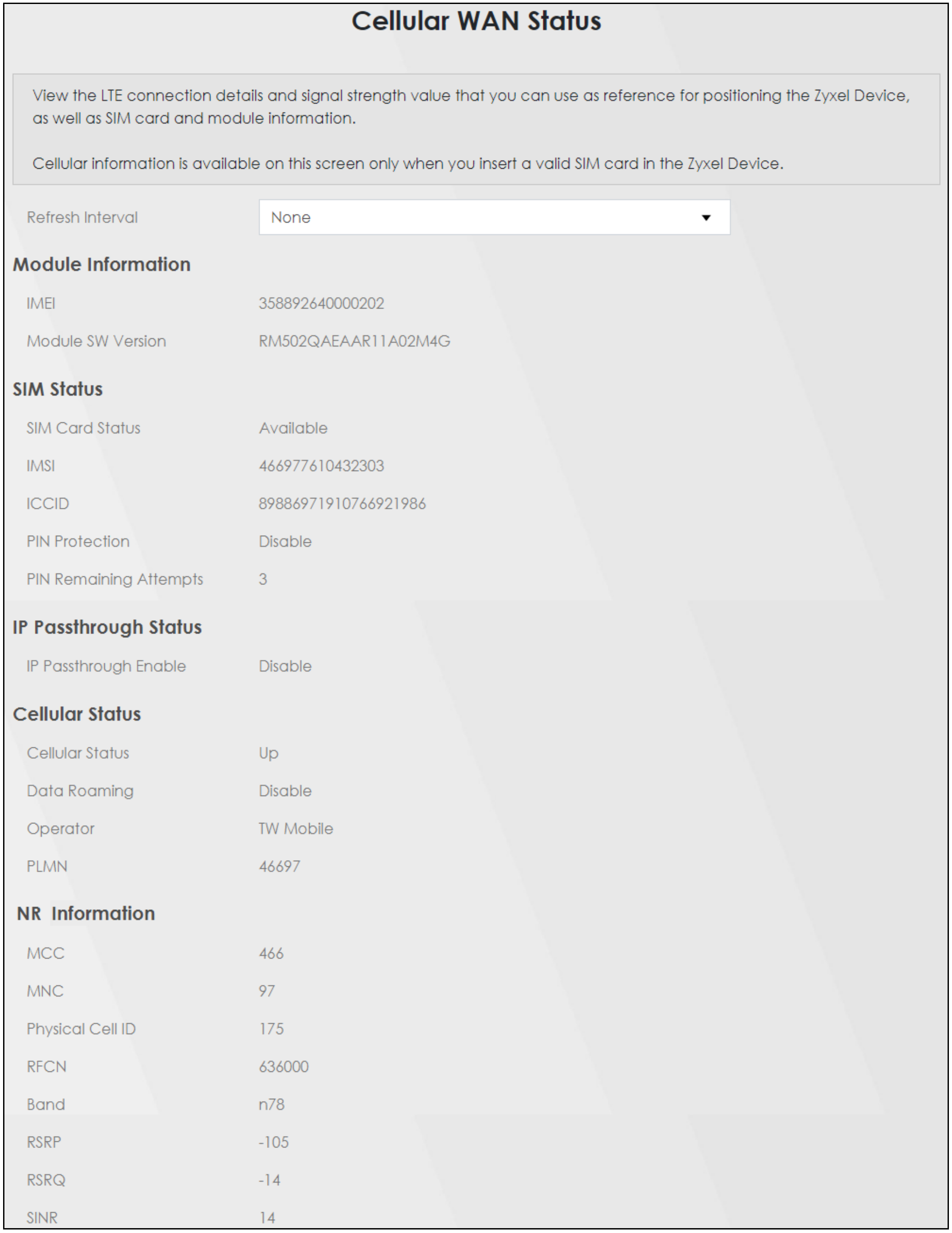
24.1 Cellular WAN Status Overview

View the cellular connection details and the signal strength value that you can use as reference for positioning the Zyxel Device, as well as SIM card and module information.

24.2 Cellular WAN Status

To open this screen, click **System Monitor > Cellular WAN Status**. Cellular information is available on this screen only when you insert a valid SIM card in the Zyxel Device.

Figure 145 System Monitor > Cellular WAN Status



Cellular WAN Status

View the LTE connection details and signal strength value that you can use as reference for positioning the Zyxel Device, as well as SIM card and module information.

Cellular information is available on this screen only when you insert a valid SIM card in the Zyxel Device.

Refresh Interval	None ▾

Module Information

IMEI	358892640000202
Module SW Version	RM502QAEAAR11A02M4G

SIM Status

SIM Card Status	Available
IMSI	466977610432303
ICCID	89886971910766921986
PIN Protection	Disable
PIN Remaining Attempts	3

IP Passthrough Status

IP Passthrough Enable	Disable

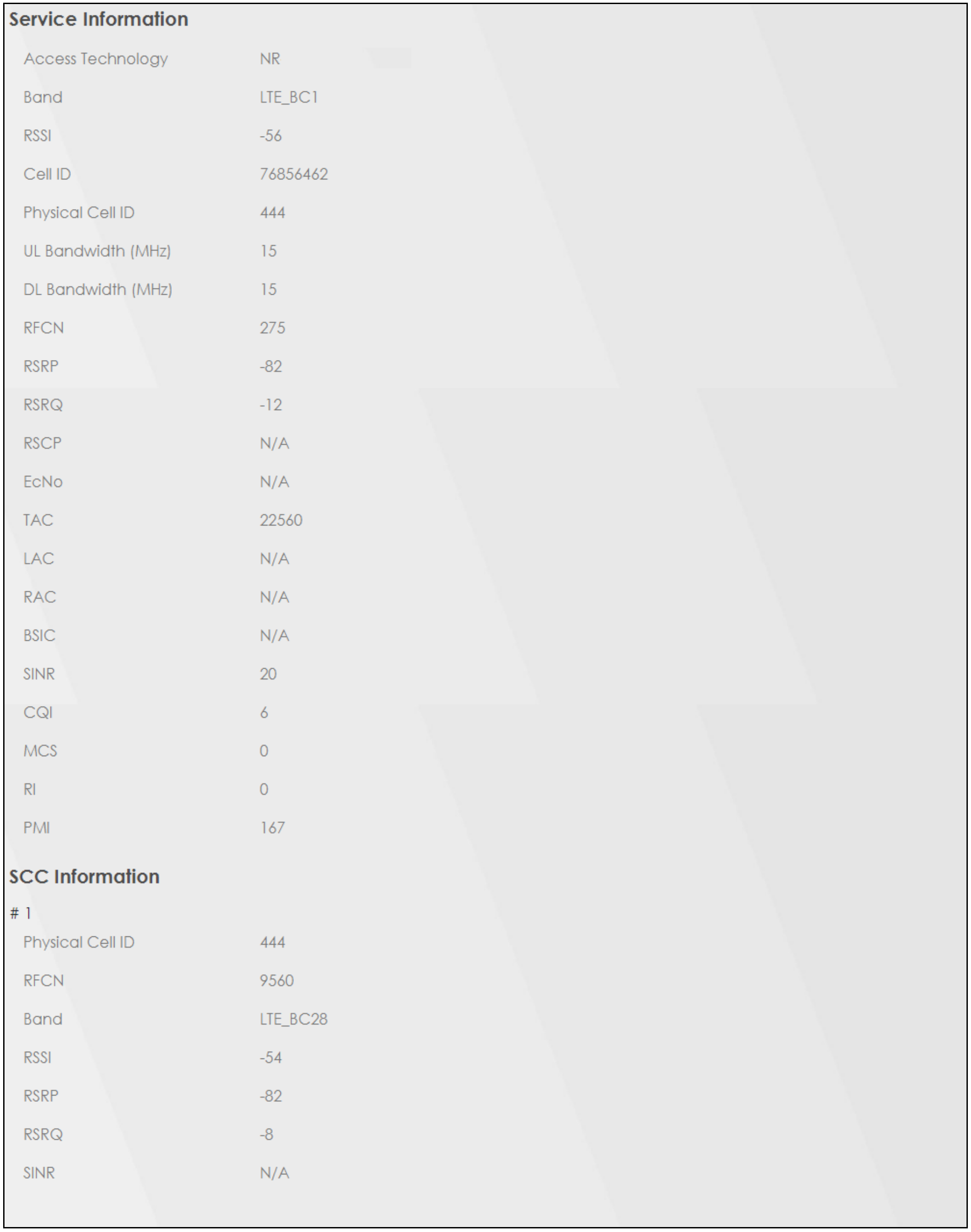
Cellular Status

Cellular Status	Up
Data Roaming	Disable
Operator	TW Mobile
PLMN	46697

NR Information

MCC	466
MNC	97
Physical Cell ID	175
RFCN	636000
Band	n78
RSRP	-105
RSRQ	-14
SINR	14

Figure 146 System Monitor > Cellular WAN Status (Service Information)



Service Information

Access Technology	NR
Band	LTE_BC1
RSSI	-56
Cell ID	76856462
Physical Cell ID	444
UL Bandwidth (MHz)	15
DL Bandwidth (MHz)	15
RFCN	275
RSRP	-82
RSRQ	-12
RSCP	N/A
EcNo	N/A
TAC	22560
LAC	N/A
RAC	N/A
BSIC	N/A
SINR	20
CQI	6
MCS	0
RI	0
PMI	167

SCC Information

1

Physical Cell ID	444
RFCN	9560
Band	LTE_BC28
RSSI	-54
RSRP	-82
RSRQ	-8
SINR	N/A

Note: The fields in the screen may differ slightly based on the Access Technology your Zyxel Device supports.

Note: The value is ‘0’ (zero) or ‘N/A’ if the Access Technology the Zyxel Device is currently connected to doesn’t have this value in that specific parameter field or there is no network connection.

The following table describes the labels in this screen.

Table 83 System Monitor > Cellular WAN Status

LABEL	DESCRIPTION
Refresh Interval	Select the time interval the Zyxel Device will check and refresh the fields shown on this screen. Select **None** to stop detection.
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Module SW Version	This shows the software version of the 5G module.
SIM Status	
SIM Card Status	This displays the SIM card status: **None -** the Zyxel Device does not detect that there is a SIM card inserted. **Waiting SIM Available** - the SIM card is detected but not available yet. **Available** - the SIM card could either have or does not have PIN code security. **Locked** - the SIM card has PIN code security, but you did not enter the PIN code yet. **Blocked** - you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card. **Error** - the Zyxel Device detected that the SIM card has errors.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (**ICCID**). This is the serial number of the SIM card.
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. This field shows **Enable** if **PIN Protection** is enabled. Otherwise, this field shows **Disable**
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
IP Passthrough Enable	This displays if IP Passthrough is enabled on the Zyxel Device. IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.
Data Roaming	This displays if data roaming is enabled on the Zyxel Device. 5G roaming is to use your Zyxel Device in an area which is not covered by your service provider. Enable roaming to ensure that your Zyxel Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Operator	This displays the name of the service provider.
PLMN	This displays the PLMN number.
Current Access Technology/Service/SCC Information	
#	This is the index number of the Secondary Component Carrier (SCC). The Zyxel Device supports Carrier Aggregation (CA) to use multiple LTE carriers simultaneously for data transmission. CA consists of a primary component carrier (PCC) and secondary component carriers (SCC). The PCC is used for control signaling and the SCC is used for increased data throughput.

Table 83 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
MCC	This shows the Mobile Country Code (MCC). MCC is a unique code that identifies the country where a Public Land Mobile Network (PLMN) is at.
MNC	This shows the Mobile Network Code (MNC). MNC is a unique code that identifies a Public Land Mobile Network (PLMN) in a country. MCC and MNC combined together are used to identify a globally unique PLMN.
Access Technology	This displays the type of mobile network to which your Zyxel Device is currently connected.
Band	This displays the current cellular band of your Zyxel Device.
RSSI	This displays the strength of the cellular signal between an associated cellular station and the Zyxel Device.
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting. The value depends on the current Access Technology: • For LTE/5G, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331.
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Zyxel Device and the mobile network it is connected to.
UL Bandwidth (MHz)	This shows the uplink cellular channel bandwidth from the Zyxel Device to base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
DL Bandwidth (MHz)	This shows the downlink cellular channel bandwidth from base station to the Zyxel Device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting. The value depends on the current Access Technology: • For LTE, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. • For 5G, it is the NR-ARFCN (New Radio Absolute Radio-Frequency Channel Number).
RSRP	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133. An undetectable signal is indicated by the lower limit, example -140 dBm. The normal range is -44 to -140. The signal is better when the value is closer to -44.
RSRQ	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example -240. The normal range is -3 to -20. The signal is better when the value is closer to -3.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device. The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example -120 dBm.
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level. The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example -240 dB.

Table 83 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber. The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN. The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003].
RAC	This displays the RAC (Routing Area Code), which is used in mobile network “packet domain service” (PS) to identify a routing area within a location area. In a mobile network, the Zyxel Device uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and uses RAC to identify the location of data service like HSDPA or LTE. The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003].
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good/bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI). PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer). PMI determines how cellular data are encoded for the antennas to improve downlink rate.

CHAPTER 25
System

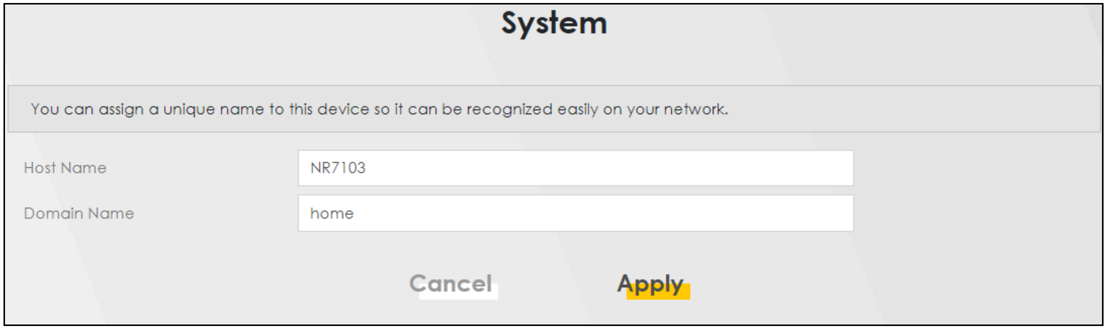
25.1 System Overview

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

25.2 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. You can use up to 30 characters, including spaces.

Figure 147 Maintenance > System



System

You can assign a unique name to this device so it can be recognized easily on your network.

Host Name: NR7103

Domain Name: home

The following table describes the labels in this screen.

Table 84 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your host Zyxel Device.
Cancel	Click **Cancel** to abandon this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 26
User Account

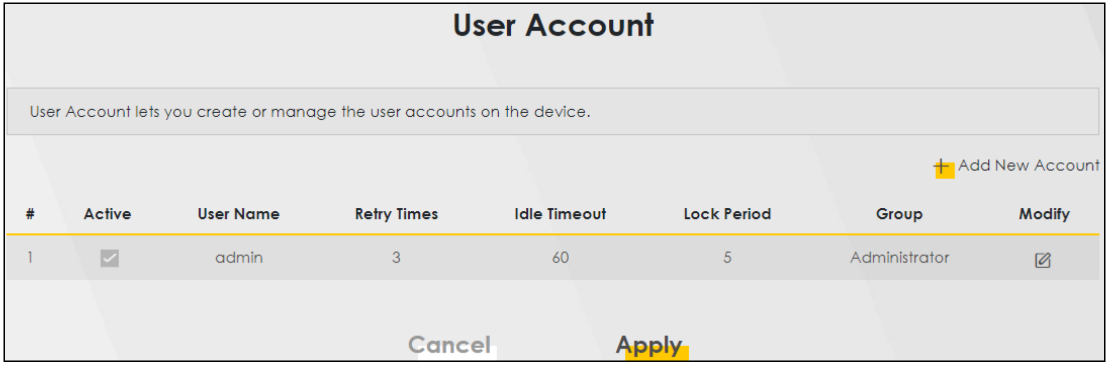
26.1 User Account Overview

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

26.2 User Account

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

Figure 148 Maintenance > User Account



User Account

User Account lets you create or manage the user accounts on the device.

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	☑	admin	3	60	5	Administrator	✎

The following table describes the labels in this screen.

Table 85 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account (up to 4 **Administrator** accounts and 4 **User** accounts).
#	This is the index number.
Active	This indicates whether the user account is active or not. The check box is selected when the user account is enabled. It is cleared when it is disabled.
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 whether this user has **Administrator** or **User** privileges.

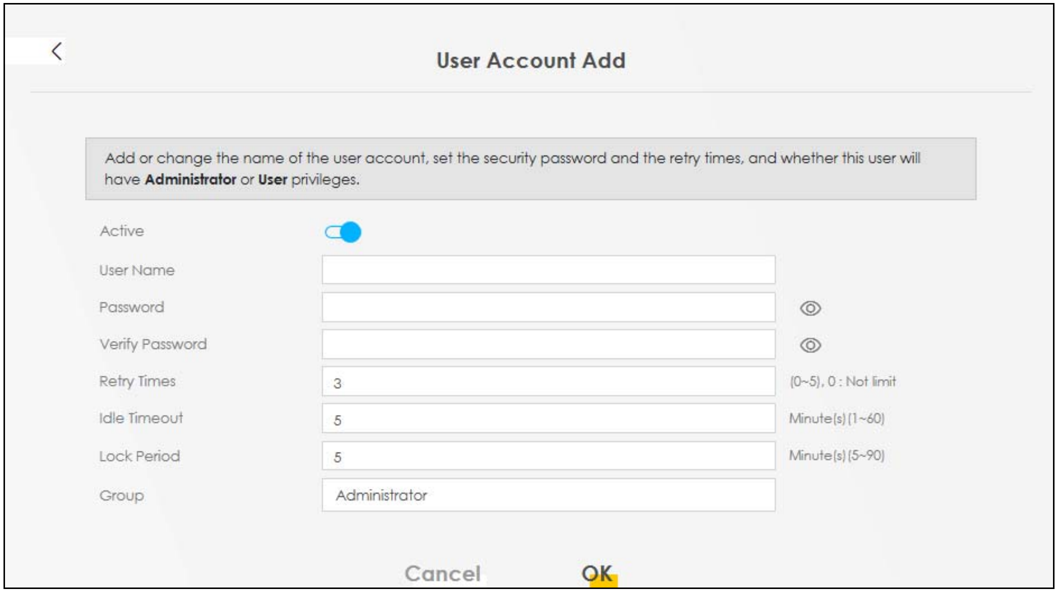
Table 85 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Modify	Click the **Edit** icon (✎) to configure the entry. Click the **Delete** icon (🗑) to remove the entry.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

26.2.1 User Account Add/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 149 Maintenance > User Account > Add/Edit



User Account Add

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.

Active	●	
User Name		
Password		
Verify Password		
Retry Times	3	(0~5), 0 : Not limit
Idle Timeout	5	Minute(s) (1~60)
Lock Period	5	Minute(s) (5~90)
Group	Administrator	

The following table describes the labels in this screen.

Table 86 Maintenance > 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 new name for the account (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign ($) vertical bar (|) ampersand (&) semicolon (;)
Password	Type your new system password (from 8-32 characters long, and must contain at least one upper case letter, one lower case letter and one number). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device.
Verify Password	Type 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.

Table 86   Maintenance > User Account > Add/Edit (continued)

LABEL	DESCRIPTION
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**.
Group	Specify whether this user will have **Administrator** or **User** privileges. The **Administrator** privileges are the following: • **Quick Start** setup. • The following screens are visible for setup: **Broadband**, **Wireless**, **Home Networking**, **Routing**, **NAT**, **DNS**, **VLAN Group**, **Interface Grouping**, **Firewall**, **MAC Filter**, **Certificates**, **Parental Control**, **Log**, **Traffic Status**, **ARP Table**, **Routing Table**, **Cellular WAN Status**, **System**, **User Account**, **Remote Management**, **TR-069 Client**, **Time**, **E-mail Notification**, **Log Setting**, **Firmware Upgrade**, **Backup/Restore**, **Reboot**, **Diagnostic**. The **User** privileges are the following: • The following screens are visible for setup: **Parental Control**, **Log**, **Traffic Status**, **ARP Table**, **Routing Table**, **Cellular WAN Status**, **User Account**, **Remote Management**, **Time**, **E-mail Notification**, **Log Setting**, **Firmware Upgrade**, **Backup/Restore**, **Reboot**, **Diagnostic**.
Cancel	Click **Cancel** to restore your previously saved settings.
OK	Click **OK** to save your changes.

CHAPTER 27
Remote Management

27.1 Overview

Remote management controls through which interface(s), which web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) can access the Zyxel Device.

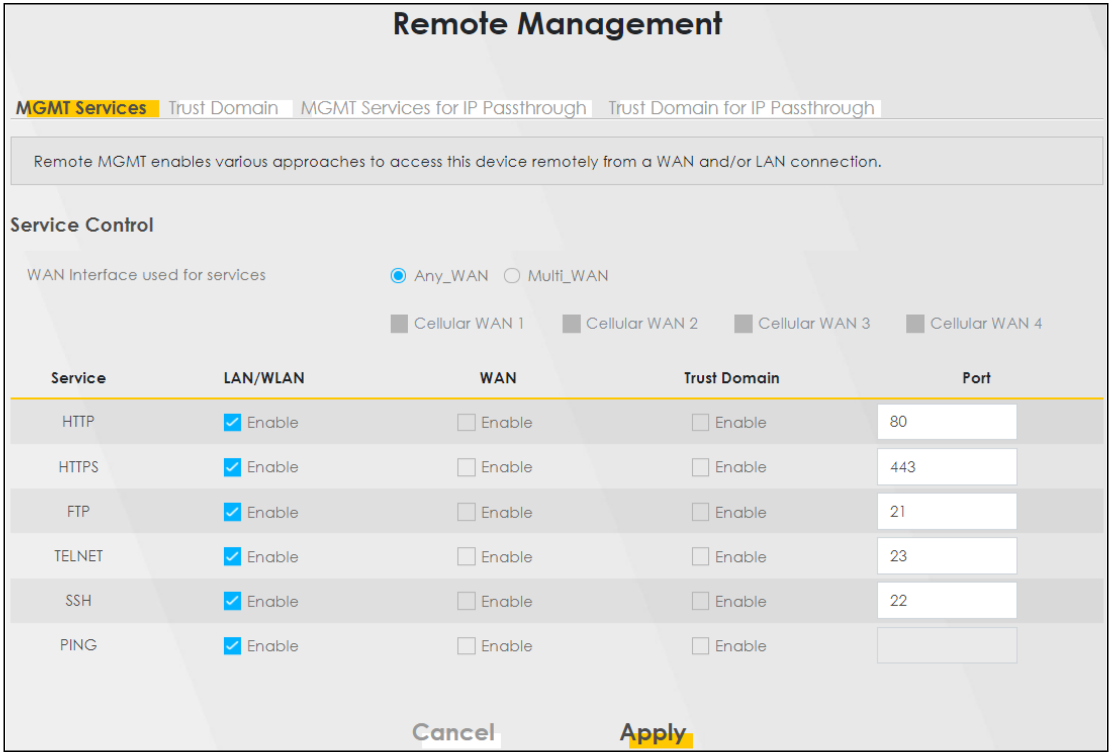
Note: The Zyxel Device is managed using the Web Configurator.

27.2 MGMT Services

The **MGMT Services** screen will be hidden if you enable the **IP Passthrough** function in **Network Setting** > **Broadband** > **Cellular IP Passthrough** (See Section 7.8 on page 81) or **Network Setting** > **Broadband** > **Cellular APN** > **Edit APN** (See Section 7.4 on page 74) screen.

Use this screen to configure the interfaces through which services can access the Zyxel Device. Click **Maintenance > Remote Management** to open the following screen.

Figure 150 Maintenance > Remote Management > MGMT Services



Remote MGMT enables various approaches to access this device remotely from a WAN and/or LAN connection.

WAN Interface used for services: ● Any_WAN ○ Multi_WAN

□ Cellular WAN 1 □ Cellular WAN 2 □ Cellular WAN 3 □ Cellular WAN 4

Service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	☑ Enable	□ Enable	□ Enable	80
HTTPS	☑ Enable	□ Enable	□ Enable	443
FTP	☑ Enable	□ Enable	□ Enable	21
TELNET	☑ Enable	□ Enable	□ Enable	23
SSH	☑ Enable	□ Enable	□ Enable	22
PING	☑ Enable	□ Enable	□ Enable	

The following table describes the fields in this screen.

Table 87 Maintenance > Remote Management > MGMT Services

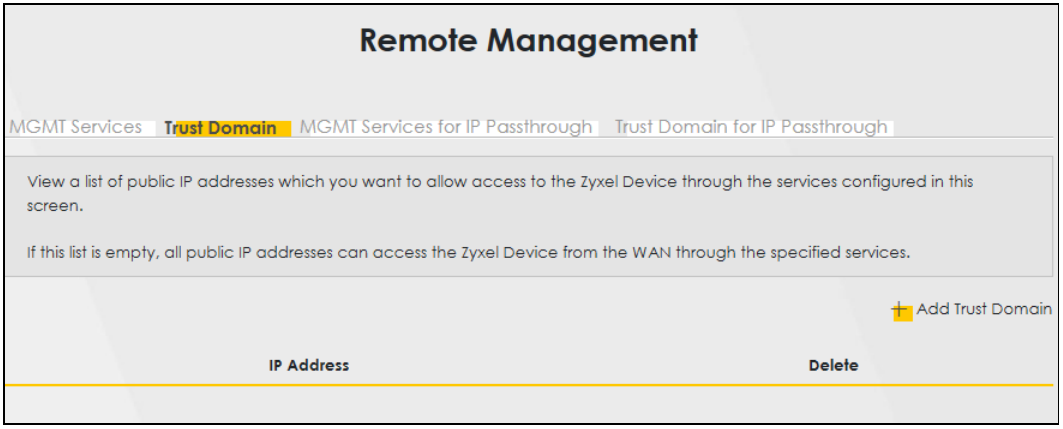
LABEL	DESCRIPTION
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Cellular WAN	Enable the cellular WAN connection configured in **Network Setting > Broadband > Cellular WAN** to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** check box 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.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

27.3 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 151 Maintenance > Remote Management > Trust Domain



Remote Management

MGMT Services
Trust Domain
MGMT Services for IP Passthrough
Trust Domain for IP Passthrough

View a list of public IP addresses which you want to allow access to the Zyxel Device through the services configured in this screen.

If this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

Add Trust Domain
IP Address
Delete

The following table describes the fields in this screen.

Table 88 Maintenance > Remote Management > Trust Domain

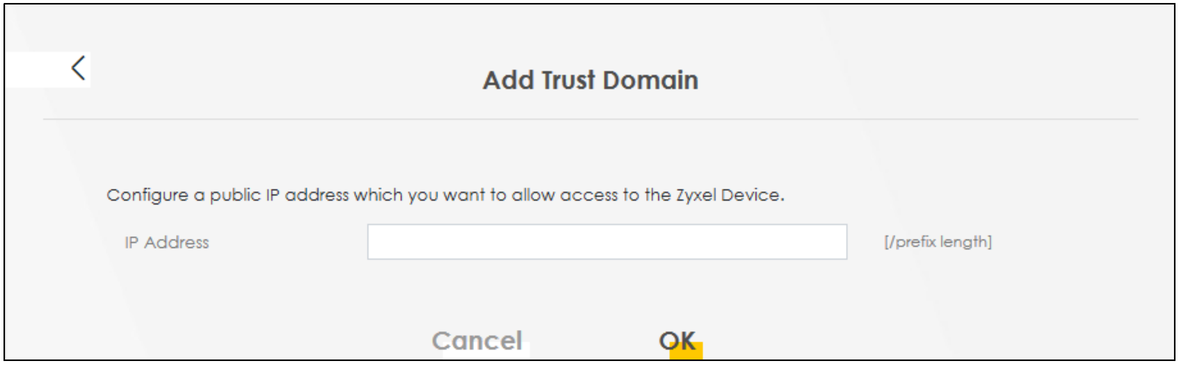
LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon (🗑) to remove the trusted host IP address.

27.4 Add Trust Domain

Enter the IP address of the management station permitted to access the local management services, and click **OK**.

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 152 Maintenance > Remote Management > Trust Domain > Add Trust Domain



Add Trust Domain

Configure a public IP address which you want to allow access to the Zyxel Device.

IP Address [/prefix length]

The following table describes the fields in this screen.

Table 89 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.

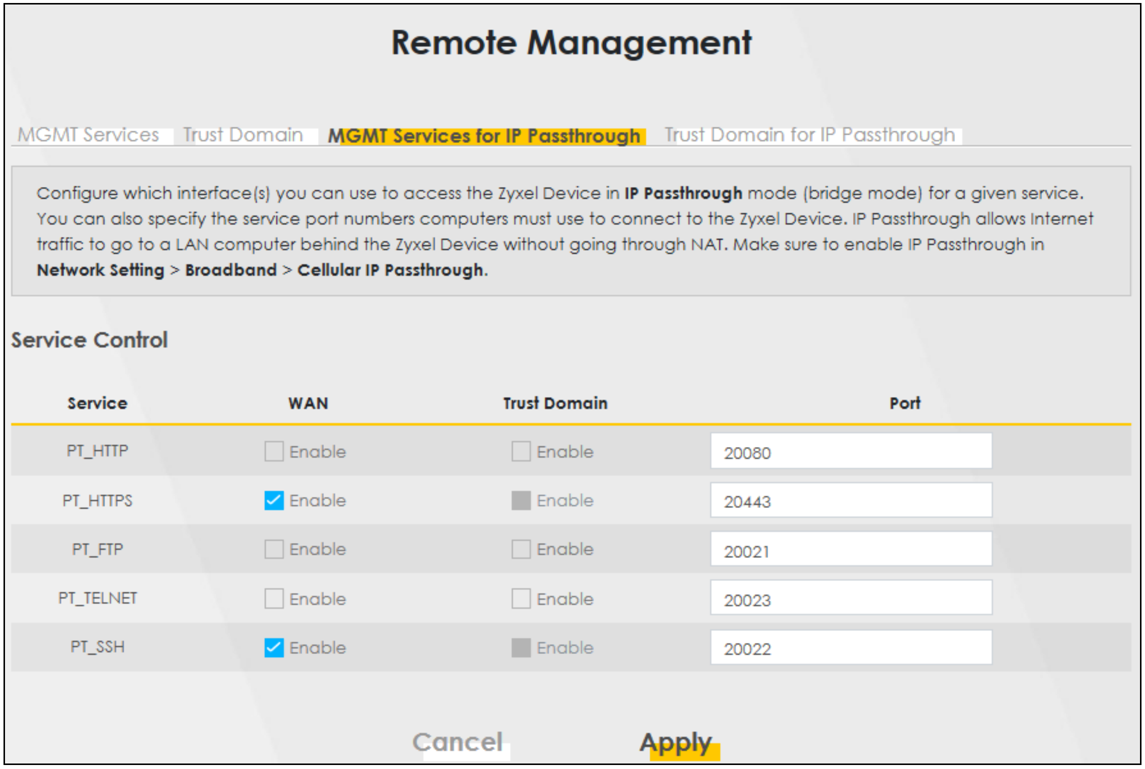
27.5 MGMT Services for IP Passthrough

Configure which interface(s) you can use to access the Zyxel Device in IP Passthrough mode (bridge mode) for a given service. You can also specify the service port numbers computers must use to connect to the Zyxel Device. IP Passthrough allows Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT. Make sure to enable IP Passthrough in **Network Setting** >

Broadband > **Cellular IP Passthrough** (See Section 7.8 on page 81) or **Network Setting** > **Broadband** > **Cellular APN** > **Edit APN** (See Section 7.4 on page 74) screen.

Click **Maintenance > Remote Management > MGMT Services for IP Passthrough** to open the following screen.

Figure 153 Maintenance > Remote Management > MGMT Services for IP Passthrough



Remote Management

MGMT Services
Trust Domain
MGMT Services for IP Passthrough
Trust Domain for IP Passthrough

Configure which interface(s) you can use to access the Zyxel Device in **IP Passthrough** mode (bridge mode) for a given service. You can also specify the service port numbers computers must use to connect to the Zyxel Device. IP Passthrough allows Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT. Make sure to enable IP Passthrough in **Network Setting** > **Broadband** > **Cellular IP Passthrough**.

Service Control

Service	WAN	Trust Domain	Port
PT_HTTP	□ Enable	□ Enable	20080
PT_HTTPS	☑ Enable	▨ Enable	20443
PT_FTP	□ Enable	□ Enable	20021
PT_TELNET	□ Enable	□ Enable	20023
PT_SSH	☑ Enable	▨ Enable	20022

The following table describes the fields in this screen.

Table 90 Maintenance > Remote Management > MGMT Services for IP Passthrough

LABEL	DESCRIPTION
Service	This is the service you may use to access the Zyxel Device.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from all Trust Domains.
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.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

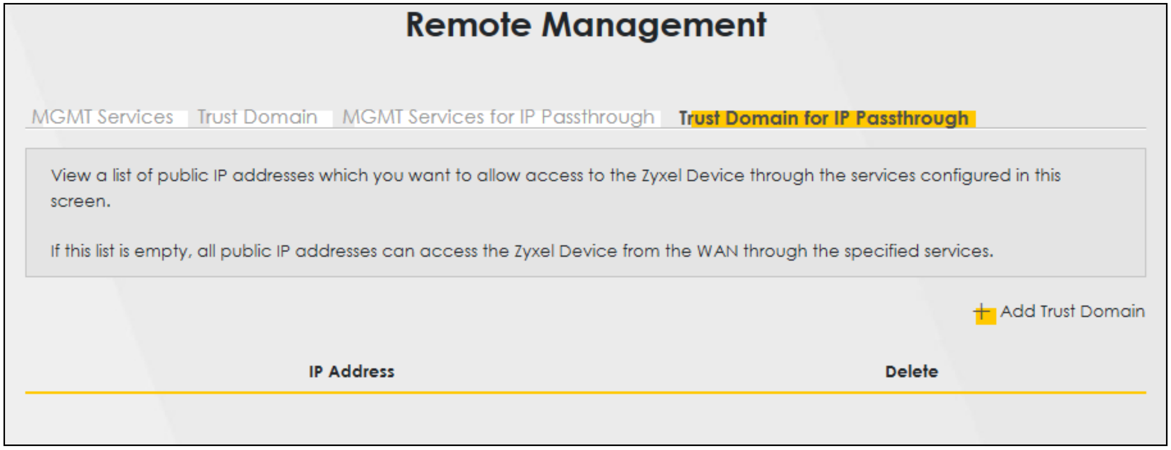
27.6 Trust Domain for IP Passthrough

Use this screen to view a list of public IP addresses/complete domain names which are allowed to access the Zyxel Device in **IP Passthrough** mode (bridge mode). IP Passthrough allows Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT. Make sure to enable IP

Passthrough in **Network Setting** > **Broadband** > **Cellular IP Passthrough** (See Section 7.8 on page 81) or **Network Setting** > **Broadband** > **Cellular APN** > **Edit APN** (See Section 7.4 on page 74) screen.

Click **Maintenance > Remote Management > Trust Domain for IP Passthrough** to open the following screen.

Figure 154 Maintenance > Remote Management > Trust Domain for IP Passthrough



Remote Management

MGMT Services
Trust Domain
MGMT Services for IP Passthrough
Trust Domain for IP Passthrough

View a list of public IP addresses which you want to allow access to the Zyxel Device through the services configured in this screen.

If this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

+ Add Trust Domain
IP Address
Delete

The following table describes the fields in this screen.

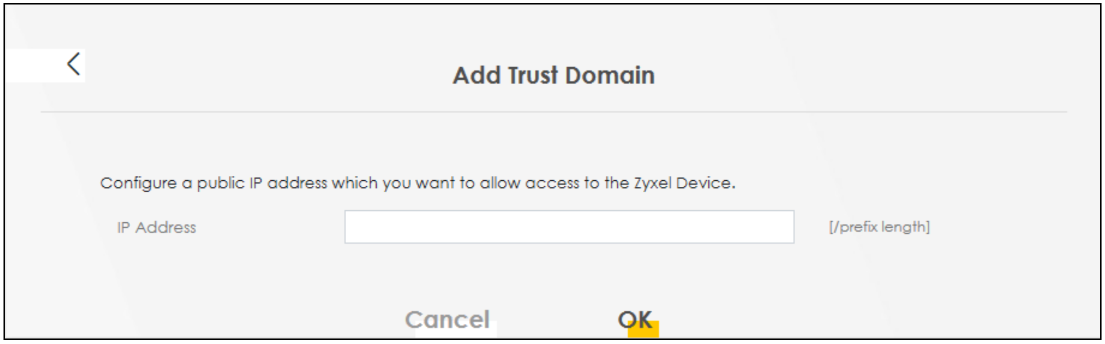
Table 91 Maintenance > Remote Management > Trust Domain for IP Passthrough

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.

27.7 Add Trust Domain

Use this screen to add a public IP address or a complete domain name of a device which is allowed to access the Zyxel Device. Click the **Add Trust Domain** button in the **Maintenance > Remote Management > Trust Domain for IP Passthrough** screen to open the following screen.

Figure 155 Maintenance > Remote Management > Trust Domain for IP Passthrough > Add Trust Domain



Add Trust Domain

Configure a public IP address which you want to allow access to the Zyxel Device.

The following table describes the fields in this screen.

Table 92   Maintenance > Remote Management > Trust Domain for IP Passthrough > 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.
Cancel	Click **Cancel** to restore your previously saved settings.
OK	Click **OK** to save your changes back to the Zyxel Device.

CHAPTER 28
TR-069 Client

28.1 Overview

This chapter explains how to configure the Zyxel Device's TR-069 auto-configuration settings.

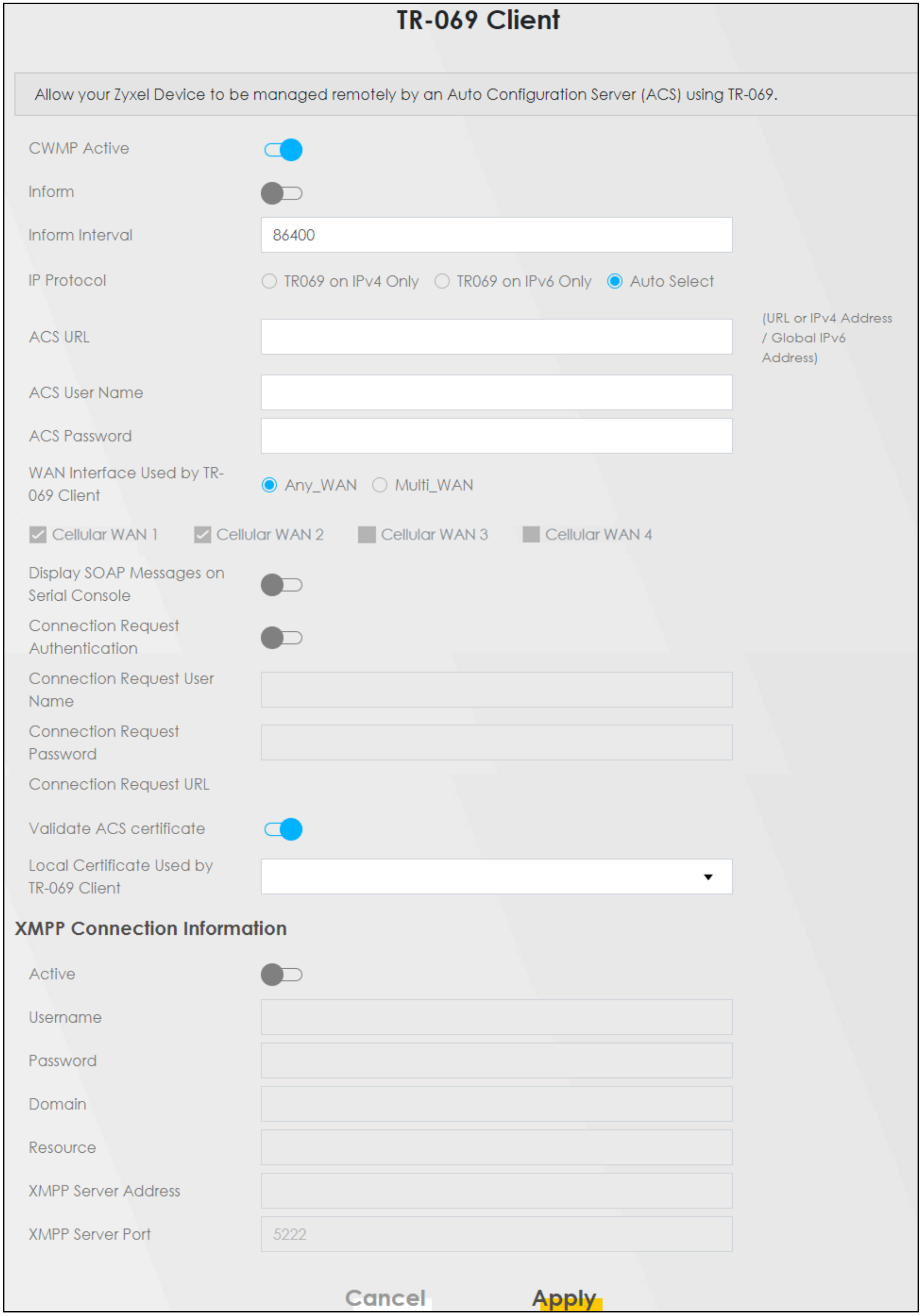
28.2 TR-069 Client

TR-069 is a protocol that defines how your Zyxel Device can be managed via a management server. TR-069 is based on sending Remote Procedure Calls (RPCs) between an (Auto-Configuration Server) ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

You can use a management server to remotely set up the Zyxel Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Zyxel Device. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Maintenance > TR-069 Client** to open the following screen.

Figure 156 Maintenance > TR-069 Client



TR-069 Client

Allow your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.

CWMP Active	● On
Inform	○ Off
Inform Interval	86400
IP Protocol	○ TR069 on IPv4 Only ○ TR069 on IPv6 Only ● Auto Select
ACS URL	(URL or IPv4 Address / Global IPv6 Address)
ACS User Name	
ACS Password	
WAN Interface Used by TR-069 Client	● Any_WAN ○ Multi_WAN

☑ Cellular WAN 1 ☑ Cellular WAN 2 ■ Cellular WAN 3 ■ Cellular WAN 4

Display SOAP Messages on Serial Console	○ Off
Connection Request Authentication	○ Off
Connection Request User Name	
Connection Request Password	
Connection Request URL	
Validate ACS certificate	● On
Local Certificate Used by TR-069 Client	▾

XMPP Connection Information

Active	○ Off
Username	
Password	
Domain	
Resource	
XMPP Server Address	
XMPP Server Port	5222

The following table describes the fields in this screen.

Table 93 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP Active	CPE WAN Management Protocol (CWMP) enables the Zyxel Device to be remotely configured via a WAN link. Communication between the Zyxel Device and the management server is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC). Click to enable (switch turns blue) to allow the Zyxel Device to be managed by a management server. Otherwise, click to disable (switch turns gray) to disallow the Zyxel Device to be managed by a management server.
Inform	Click to enable (switch turns blue) the Zyxel Device to send periodic inform via TR-069 on the WAN. Otherwise, click to disable (switch turns gray).
Inform Interval	Enter the time interval (in seconds) at which the Zyxel Device sends information to the auto-configuration server.
IP Protocol	Select the type of IP protocol to allow TR-069 to operate on, or choose **Auto Select** to have the Zyxel Device set for you.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select **Any_WAN**, the Zyxel Device automatically passes the TR-069 traffic when any WAN connection is up. If you select **Multi_WAN**, you also need to select two or more pre-configured WAN interfaces. The Zyxel Device automatically passes the TR-069 traffic when one of the selected WAN connections is up.
Cellular WAN	The Zyxel Device automatically passes the TR-069 traffic when cellular WAN connection is up.
Display SOAP messages on serial console	Click to enable (switch turns blue) the dumping of all SOAP messages during the ACS server communication with the Zyxel Device.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the Zyxel Device, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the Zyxel Device, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the Zyxel Device.
Validate ACS Certificate	Click to enable (switch turns blue) the validation of a local certificate used by TR-069 client.
Local certificate used by TR-069 Client	You can choose a local certificate used by TR-069 client. The local certificate should be imported in the **Security** > **Certificates** > **Local Certificates** screen.
XMPP Connection Information	

Table 93 Maintenance > TR-069 Client (continued)

LABEL	DESCRIPTION
Active	eXtensible Messaging and Presence Protocol (XMPP) is a protocol that allows the Auto-Configuraiton Servers (ACS) (TR-069 Server) to build connection with the Zyxel Device. Originally, with old procedures, ACS doesn't know when a inform message from the Zyxel Device arrives. ACS thus takes a passive role in the connection building process. By deploying XMPP, ACS is able to build a connection with the Zyxel Device through XMPP server. Both the Zyxel Device and ACS have a registered account on XMPP server. A two-way communication is established. The connection stays active until you disable it. Click this to enable XMPP connection. Note: Enable XMPP connection will cause higher data consumption.
Username	Users of XMPP should have unique Jabber Identifiers (JIDs). A JID identifies an individual on the Internet. It consists of three parts (not all restricted): node, domain, and resource. Use these fields of the Zyxel Device's JID to enter this and the following fields. Enter the username of the Zyxel Device's account registered on the XMPP server.
Password	Enter the password of the Zyxel Device's account registered on the XMPP server.
Domain	Enter the XMPP domain name of the Zyxel Device's account. The domain name should be an qualified domain name, IPv4/IPv6 address or unqualified host name.
Resource	XMPP resource links different device clients to one account. Enter the resource of the Zyxel Device's XMPP account. This should be presented in UTF-8 format.
XMPP Server Address	Enter the IP address of the XMPP server. The Zyxel Device will use the address to connect to the XMPP server.
XMPP Server Port	Enter the TCP port reserved for the XMPP server. The default is 5222. (1~65535)
Cancel	Click **Cancel** to restore the screen's last saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 29
Time Settings

29.1 Time Settings Overview

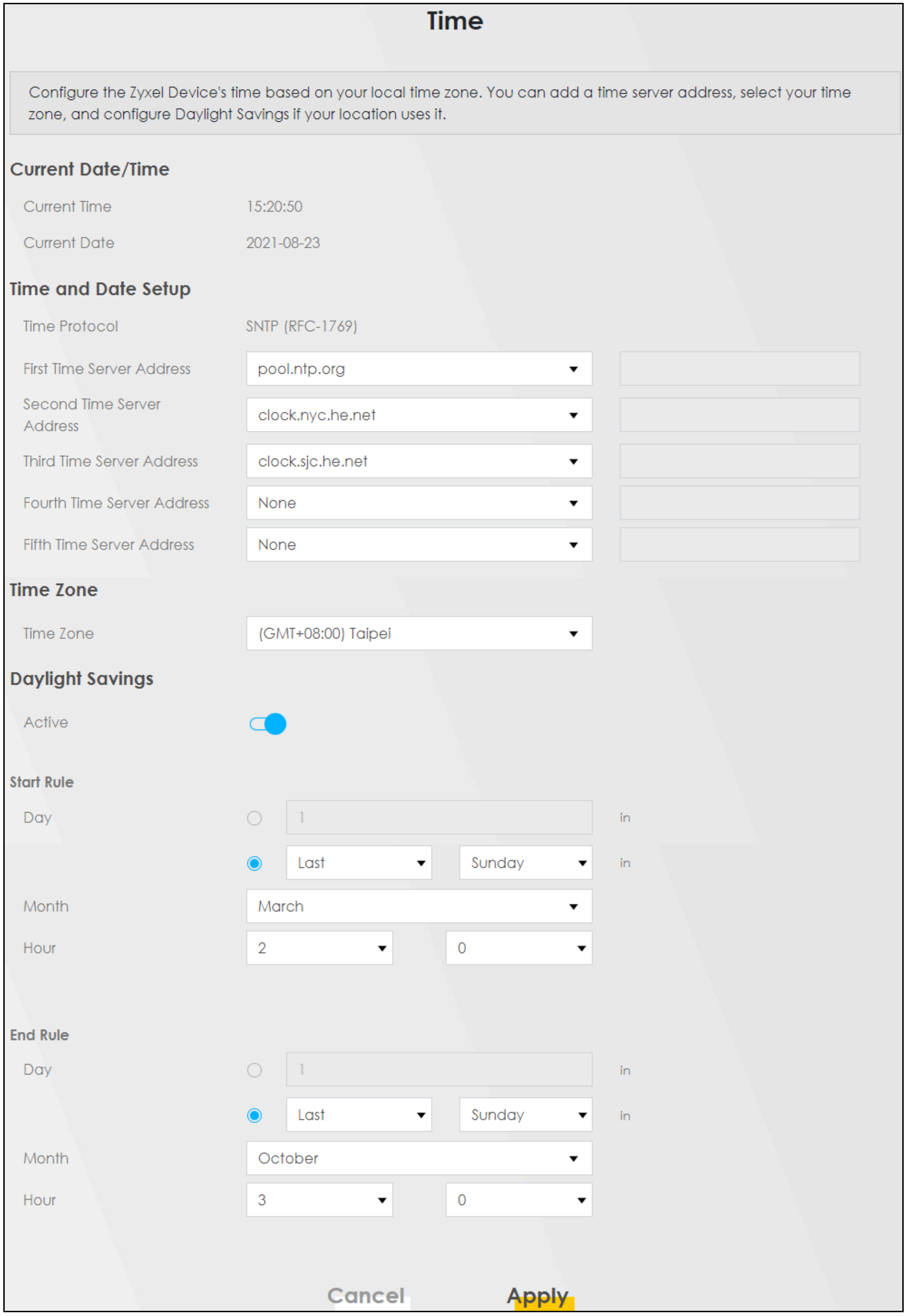
This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

29.2 Time

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

To change your Zyxel Device's time and date, click **Maintenance > Time**. The screen appears as shown.

Figure 157 Maintenance > Time



Time

Configure the Zyxel Device's time based on your local time zone. You can add a time server address, select your time zone, and configure Daylight Savings if your location uses it.

Current Date/Time

Current Time 15:20:50

Current Date 2021-08-23

Time and Date Setup

Time Protocol SNTP (RFC-1769)

First Time Server Address pool.ntp.org

Second Time Server Address clock.nyc.he.net

Third Time Server Address clock.sjc.he.net

Fourth Time Server Address None

Fifth Time Server Address None

Time Zone

Time Zone (GMT+08:00) Taipei

Daylight Savings

Active ●

Start Rule

Day ○ 1 in

● Last Sunday in

Month March

Hour 2 0

End Rule

Day ○ 1 in

● Last Sunday in

Month October

Hour 3 0

The following table describes the fields in this screen.

Table 94 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.

Table 94 Maintenance > Time (continued)

LABEL	DESCRIPTION
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.
First ~ Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you don't 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 30
E-mail Notification

30.1 E-mail Notification Overview

A mail server is an application or a computer that can receive, forward and deliver e-mail messages.

To have the Zyxel Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

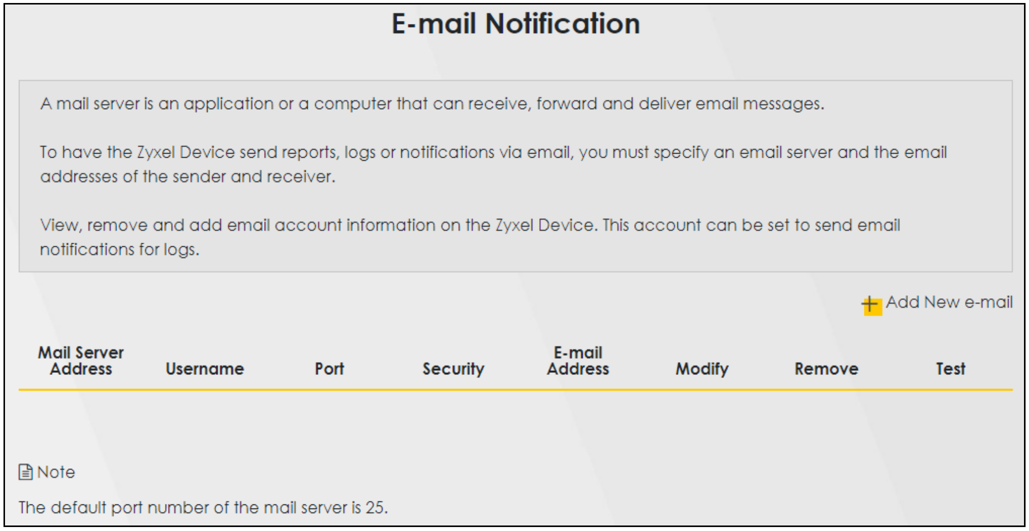
30.2 E-mail Notification

Use this screen to view, remove and add e-mail account information on the Zyxel Device. This account can be set to receive e-mail 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 158 Maintenance > E-mail Notification



E-mail Notification

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 via email, you must specify an email server and the email addresses of the sender and receiver.

View, remove and add email account information on the Zyxel Device. This account can be set to send email notifications for logs.

Note

The default port number of the mail server is 25.

The following table describes the labels in this screen.

Table 95 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.

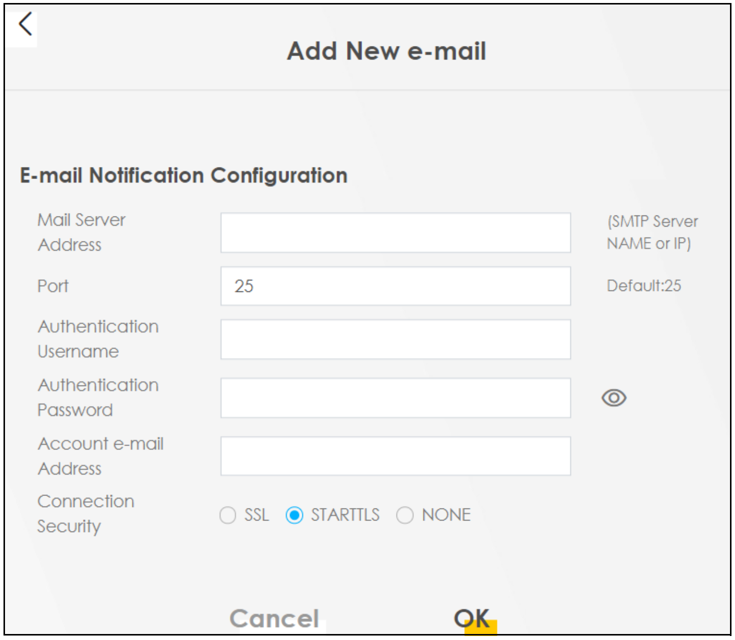
Table 95 Maintenance > E-mail Notification (continued)

LABEL	DESCRIPTION
User name	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 e-mail address that you want to be in the from/sender line of the e-mail that the Zyxel Device sends.
Modify	Click the **Edit** icon (✎) to edit the email notification settings.
Remove	Click the **Delete** icon (🗑) to delete the selected entry(ies).
Test	Click this to send a test email to the configured email address.

30.2.1 E-mail Notification Edit

Click the **Add** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 159 Maintenance > E-mail Notification > Add



Add New e-mail

E-mail Notification Configuration

Mail Server Address		(SMTP Server NAME or IP)
Port	25	Default:25
Authentication Username		
Authentication Password		
Account e-mail Address		
Connection Security	○ SSL ● STARTTLS ○ NONE	

The following table describes the labels in this screen.

Table 96 Maintenance > E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account e-mail Address** field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication User name	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account e-mail Address** field.
Authentication Password	Enter the password associated with the user name above.

Table 96   Maintenance > E-mail Notification > Add (continued)

LABEL	DESCRIPTION
Account e-mail Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Zyxel Device sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Connection Security	Select **SSL** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS. Select **NONE** to disable the connection security.
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 31
Log Setting

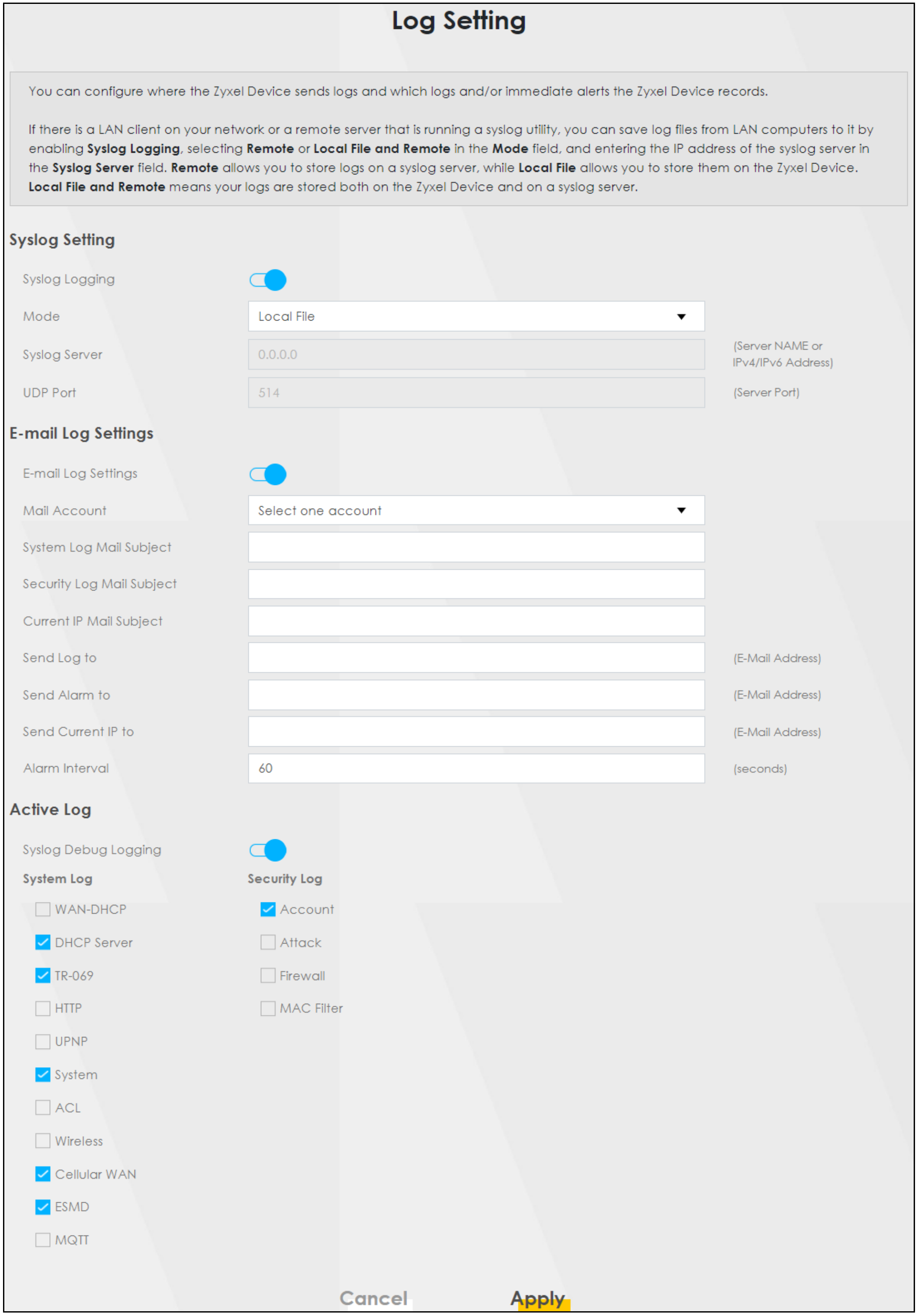
31.1 Log Setting Overview

Use this screen to configure where the Zyxel Device sends logs, and which type of logs the Zyxel Device records.

31.2 Log Setting

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 160 Maintenance > Log Setting



Log Setting

You can configure where the Zyxel Device sends logs and which logs and/or immediate alerts the Zyxel Device records.

If there is a LAN client on your network or a remote server that is running a syslog utility, you can save log files from LAN computers to it by enabling **Syslog Logging**, selecting **Remote** or **Local File and Remote** in the **Mode** field, and entering the IP address of the syslog server in the **Syslog Server** field. **Remote** allows you to store logs on a syslog server, while **Local File** allows you to store them on the Zyxel Device. **Local File and Remote** means your logs are stored both on the Zyxel Device and on a syslog server.

Syslog Setting

Syslog Logging	●	
Mode	Local File ▼	
Syslog Server	0.0.0.0	(Server NAME or IPv4/IPv6 Address)
UDP Port	514	(Server Port)

E-mail Log Settings

E-mail Log Settings	●	
Mail Account	Select one account ▼	
System Log Mail Subject		
Security Log Mail Subject		
Current IP Mail Subject		
Send Log to		(E-Mail Address)
Send Alarm to		(E-Mail Address)
Send Current IP to		(E-Mail Address)
Alarm Interval	60	(seconds)

Active Log

Syslog Debug Logging ●

System Log

- ☐ WAN-DHCP
- ☑ DHCP Server
- ☑ TR-069
- ☐ HTTP
- ☐ UPNP
- ☑ System
- ☐ ACL
- ☐ Wireless
- ☑ Cellular WAN
- ☑ ESMD
- ☐ MQTT

Security Log

- ☑ Account
- ☐ Attack
- ☐ Firewall
- ☐ MAC Filter

The following table describes the fields in this screen.

Table 97 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Click the switch (it will turn blue) to enable syslog logging. Note: A warning appears upon enabling **Syslog Logging**. Just click **OK** to continue.
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 Setting	Click the switch (it will turn blue) to allow the sending via e-mail the system and security logs to the e-mail 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 e-mail (for example Zyxel System Log). Up to 127 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 e-mail (for example Zyxel Security Log). Up to 127 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 e-mail recipient. The log's format is plain text file sent as an e-mail 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 e-mail attachment.
Alarm Interval	Select the frequency of showing of the alarm.
Active Log	
Syslog Debug Logging	Click the switch (it will turn blue) to enable syslog debug logging.
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.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 32 Firmware Upgrade

32.1 Overview

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

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

32.2 Firmware Upgrade

This screen lets you upload new firmware to your Zyxel Device by using the following methods.

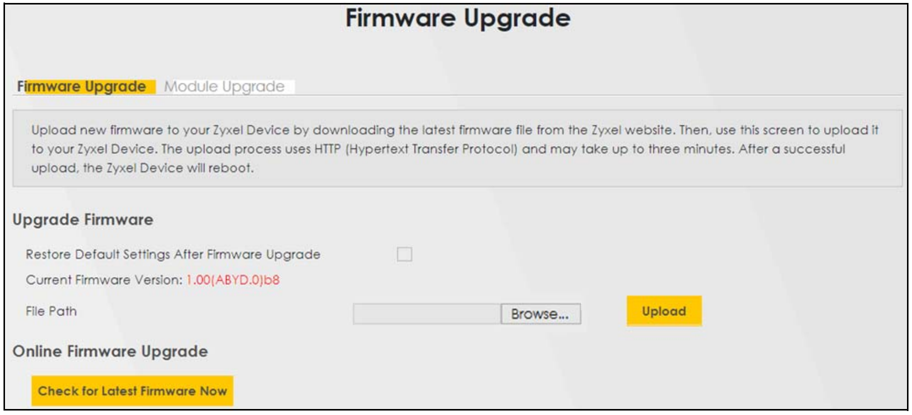
- Download the latest firmware file from the Zyxel website.
- Make sure your Zyxel Device is connected to the Internet. Check for new firmware online from the Zyxel server and download the firmware file to the Zyxel Device.

Upload the firmware file to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol). The upload may take up to three 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 161 Maintenance > Firmware Upgrade



Firmware Upgrade

Upload new firmware to your Zyxel Device by downloading the latest firmware file from the Zyxel website. Then, use this screen to upload it to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the Zyxel Device will reboot.

Upgrade Firmware

Restore Default Settings After Firmware Upgrade □

Current Firmware Version: 1.00(ABYD.0)b8

File Path

Online Firmware Upgrade

The following table describes the labels in this screen.

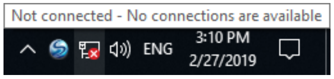
Table 98 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select this to restore the factory-default to the Zyxel Device after upgrading the firmware. Make sure this is clear if you don't want the Zyxel Device to lose all its current configurations and return to the factory defaults. Note: Make sure to backup the Zyxel Device's configuration settings first in case the restore to factory-default process is not successful. Refer to Section 33.2 on page 233.
Current Firmware Version	This is the present firmware version.
File Path	Enter the location of the file you want to upload in this field or click **Browse** to find it.
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 three minutes.
Online Firmware Upgrade	
Check for latest firmware now	With the Zyxel Device connected to the Internet, click this to allow the Zyxel Device to check for new firmware online from the Zyxel server. If a newer firmware is available, follow the online prompt to upload the new firmware to your Zyxel Device.

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

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 162 Network Temporarily Disconnected



Not connected - No connections are available

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

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

32.3 Module Upgrade

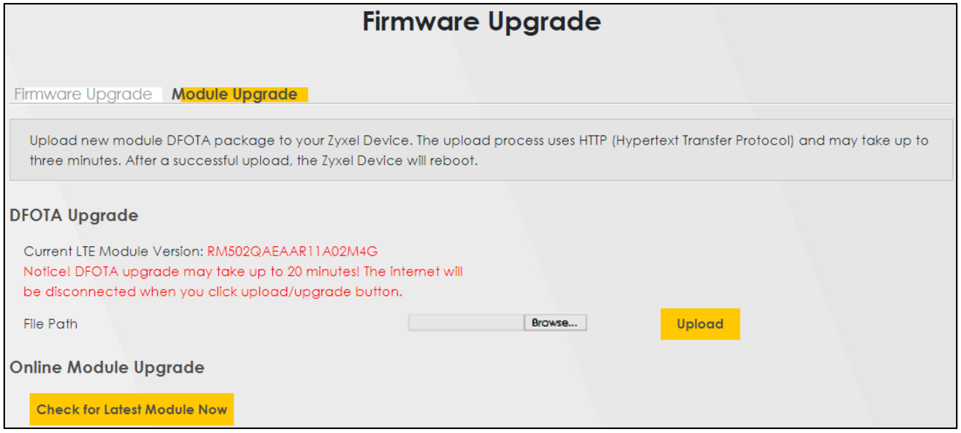
Use this screen to upload new firmware specific to the built-in LTE module in order to improve the LTE module's reliability and performance.

Delta Firmware Upgrade Over The Air (DFOTA) compares the current module's firmware version and download only the component that needs updating.

Click **Maintenance** > **Firmware Upgrade** > **Module Upgrade** to open the following screen.

Do NOT turn off the Zyxel Device while firmware upload is in progress!

Figure 163 Maintenance > Firmware Upgrade > Module Upgrade



Upload new module DFOTA package to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the Zyxel Device will reboot.

Current LTE Module Version: RM502QAEAAR11A02M4G

Notice! DFOTA upgrade may take up to 20 minutes! The internet will be disconnected when you click upload/upgrade button.

File Path

The following table describes the labels in this screen.

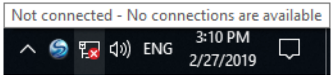
Table 99 Maintenance > Firmware Upgrade > Module Upgrade

LABEL	DESCRIPTION
DFOTA Upgrade	
Current LTE Module Version	This is the present module version.
File Path	Enter the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click this to find the .zip file you want to upload.
Upload	Click this to begin the upload process. This process may take up to three minutes.
Online Module Upgrade	
Check for latest Module now	With the Zyxel Device connected to the Internet, click this to allow the Zyxel Device to check for new module online from the Zyxel server. If a newer module is available, follow the online prompt to upload the new module to your Zyxel Device.

After you see the module updating screen, wait about 20 minutes before logging into the Zyxel Device again.

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 164 Network Temporarily Disconnected



Not connected - No connections are available

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

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

CHAPTER 33
Backup/Restore

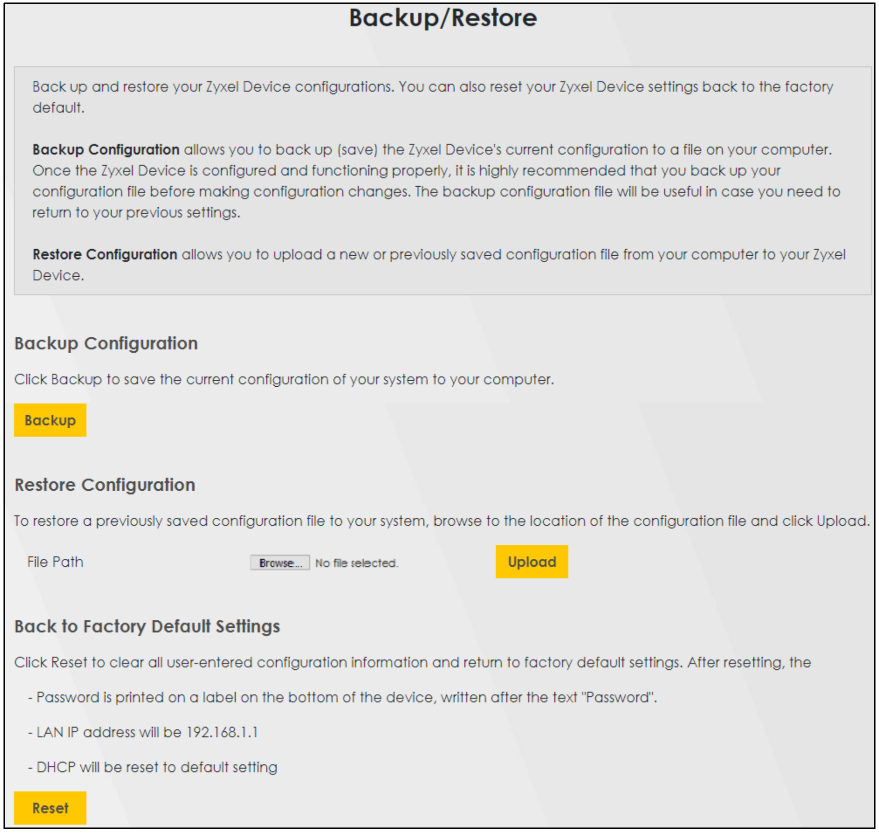
33.1 Backup/Restore Overview

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

33.2 Backup/Restore

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

Figure 165 Maintenance > Backup/Restore



Backup/Restore

Back up and restore your Zyxel Device configurations. You can also reset your Zyxel Device settings back to the factory default.

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once the 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.

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

Backup Configuration

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

Restore Configuration

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

File Path: No file selected.

Back to Factory Default Settings

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

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

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 100 Restore Configuration

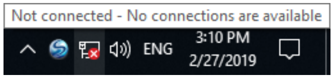
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your Zyxel Device 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 166 Network Temporarily Disconnected



Not connected - No connections are available

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).

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

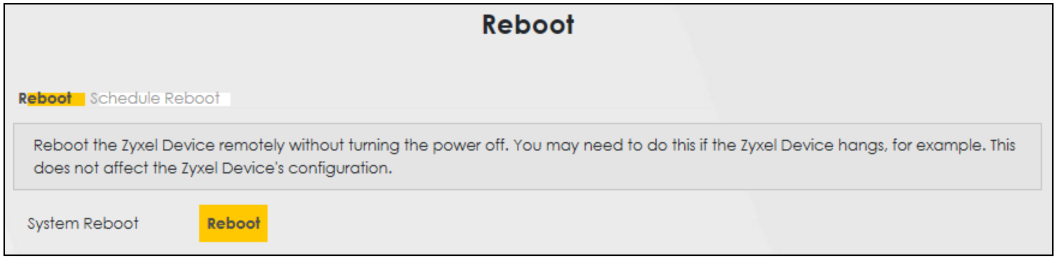
Note: You can also use the **Reset** button on the bottom panel of the Zyxel Device to restore the factory default settings. See Section 2.6 on page 24.

33.3 Reboot

System Reboot allows you to reboot 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 reboot.

Figure 167 Maintenance > Reboot



Reboot 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.

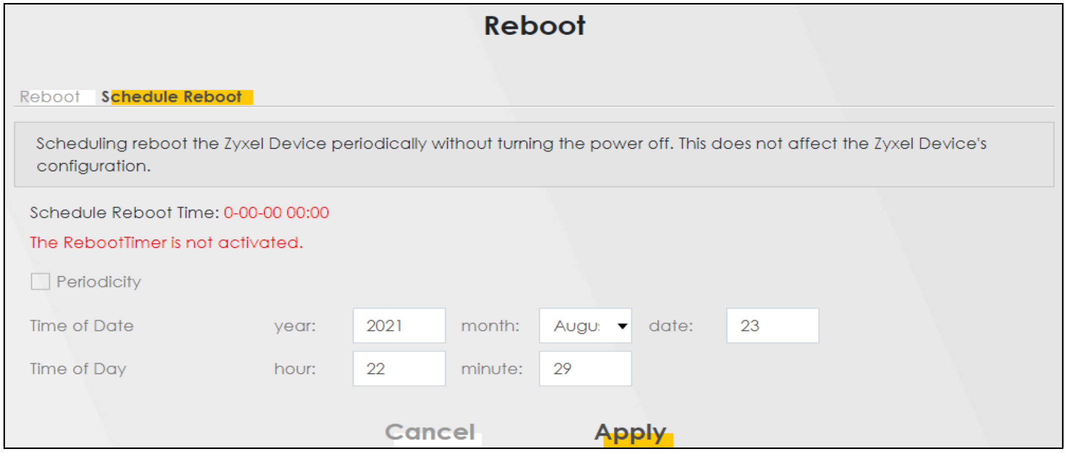
System Reboot

33.4 Schedule Reboot

Use the **Schedule Reboot** screen to schedule the date and time to reboot the Zyxel Device remotely without turning the power off. You can also select a specific day of the week and time to periodically reboot the Zyxel Device remotely.

Click **Maintenance** > **Reboot** > **Schedule Reboot**.

Figure 168 Maintenance > Reboot > Schedule Reboot



Scheduling reboot the Zyxel Device periodically without turning the power off. This does not affect the Zyxel Device's configuration.

Schedule Reboot Time: 0-00-00 00:00

The RebootTimer is not activated.

□ Periodicity

Time of Date year: 2021 month: Augu: date: 23

Time of Day hour: 22 minute: 29

The following table describes the labels in this screen.

Table 101 Maintenance > Reboot > Schedule Reboot

LABEL	DESCRIPTION
Periodically	Click this switch to enable the Zyxel Device to reboot periodically.
Day of Week	Select the day of the week to apply periodic rebooting. **Day of Week** is not available when the previous field **Periodically** is not selected.
Time of Date	Select the date of the year that you plan to reboot the Zyxel Device remotely.
Time of Day	Specify the time of the day that you plan to reboot the Zyxel Device remotely.
Cancel	Click **Cancel** to close the window with changes unsaved.
Apply	Click **Apply** to save the changes back to the Zyxel Device.

CHAPTER 34
Diagnostic

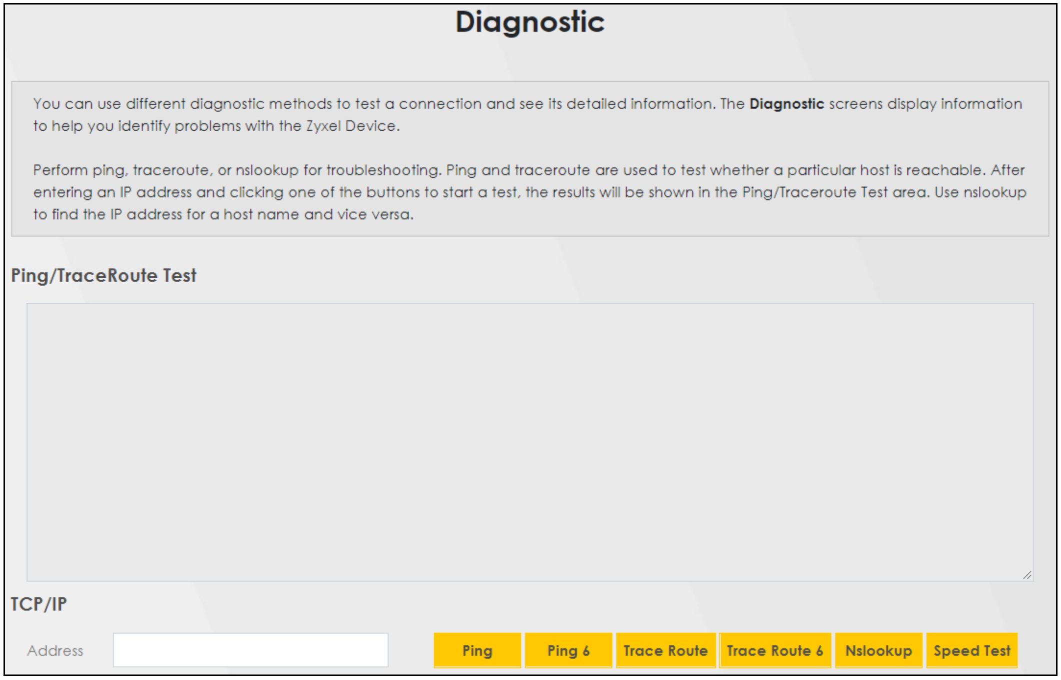
34.1 Diagnostic Overview

You can use different diagnostic methods to test a connection and see its detailed information. The **Diagnostic** screen display information to help you identify problems with the Zyxel Device.

34.2 Ping/TraceRoute/Nslookup Test/Speed Test

Use this screen to ping, traceroute, nslookup, or speed test 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 **Ping/Traceroute Test** area. Use nslookup to find the IP address for a host name and vice versa. Use speed test to determine the download and upload speed. Click **Maintenance > Diagnostic** to open the **Ping/TraceRoute Test** screen shown next.

Figure 169 Maintenance > Diagnostic



Diagnostic

You can use different diagnostic methods to test a connection and see its detailed information. The **Diagnostic** screens display information to help you identify problems with the Zyxel Device.

Perform 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 Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa.

Ping/TraceRoute Test

TCP/IP

Address

The following table describes the fields in this screen.

Table 102 Maintenance > Diagnostic

LABEL	DESCRIPTION
Ping/ TraceRoute Test	The result of tests is shown here in the info area.
TCP/IP	
Address	Enter either an IP address or a host name to start a test.
Ping	Click this button 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	Click this button 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	Click this button to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Click this button to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Click this button to perform a DNS lookup on the IP address or host name.
Speed Test	Click this button to perform an upload and download throughput test.

PART III
Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your Zyxel Device.

CHAPTER 35
Troubleshooting

35.1 Overview

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

- Power and Hardware Problems
- Device Access Problems
- Cellular Problems
- Internet Problems
- WiFi Problems
- UPnP Problems

35.2 Power and Hardware Problems

The Zyxel Device does not turn on.

1 Make sure the PoE is connected to the Zyxel Device and plugged in to an appropriate power source.

2 Make sure the power source is turned on.

3 Turn the Zyxel Device off and on.

4 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LEDs. See Section 2.3 on page 21.

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.

35.3 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. Refer to Section 33.2 on page 233.

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. Refer to Section 33.2 on page 233.

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 (Section 9.2 on page 108), 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. See Section 2.3 on page 21.
3. Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
4. If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance** > **Remote Management**).
5. Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.
6. 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 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.

2 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.

3 Turn the Zyxel Device off and on.

4 If this does not work, you have to reset the Zyxel Device to its factory default.

I cannot connect to the Zyxel Device using FTP, Telnet, SSH, or Ping.

1 See the Remote Management section for details on allowing web services (such as HTTP, HTTPS, FTP, 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.

35.4 Cellular Problems

The SIM card cannot be detected.

1 Disconnect the Zyxel Device from the power supply.

2 Remove the SIM card from its slot.

3 Clean the SIM card slot of any loose debris using compressed air.

4 Clean the gold connectors on the SIM card with a clean lint-free cloth.

5 Insert the SIM card into its slot and connect the Zyxel Device to the power supply to restart it.

I get an **Invalid** SIM card alert.

1 Make sure you have an active plan with your ISP.

2 Make sure that the Zyxel Device is in the coverage area of a cellular network.

I get a weak cellular signal.

1 Find the location of your nearest cellular base stations, then install the Zyxel Device towards the direction of those sites. The nearest site or site with a direct line-of-sight is usually preferred.

Note: It is best to test towards more than one cellular site, as the nearest site / line-of-sight is not always the best due to the terrain, interference, density of usage, and so on. All of these factors influence the stability, availability and throughput of the link to the Zyxel Device.

2 Position the Zyxel Device towards a direction where coverage is expected (example the nearest town).

3 Conduct test measurements using the Web Configurator's **System Monitor** > **Cellular WAN Status** screen to obtain a report of the cellular network signal strength and quality at various test positions.

Note: It is best to reboot the Zyxel Device before each test measurement is taken to ensure that it is not camping on the previous cellular site. This is because the Zyxel Device can 'lock' onto the previous cellular site even when the new cellular site is at a much better signal level and quality.

Although installing the Zyxel Device as high as possible is the usual rule of thumb, it is sometimes possible that the Zyxel Device is in a weak coverage spot at that specific height. Adjust the height to achieve the best service possible.

Note: Cellular network signals and quality can fluctuate. A measurement taken now and a few moments later can differ substantially even if nothing apparent has changed – this can be due to many aspects, such as fading, reflections, interference, capacity due to high network traffic, and so on.

It is possible that the network topology and usage changes over time, even from one minute to the next as network utilization increases. If poor performance is experienced at a later stage, re-test different installation locations again. It is possible that the current serving cellular site has become over utilized or is out-of-service. As the network design and topology changes, so will the experience change, either for the better or for the worse.

35.5 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 Check the SIM card. Maybe it has wrong settings (refer to Section 7.5 on page 76), the account has expired, it needs to be removed and reinserted (refer to the Quick Start Guide), or it is missing. See Section 35.4 on page 241 for possible SIM card problems.

3 Make sure you entered your ISP account information correctly on the **Network Setting** > **Broadband** screen. Fields on this screen are case-sensitive, so make sure [Caps Lock] is not on.

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

5 If the problem continues, contact your ISP.

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 Check the signal strength. Look at the LEDs, and check the LED section for more information. If the signal strength is low, try moving the Zyxel Device closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 For models that support external antennas, connect two external antennas to improve the cellular WAN signal strength. Point the antennas to the base stations directions if you know where they are, or try pointing the antennas in different directions and check which provides the strongest signal to the Zyxel Device. See the Introduction chapter for more information.

4 Turn the Zyxel Device off and on.

5 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions in Section on page 240.

Note: If your Zyxel Device is an outdoor-type, inclement weather like rain and hot weather may affect cellular signals.

35.6 WiFi Problems

The WiFi connection is 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 the WiFi client closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless 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.

35.7 UPnP Problems

My computer cannot detect UPnP settings from the Zyxel Device.

1. Make sure that UPnP is enabled in your computer. For Windows 7, see Section 9.6 on page 117. For Windows 10, see Section 9.7 on page 121.

2. On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings** > **Home Networking** > **UPnP** screen. See Section 9.4 on page 115 for details.

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.

APPENDIX A
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 103 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 104 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 105 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`

Table 105 Reserved Multicast Address (continued)

MULTICAST ADDRESS
`FF0E:0:0:0:0:0:0:0`
`FF0F:0:0:0:0:0:0:0`

Subnet Masking

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

Interface ID

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

EUI-64

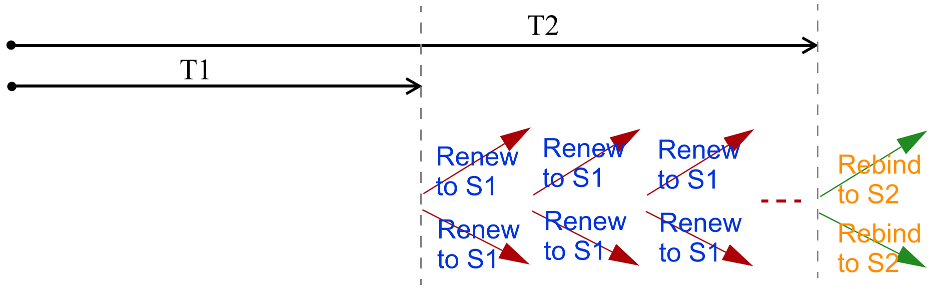
The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth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

MAC	00 : 13 : 49 : 12 : 34 : 56
EUI-64	02 : 13 : 49 : FF : FE : 12 : 34 : 56

Identity Association

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

client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

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

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

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The 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 7

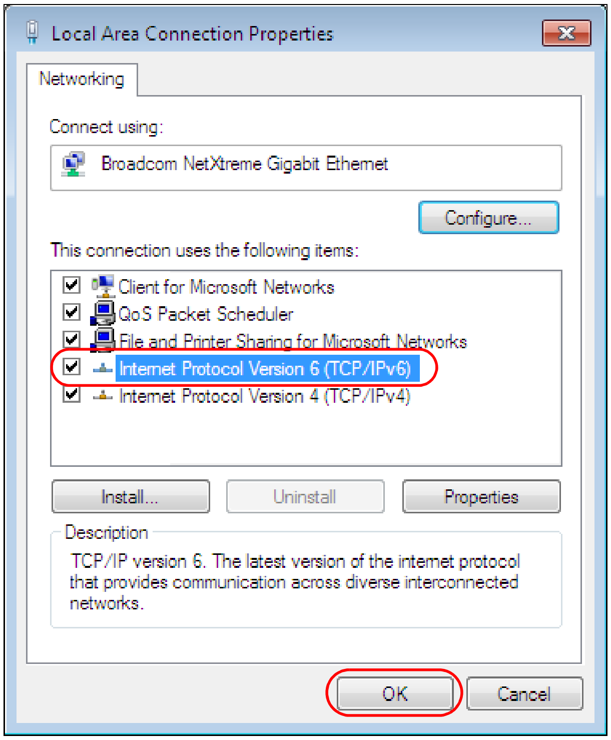
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



Local Area Connection Properties

Networking

Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

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

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

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

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

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

APPENDIX B
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

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

For Zyxel Networks 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 Corporation
- https://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- 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 BY
- https://www.zyxel.by

Bulgaria

- Zyxel България
- 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.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
- https://www.zyxel.com/it/it/

Netherlands

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

Norway

- Zyxel Communications
- 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

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd
- https://www.zyxel.com/es/es/

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

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

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

North America

USA

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

APPENDIX C
Legal Information

Copyright

Copyright © 2021 by Zyxel and/or its affiliates.

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

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

Disclaimer

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

Regulatory Notice and Statement

EUROPEAN UNION and UNITED KINGDOM

CE and UKCA

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for wireless products relevant to the EU, United Kingdom and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. 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 for operation in the band 5150 – 5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:

NR7101

- WCDMA Band I/III/VIII is 24 dBm
- LTE Band 1/3/7/8/20/28/32/34/38/40/42/43 is 23 dBm
- NR band n41/n77/n78 is 26 dBm
- WiFi The band 2400 -2483.5 MHz is 86.1 mW

NR7102

- WCDMA Band I/VIII is 24 dBm
- LTE Band 1/3/7/8/20/28/38/40/42/43 is 23 dBm
- NR Band n1/n3/n7/n8/n20/n28/n38/n40/n41/n77/n78 is 26 dBm
- WiFi The band 2400 – 2483.5 MHz is 84.92 mW

NR7103/NR7123

- WCDMA Band I/VIII is 24 dBm
- LTE Band 1/3/7/8/20/28/38/40/42 is 23 dBm
- NR Band n1/n3/n28/n38/n78 is 26 dBm
- WiFi The band 2400 – 2483.5 MHz is 77.98 mW

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/EC. **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.
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..
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. **National Restrictions** • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
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/EE.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
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 http://www.sviluppoeconomico.gov.it/ for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. • 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
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.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.

Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että 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.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- 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 use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your Zyxel Device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the Zyxel Device ventilation slots as insufficient airflow may harm your Zyxel Device. For example, do not place the Zyxel Device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this Zyxel Device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the Zyxel Device.
- Do not open the Zyxel Device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this Zyxel Device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this Zyxel 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 adapter first before connecting it to a power outlet.
- Do not allow anything to rest on the power adapter or cord and do NOT place the product where anyone can walk on the power adapter or cord.
- Please use the provided or designated connection cables/power cables/adapters. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adapter or cord is damaged, it might cause electrocution. Remove it from the Zyxel Device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- The following warning statements apply, where the disconnect device is not incorporated in the Zyxel Device or where the plug on the power supply cord is intended to serve as the disconnect device,

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

  - For pluggable devices, the socket-outlet shall be installed near the Zyxel Device and shall be easily accessible.

Environment Statement

(Wireless settings, 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：
- 第十二條 經型式認證合格之低功率射頻電機，非經許可，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。
- 第十四條 低功率射頻電機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。
- 前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機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。
- 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，使用或維修此設備。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。
- 請插在正確的電壓供給插座 (如 : 北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用 :
- – 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
- – 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

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

Explanation of the Symbols

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

Viewing Certifications

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

Zyxel Limited Warranty

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

Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the Zyxel Device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

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

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.

https://www.zyxel.com/form/gpl_oss_software_notice.shtml

Index