ZYXEL

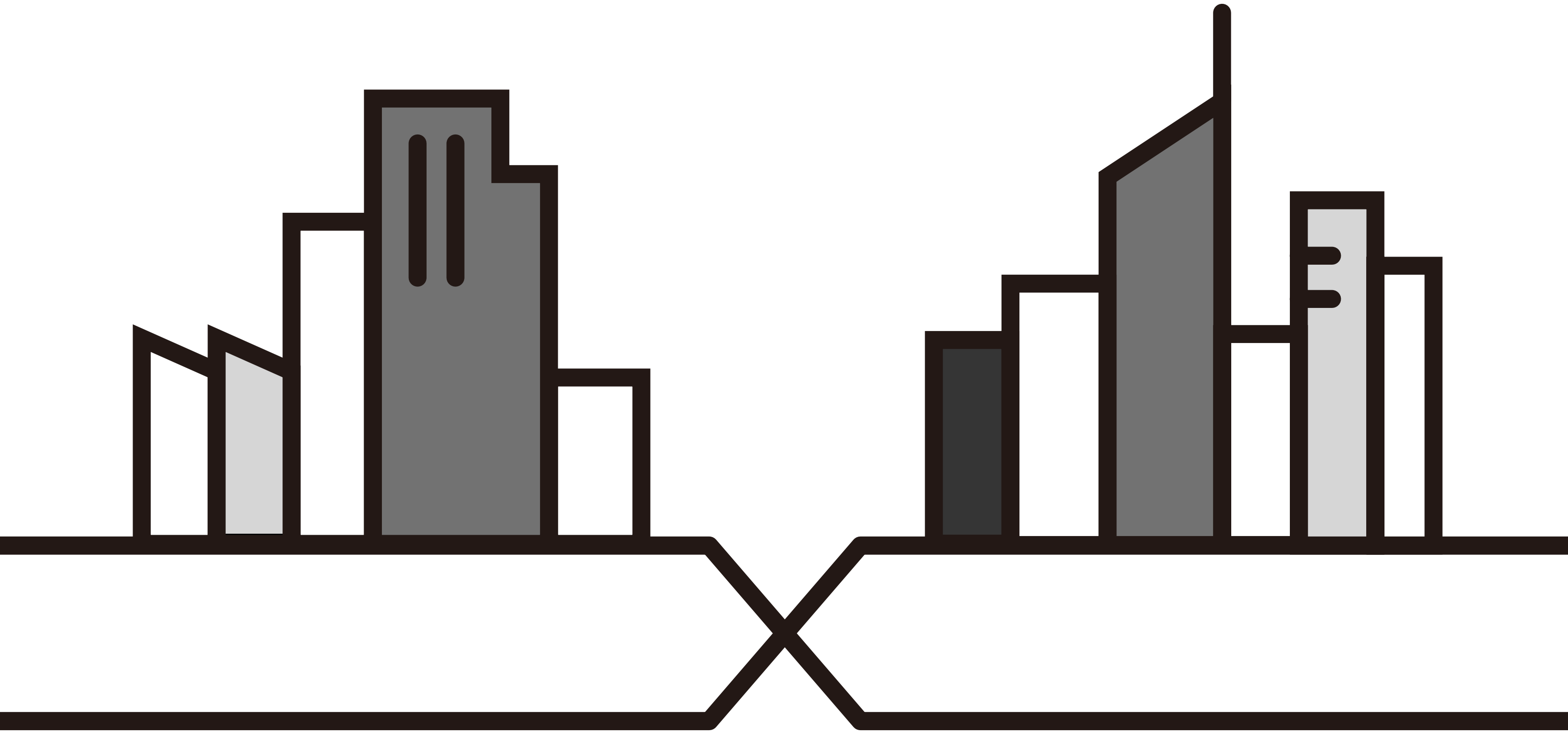
User's Guide

NR/FWA 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 Edition 5, 9/2023



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

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

- More Information

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

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your Zyxel Device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting** > **Routing** > **DNS Route** means you first click **Network Setting** in the navigation panel, then the **Routing** submenu, and then finally the **DNS Route** tab to get to that screen.

Icons Used in Figures

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

Zyxel Device 	Generic Router 	Switch
Server 	Firewall 	USB Storage Device
Printer 	4G LTE/5G NR Base Station 	

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

The Zyxel Device consists of the following models:

- NR7101
- NR7102
- NR7103
- NR7123
- NR7302
- NR7303
- FWA710

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.

Note: At the time of writing, the USB port is for troubleshooting only.

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

Table 1 Model Feature Comparison

FEATURE/MODEL		NR7101	NR7102	NR7103	NR7123	NR7302	NR7303	FWA710
2.4G WiFi		YES	YES	YES	YES	YES	YES	YES
Access Technology (ACT)	5G	YES	YES	YES	YES	YES	YES	YES
	4G	YES	YES	YES	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	4.0 Gbps/ 900 Mbps	4.67 Gbps/ 1.25Gbps	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	2.0 Gbps/ 200 Mbps	1.6 Gbps/ 211Mbps	1.4 Gbps/ 200 Mbps
Gigabit Ethernet Port		1G	2.5G	2.5G	2.5G	2.5G	2.5G	2.5G
USB port		NO	NO	YES	YES	NO	YES	YES
WiFi/WPS Button		YES	NO	NO	NO	NO	NO	NO
WPS Button (on Web Configurator)		YES	YES	YES	YES	NO	NO	YES
LED Indicator		1	2	2	2	2	2	2

Table 1 Model Feature Comparison (continued)

FEATURE/MODEL	NR7101	NR7102	NR7103	NR7123	NR7302	NR7303	FWA710
PoE Injector	YES	YES	YES	YES	YES	YES	YES
Wall Mounting	YES	YES	YES	YES	YES	YES	YES
Pole Mounting	YES	YES	YES	YES	YES	YES	YES
Sill Mounting	NO	NO	NO	YES	YES	YES	NO
Cellular PLMN (Public Land Mobile Network)	YES	YES	YES	YES	YES	YES	YES
Cellular Lock	YES	YES	NO	NO	YES	YES	NO
MLD (Multicast Listener Discovery) Proxy	NO	NO	YES	YES	NO	NO	YES
Proxy ARP (Address Resolution Protocol)	YES	YES	NO	NO	YES	YES	NO
FQ_Codel (Fair Queuing with Controlled Delay)	YES	YES	NO	NO	NO	NO	NO
Network Monitoring	YES	YES	NO	NO	YES	NO	NO
DHCP (Dynamic Host Configuration Protocol) server	YES	YES	YES	YES	YES	YES	YES
Custom DHCP	NO	NO	NO	NO	YES	YES	NO
NAT (Network Address Translation)	YES	YES	YES	YES	YES	YES	YES
DMZ (DeMilitarized Zone)	YES	YES	YES	YES	YES	YES	YES
ALG (Application Layer Gateway)	YES	YES	NO	NO	YES	NO	NO
Port Forwarding	YES	YES	YES	YES	YES	YES	YES
Port Triggering	YES	YES	NO	NO	YES	NO	NO
IP Passthrough	YES	YES	YES	YES	YES	YES	YES
Dynamic DNS (Domain Name System) for the first APN (Access Point Name)	YES	YES	YES	YES	YES	YES	YES
Static Route Setting	YES	YES	YES	YES	YES	YES	YES
Dynamic Route Setting for RIP (Routing Information Protocol)	YES	YES	NO	NO	YES	NO	NO
Cellular APN VLAN Settings	NO	NO	NO	NO	YES	NO	NO
VLAN Group	YES	YES	NO	NO	YES	YES	NO
Interface Grouping	YES	YES	NO	NO	YES	YES	NO
Local and Remote Device Management	YES	YES	YES	YES	YES	YES	YES
ARP (Address Resolution Protocol)	YES	YES	YES	YES	YES	YES	YES
Stateful Packet Inspection (SPI) Firewall	YES	YES	YES	YES	YES	YES	YES
Denial of Service (DoS) Protection	YES	YES	YES	YES	YES	YES	YES
Filter of LAN MAC address, LAN IP address and URLs	YES	YES	YES	YES	YES	YES	YES
Parental Control	NO	NO	YES	YES	NO	NO	YES

Table 1 Model Feature Comparison (continued)

FEATURE/MODEL	NR7101	NR7102	NR7103	NR7123	NR7302	NR7303	FWA710
Email Notification	YES	YES	NO	NO	YES	NO	NO
Firmware Upgrade	YES	YES	YES	YES	YES	YES	YES
Module Upgrade	YES	YES	NO	NO	NO	NO	NO
XMPP (eXtensible Messaging and Presence Protocol) Connection (TR-069)	YES	YES	NO	NO	YES	NO	NO
Remote Management Through TR-069	YES	YES	YES	YES	YES	YES	YES
Remote Management Through TR-369	NO	NO	NO	NO	YES	YES	NO
Internet Connection Test Through TR-471	NO	NO	NO	NO	YES	NO	NO
Latest Firmware Version Supported	1.00	1.00	1.00	1.00	1.00	1.00	1.00

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)

The Zyxel Device WiFi is for local management so you cannot access the Internet through WiFi. 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

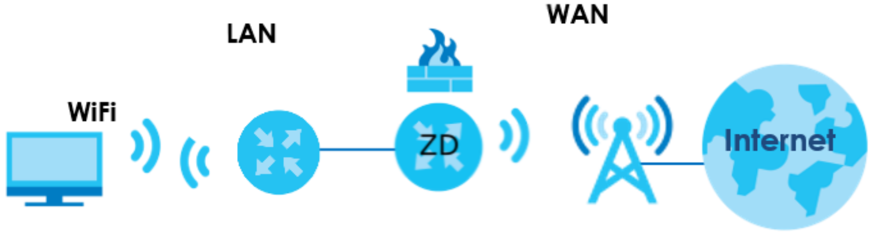
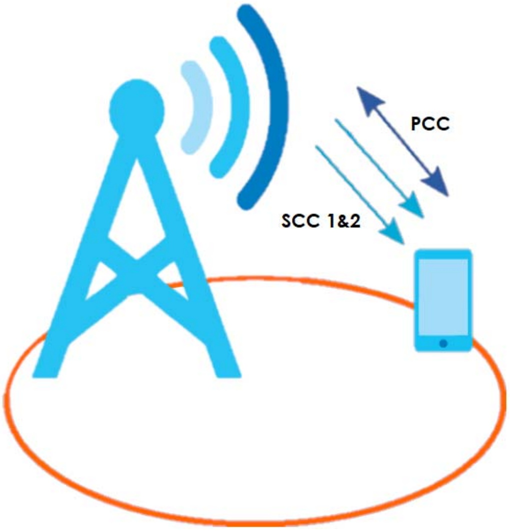


Figure 2 Zyxel Device's Configuration Through WiFi Connection

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 Carrier Aggregation 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.

- Zyxel Air app. The Zyxel Air app is available on App Store for Apple devices and Google Play for Android devices. Use the Zyxel Air app 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 is not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Refer to Section 33.2 on page 260. 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.

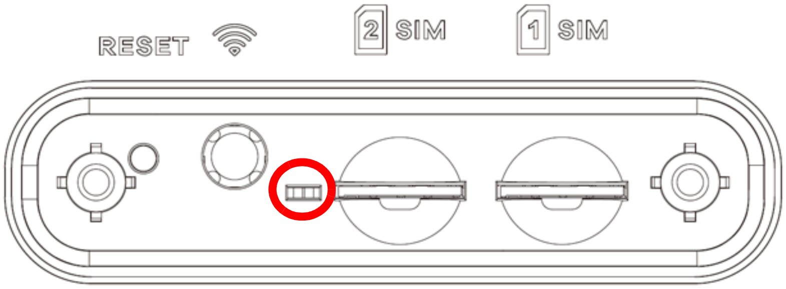
2.2 LEDs (Lights)

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

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

2.2.1 Zyxel Device Model with Single LED

Figure 4 NR7101 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.

2.2.2 Zyxel Device Models With Multiple LEDs

Figure 5 NR7102 LEDs

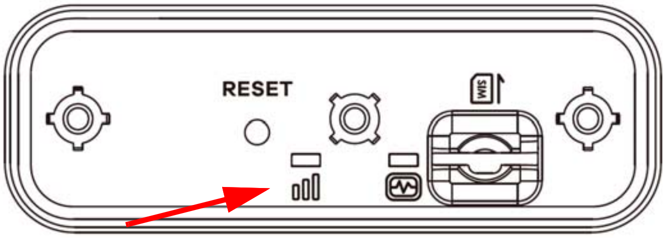


Figure 6 NR7103 / NR7123 / FWA710 LEDs

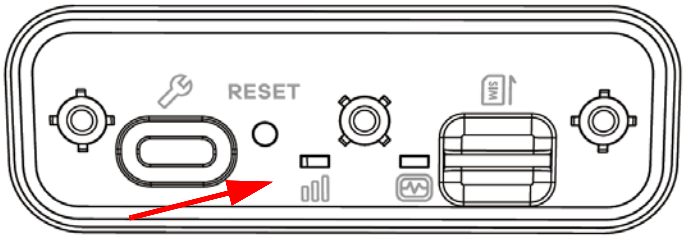
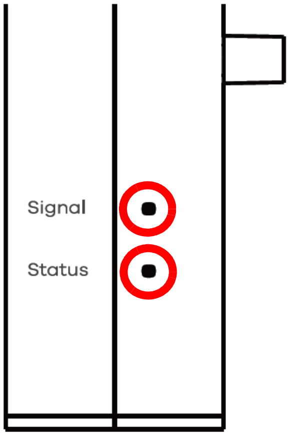


Figure 7 NR7302 / NR7303 LEDs



The following are the Zyxel Device's LED descriptions.

Table 3 NR7102 / NR7103 / NR7123 / FWA710 LED Behavior

LED	COLOR	STATUS	DESCRIPTION
Signal 📶	Green	On	The cellular signal strength is excellent.
	Amber	On	The cellular signal strength is fair.
	Red	On	The cellular signal strength is weak.
		Blinking	There is no cellular signal, or signal strength is below the weak level.

Table 3 NR7102 / NR7103 / NR7123 / FWA710 LED Behavior (continued)

LED	COLOR	STATUS	DESCRIPTION
Status	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 on.
	Red	On	There is a system failure.
		Blinking	The Zyxel Device is booting.
	Green / Amber / Red	Looping	Firmware upgrade is in progress.

Table 4 NR7302 / NR7303 LED Behavior

LED	COLOR	STATUS	DESCRIPTION
Signal	Green	On	The 5G cellular signal strength is excellent.
		Blinking	The 4G cellular signal strength is excellent.
	Amber	On	The 5G cellular signal strength is fair.
		Blinking	The 5G cellular signal strength is fair.
	Red	On	The 5G cellular signal strength is weak.
		Blinking	The 4G cellular signal strength is weak.
	Off	Not connected to the Internet.	
Status	Green	On	The Zyxel Device is connected to the Internet with WiFi off.
		Fast blinking	The Zyxel Device is trying to connect to the Internet with WiFi off.
		Slow blinking	The Zyxel Device is booting.
	Amber	On	The Zyxel Device is connected to the Internet with WiFi on.
		Fast blinking	The Zyxel Device is trying to connect to the Internet with WiFi on.
	Red	On	There is a system failure.
	Green / Amber / Red	Looping	Firmware upgrade is in progress.
	Off	Power is off.	

2.3 Ports Panel

The connection ports are located on the ports panel.

Figure 8 NR7101 Ports Panel

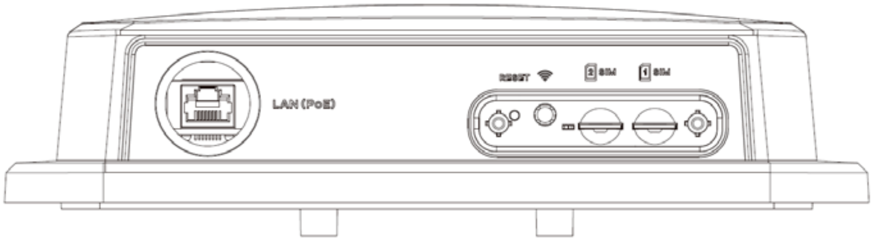


Figure 9 NR7102 Ports Panel

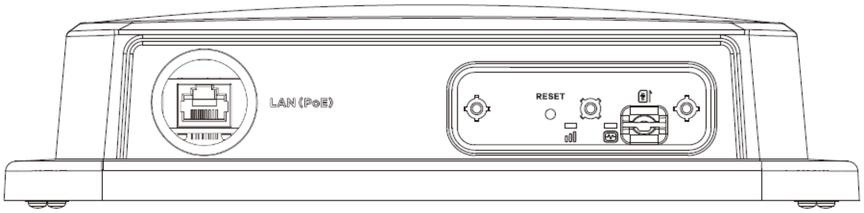


Figure 10 NR7103 / FWA710 Ports Panel

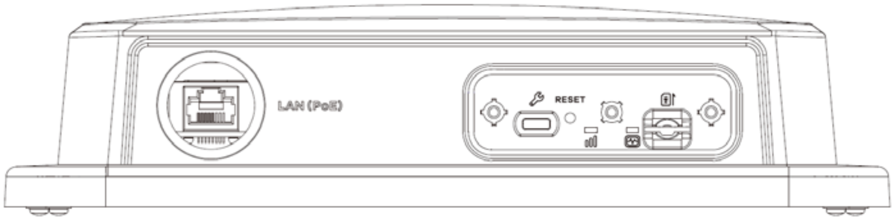


Figure 11 NR7123 Ports Panel

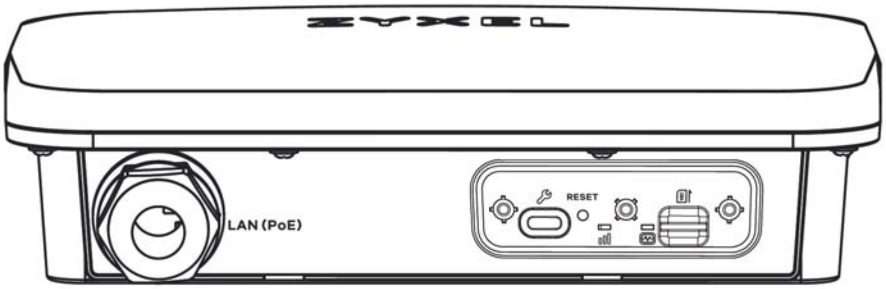
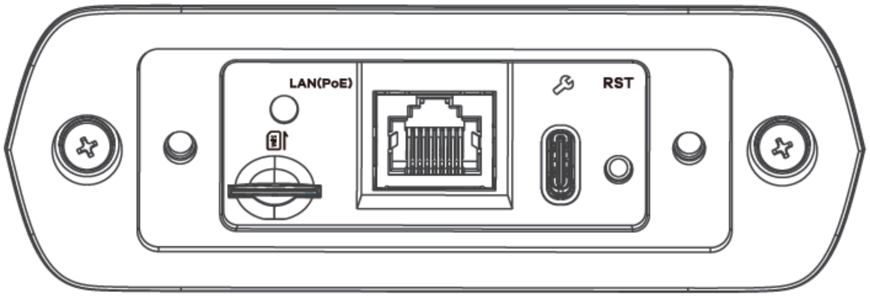


Figure 12 NR7302 / NR7303 Ports Panel



The following table describes the items on the ports panel.

Table 5 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.

2.4 WiFi/WPS Button

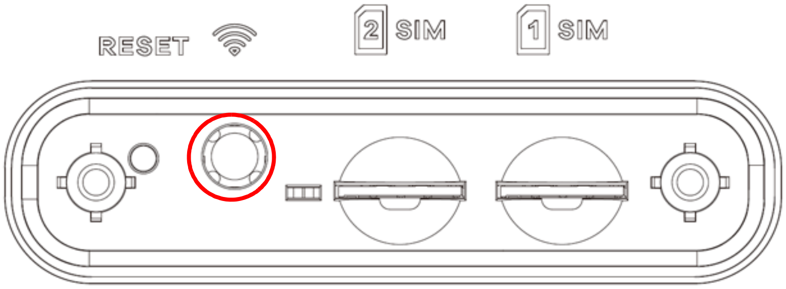
Use the **WiFi/WPS** button on the Zyxel Device to turn on/off the WiFi network or quickly build a WiFi connection with a WiFi client.

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 16 to check if your Zyxel Device has a **WiFi/WPS** button.

Note: You can also find a **WPS** button on the Web Configurator.

Figure 13 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.

2.5 RESET Button

Insert a thin object into the **RESET/RST** hole of the Zyxel Device to reboot or reset to its factory default configurations.

Reboot

This allows you to restart the Zyxel Device without turning the power off. You may need to do this if the Zyxel Device hangs.

Reset

Reset the Zyxel Device to its factory-defaults 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/RST** button on the bottom panel.

Table 6 Reset/RST Button

LABELS	FUNCTIONS	DESCRIPTION
RESET/RST	Reset	Press the **RESET/RST** button for more than five seconds.
	Reboot	Press the **RESET/RST** button for more than two but less than five seconds.

Note: Make sure the Zyxel Device and the **Status** LED is on.

Figure 14 NR7101 Reset Button

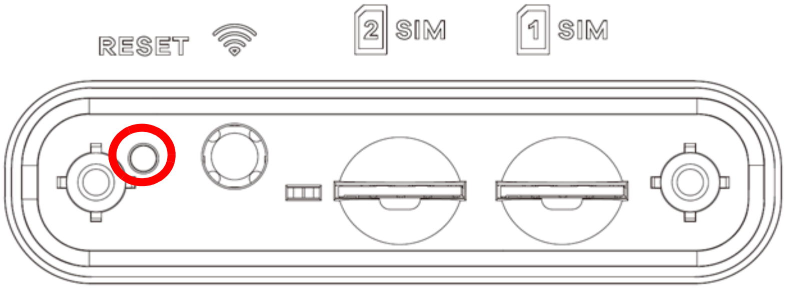


Figure 15 NR7102 Reset Button

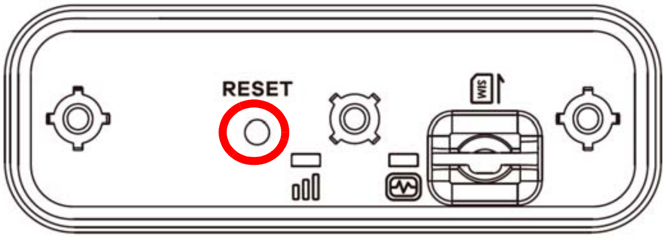


Figure 16 NR7103 / NR7123 / FWA710 Reset Button

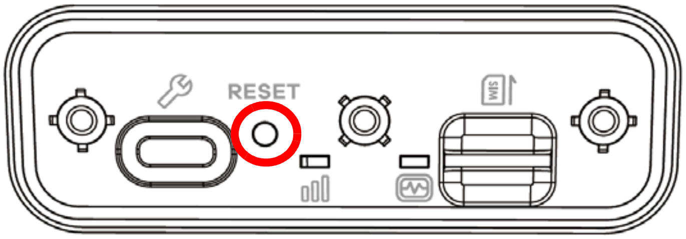
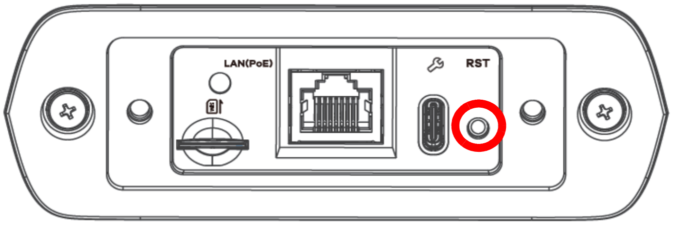


Figure 17 NR7302 / NR7303 Reset Button



CHAPTER 3 Web Configurator

3.1 Overview

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

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

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

3.1.1 Access the Web Configurator

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

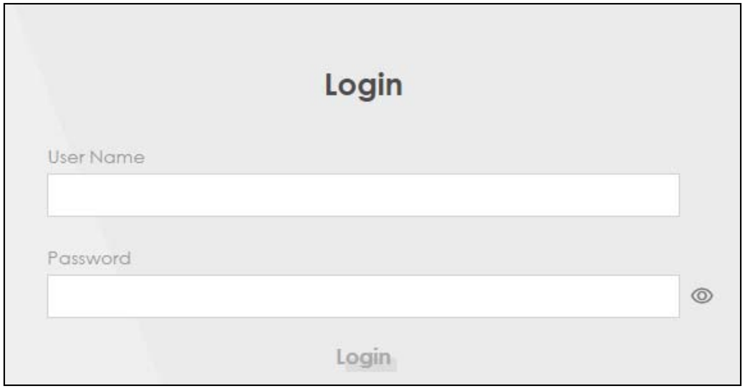
2 Make sure your computer has an IP address in the same subnet as the Zyxel Device.

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

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

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

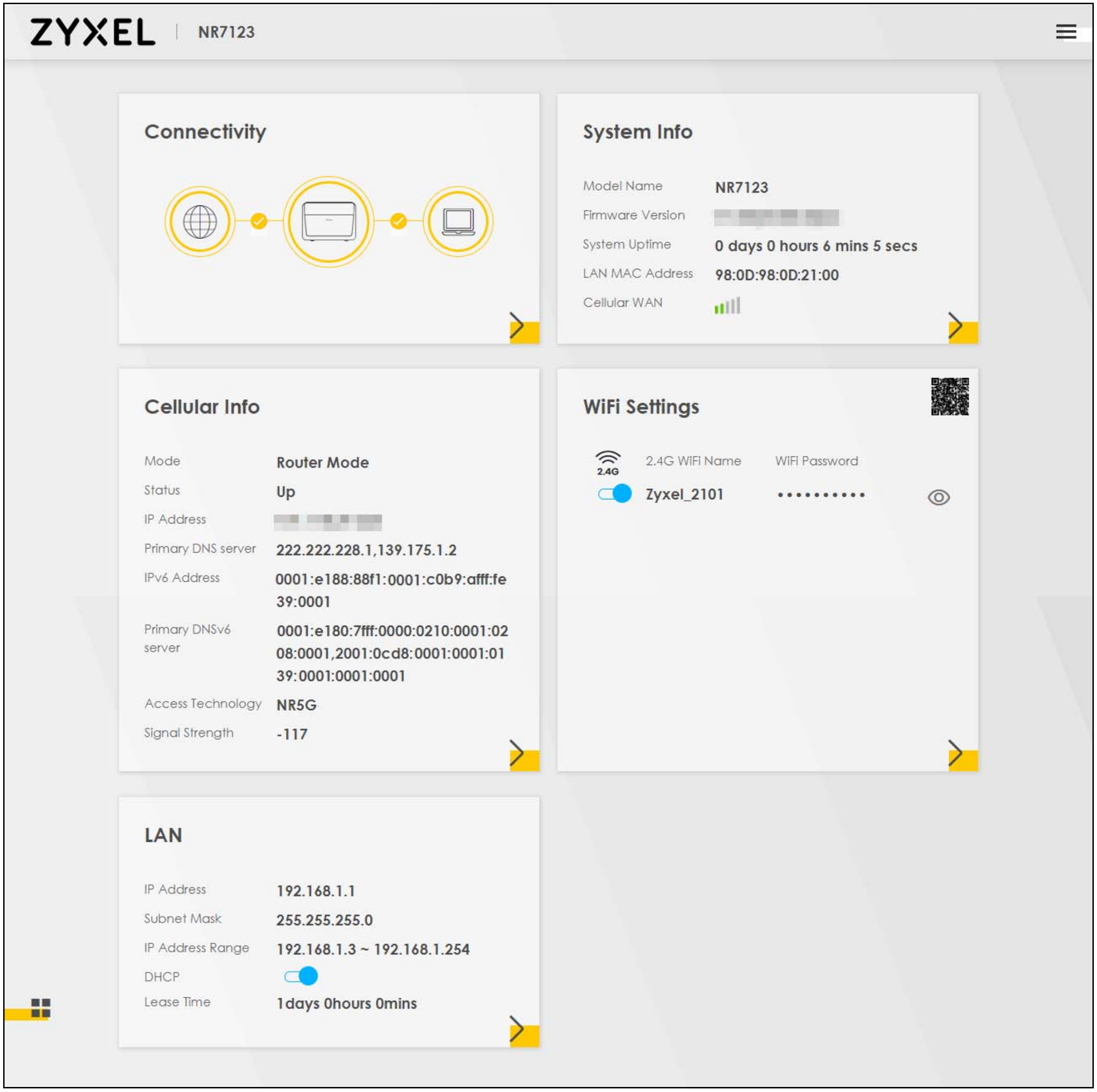
Figure 18 Login Screen



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.

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

Figure 19 Connection Status



Connectivity

System Info

Model Name	NR7123
Firmware Version	[redacted]
System Uptime	0 days 0 hours 6 mins 5 secs
LAN MAC Address	98:0D:98:0D:21:00
Cellular WAN	

Cellular Info

Mode	Router Mode
Status	Up
IP Address	[redacted]
Primary DNS server	222.222.228.1,139.175.1.2
IPv6 Address	0001:e188:88f1:0001:c0b9:afff:fe39:0001
Primary DNSv6 server	0001:e180:7fff:0000:0210:0001:0208:0001,2001:0cd8:0001:0001:0139:0001:0001:0001
Access Technology	NR5G
Signal Strength	-117

WiFi Settings

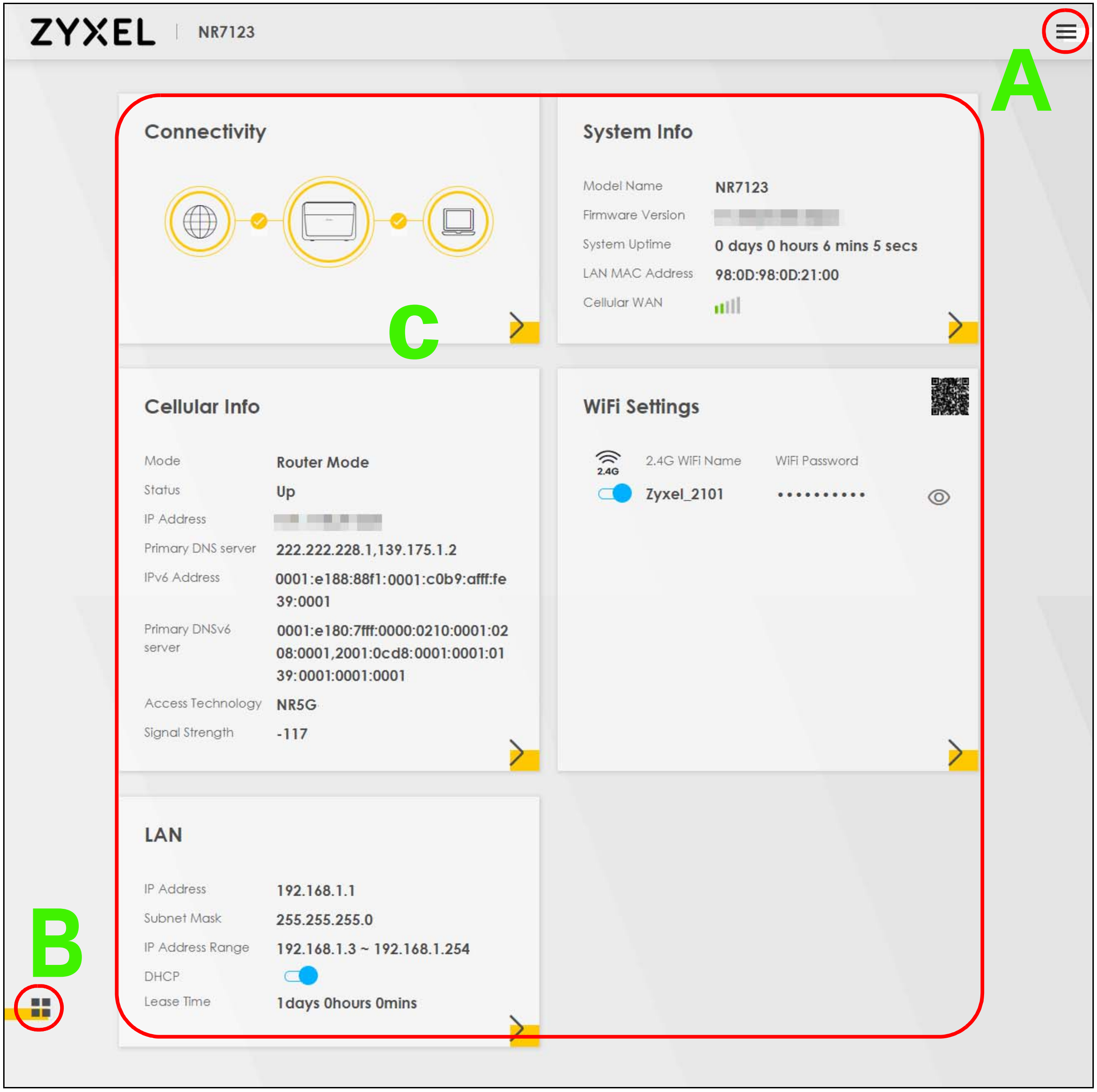
	2.4G WiFi Name	WiFi Password
2.4G	Zyxel_2101	••••••••••

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 20 Screen Layout



System Info

Model Name	NR7123
Firmware Version	[redacted]
System Uptime	0 days 0 hours 6 mins 5 secs
LAN MAC Address	98:0D:98:0D:21:00
Cellular WAN	

Cellular Info

Mode	Router Mode
Status	Up
IP Address	[redacted]
Primary DNS server	222.222.228.1,139.175.1.2
IPv6 Address	0001:e188:88f1:0001:c0b9:afff:fe39:0001
Primary DNSv6 server	0001:e180:7fff:0000:0210:0001:0208:0001,2001:0cd8:0001:0001:0139:0001:0001:0001
Access Technology	NR5G
Signal Strength	-117

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

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

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

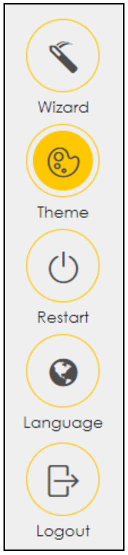
3.2.1 Settings Icon

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

3.2.1.1 Side Bar

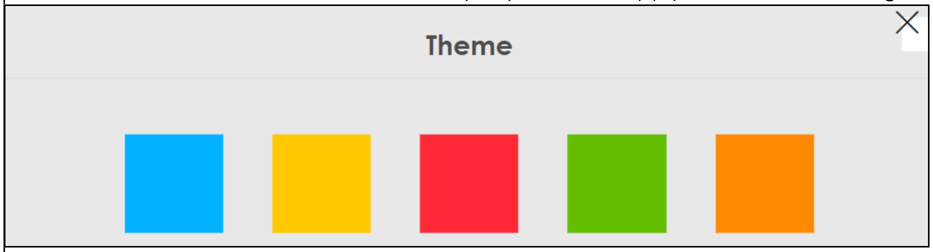
The side bar provides some icons on the right hand side.

Figure 21 Side Bar



The icons provide the following functions.

Table 7 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
Wizard	**Wizard**: Click this icon to open screens where you can configure the Zyxel Device's time zone and WiFi settings.
Theme	**Theme**: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
Language	**Language**: Select the language you prefer.
Restart	**Restart**: Click this icon to reboot the Zyxel Device without turning the power off.
Logout	**Logout**: Click this icon to log out of the Web Configurator.

3.2.1.2 Navigation Panel

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

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

Figure 22 Navigation Panel

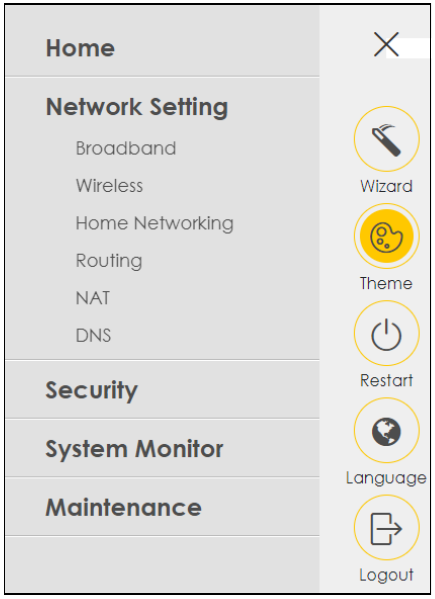


Table 8 Navigation Panel Summary

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. You can also add new WAN connections.
	Cellular WAN	Use this screen to configure a cellular WAN connection.
	Cellular APN	Use this screen to configure 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 PLMNs and select your preferred network.
	Cellular IP Passthrough	Use this screen to enable IP Passthrough on the Zyxel Device.
	Cellular Lock (LTE)	Use this screen to enable or disable PCI Lock for 4G LTE connections.
	Cellular Lock (5G)	Use this screen to enable or disable PCI Lock for 5G NR connections.

Table 8 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
	ESIM	Use this screen to download a subscription profile from your service provider and activate it on your Zyxel Device.
Wireless	General	Use this screen to configure the WiFi settings and WiFi authentication or 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 WiFi 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.
	Custom DHCP	Use this screen to configure additional DHCP options.
	GRE Tunnel	Use this screen to configure a GRE tunnel.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers.
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable the ALGs (Application Layer Gateways) in the Zyxel Device to allow applications to operate through NAT.
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	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	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.
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	Use this screen to define time periods and days during which the Zyxel Device performs parental control and/or block web sites with the specific URL.

Table 8 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the 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. Levels include: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: • Account • Attack • Firewall • MAC Filter
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
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 to the Zyxel Device’s WiFi.
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 and/or LAN connection.
	Trust Domain for IP Passthrough	Use this screen to enable public IP addresses to access this Zyxel Device remotely from a WAN and/or LAN 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.

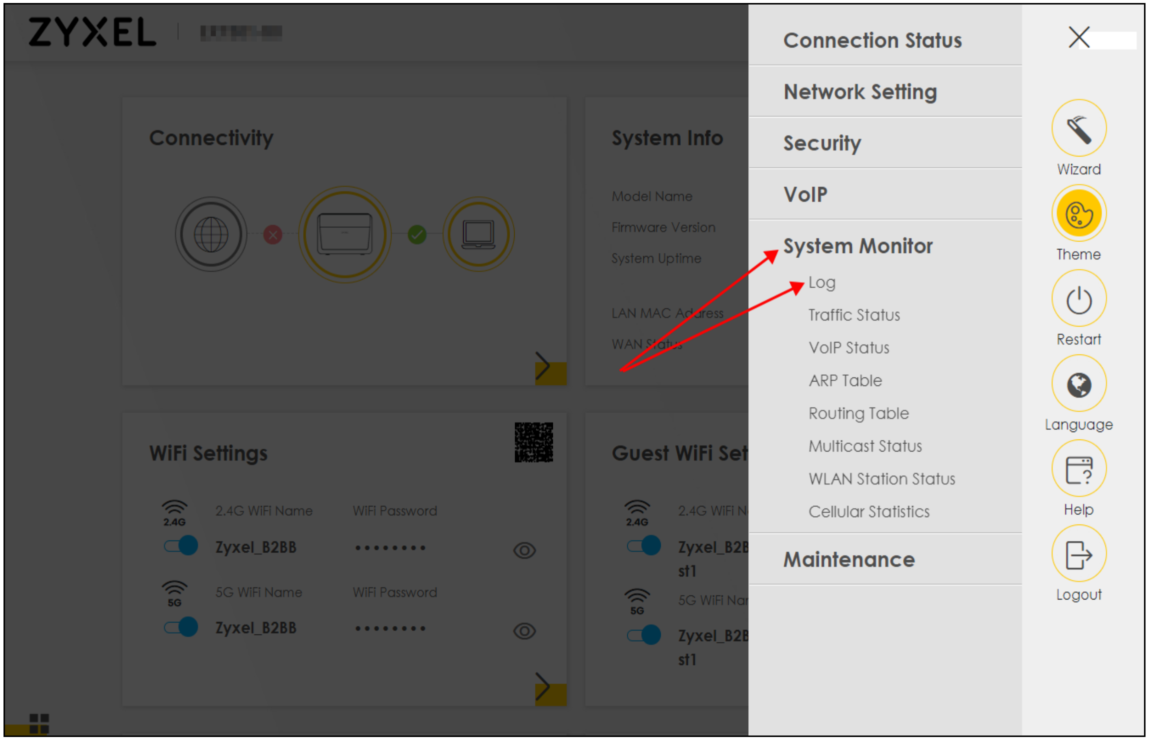
Table 8 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
TR-369 Local Agent	MQTT	Use the screen to manage the profile settings that the Zyxel Device will use to register with an MQTT broker.
	Agent	Use this screen to set the Zyxel Device as an agent, select a cellular WAN, and configure the Message Transfer Protocol (MTP) to receive USP messages from controllers.
	Controller	Use this screen to configure controller settings for topics the Zyxel Device agent should publish to this controller.
Time	Time	Use this screen to change your Zyxel Device’s time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Setting	Log Setting	Use this screen to change your Zyxel Device’s log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
	Module Upgrade	Use this screen to upload the 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	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.

3.2.1.3 Dashboard

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

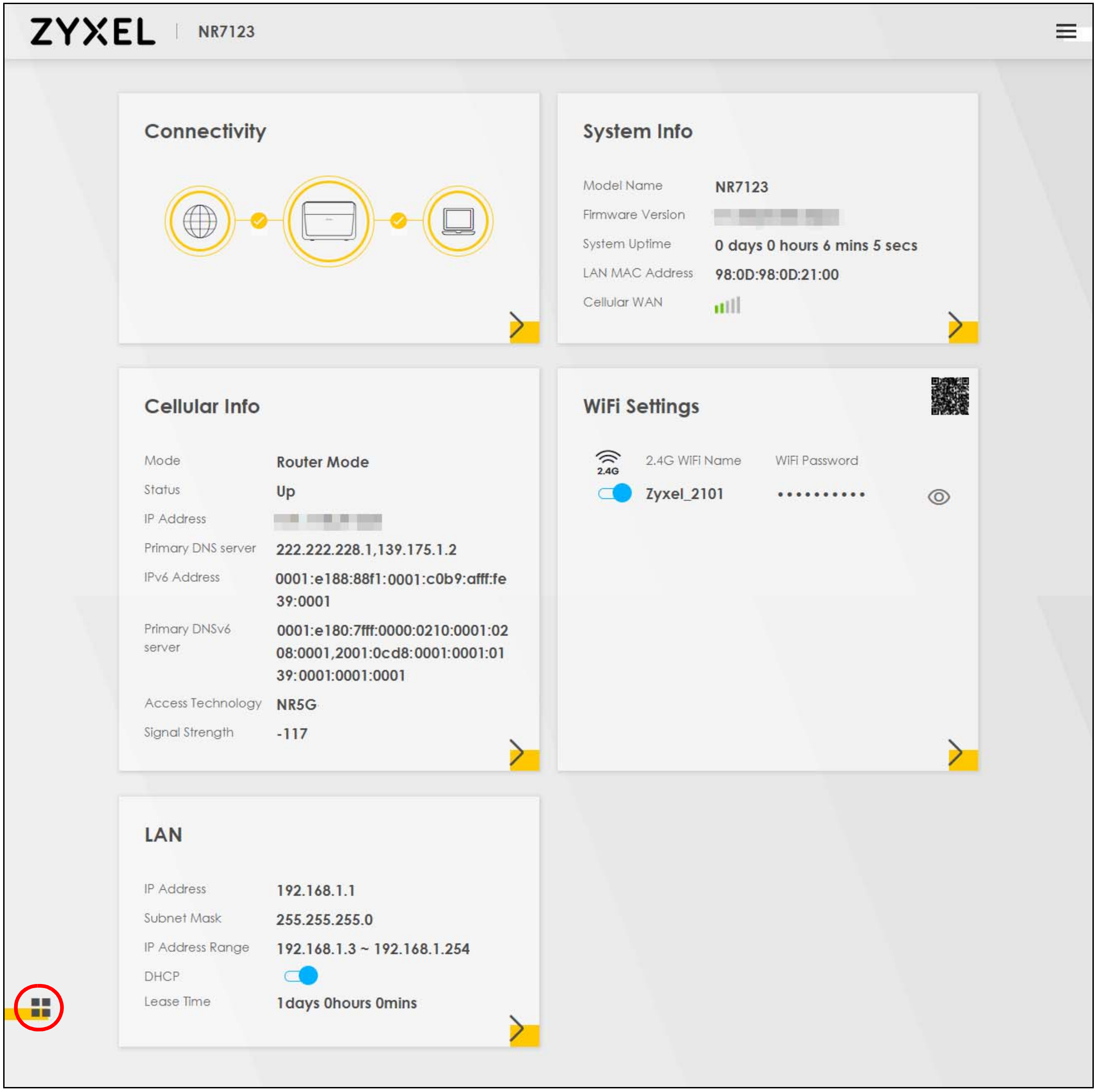
Figure 23 Navigation Panel



3.2.2 Widget Icon

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

Figure 24 Dashboard Widget



Connectivity

System Info

Model Name	NR7123
Firmware Version	[redacted]
System Uptime	0 days 0 hours 6 mins 5 secs
LAN MAC Address	98:0D:98:0D:21:00
Cellular WAN	

Cellular Info

Mode	Router Mode
Status	Up
IP Address	[redacted]
Primary DNS server	222.222.228.1,139.175.1.2
IPv6 Address	0001:e188:88f1:0001:c0b9:afff:fe39:0001
Primary DNSv6 server	0001:e180:7fff:0000:0210:0001:0208:0001,2001:0cd8:0001:0001:0139:0001:0001:0001
Access Technology	NR5G
Signal Strength	-117

WiFi Settings

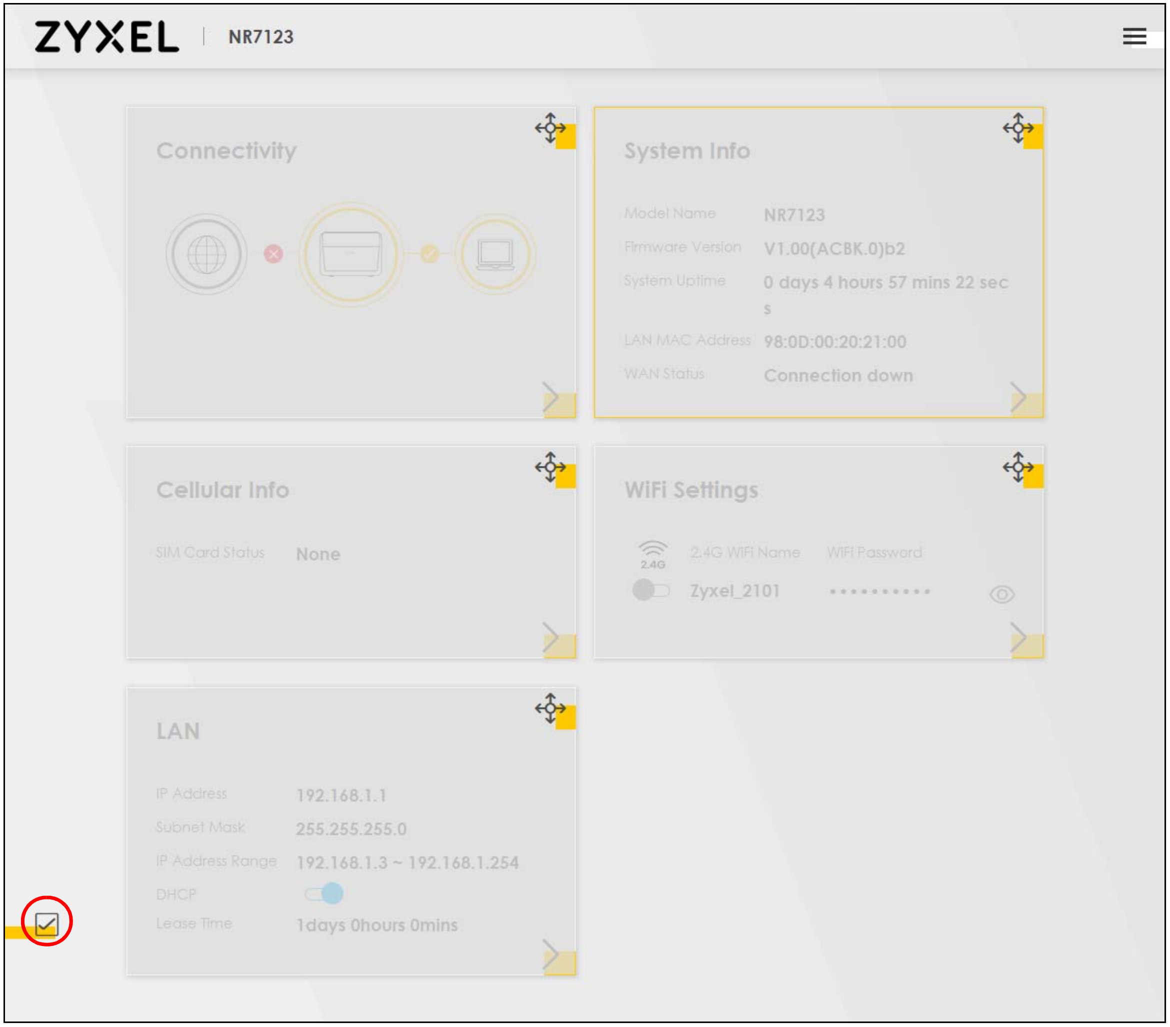
2.4G WiFi Name	WiFi Password
Zyxel_2101	••••••••••

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

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

Figure 25 Check Icon



ZYXEL | NR7123

Connectivity

System Info

Model Name NR7123

Firmware Version V1.00(ACBK.0)b2

System Uptime 0 days 4 hours 57 mins 22 secs

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 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

CHAPTER 4
Quick Start

4.1 Quick Start Overview

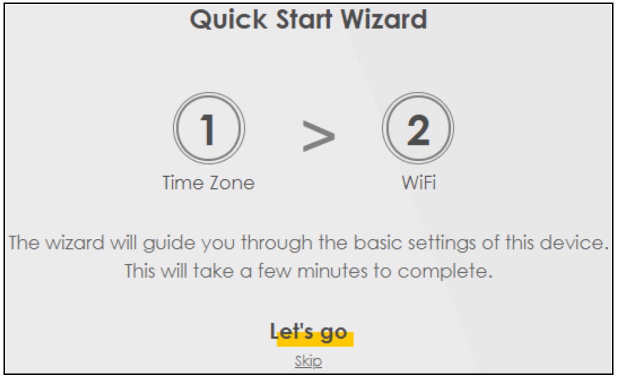
Use the **Wizard** screens to configure the Zyxel Device's time zone and WiFi settings.

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

4.2 Quick Start Setup

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

Figure 26 Wizard – Home



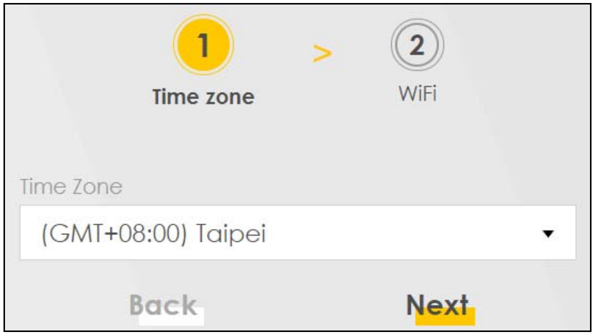
Quick Start Wizard

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

4.3 Quick Start Setup – Time Zone

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

Figure 27 Wizard – Time Zone



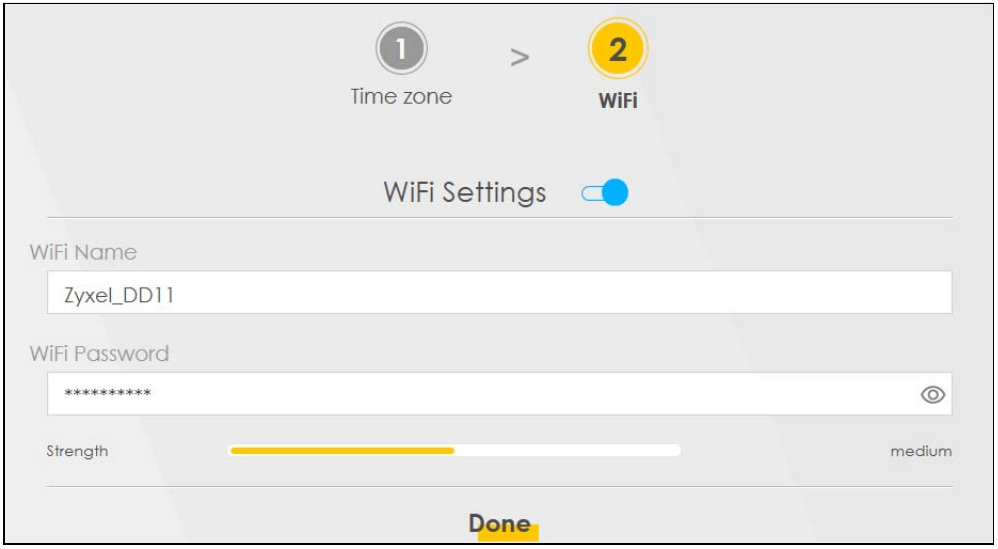
Time Zone

(GMT+08:00) Taipei

4.4 Quick Start Setup – WiFi

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

Figure 28 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.

4.5 Quick Start Setup – Finish

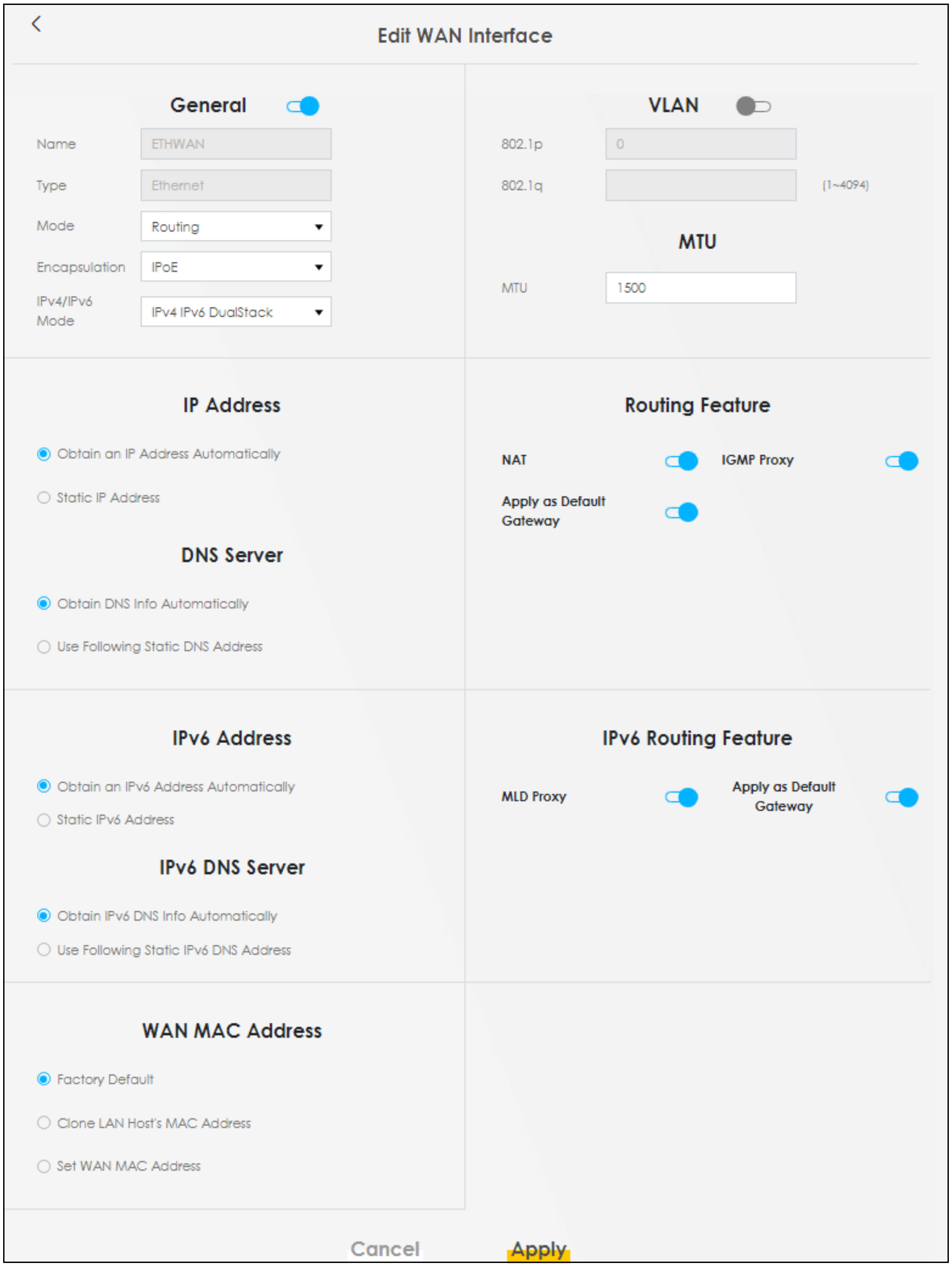
Your Zyxel Device saves and applies your settings.

CHAPTER 5
Web Interface Tutorials

5.1 Web Interface Overview

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

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



Edit WAN Interface

General

Name: ETHWAN

Type: Ethernet

Mode: Routing

Encapsulation: IPoE

IPv4/IPv6 Mode: IPv4 IPv6 DualStack

VLAN

802.1p: 0

802.1q: (1~4094)

MTU

MTU: 1500

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

DNS Server

● Obtain DNS Info Automatically

○ Use Following Static DNS Address

Routing Feature

NAT

IGMP Proxy

Apply as Default Gateway

IPv6 Address

● Obtain an IPv6 Address Automatically

○ Static IPv6 Address

IPv6 DNS Server

● Obtain IPv6 DNS Info Automatically

○ Use Following Static IPv6 DNS Address

IPv6 Routing Feature

MLD Proxy

Apply as Default Gateway

WAN MAC Address

● Factory Default

○ Clone LAN Host's MAC Address

○ Set WAN MAC Address

5.2 WiFi Network Setup

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

However, the WiFi network is only for configuring the Zyxel Device. Remember to turn it off after all configurations are done.

Figure 29 Zyxel Device Configuration through WiFi Connection

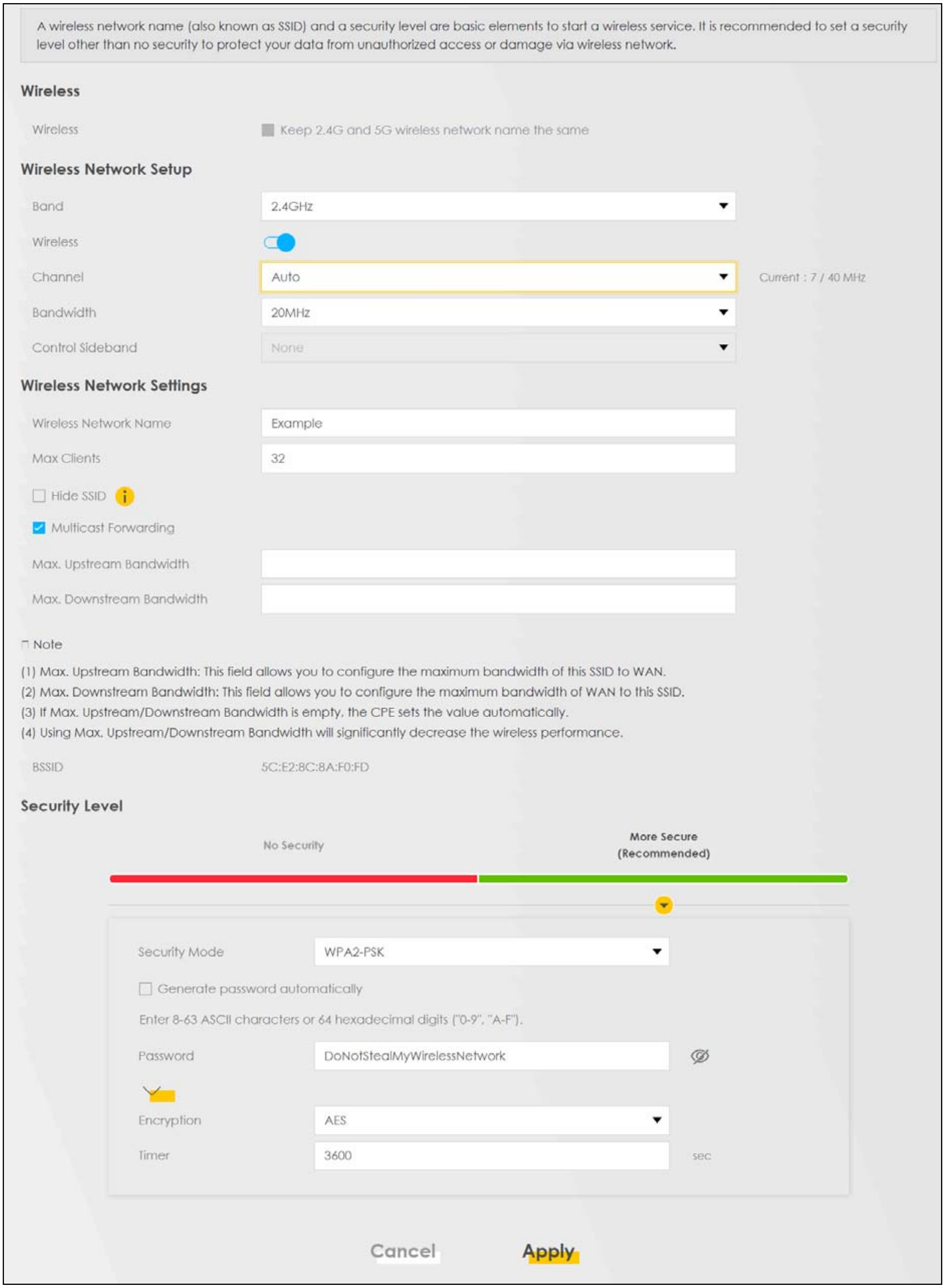
See the label on the Zyxel Device for the WiFi network settings and then connect manually to the Zyxel Device. Alternatively, you can connect to the Zyxel Device WiFi network using WPS.

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**.



A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than no security to protect your data from unauthorized access or damage via wireless network.

Wireless

Wireless ■ Keep 2.4G and 5G wireless network name the same

Wireless Network Setup

Band	2.4GHz ▼	
Wireless	●	
Channel	Auto ▼	Current : 7 / 40 MHz
Bandwidth	20MHz ▼	
Control Sideband	None ▼	

Wireless Network Settings

Wireless Network Name	Example
Max Clients	32

□ Hide SSID

☑ Multicast Forwarding

Max. Upstream Bandwidth	
Max. Downstream Bandwidth	

Note

(1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.
(2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.
(3) If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.
(4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID 5C:E2:8C:8A:F0:FD

Security Level

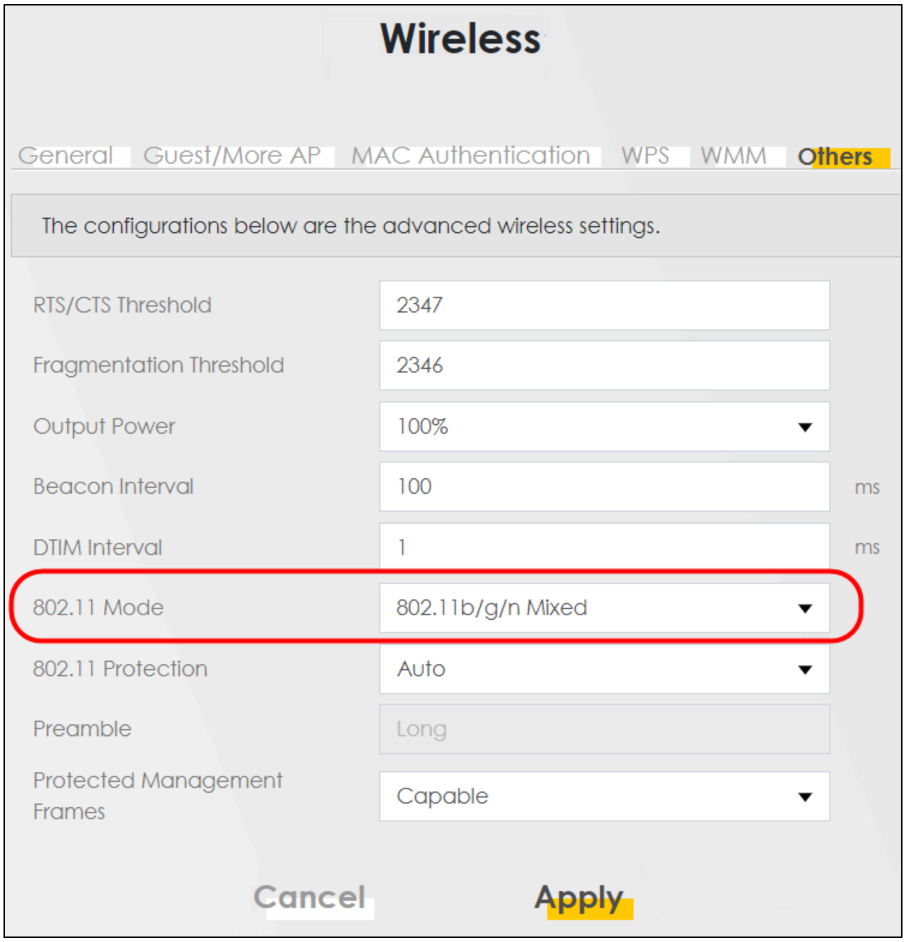
Security Mode WPA2-PSK ▼

□ Generate password automatically

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

Password	DoNotStealMyWirelessNetwork	
Encryption	AES ▼	
Timer	3600	sec

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



The configurations below are the advanced wireless settings.

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

You can now use the WPS feature to establish a WiFi connection between your notebook and the Zyxel Device. Now use the new security settings to connect to the Internet through the Zyxel Device using WiFi.

5.2.2 Setting Up a Guest Network

The Zyxel Device authenticates the WiFi device using the PIN, and then sends the WiFi network settings to the device using WPS. This process may take up to 2 minutes. The WiFi device is then able to connect to the WiFi network securely.

5.3 Cellular Network Setup

This section shows you how to set up a cellular network.

5.3.1 Setting up a Cellular Network Connection

This section gives you an example on 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 card 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.

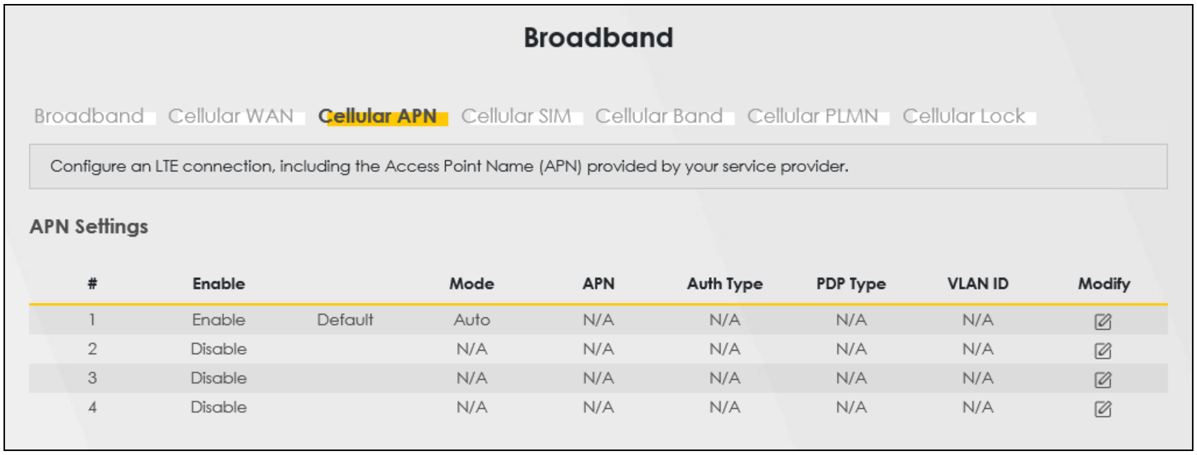
3 If your SIM has a PIN Code, enter this code in the **Network Setting** > **Broadband** > **Cellular SIM** screen.

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.



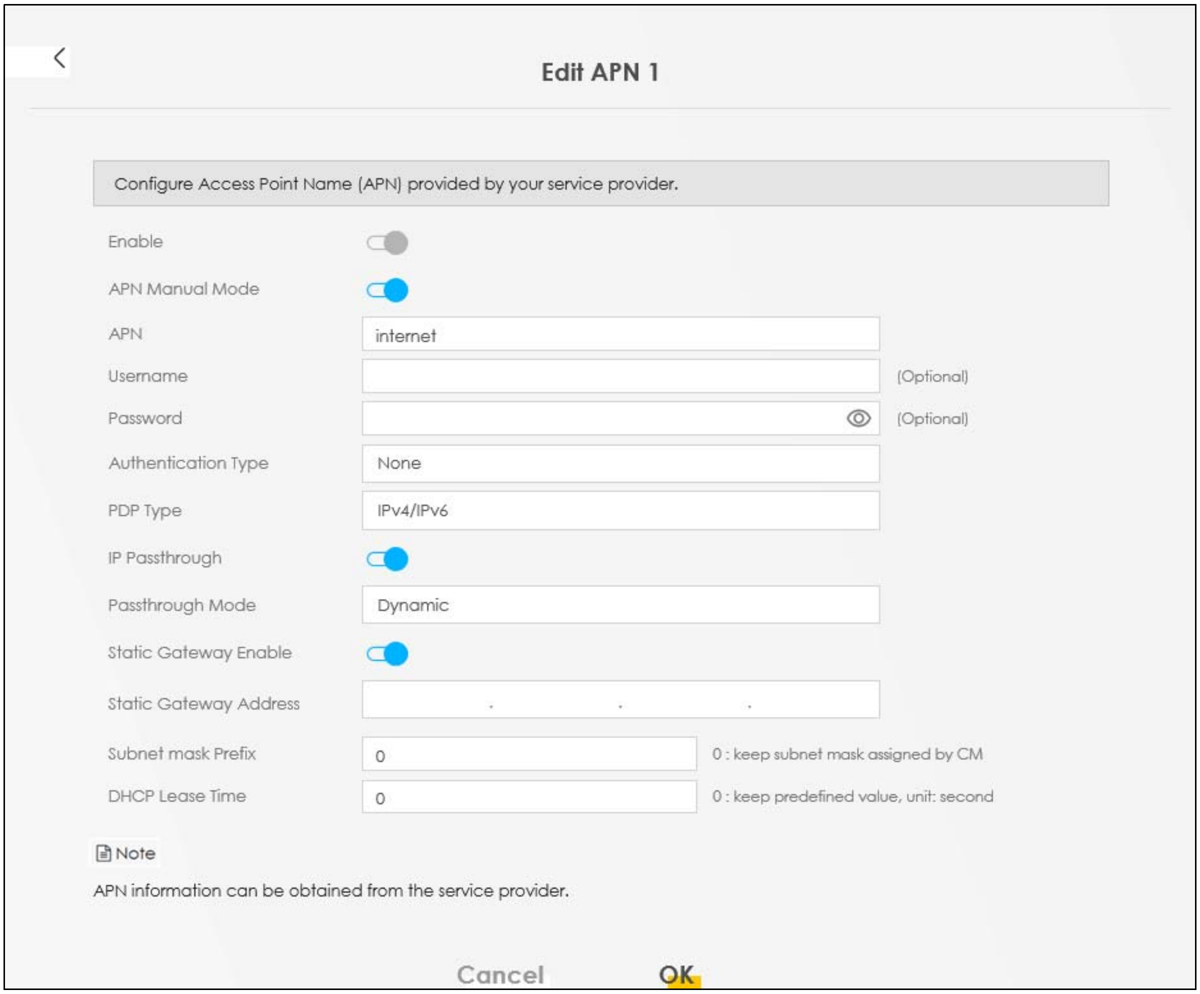
Broadband

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 enter 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

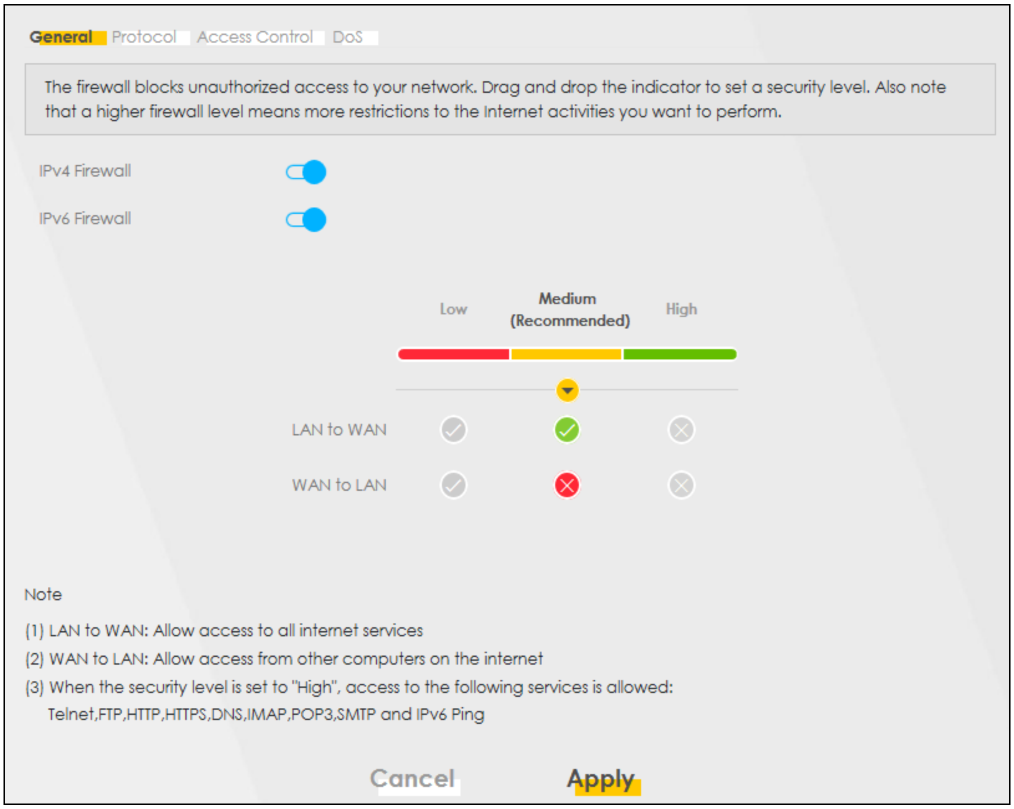
This section shows you how to configure a Firewall rule, Parental Control rule, and MAC Filter rule.

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**.



The firewall blocks unauthorized access to your network. Drag and drop the indicator to set a security level. Also note that a higher firewall level means more restrictions to the Internet activities you want to perform.

IPv4 Firewall ●

IPv6 Firewall ●

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

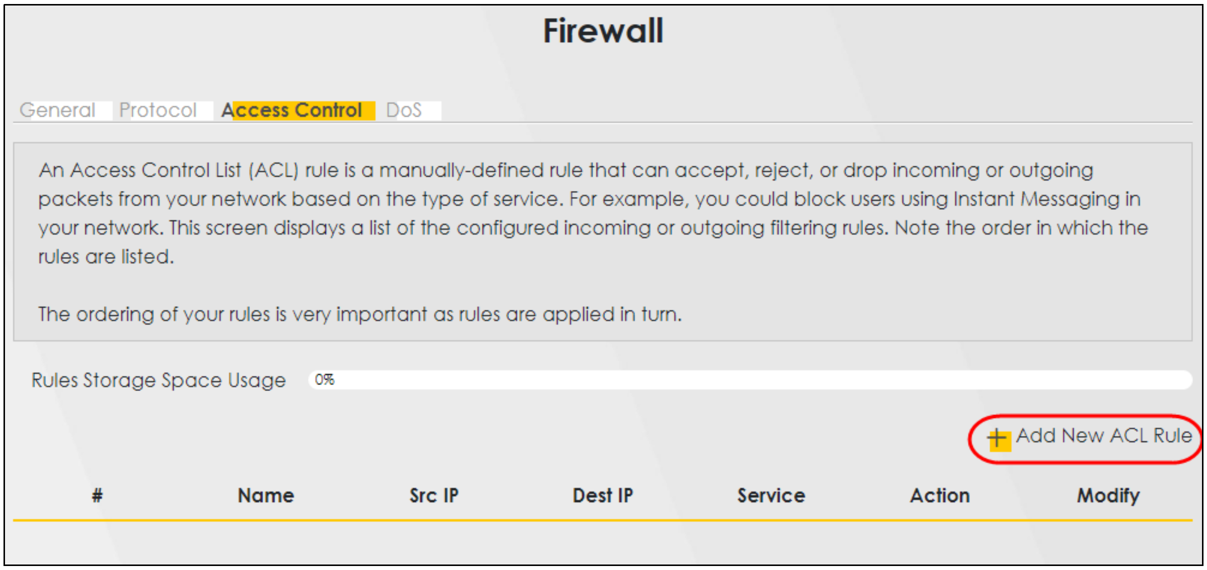
Note

(1) LAN to WAN: Allow access to all internet services

(2) WAN to LAN: Allow access from other computers on the internet

(3) When the security level is set to "High", access to the following services is allowed: Telnet,FTP,HTTP,HTTPS,DNS,IMAP,POP3,SMTP and IPv6 Ping

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



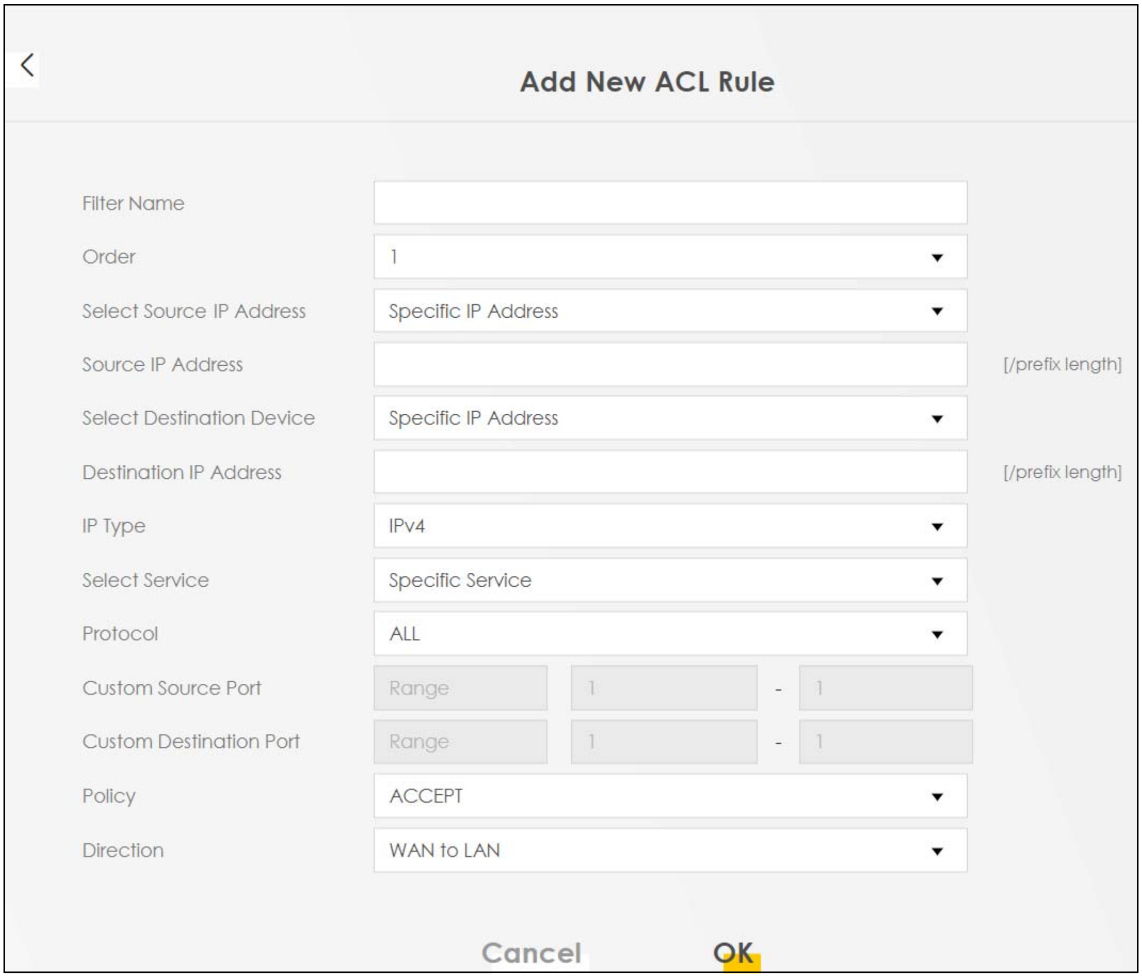
An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network based on the type of service. For example, you could block users using Instant Messaging in your network. This screen displays a list of the configured incoming 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 Use the following fields to configure and apply a new ACL (Access Control List) 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.

Note: The style and features of your parental control 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.

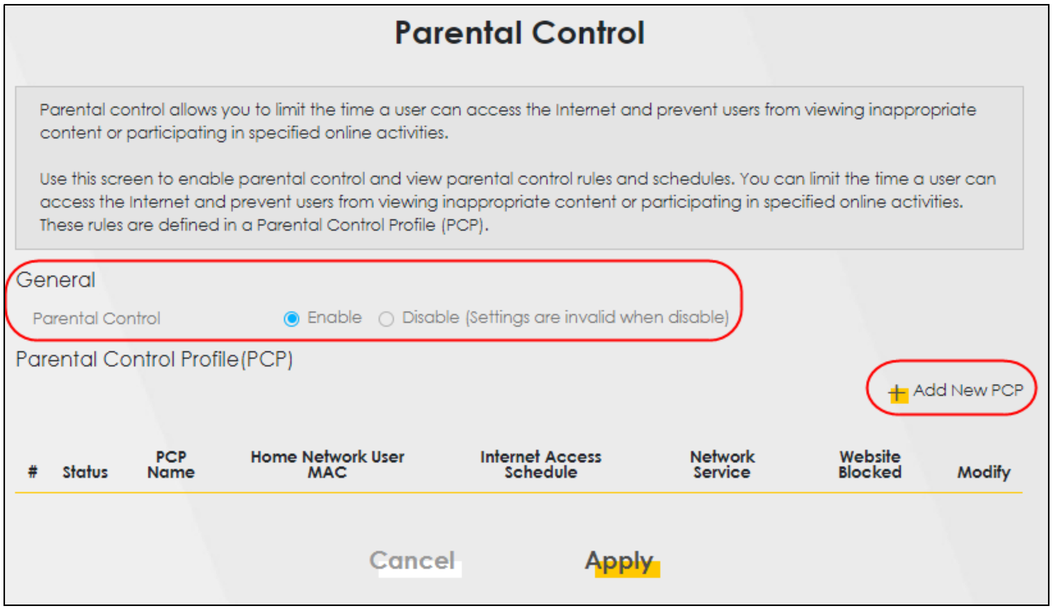
This example shows you how to block a user from accessing the Internet during time for studying. It also shows you how to stop a user from accessing specific websites.

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

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

Parental Control Screen

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



Parental Control

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.

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).

General

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

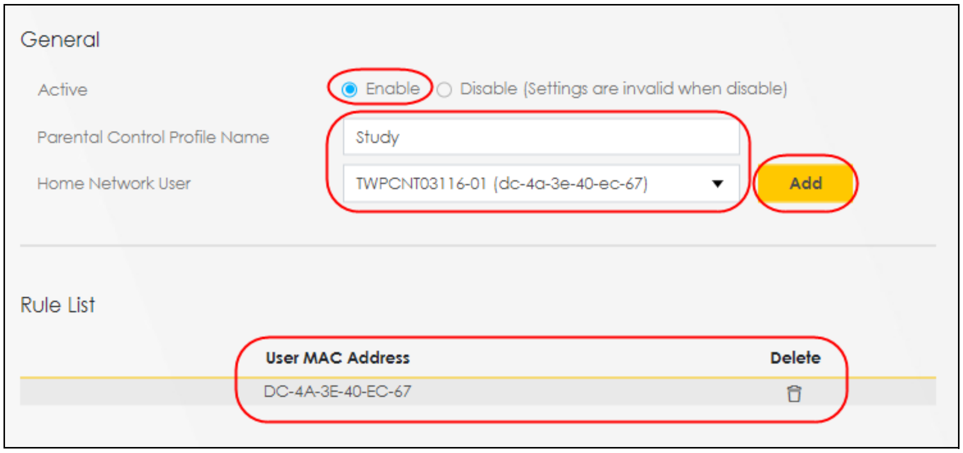
Parental Control Profile(PCP)

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

Add New PCP Screen

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

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



General

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

Parental Control Profile Name: Study

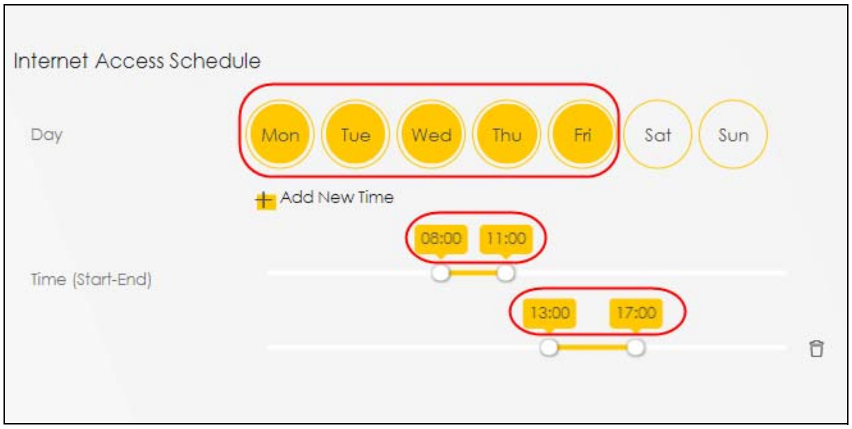
Home Network User: TWPCNT03116-01 (dc-4a-3e-40-ec-67)

Rule List

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

2 Under **Internet Access Schedule**:

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



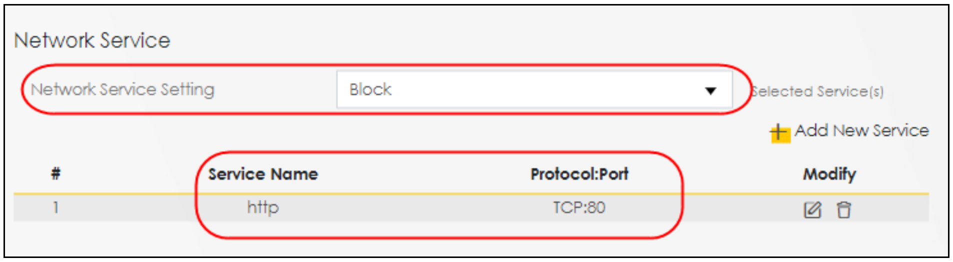
Internet Access Schedule

Day: Mon, Tue, Wed, Thu, Fri, Sat, Sun

Time (Start-End): 08:00 – 11:00; 13:00 – 17:00

3 Under **Network Service**:

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



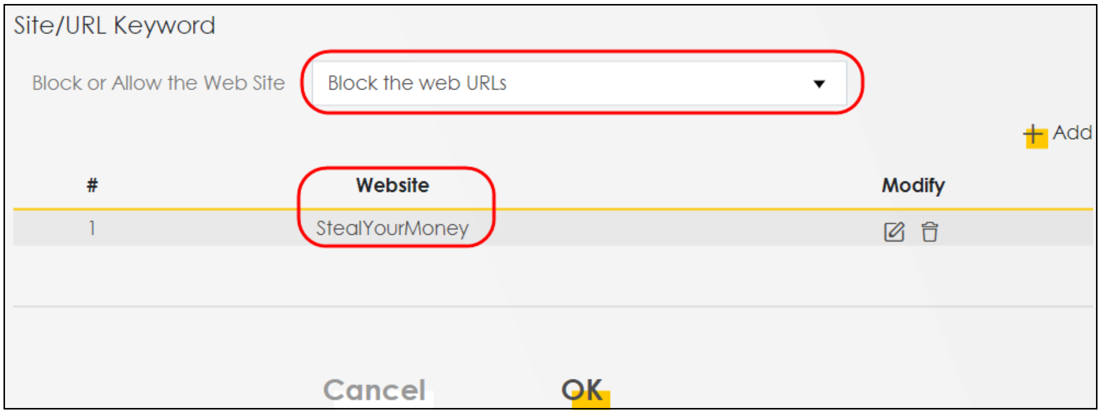
Network Service

Network Service Setting: Block

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

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

- Select **Block the web URLs** in **Block or Allow the Web Site**.
- Click **Add**, then use the parameter given above to configure settings for the URL keyword you are blocking.



Site/URL Keyword

Block or Allow the Web Site: Block the web URLs

#	Website	Modify
1	StealYourMoney	

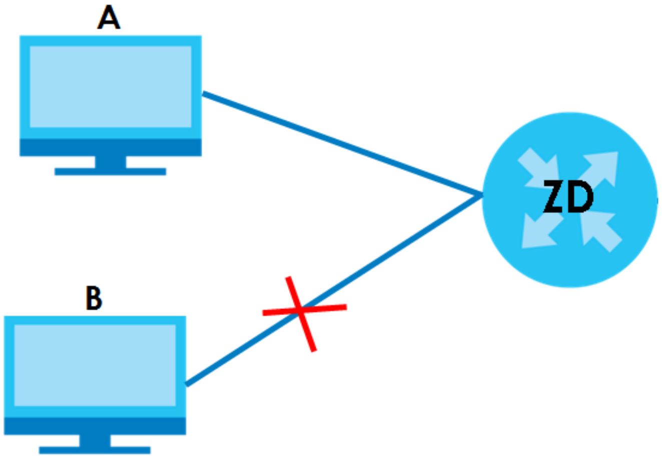
5 Click **OK** to save your settings.

5.4.3 Configuring a MAC Address Filter for Wired LAN Connections

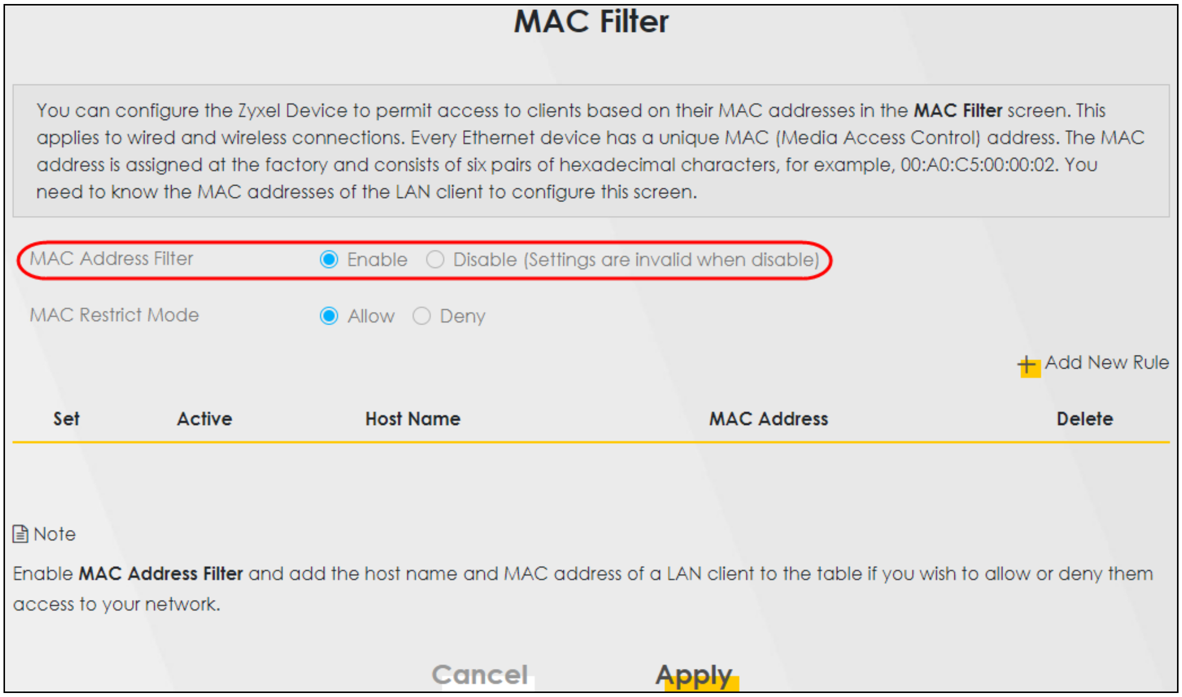
You can use a MAC address filter to exclusively allow or permanently block someone from the wired LAN network.

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

Figure 30 Configure a MAC Address Filter Example



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)

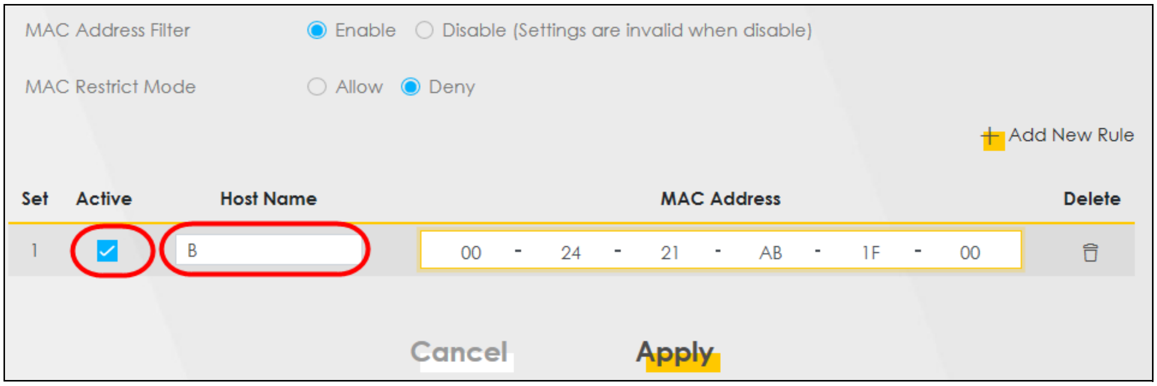
MAC Restrict Mode ● Allow ○ Deny

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

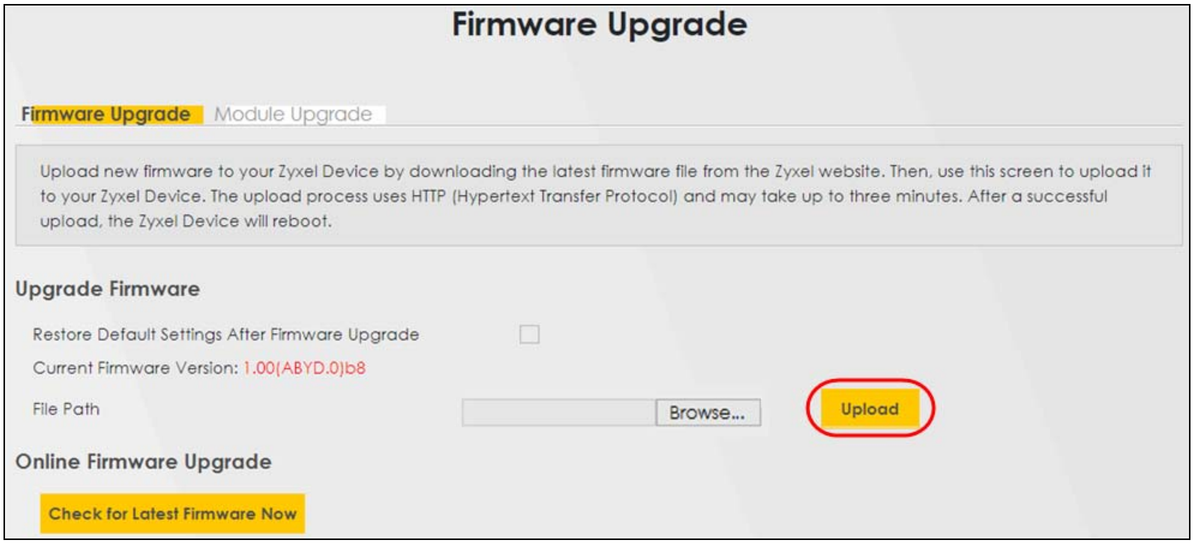
This section shows you how to upgrade the Zyxel Device firmware, back up the configuration and restore the Zyxel Device to its previous or default settings.

5.5.1 Upgrading the Firmware

1 Download the correct firmware file from the download library at the Zyxel website. The model code for the Zyxel Device in this example is v5.13(ABLZ.1) Note the model code for your Zyxel 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

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

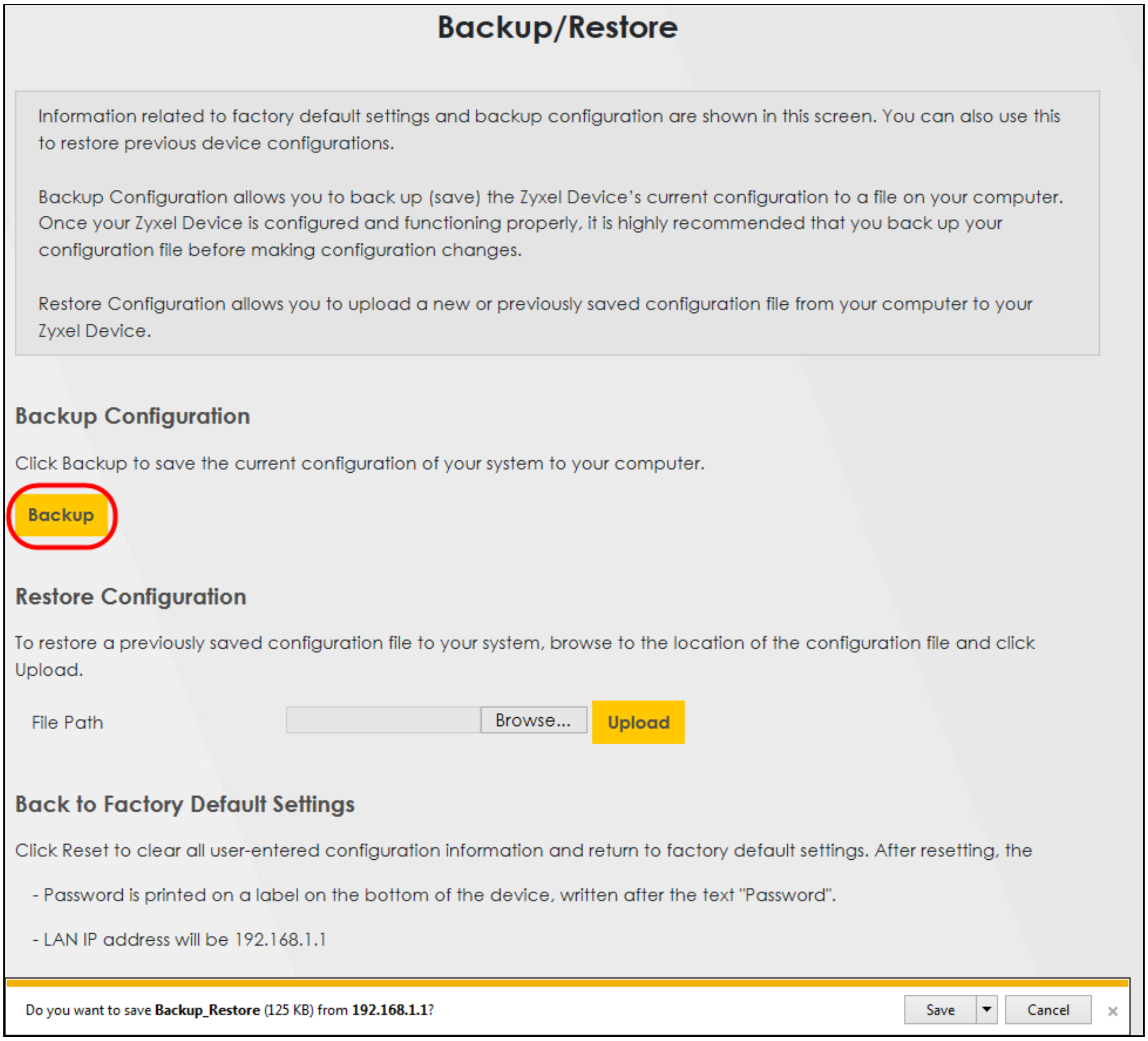
4 This process may take up to 2 minutes to finish. After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

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

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

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

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

Backup Configuration

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

Restore Configuration

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

Back to Factory Default Settings

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

- Password is printed on a label on the bottom of the device, written after the text "Password".

- LAN IP address will be 192.168.1.1

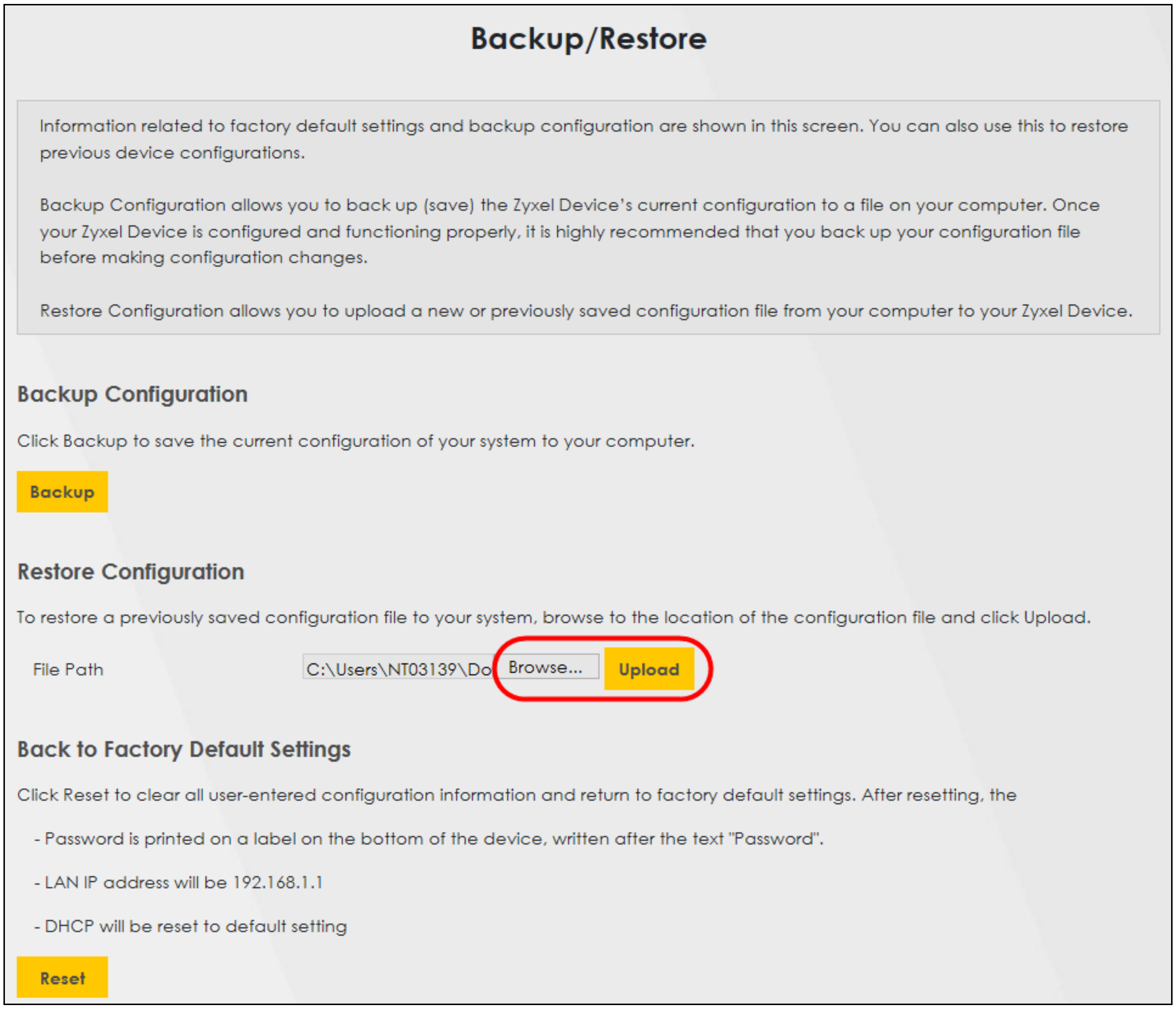
Do you want to save **Backup_Restore** (125 KB) from **192.168.1.1**?

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

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

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

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

Backup Configuration

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

Backup

Restore Configuration

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

File Path C:\Users\NT03139\Do Browse... Upload

Back to Factory Default Settings

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

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

Reset

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

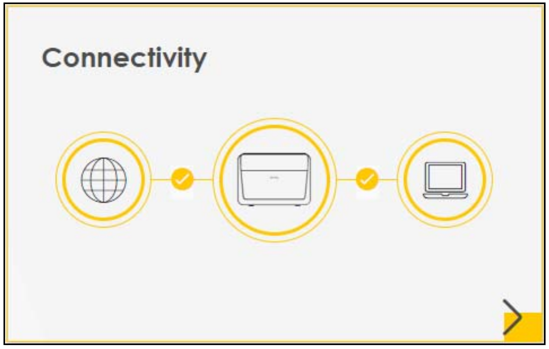
6.1 Connection Status Overview

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

6.1.1 Connectivity

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

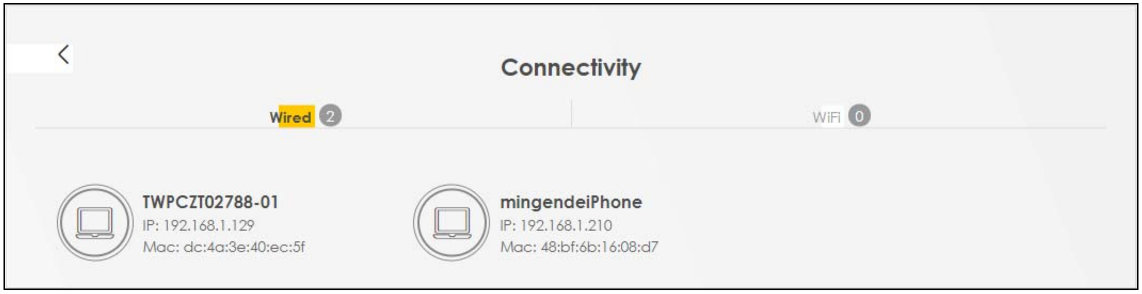
Figure 31 Connectivity



Connectivity

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

Figure 32 Connectivity: Connected Devices



Connectivity

TWPCZT02788-01
IP: 192.168.1.129
Mac: dc:4a:3e:40:ec:5f

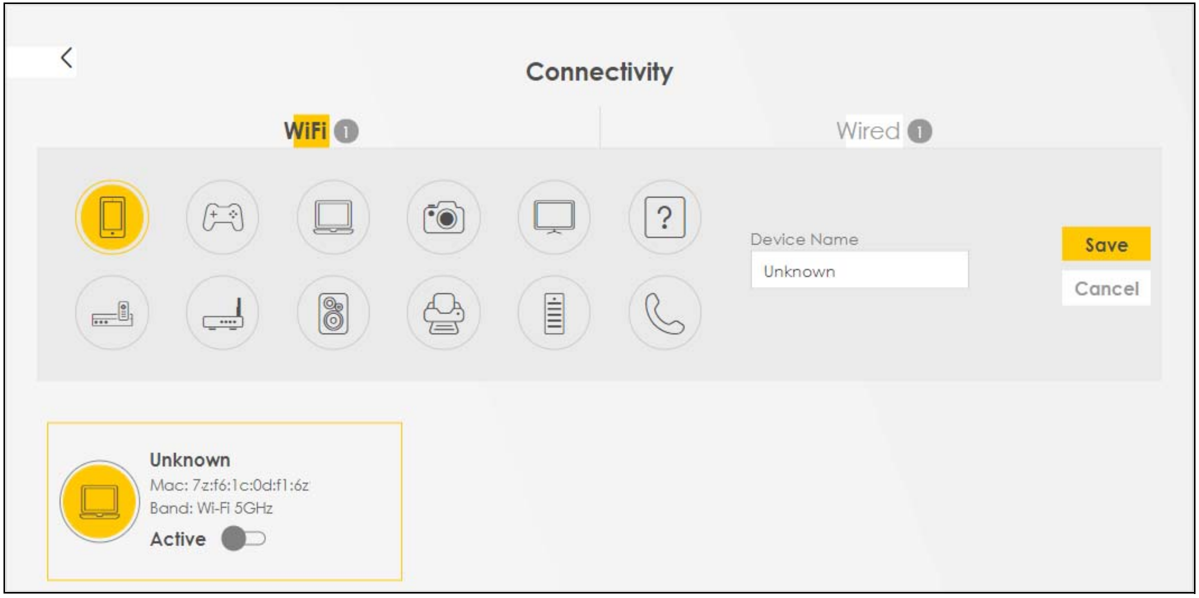
mingendeiPhone
IP: 192.168.1.210
Mac: 48:bf:6b:16:08:d7

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'll see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Slide the switch to the right to block a connected WiFi client. Click **Save** to save your changes.

6.1.2 Icon and Device Name

Select an icon and/or enter a name in the **Device Name** field for a connected device. Click the switch to the right to block a connected WiFi client. Click **Save** to save your changes.

Figure 33 Connectivity: Edit



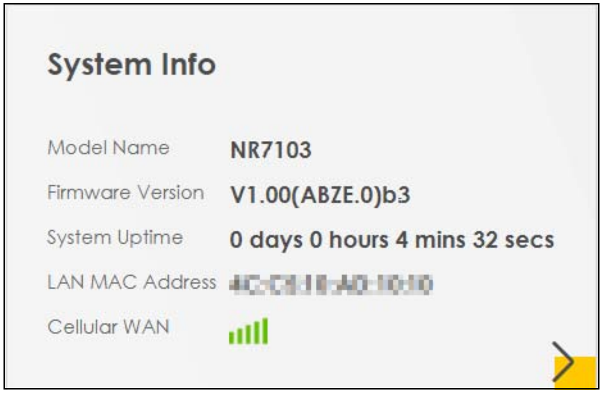
Device Name: Unknown

Unknown
Mac: 7z:f6:1c:0d:f1:6z
Band: Wi-Fi 5GHz
Active

6.1.3 System Info

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

Figure 34 System Info

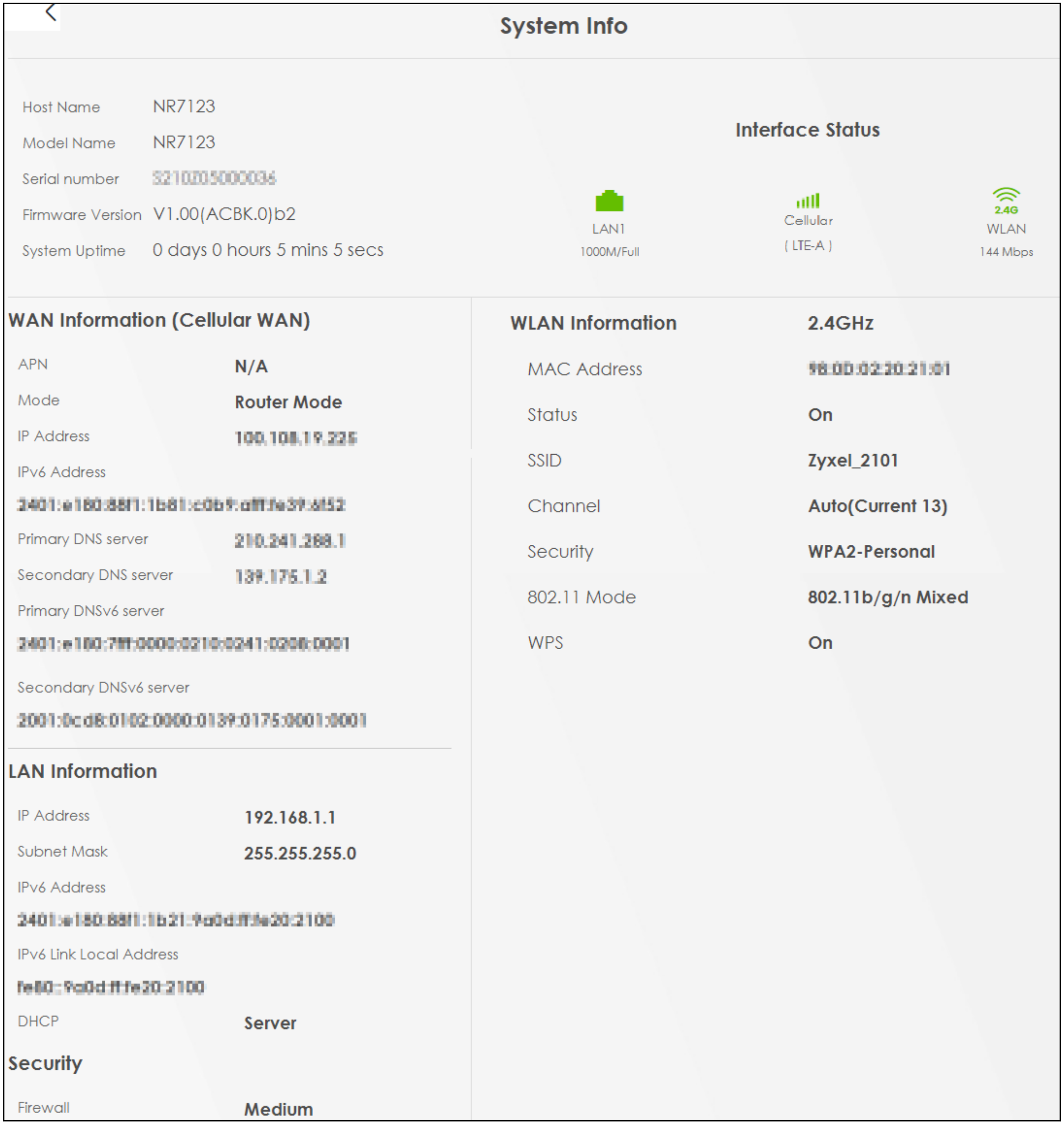


System Info

Model Name	NR7103
Firmware Version	V1.00(ABZE.0)b3
System Uptime	0 days 0 hours 4 mins 32 secs
LAN MAC Address	[redacted]
Cellular WAN	

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

Figure 35 System Info: Detailed Information



System Info

Host Name	NR7123
Model Name	NR7123
Serial number	[redacted]
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	[redacted]
IPv6 Address	[redacted]
Primary DNS server	[redacted]
Secondary DNS server	[redacted]
Primary DNSv6 server	[redacted]
Secondary DNSv6 server	[redacted]

LAN Information

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IPv6 Address	[redacted]
IPv6 Link Local Address	[redacted]
DHCP	Server

Security

Firewall	Medium

WLAN Information	2.4GHz
MAC Address	[redacted]
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 9 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.

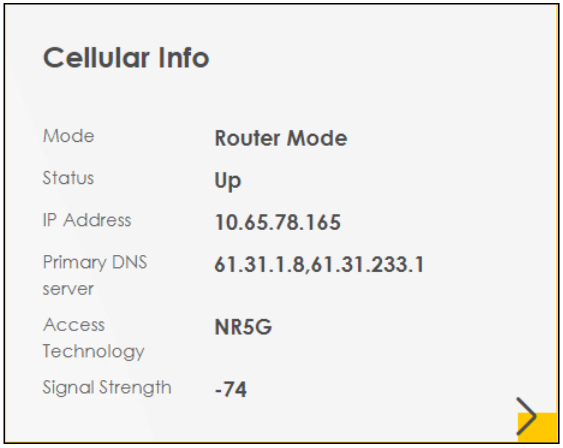
Table 9 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
WAN Information (These fields display when you have a WAN connection.)	
Link Type	This field displays the type of WAN connection that the Zyxel Device is currently using, such as **Cellular WAN** or **Ethernet**.
APN	This field displays the Access Point Name (APN).
Mode	This field displays the current mode of your Zyxel Device.
Connect Time	This field displays the current WAN connection 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 field displays the current link-local address of the Zyxel Device for the LAN interface. A link-local address is a special type of the IP address that is only valid for communication within the local network segment or broadcast domain of the device. Typically, link-local addresses are used for automatic address configuration and neighbor discovery protocols.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: **Server** – The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** – The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **Disable** – The Zyxel Device is not providing any DHCP services to the LAN.
Security	
Firewall	This displays the firewall's current security level (**High**, **Medium**, **Low**, or **Disabled**).
WLAN Information	
MAC Address	This shows the WiFi adapter MAC (Media Access Control) Address of the WiFi interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a WLAN.
Channel	This is the channel number currently used by the WiFi interface.
Security	This displays the type of security mode the WiFi interface is using in the WLAN.
802.11 Mode	This displays the type of 802.11 mode the WiFi interface is using in the WLAN.
WPS	This displays whether WPS is activated on the WiFi interface.

6.1.4 Cellular Info

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

Figure 36 Cellular Info

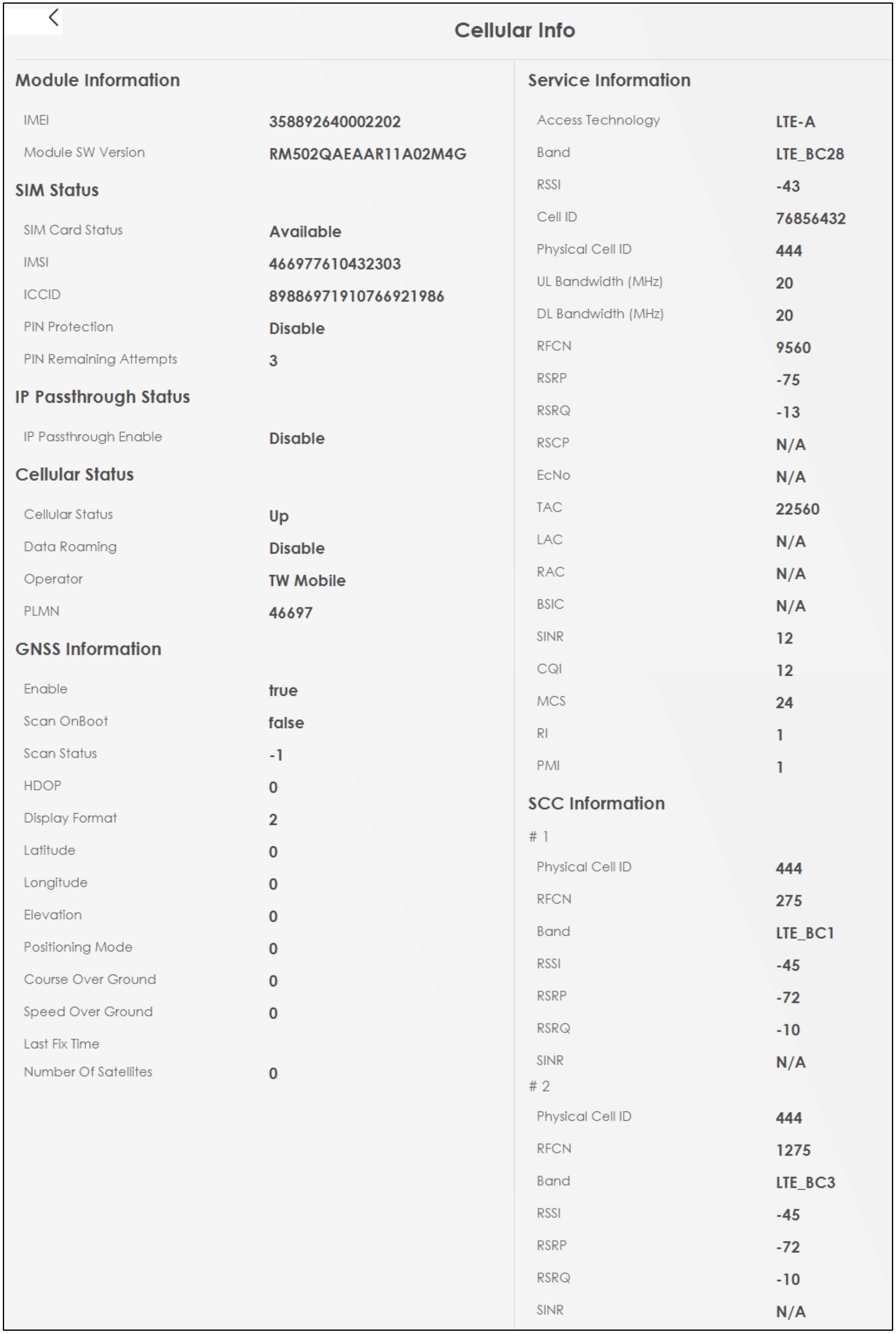


Cellular Info

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 37 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 does not have this value in that specific parameter field or there is no network connection.

The following table describes the labels in this screen.

Table 10 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 cellular network 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 do 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. Without the PIN code, you cannot use the SIM card. Shows **Enable** if the service provider requires you to enter a PIN to use the SIM card. Shows **Disable** if the service provider lets you use the SIM without inputting a PIN, or you disable **PIN Protection** in **Network Setting** > **Broadband** > **Cellular SIM**.
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.
IP Passthrough Mode	This displays the IP Passthrough mode. This displays **Dynamic** and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device. This displays **Fixed** and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.

Table 10 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
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.
PLMN	This displays the PLMN (Public Land Mobile Network) number.
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. Note: Not all models support the GNSS feature.	
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.

Table 10 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
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.
NR-NSA Information	
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.
Service Information/SCC Information Note: If the cellular service provider supports carrier aggregation (CA), then this section displays statistics for the connection's primary component carrier (PCC).	
#	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 the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.
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.
RSSI (dBm)	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 the 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 the 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.

Table 10 Cellular Info: Detailed Information (continued)

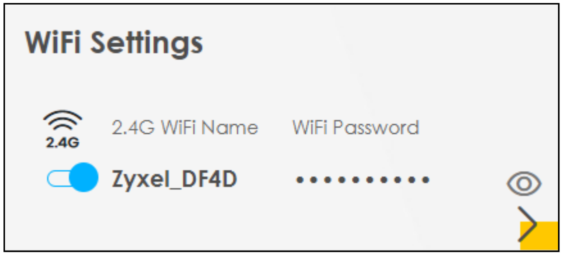
LABEL	DESCRIPTION
RSRQ	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable 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.
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 (dB)	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 or 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.
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.

6.1.5 WiFi Settings

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

Note: WiFi of the Zyxel Device is only used for configuration.

Figure 38 WiFi Settings



WiFi Settings

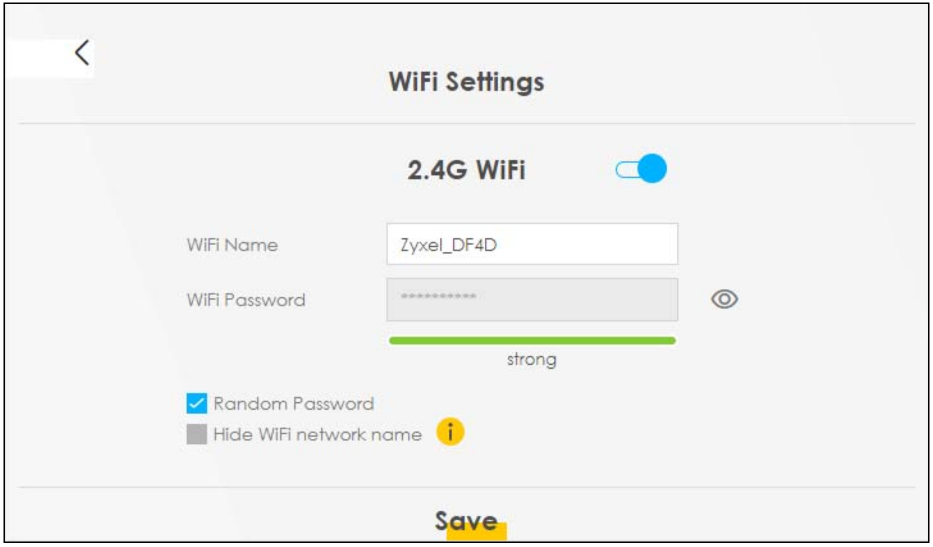
2.4G 2.4G WiFi Name WiFi Password

Zyxel_DF4D ••••••••••

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

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

Figure 39 WiFi Settings: Configuration



WiFi Settings

2.4G WiFi

WiFi Name: Zyxel_DF4D

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

strong

☑ Random Password

□ Hide WiFi network name

Save

Each field is described in the following table.

Table 11 WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4 GHz WiFi	Slide the switch button to enable or disable the 2.4G WiFi network. When the switch turns blue, the function is enabled.
WiFi 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 for the WiFi. You can use up to 32 printable characters, including spaces.

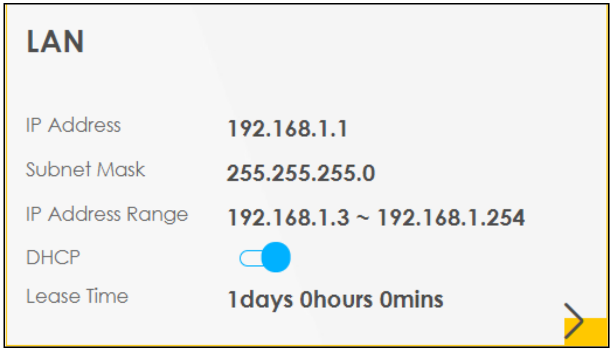
Table 11 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually enter a pre-shared key from 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces. Click the Eye icon to show or hide the password for your WiFi network. When the Eye icon is slashed ⊘, you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

6.1.6 LAN

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

Figure 40 LAN



LAN

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

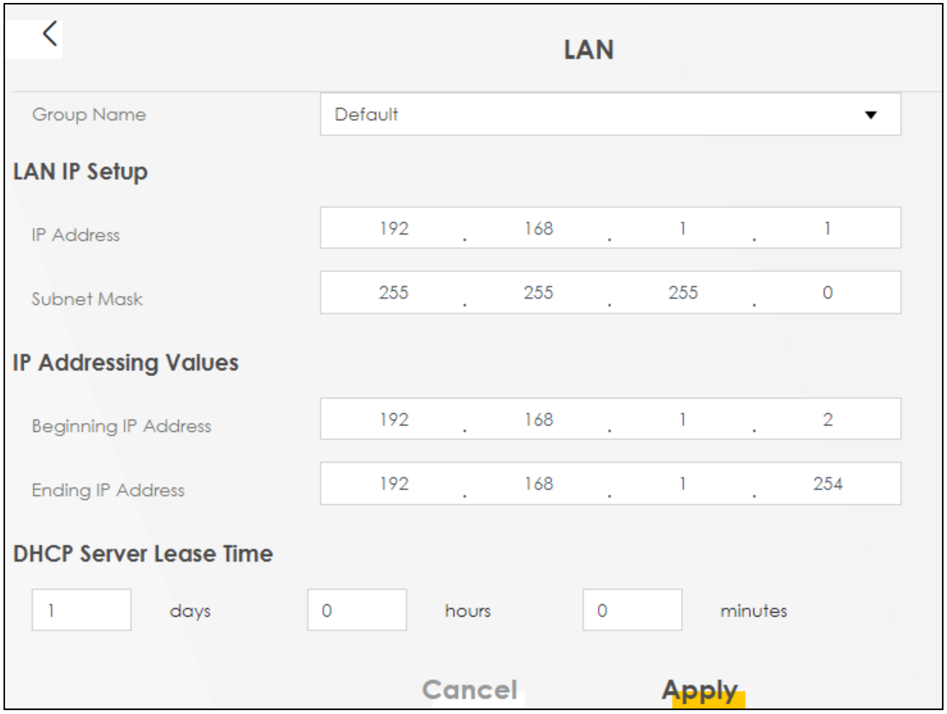
IP Address Range 192.168.1.3 ~ 192.168.1.254

DHCP ●

Lease Time 1days 0hours 0mins

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

Figure 41 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 12 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, (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
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.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

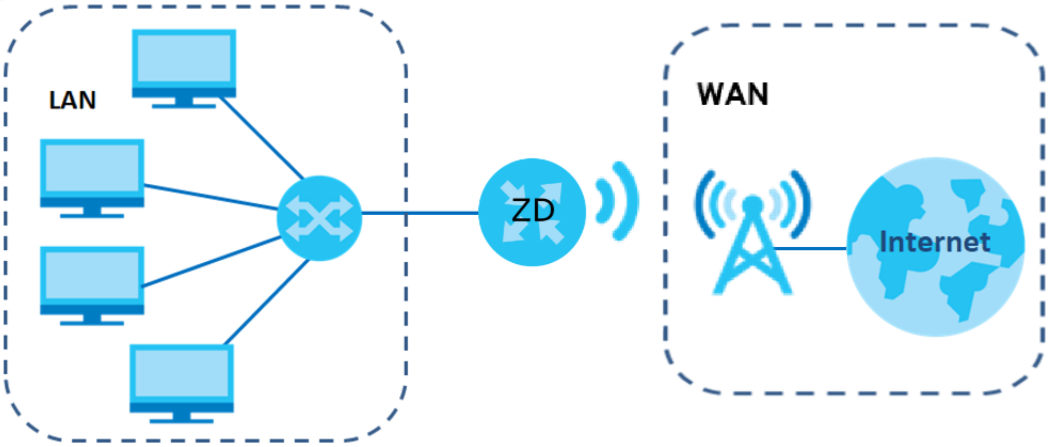
CHAPTER 7
Broadband

7.1 Broadband Overview

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

A 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 42 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 73).
- Use the **Cellular WAN** screen to configure a cellular WAN connection (Section 7.3 on page 76).
- 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 77).
- Use the **Cellular SIM** screen to enter the PIN of your SIM card (Section 7.5 on page 81).
- 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 73).
- Use the **Cellular PLMN** screen to display available Public Land Mobile Networks (Section 7.7 on page 83).
- Use the **Cellular IP Passthrough** screen to configure a WAN connection (Section 7.8 on page 86).
- Use the **Cellular Lock (LTE)** screen to configure cellular lock on Zyxel Device that use 4G LTE connections (Section 7.9 on page 87).
- Use the **Cellular Lock (5G)** screen to configure cellular lock on Zyxel Device that use NR (5G) connections (Section 7.10 on page 89).

- Use the **ESIM** screen to download an eSIM subscription from your service provider and activate it on your Zyxel Device (Section 7.11 on page 91).

Table 13 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

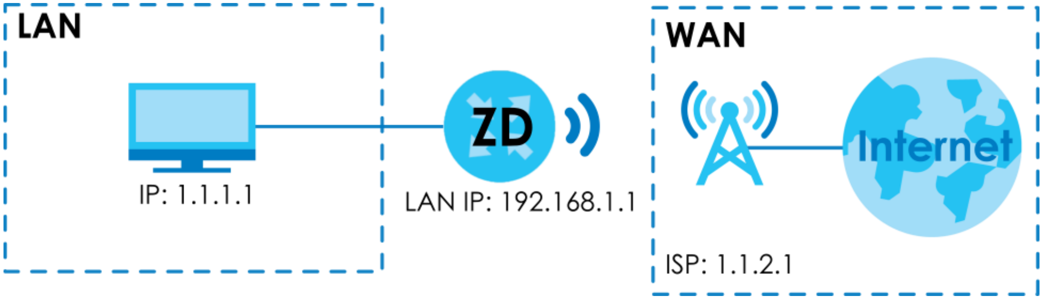
Access Point Name (APN) is a unique string which indicates a cellular network. An APN is required for cellular stations to enter the cellular network and then the Internet.

IP Passthrough

The Zyxel Device supports IP passthrough which allows Internet traffic to go to a LAN device behind the Zyxel Device without going through Network Address Translation (NAT). Your LAN device will have the public IP assigned by the ISP. Use this for applications that require a direct connection to the Internet using a public IP address, such as gaming or web server.

Note: The NAT function and DHCP pool are restricted for WAN connection that has IP Passthrough enabled.

Figure 43 IP Passthrough Example

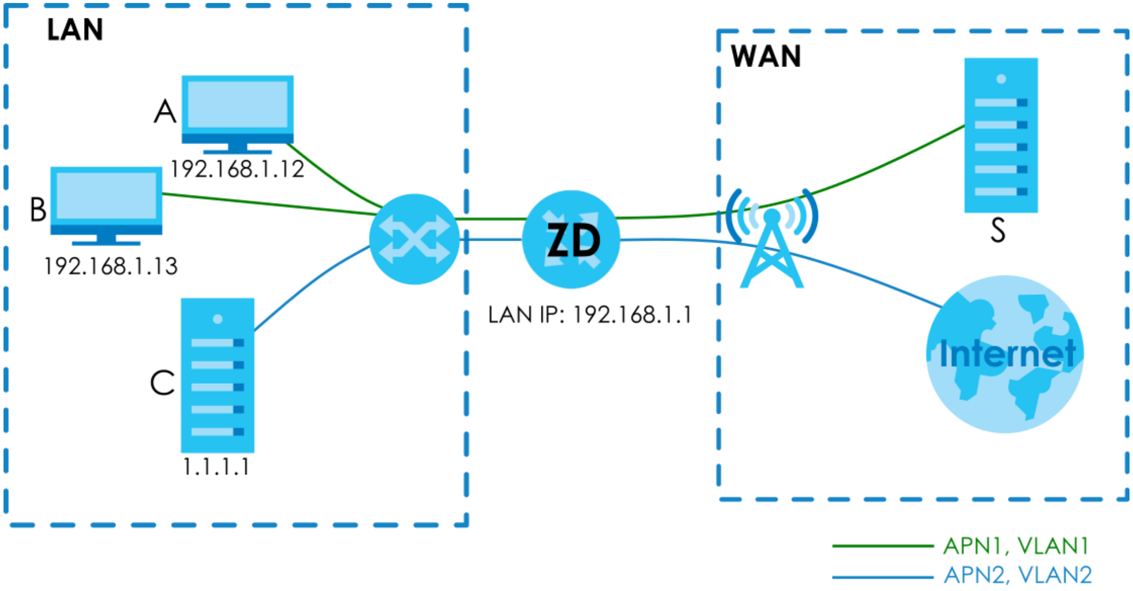


Cellular APN with VLAN Tagging

Use VLAN tags to separate LAN traffic from different WAN connections. You need a VLAN-aware device on your LAN, such as a switch. For example, say you configured two WAN connections **APN 1** and **APN 2** on the Zyxel Device (**ZD**). WAN 1 (**APN 1**) connects to the ISP management server (**S**). WAN 2 (**APN 2**) connects to the Internet. Enable **IP Passthrough** on **APN 2** and set its **VLAN ID** to **VLAN 2**. Meanwhile, keep **IP Passthrough** disabled on **APN 1** to use NAT.

Client **A**, **B** and client **C** connect to the Zyxel Device (**ZD**) through a switch that supports VLAN. Client **A**, **B** are in VLAN 1; client **C** is in VLAN 2. WAN traffic (**APN 1** and **APN 2**) can now go to different LAN clients according to the VLAN tag. Clients **A**, **B** get IP addresses assigned by NAT on the Zyxel Device. Clients **C** gets the ISP-assigned public IP 1.1.1.1.

Figure 44 Cellular Example



7.1.3 Before You Begin

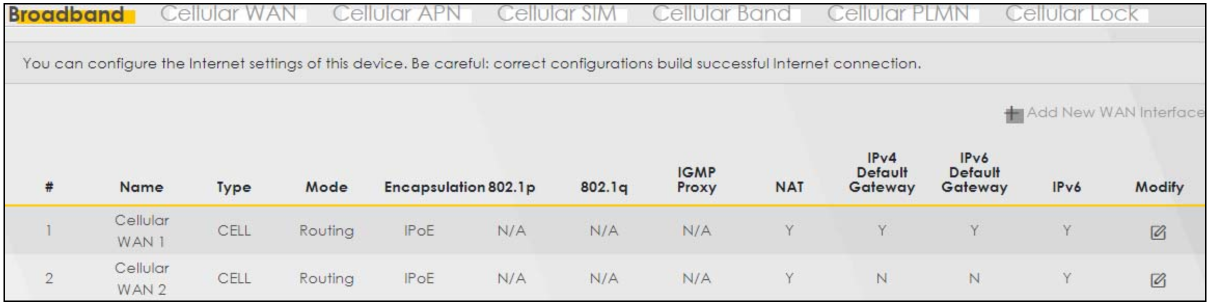
You may need to know your Internet access settings such as cellular APN, WAN IP address and SIM card's PIN code if the Status light on your Zyxel Device shows disconnection of the Internet. Get this information from your service provider.

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.

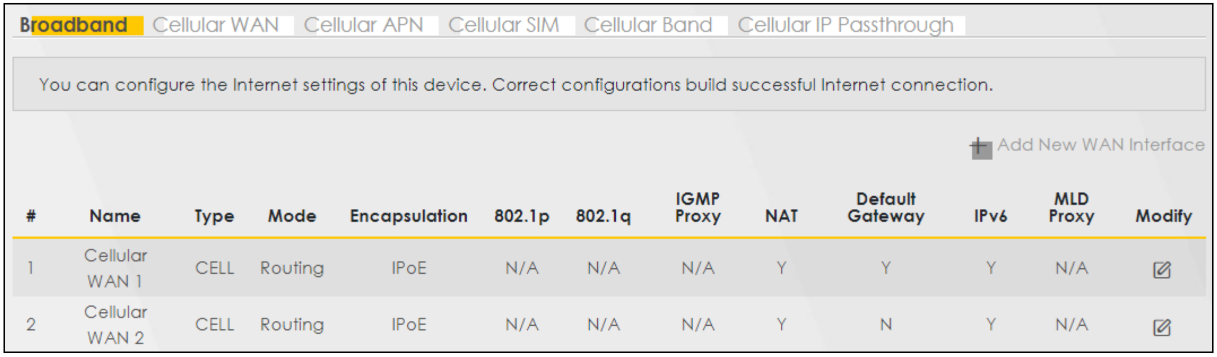
Figure 45 Network Setting > Broadband (with **IPv4** and **IPv6 Default Gateway**)



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 46 Network Setting > Broadband (with **MLD Proxy**)



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.

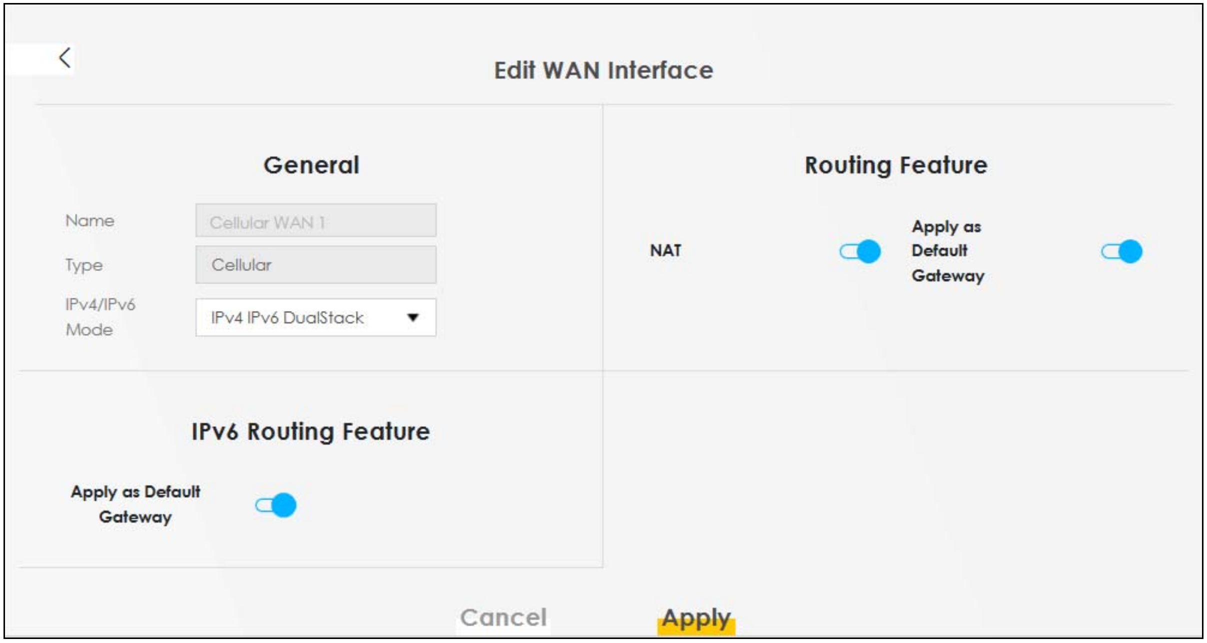
Table 14 Network Setting > Broadband

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 47 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 ●

Apply as Default Gateway ●

IPv6 Routing Feature

Apply as Default Gateway ●

The following table describes the labels in this screen.

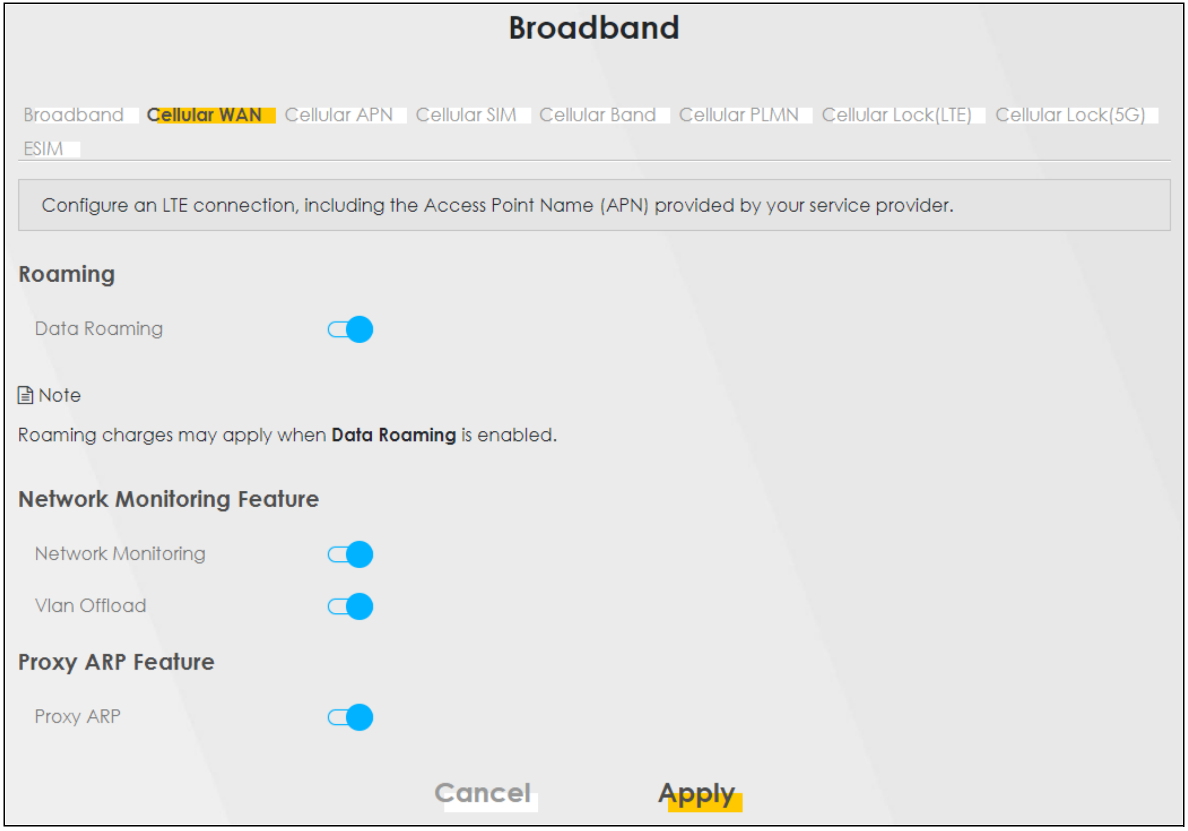
Table 15 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

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 48 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

Vlan Offload

Proxy ARP Feature

Proxy ARP

The following table describes the labels in this screen.

Table 16 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.

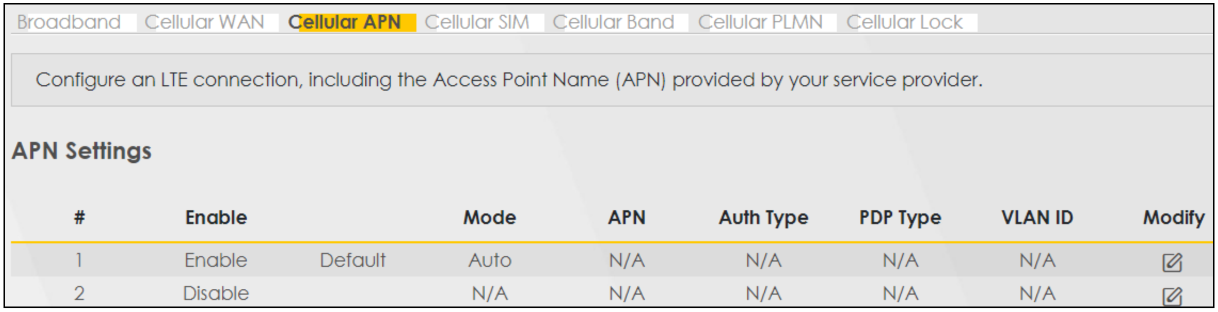
Table 16 Network Setting > Broadband > Cellular WAN (continued)

LABEL	DESCRIPTION
VLAN Offload	If you enabled **TX Tagging** for VLANs in **Network Setting** > **VLAN Group** > **Add New VLAN Group/ Edit**, then enable **VLAN Offload** to allow incoming tagged packets to pass through the IPA (Internet Packet Accelerator) in order to improve data transmission to LAN clients. Alternatively, disable this field to only allow untagged packets to pass through the IPA. An IPA is a hardware component that accelerates data transmission over networks. IPA processes network functions such as routing, filtering, network address translation and aggregation.
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.
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 49 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 17 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.

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

LABEL	DESCRIPTION
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 **N/A** 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 of this APN.
Modify	Click the **Edit** icon (✎) to configure a cellular connection, including the APN provided by your service provider.

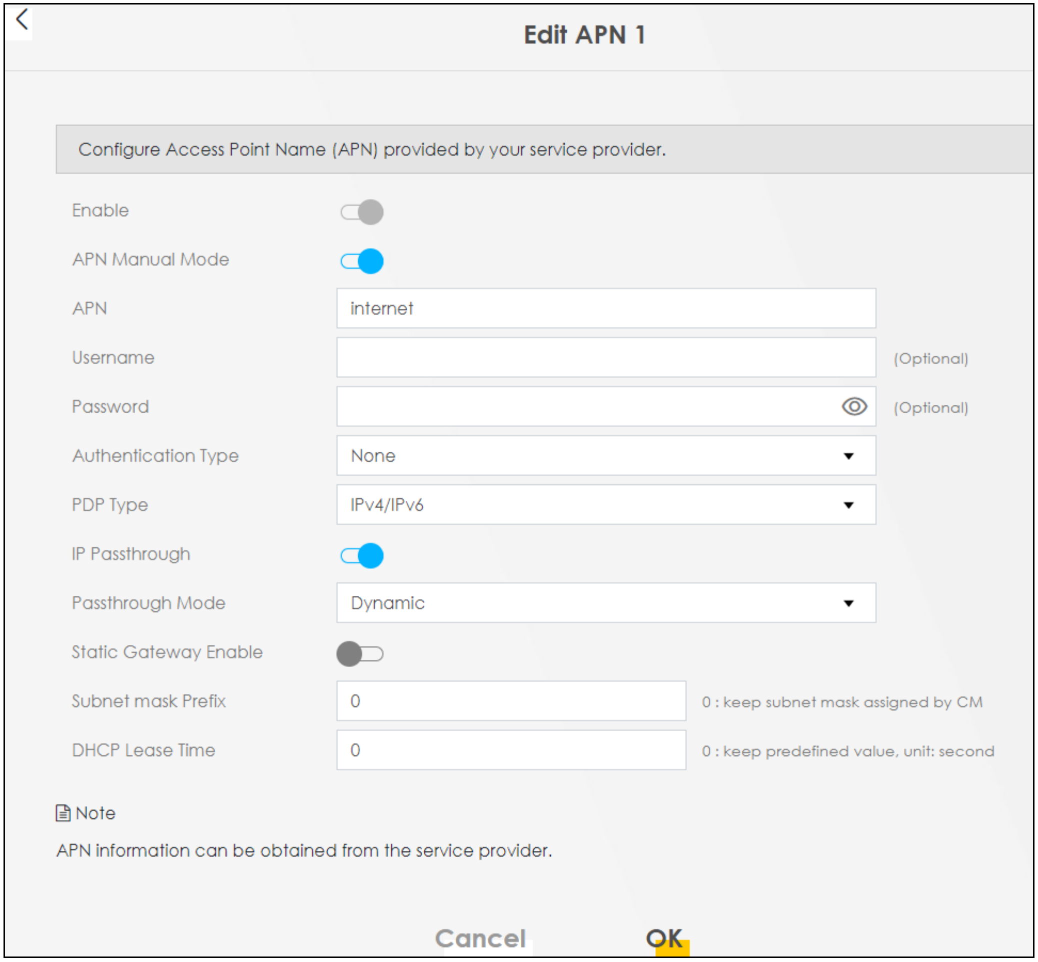
7.4.1 Edit APN

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. See Section 7.1.2 on page 72 for more information about IP passthrough.

Note: In some models you configure **IP Passthrough** in **Network Setting** > **Broadband** > **Cellular IP Passthrough**.

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

Figure 50 Network Setting > Broadband > Cellular APN > Edit APN



Edit APN 1

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

Enable	off	
APN Manual Mode	on	
APN	internet	
Username		(Optional)
Password		(Optional)
Authentication Type	None	
PDP Type	IPv4/IPv6	
IP Passthrough	on	
Passthrough Mode	Dynamic	
Static Gateway Enable	off	
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 18 Network Setting > Broadband > Cellular APN > Edit APN

LABEL	DESCRIPTION
Enable	Slide this to the right to enable the cellular connection of this APN on the Zyxel Device.
APN Manual Mode	Disable this to have the Zyxel Device configure the APN of a cellular network automatically. Otherwise, slide this to the right 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 18 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	Slide this to the right to enable IP passthrough to allow Internet traffic of this cellular connection to go to a LAN device behind the Zyxel Device without going through NAT. Your LAN device will have the public IP assigned by the ISP. Use the **Passthrough Mode** field to decide which LAN device will get the ISP-assigned IP. Otherwise, slide this to the left to disable IP passthrough. See Section 7.1.2 on page 72 for more information about IP passthrough on the Zyxel Device.
Passthrough Mode	This field is only available when you enable **IP Passthrough**. Select **Dynamic** to allow traffic to be forwarded to the first LAN device that sends a DHCP request to the Zyxel Device. Select **Fixed** to specify a LAN device (for example, Client A) by entering its MAC address.
Static Gateway Enable	This field is only available when you enable **IP Passthrough**. A gateway connects the Zyxel Device to the Internet. The Zyxel Device needs to know the IP address of the gateway to route traffic from the Zyxel Device local network to external networks. When the ISP DHCP server assigns an IP address to the Zyxel Device, it includes the default gateway IP address and subnet mask value in the DHCP Offer/Ack packets. Slide this to the left to have the Zyxel Device automatically use the default gateway IP address and subnet mask sent by the ISP DHCP server. If required for **IP Passthrough**, slide this to the right to manually configure a static gateway address and enter the exact **Static Gateway** IP **Address** given by your ISP.
Subnet Mask Prefix	This field is only available when you enable **IP Passthrough**. This defines the number of LAN clients that can get a public IP address with **IP Passthrough**. This mask is determined by the ISP. Enter the subnet mask prefix length of the Zyxel Device network. The Zyxel Device will use this subnet mask you configured. To use the **Subnet Mask Prefix** you configured, you need to enable **Proxy ARP** in **Network Setting** > **Broadband** > **Cellular WAN**.
DHCP Lease Time	This field is only available when you enable **IP Passthrough**. Enter the DHCP lease time for a DHCP client when **IP Passthrough** is enabled.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

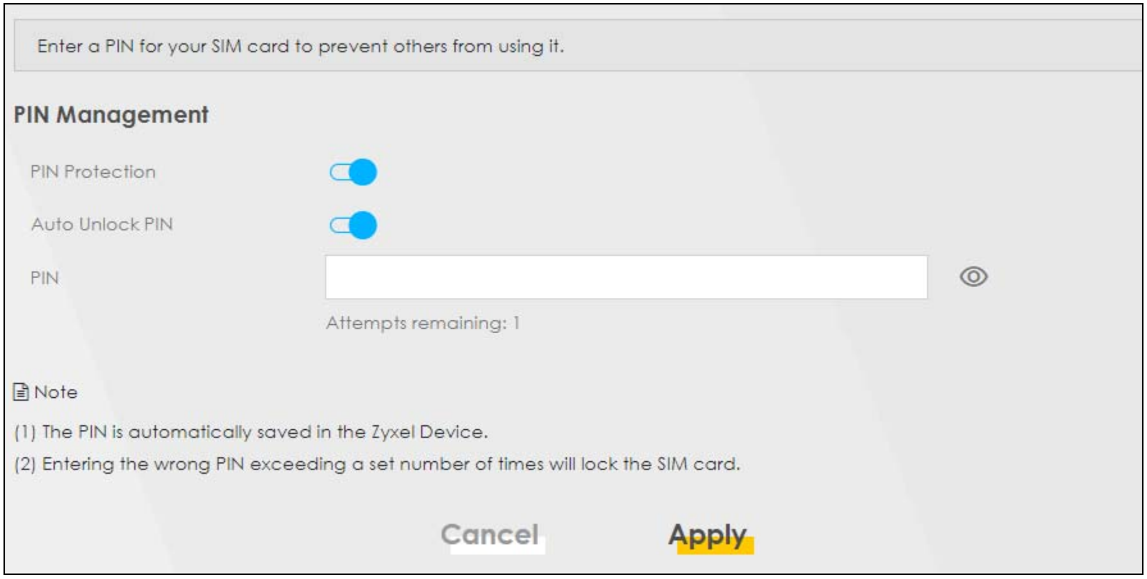
7.5 Cellular SIM Configuration

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 51 Network Setting > Broadband > Cellular SIM



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

PIN Management

PIN Protection ●

Auto Unlock PIN ●

PIN

Attempts remaining: 1

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 19 Network Setting > Broadband > Cellular SIM

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. Slide the switch to the right if you want the SIM to use a PIN lock. Slide the switch to the left 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.
Auto Unlock PIN	If **PIN Protection** is enabled, the SIM card requires a PIN code to unlock the PIN lock. Slide the switch to the right to have the Zyxel Device automatically unlock the PIN lock. Otherwise, slide the switch to the left. You will need to manually enter the PIN every time you reboot the Zyxel Device or reinsert the SIM card to use the SIM card.
PIN Modification	

Table 19 Network Setting > Broadband > Cellular SIM (continued)

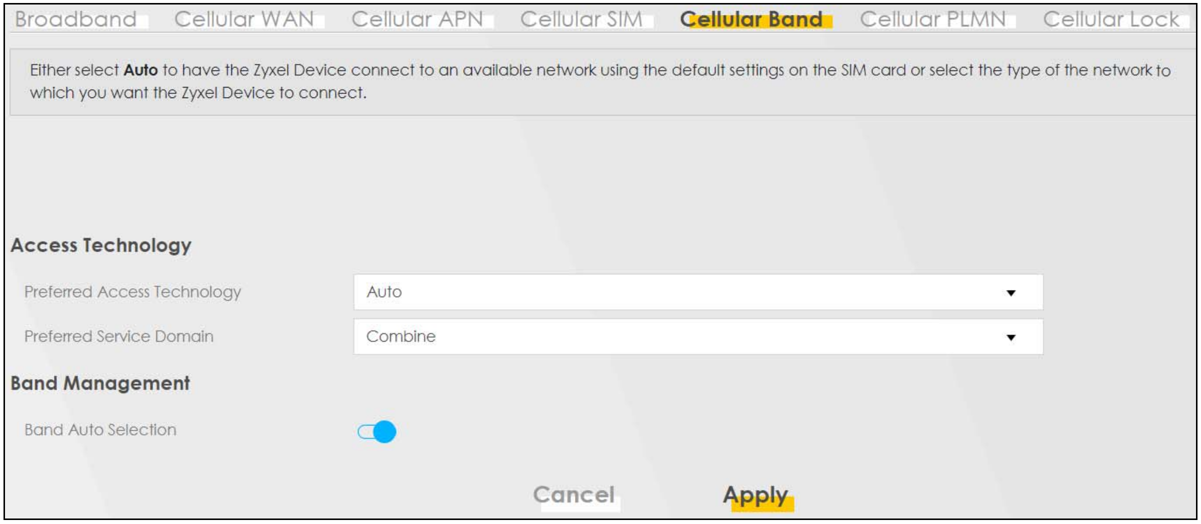
LABEL	DESCRIPTION
more...	Click this ⌃ to show more fields in this section. Click this ⌄ to hide them. Note: **PIN modification** and its following fields will show upon enabling **PIN Protection** in the previous field.
New PIN	Enter a 4-digit code to set as the new PIN code. Note: This field will show 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 52 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: on

The following table describes the fields in this screen.

Table 20 Network Setting > Broadband > Cellular Band

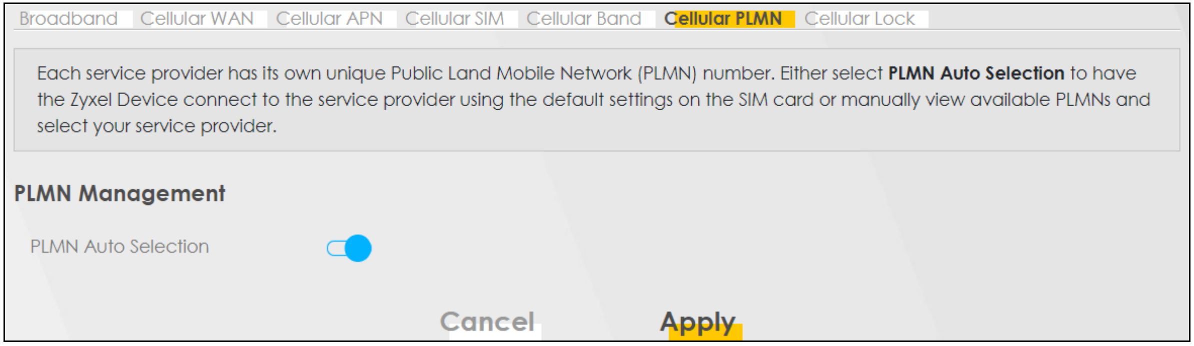
LABEL	DESCRIPTION
Access Technology	
Preferred Access Technology	Select the Access Technology which you want the Zyxel Device to use and click **Apply** to save your settings. Otherwise, select **Auto** to have the Zyxel Device connect to an available network using the default settings on the SIM card. 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	Slide this to the right to enable automatic frequency band selection as provided by your service provider. Otherwise, slide 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 53 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: enabled

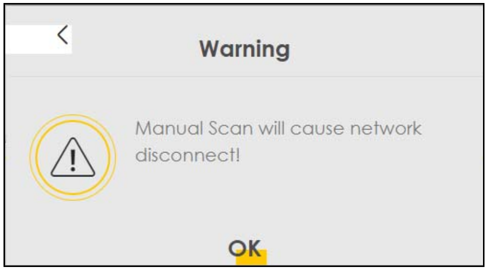
The following table describes the labels in this screen.

Table 21 Network Setting > Broadband > Cellular PLMN

LABEL	DESCRIPTION
PLMN Management	
PLMN Auto Selection	Slide this to the right 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 54 Network Setting > Broadband > Cellular PLMN > Manual Scan Warning

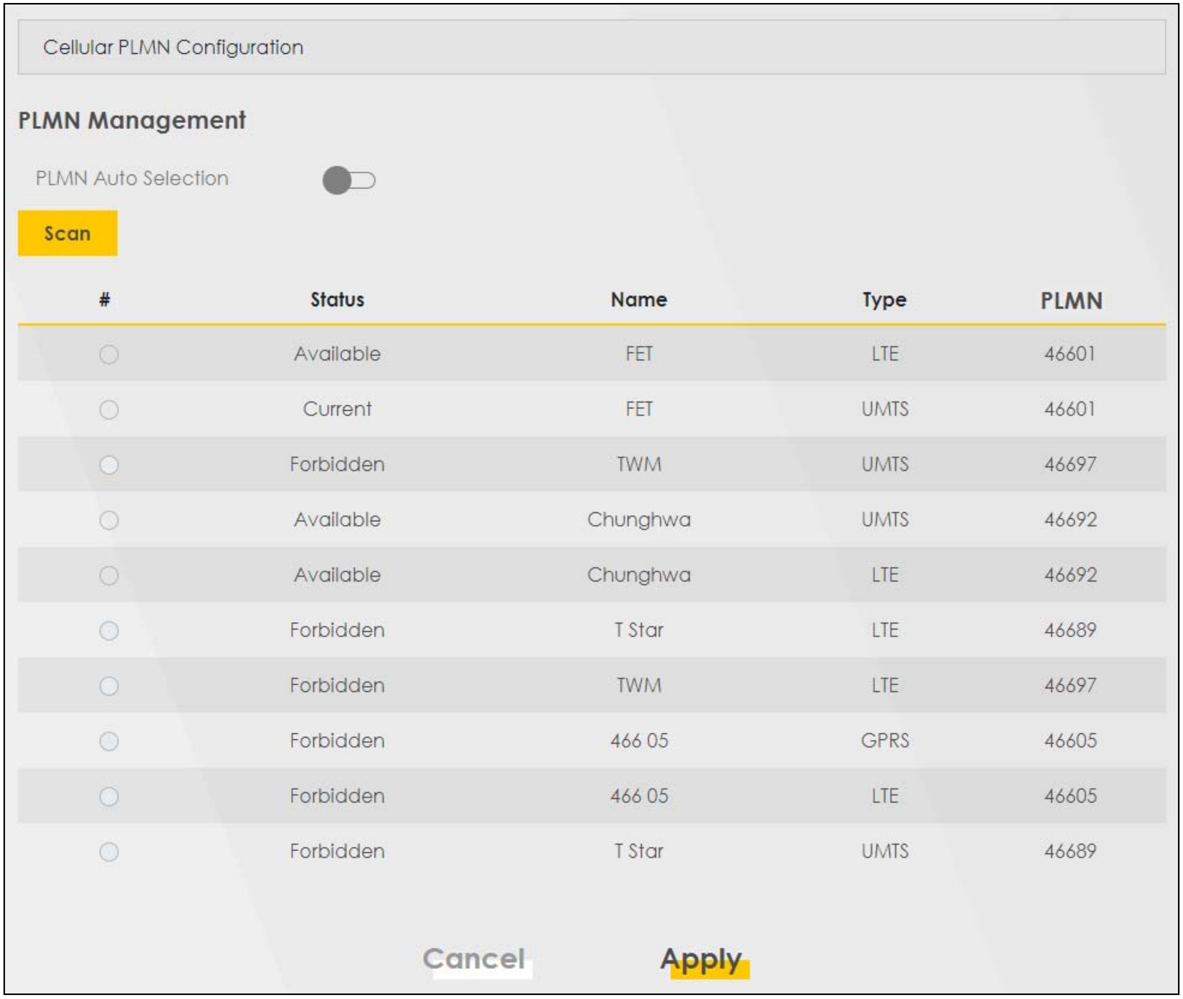


Warning

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 55 Network Setting > Broadband > Cellular PLMN > Scan



Cellular PLMN Configuration

PLMN Management

PLMN Auto Selection

#	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 22 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.

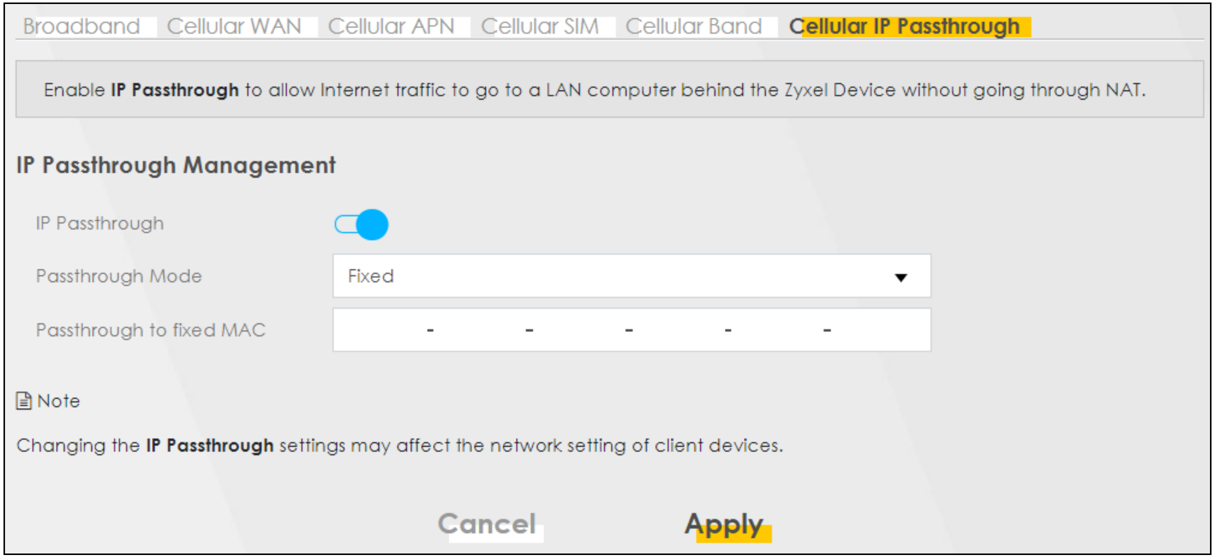
Select from the network list and click **Apply**.

7.8 Cellular IP Passthrough

Enable **IP Passthrough** to allow Internet traffic to go to a LAN device behind the Zyxel Device without going through NAT. See Section 7.1.2 on page 72 for more information about IP passthrough on the Zyxel Device.

Note: This screen is not available for models that support the **IP Passthrough** settings in the **Network Setting** > **Broadband** > **Cellular APN** > **Edit** screen.

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



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: - - - - -

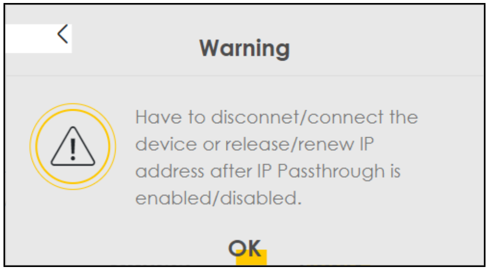
Note

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

Figure 56 Network Setting > Broadband > Cellular IP Passthrough

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 57 Network Setting > Broadband > Cellular IP Passthrough > Enable Warning


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 23 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.

Table 23 Network Setting > Broadband > IP Passthrough (continued)

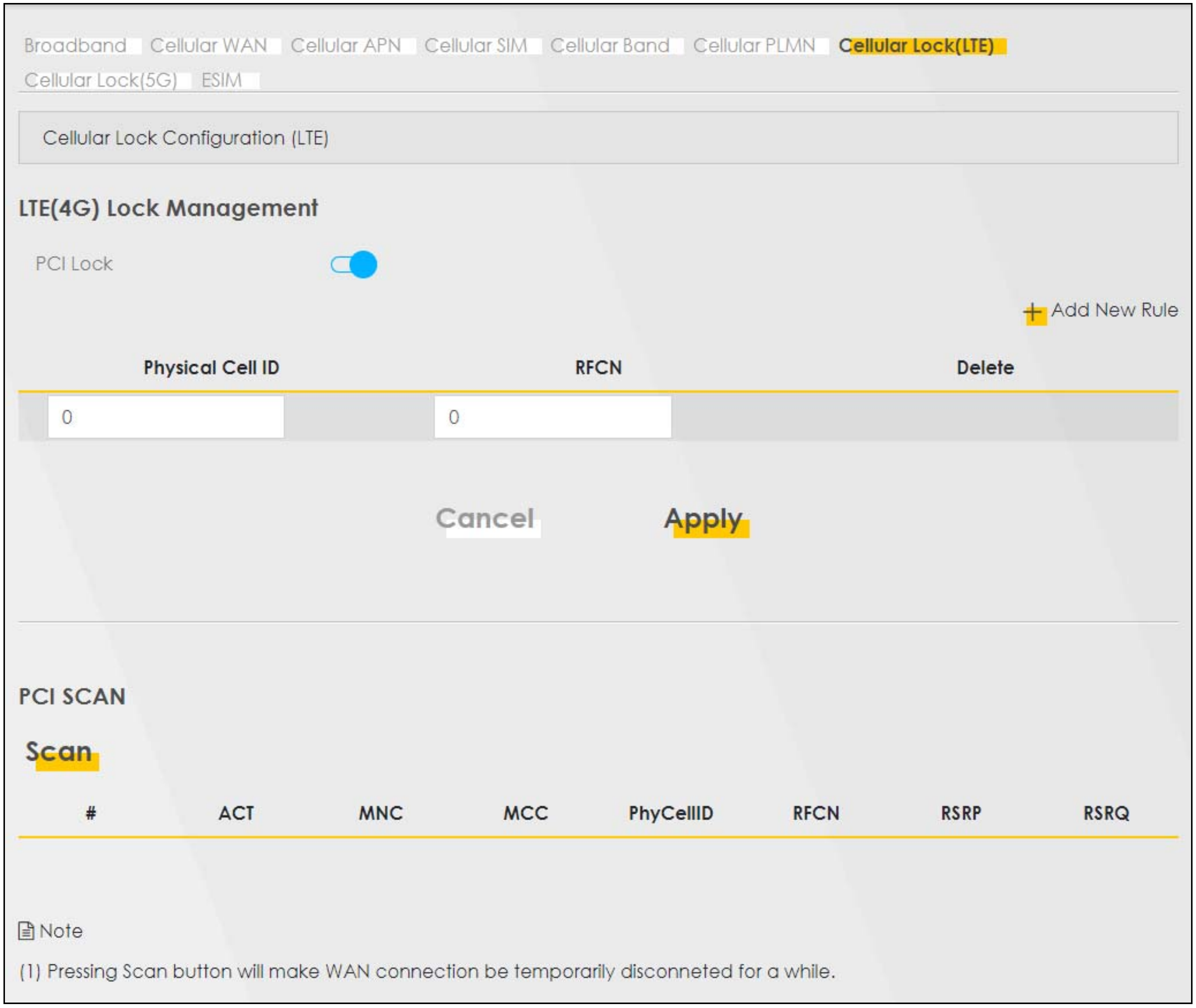
LABEL	DESCRIPTION
Passthrough Mode	Select **Dynamic** to allow traffic to be forwarded to the first LAN computer on the local network of the Zyxel Device. Select **Fixed** to specify a computer (for example, Client A) by entering its MAC address. Note: This field will show upon enabling **IP Passthrough** in the previous field.
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 (LTE)

Use this screen to configure cellular lock on Zyxel Devices that use 4G LTE connections.

To lock a base station identified by its Physical Cell ID, go to **Network Setting** > **Broadband** > **Cellular Lock (LTE)**.

Figure 58 Network Setting > Broadband > Cellular Lock (LTE)



(1) Pressing Scan button will make WAN connection be temporarily disconneted for a while.

The following table describes the fields in this screen.

Table 24 Network Setting > Broadband > Cellular Lock (LTE)

LABEL	DESCRIPTION
LTE(4G) Lock Management	
PCI Lock	Slide this to the right to enable PCI (Physical Cell Identifier) Lock on base stations when the Zyxel Device has 4G LTE connections. Physical Cell ID (PCI) is an identifier for a cell, namely a cellular base station. PCI and Radio Frequency Channel Number (RFCN) are combined to specify the base station.
Add New Rule	Click to add a new cellular lock rule.
Physical Cell ID	Enter the PCI number (0 – 504) of the base station to which you want the Zyxel Device to connect.
RFCN	Enter the RFCN (Radio Frequency Channel Number) for the LTE frequency of the specified PCI (1 – 65535).
Delete	Click the **Delete** icon to remove an entry.
Cancel	Click this to return to previous settings without saving.
Apply	Click this to save and apply your changes.
Scan	Note: Clicking **Scan** will cause a temporary Internet disconnection.

Table 24 Network Setting > Broadband > Cellular Lock (LTE) (continued)

LABEL	DESCRIPTION
ACT	This shows the Access Technology (ACT) of the cell.
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.
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.
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 66 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 66 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 67 for more information.

7.10 Cellular Lock (5G)

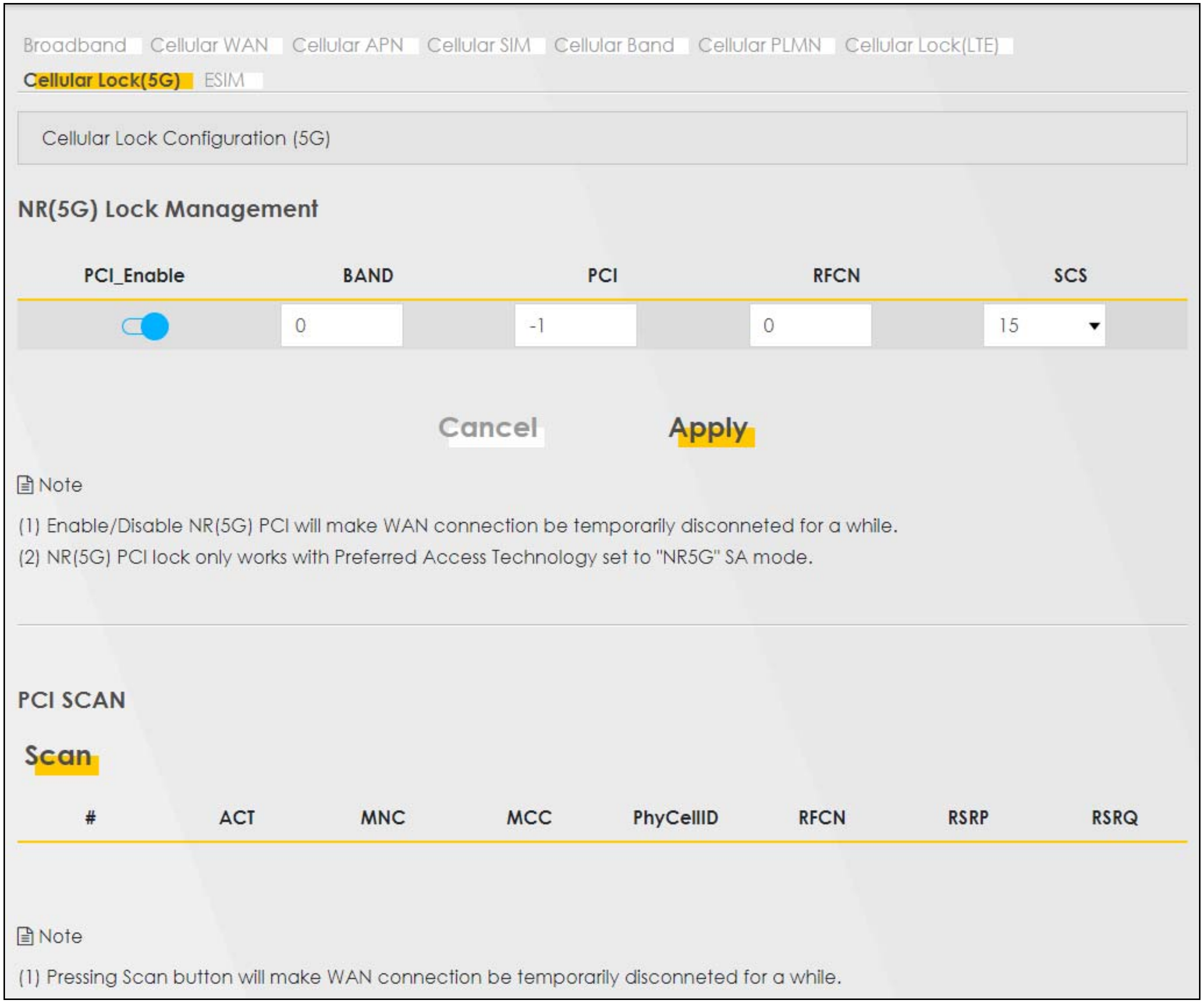
Use this screen to configure cellular lock on Zyxel Devices that use NR (5G) connections.

To lock a base station identified by its Physical Cell ID and band, go to **Network Setting** > **Broadband** > **Cellular Lock (5G)**.

Note: Enabling/Disabling Cellular Lock will cause a temporary WAN disconnection.

Note: NR (5G) Cellular Lock only works when the Zyxel Device is using the NR5G-SA mode. Make sure the **Preferred Access Technology** on the **Network Setting** > **Broadband** > **Cellular Band** screen is set to **NR5G-SA** or **NR5G-SA/NR5G-NSA/5G (Auto Switch)**.

Figure 59 Network Setting > Broadband > Cellular Lock (5G)



Cellular Lock Configuration (5G)

NR(5G) Lock Management

PCI_Enable	BAND	PCI	RFCN	SCS
●	0	-1	0	15 ▾

Note

(1) Enable/Disable NR(5G) PCI will make WAN connection be temporarily disconneted for a while.

(2) NR(5G) PCI lock only works with Preferred Access Technology set to "NR5G" SA mode.

PCI SCAN

#	ACT	MNC	MCC	PhyCellID	RFCN	RSRP	RSRQ

Note

(1) Pressing Scan button will make WAN connection be temporarily disconneted for a while.

The following table describes the fields in this screen.

Table 25 Network Setting > Broadband > Cellular Lock (5G)

LABEL	DESCRIPTION
NR(5G) Lock Management	
PCI_Enable	Slide this to the right to enable PCI (Physical Cell Identifier) Lock on a base station when the Zyxel Device has a NR (5G) connection.
Band	Enter the band number to which you choose to connect. Note: Make sure to select the same band in the **Network Setting** > **Broadband** > **Cellular Band** screen so as the Zyxel Device can connect to that band.
PCI	Use this to enter the PCI number of the base station you want the Zyxel Device to connect to (0 – 504).
RFCN	Enter the RFCN (Radio Frequency Channel Number) for the NR (5G) frequency of the specified PCI (1 – 65535).
SCS	Select the Subcarrier Spacing (SCS) from the drop-down list. Subcarriers are small signal carriers that divide a frequency channel, which is the main carrier wave. Subcarrier spacing is the space between each subcarrier. At the time of writing, SCS ranges from 15-120 KHz.You should select the same SCS that is used by the ISP.

Table 25 Network Setting > Broadband > Cellular Lock (5G) (continued)

LABEL	DESCRIPTION
Cancel	Click this to exit this screen without saving.
Apply	Click this to save your changes.
Scan	Note: Clicking **Scan** will cause a temporary Internet disconnection.
ACT	This shows the Access Technology (ACT) of the cell.
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.
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.
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 66 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 66 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 67 for more information.

7.11 eSIM

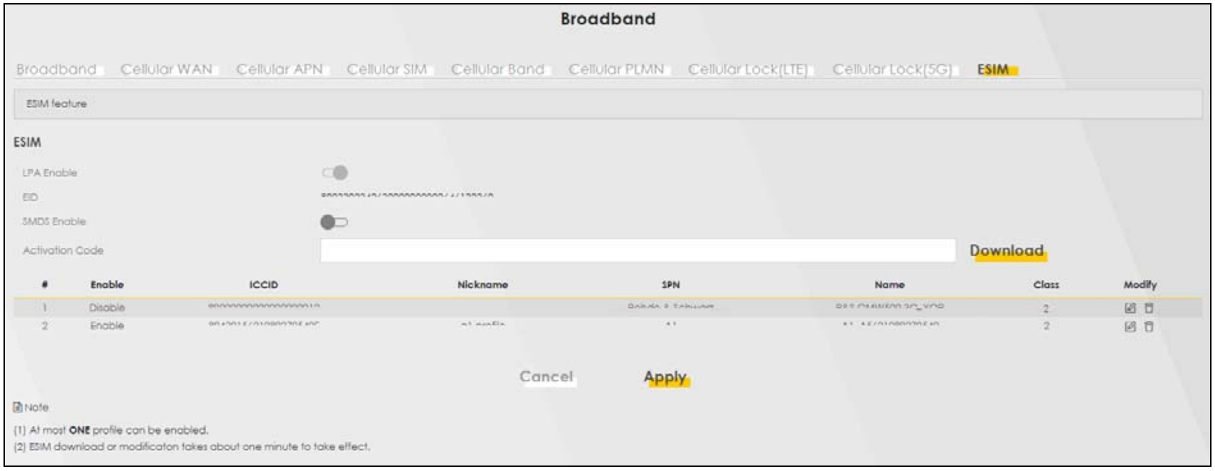
eSIM (embedded SIM) is a digital SIM which stores information that allows you to connect to a specific cellular (4G/5G) network. With eSIM, you do not need a different physical SIM card for each different service provider.

First, purchase an eSIM subscription from a service provider. Then, activate the subscription through the Web Configurator to connect to the cellular network of that service provider.

Use this screen to download an eSIM subscription from your service provider and activate it on your eSIM.

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

Figure 60 Network Setting > Broadband > ESIM



LPA Enable ●

EID [illegible]

SMDS Enable ○

Activation Code

#	Enable	ICCID	Nickname	SPN	Name	Class	Modify
1	Disable	[illegible]		[illegible]	[illegible]	2	
2	Enable	[illegible]	[illegible]	[illegible]	[illegible]	2	

Note

(1) At most **ONE** profile can be enabled.

(2) ESIM download or modificaton takes about one minute to take effect.

The following table describes the labels in this screen.

Table 26 Network Settings > Broadband > ESIM

LABEL	DESCRIPTION
LPA Enable	LPA (Local Profile Assistant) allows you to download an encrypted service provider profile to the Zyxel Device. A profile is the service provider's data related to a subscription. Note: At the time of writing, you can add 7 eSIM subscriptions to your Zyxel Device, but you can only enable one at a time. Click this switch to the right to use an eSIM subscription. Alternatively, click this switch to the left to use a nano SIM card inserted into the Zyxel Device.
EID	This displays the eUICC (embedded Universal Integrated Circuit Card) identifier or eSIM identifier (EID). The EID is the serial number of the eSIM.
SMDS Enable	SM-DS (Subscription Manager-Discovery Server) is a method of downloading an eSIM subscription to the Zyxel Device. SM-DS allows you to download an eSIM subscription without specifying the SM-DP+ (Subscription Manager-Data Preparation +) address. SM-DP+ is a platform that stores digital eSIM subscriptions. Click this switch to the right if your service provider supports SM-DS. Then click **Download**.
Activation Code	Get the activation code from your service provider if your service provider does not support SM-DS. Enter the activation code here. Note: This field is only available when **SMDS Enable** is not selected.
Download	Click **Download** to download an eSIM subscription to your Zyxel Device.
#	This displays the index number of the entry.
Enable	This displays the status of an eSIM subscription. You can change this in the **Edit ESIM Profile # n** screen. Note: Only one eSIM subscription can be active at a time.
ICCID	This displays the Integrated Circuit Card Identification Number (ICCID). This is an 18 to 22-digit code containing the eSIM subscription's country code, operator code, and identification number.
Nickname	This displays the descriptive name of the eSIM subscription. You can change this in the **Edit ESIM Profile # n** screen.
SPN	This displays the name of the service provider.
Name	This displays the name of the eSIM subscription with your service provider.
Class	This displays **2** for an eSIM subscription.

Table 26 Network Settings > Broadband > ESIM (continued)

LABEL	DESCRIPTION
Modify	Click the modify icon to go to the **Edit ESIM Profile # n** screen. See Section 7.11.1 on page 93 for more information. Click the delete icon to remove an eSIM subscription. The Zyxel Device confirms you want to remove it before doing so.
Cancel	Click **Cancel** to not save your settings and return to the previous screen.
Apply	Click **Apply** to save your changes and return to the previous screen.

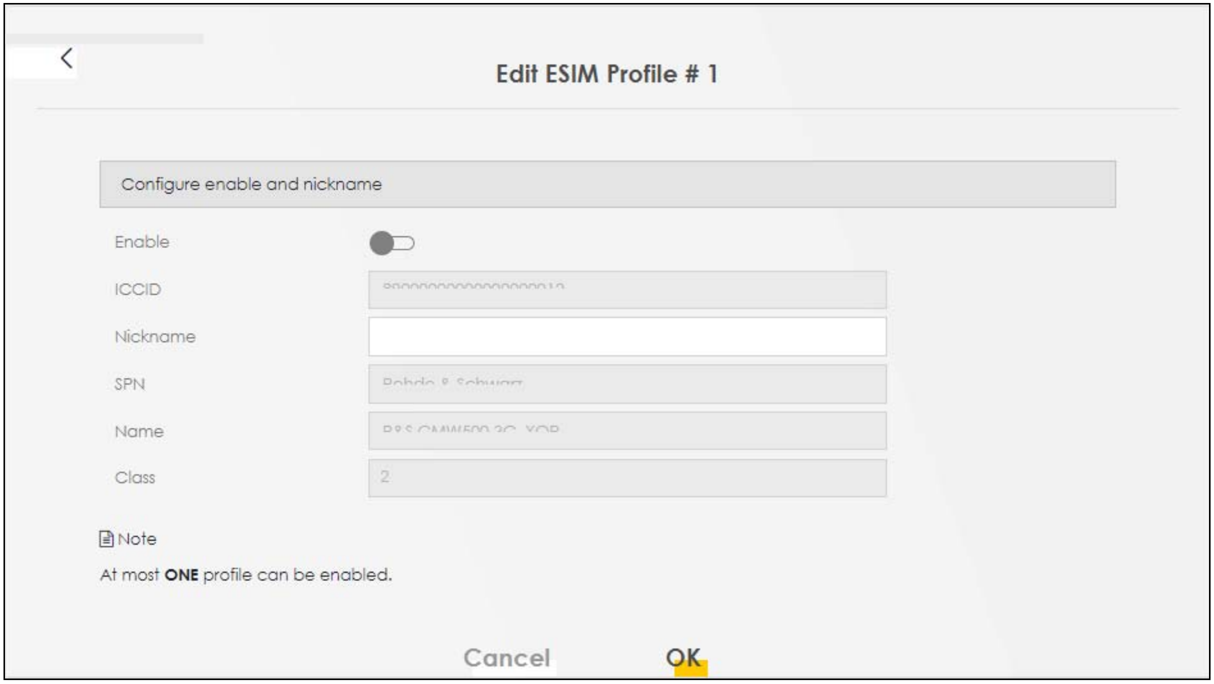
7.11.1 Edit eSIM Profile

Click the **Edit** icon (✎) in the **eSIM** screen. Use this screen to do the following:

- Enable/disable the eSIM subscription
- Assign a **Nickname** to the eSIM subscription
- View the **ICCID**, **SPN**, **Name** and **Class** information provided by your service provider. See Table 26 on page 92 for more information.

Note: Except for the **Nickname**, eSIM subscription information is obtained from the service provider.

Figure 61 Network Setting > Broadband > eSIM > Edit eSIM Profile



Edit ESIM Profile # 1

Configure enable and nickname

Enable ○●

ICCID 89000000000000000010

Nickname

SPN Rohde & Schwarz

Name R&S CMW500 3G YQR

Class 2

Note

At most **ONE** profile can be enabled.

The following table describes the fields in this screen.

Table 27 Network Setting > Broadband > eSIM > Edit eSIM Profile

LABEL	DESCRIPTION
Enable	Click this switch to the right to enable the eSIM subscription on the Zyxel Device. Note: Only one eSIM subscription can be active at a time. After enabling an eSIM subscription, the previous eSIM subscription will automatically be disabled.
ICCID	This displays the Integrated Circuit Card Identification Number (ICCID). This is an 18 to 22-digit code containing the eSIM subscription's country code, operator code, and identification number.
Nickname	This field allows you to display a descriptive name of the eSIM subscription. Enter a descriptive name of up to 31 printable ASCII characters including spaces.
SPN	This displays the name of the service provider.
Name	This displays the name of the eSIM subscription with your service provider.
Class	This displays **2** for an eSIM subscription.
Cancel	Click this to exit this screen without saving.
OK	Click this to save your changes.

CHAPTER 8 Wireless

8.1 Wireless Overview

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

Note: The WiFi network is only for configuring the Zyxel Device. Remember to turn it off after all configurations are done.

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 96)
- Use the **MAC Authentication** screen to allow or deny WiFi clients based on their MAC addresses from connecting to the Zyxel Device (Section 8.3 on page 100).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 8.4 on page 102).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 8.5 on page 103).

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 8.6 on page 105 for advanced technical information on WiFi networks.

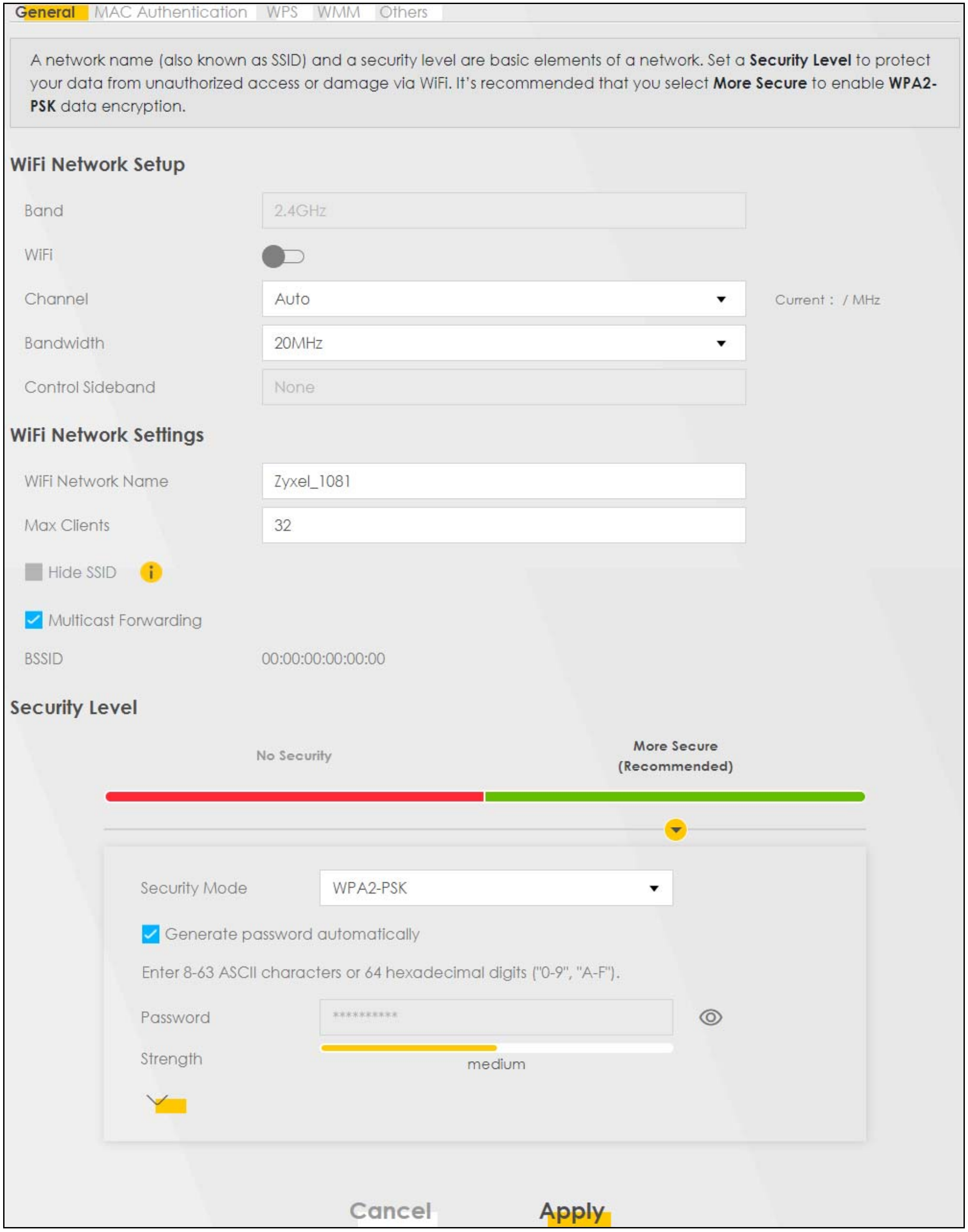
8.2 Wireless General Settings

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

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

Figure 62 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 WiFi labels in this screen.

Table 28 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless/WiFi Network Setup	
Band	This shows the WiFi band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n WiFi clients.
Wireless/WiFi	Click this switch to enable or disable WiFi in this field. When the switch turns blue, the function is enabled. Otherwise, it is not.

Table 28 Network Setting > Wireless > General (continued)

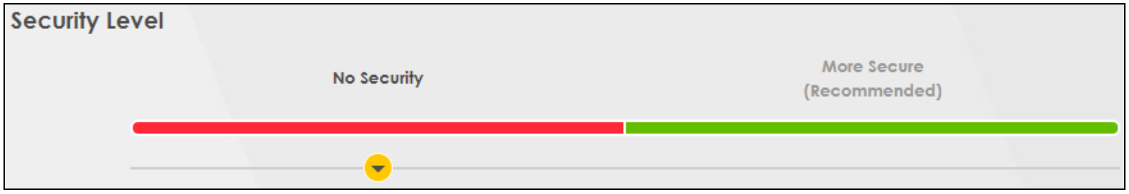
LABEL	DESCRIPTION
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use **Auto** to have the Zyxel Device automatically determine a channel to use.
Bandwidth	Select whether the Zyxel Device uses a WiFi channel width of **20MHz**, **40MHz** or **20/40MHz**. The available options will be shown in the drop list. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. 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.
Wireless/WiFi Network Settings	
Wireless/WiFi Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for this WiFi network. You can use up to 32 printable characters, including spaces.
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 Setting** > **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 WiFi is enabled.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.2.1 No Security

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

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

Figure 63 Wireless > General: No Security



The following table describes the labels in this screen.

Table 29 Wireless > General: No Security

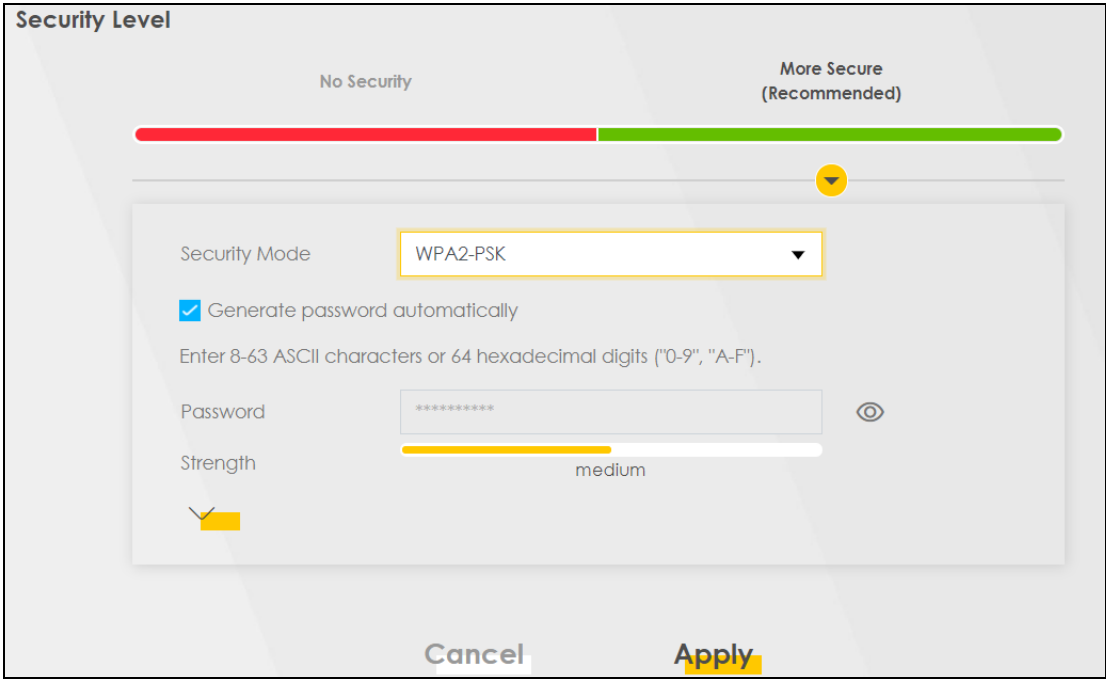
LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all WiFi connections without data encryption or authentication.

8.2.2 More Secure (Recommended)

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

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

Figure 64 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 30 Wireless > General: More Secure: WPA2-PSK

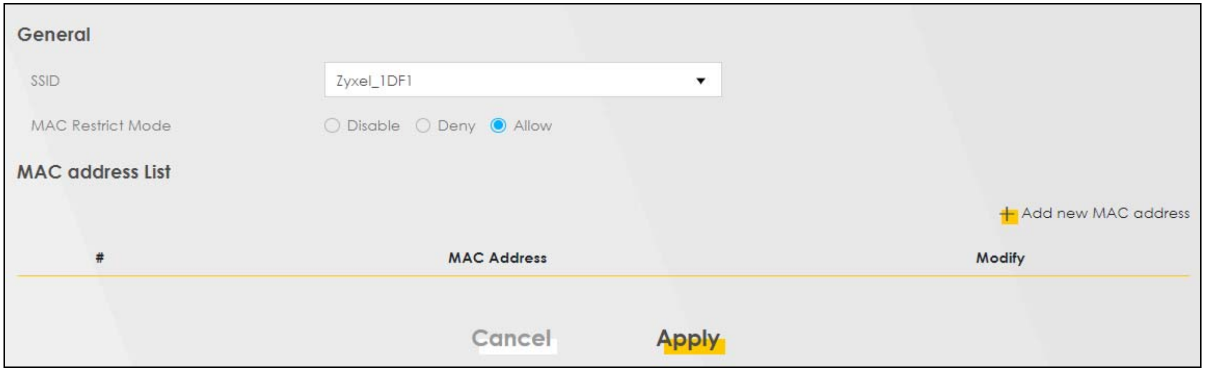
LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable 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. You can use 8 – 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: More than 63 hexadecimal characters are not accepted for WPS. Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it is hidden.
Click this to show more fields in this section. Click this to hide them.	
Encryption	**AES** is the default data encryption type, which uses a 128-bit key. Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your WiFi clients can all use AES. Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. Note: Not all models support **TKIP+AES** encryption.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

8.3 MAC Authentication

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

Note: You can have up to 25 MAC authentication rules.Use this screen to view your Zyxel Device's MAC filter settings and add new MAC filter rules. Click **Network Setting** > **Wireless** > **MAC Authentication**. The screen appears as shown.

Figure 65 Network Setting > Wireless > MAC Authentication



General

SSID: Zyxel_1DF1

MAC Restrict Mode: ○ Disable ○ Deny ● Allow

MAC address List

#	MAC Address	Modify

The following table describes the labels in this screen.

Table 31 Network Setting > Wireless > MAC Authentication

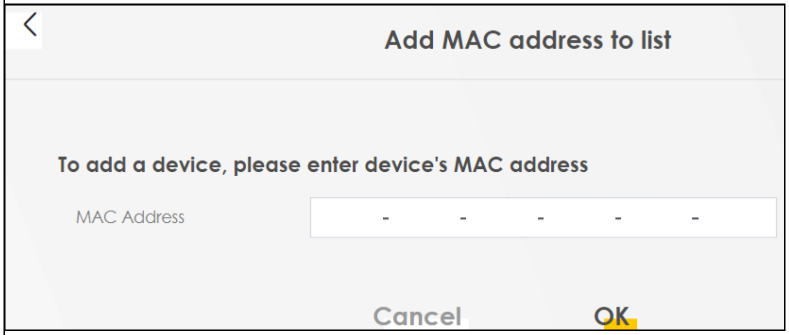
LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the Zyxel Device. 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 WiFi 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.  Add MAC address to list To add a device, please enter device's MAC address MAC Address: - - - - -
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the WiFi devices that are allowed or denied access to the Zyxel Device.
Modify	Click the **Edit** icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the **Delete** icon to delete the entry.

Table 31 Network Setting > Wireless > MAC Authentication (continued)

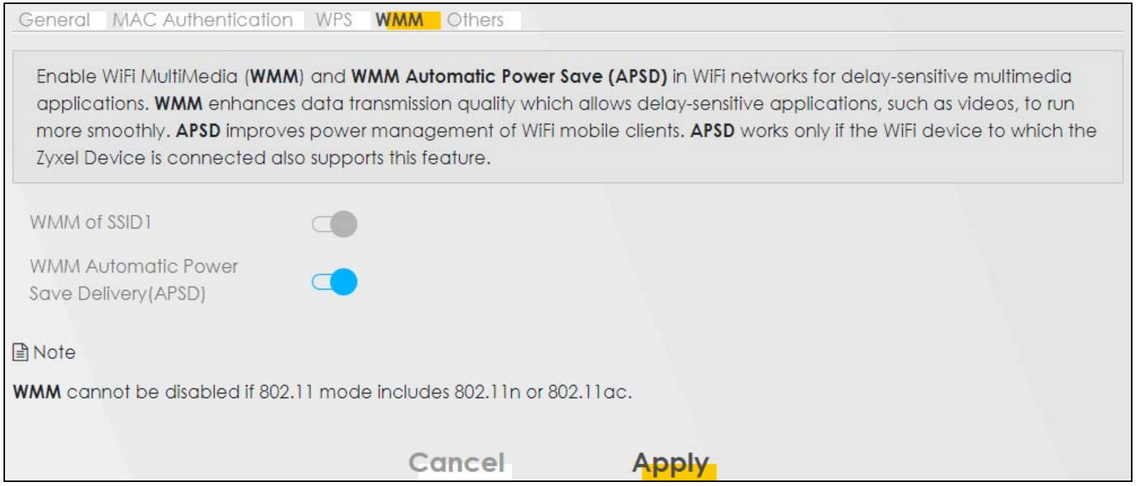
LABEL	DESCRIPTION
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

8.4 WMM

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

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

Figure 66 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 32 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM of SSID1	Select **On** to have the Zyxel Device automatically give the WiFi network (SSID) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi 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 WiFi device to which the Zyxel Device is connected also supports this feature.

Table 32 Network Setting > Wireless > WMM (continued)

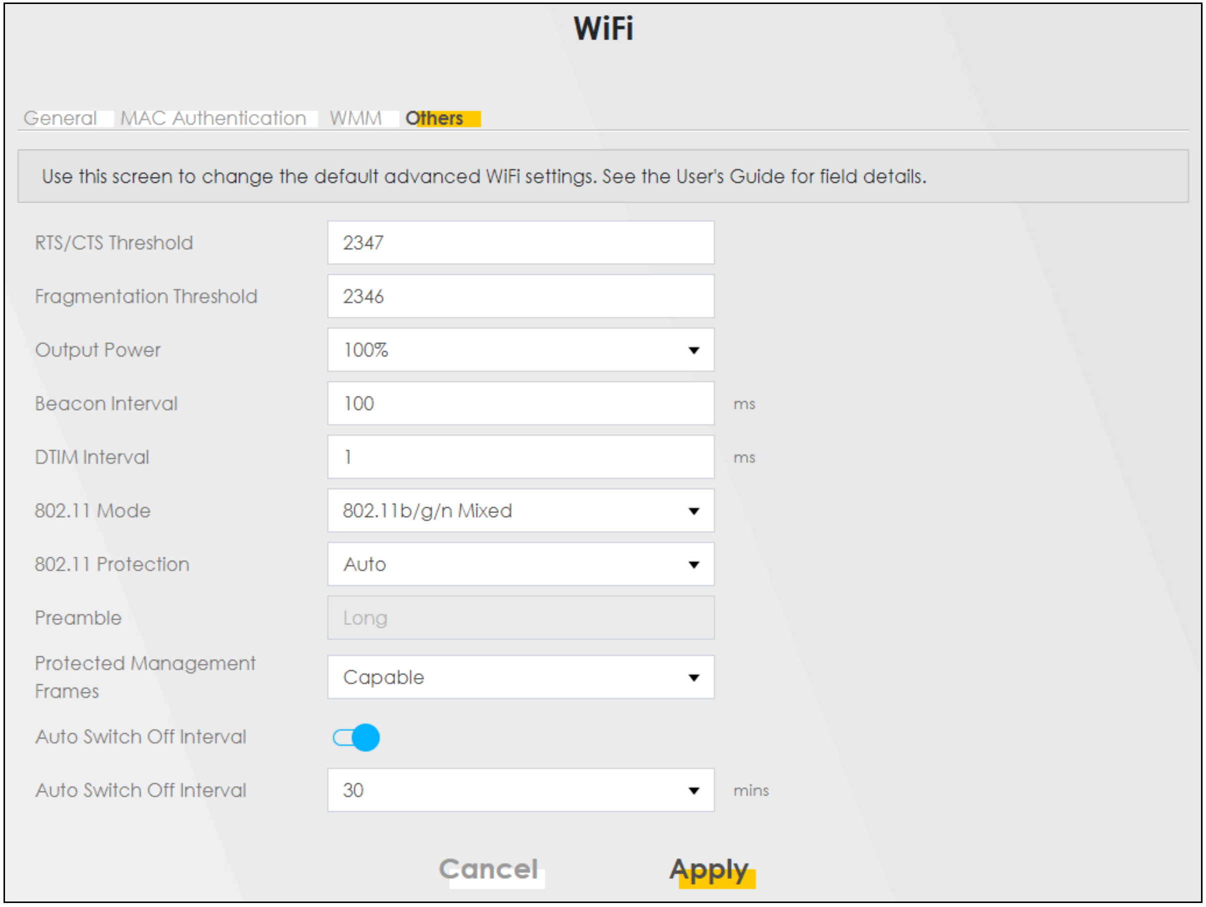
LABEL	DESCRIPTION
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.5 Others Screen

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

See Section 8.6.2 on page 106 for detailed definitions of the terms listed here.

Figure 67 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	●	
Auto Switch Off Interval	30	mins

The following table describes the labels in this screen.

Table 33 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50 ms to 1000 ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and Multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	For 2.4 GHz frequency WiFi devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi 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 IEEE 802.11n compliant WiFi 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. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 8.6.6 on page 109 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
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 **0**,**15**, **30**, **45** or **60** minutes from the drop down menu. The default setting is **30** minutes. Select **0** minute to disable the **Auto Switch Off Interval.**

Table 33 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.6 Technical Reference

This section discusses WiFi in depth.

8.6.1 WiFi Network Overview

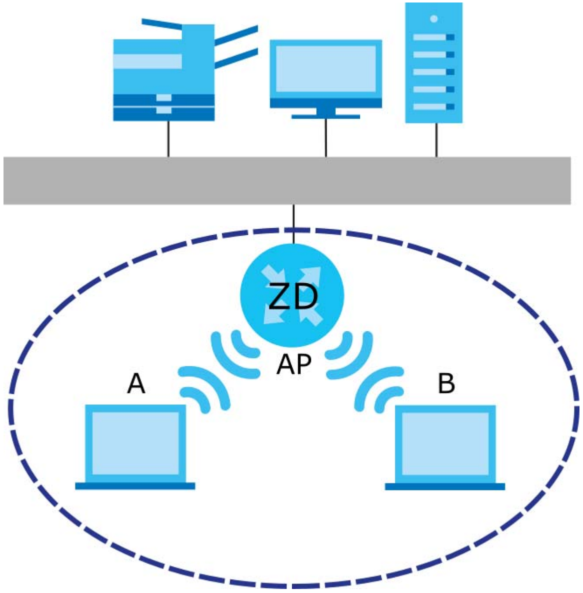
WiFi networks consist of WiFi clients, access points and bridges.

- 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 68 Example of a WiFi Network



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

Every WiFi network must follow these basic guidelines.

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

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

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

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

8.6.2 Additional WiFi Terms

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

Table 34 Additional WiFi Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a WiFi network which covers a large area, WiFi 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 WiFi 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 WiFi devices never have to get permission to send information to the Zyxel Device.
Preamble	A preamble affects the timing in your WiFi network. There are two preamble modes: long and short. If a WiFi device uses a different preamble mode than the Zyxel Device does, it cannot communicate with the Zyxel Device.
Authentication	The process of verifying whether a WiFi device is allowed to use the WiFi 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.

8.6.3 WiFi Security Overview

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

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

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

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

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

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

8.6.3.1 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.

8.6.3.2 MAC Address Filter

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

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

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

8.6.3.3 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 8.6.3.3 on page 107 for information about this.)

[1] Some wireless devices, such as scanners, can detect WiFi networks but cannot use WiFi 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.

Table 35 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.

8.6.4 Signal Problems

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

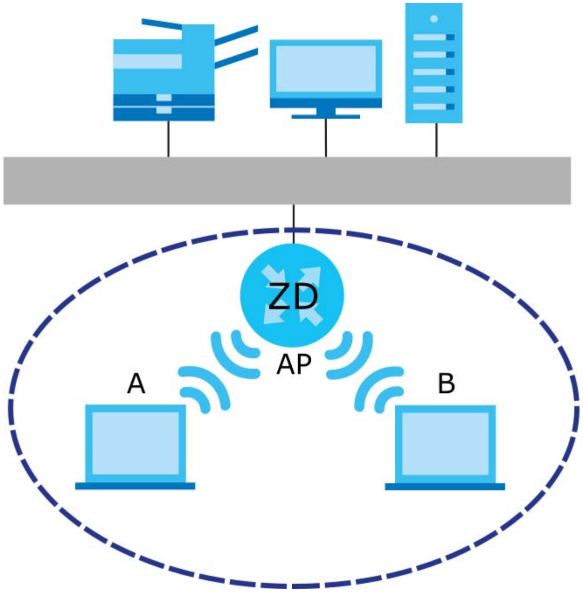
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters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

8.6.5 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 69 Basic Service Set



8.6.6 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 WiFi adapters support long preamble, but not all support short preamble.

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

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

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

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

8.6.7 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 2 minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

8.6.7.1 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 WiFi range of one another.

2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the Zyxel Device).

3 Press the button on one of the devices (it does not matter which). For the Zyxel Device you must press the **WiFi** button for more than 5 seconds.

4 Within 2 minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

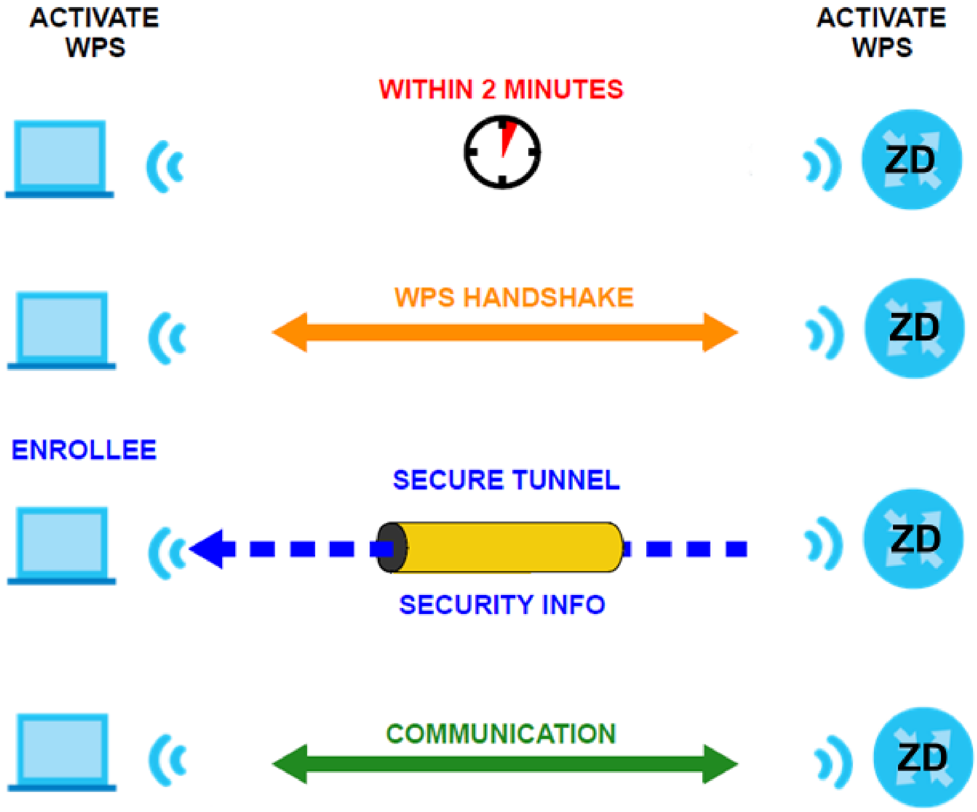
If you need to make sure that WPS worked, check the list of associated WiFi clients in the AP's configuration utility. If you see the WiFi client in the list, WPS was successful.

8.6.7.2 How WPS Works

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

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

Figure 70 How WPS Works



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

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

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

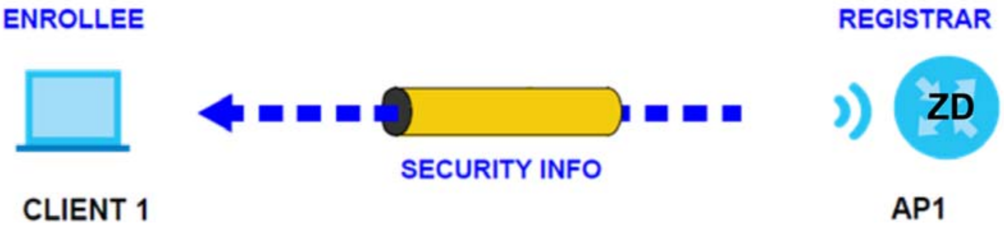
By default, a WPS device is ‘un-configured’. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is un-configured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

8.6.7.3 Example WPS Network Setup

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

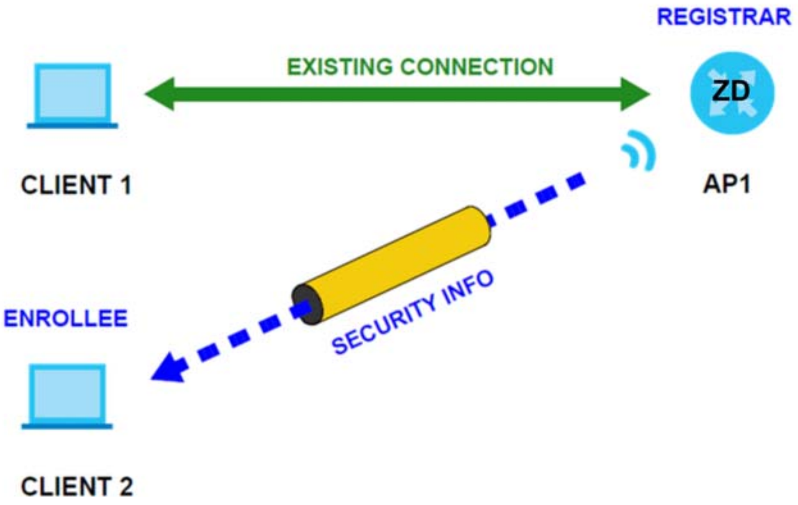
The following figure shows a sample network. In step 1, both **AP1** and **Client 1** are un-configured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 71 WPS: Example Network Step 1



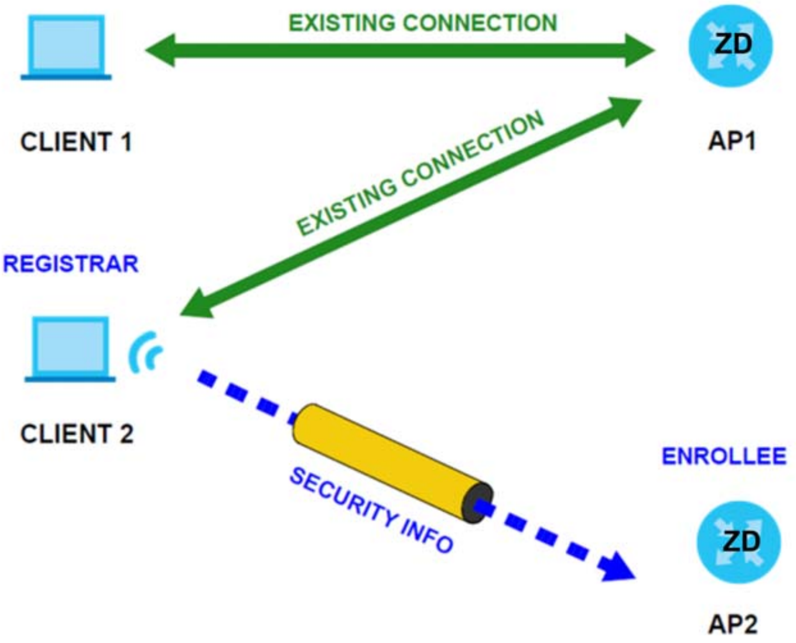
In step **2**, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 72 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 73 WPS: Example Network Step 3



8.6.7.4 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

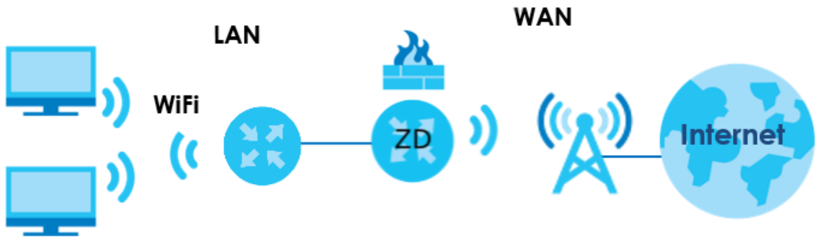
CHAPTER 9 Home Networking

9.1 Home Networking Overview

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

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

Figure 74 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 116).
- 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 121).
- Use the **UPnP** screen to enable UPnP (Section 9.4 on page 123).
- Use the **Custom DHCP** screen to set additional DHCP options (Section 9.5 on page 124).
- Use the **GRE Tunnel** screen to configure a GRE tunnel (Section 9.6 on page 126).

9.1.2 What You Need To Know

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

9.1.2.1 About LAN

IP Address

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

Subnet Mask

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

DHCP

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

DNS

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

RADVD (Router Advertisement Daemon)

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

9.1.2.2 About UPnP

How do I know if I am using UPnP?

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

NAT Traversal

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

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

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

Cautions with UPnP

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

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

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

UPnP and Zyxel

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

See Section 9.8 on page 131 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.

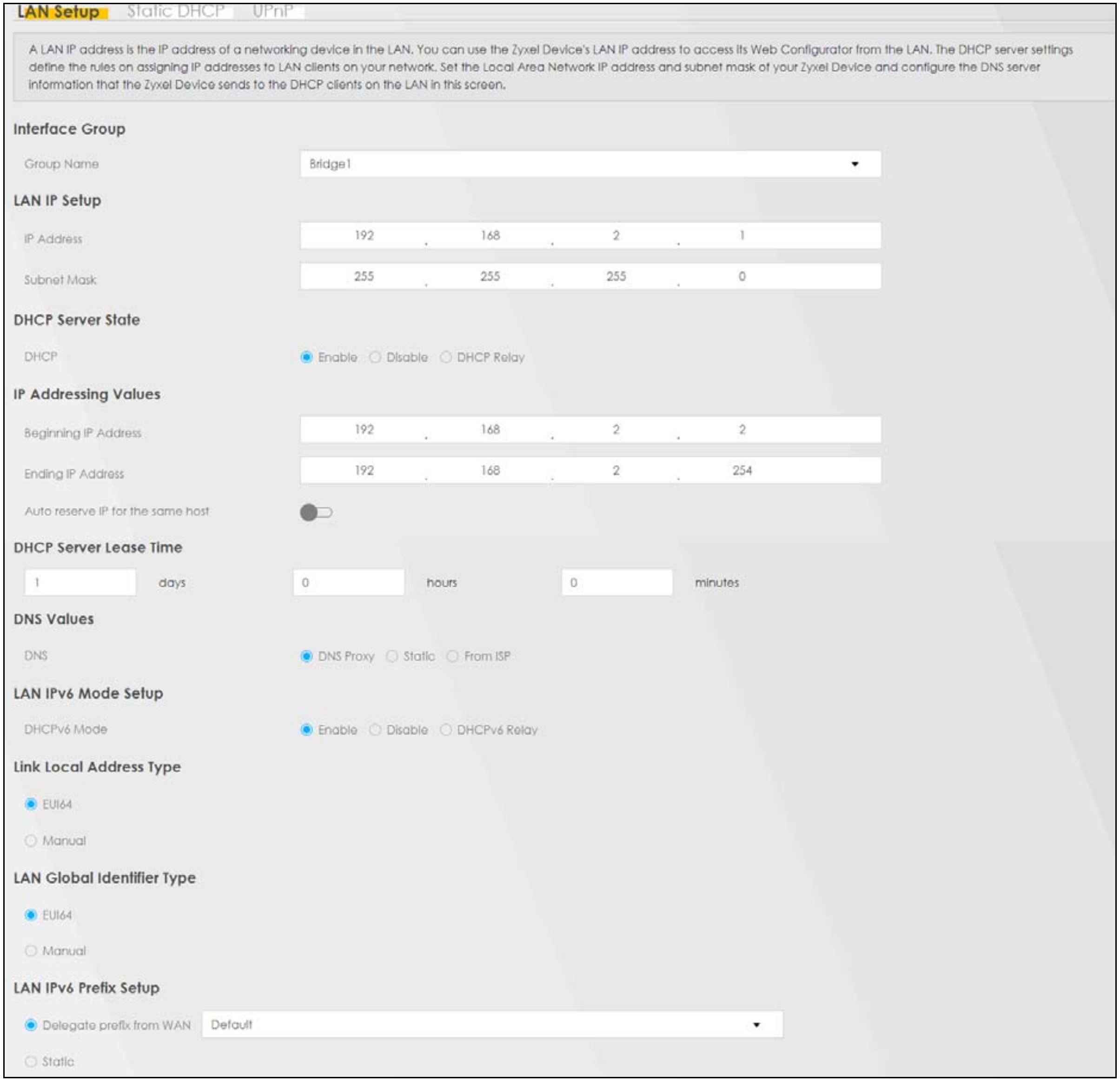
Follow these steps to configure your LAN settings.

1. Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your Zyxel Device.

2. Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

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

Figure 75 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

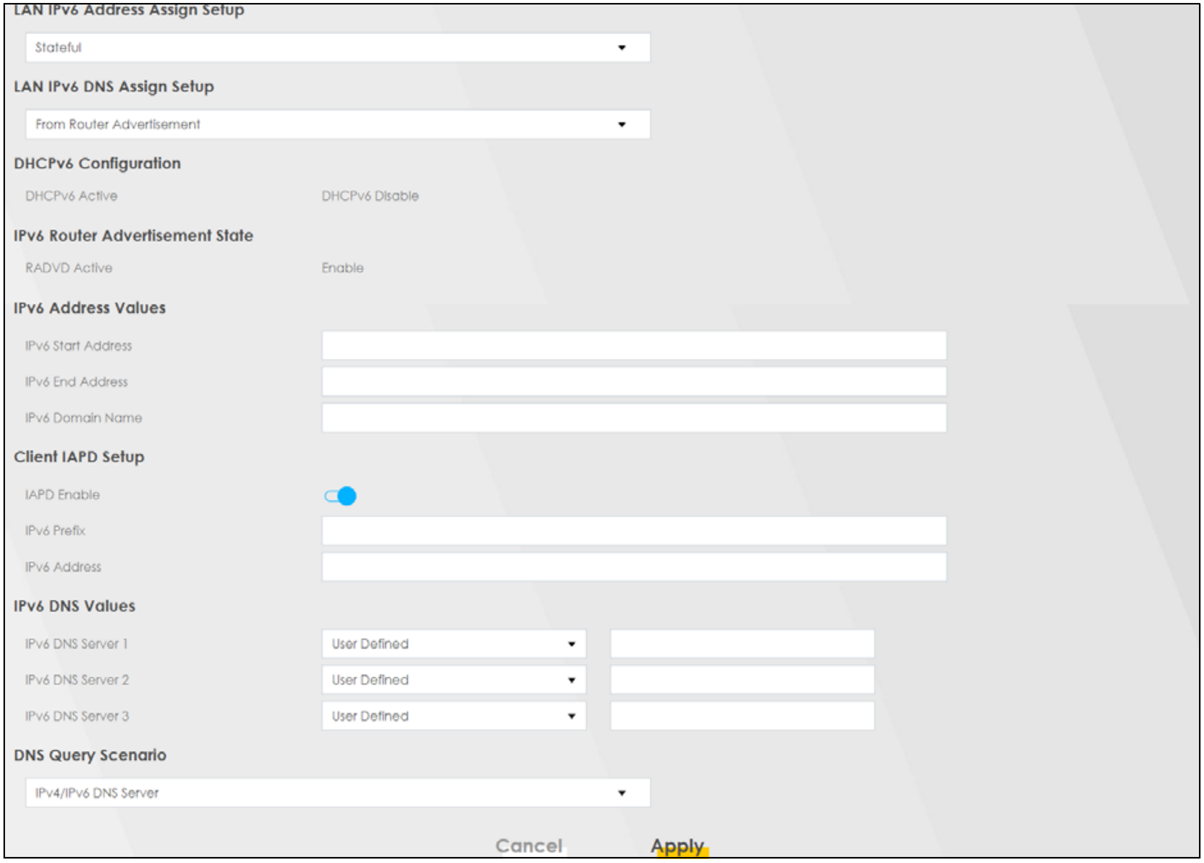
○ Manual

LAN IPv6 Prefix Setup

● Delegate prefix from WAN: Default ▾

○ Static

Figure 76 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 36 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group that you want to configure its LAN settings.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select **Enable** to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. If you select **DHCP Relay**, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
DHCP Relay Server Address This field is only available when you select **DHCP Relay** in the **DHCP** field.	
IP Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.

Table 36 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
IP Addressing Values The **IP Addressing Values** fields appear only when you select **Enable** in the **DHCP** field.	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
DHCP Server Lease Time This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.	
Days/Hours/Minutes	DHCP server leases an address to a new client device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different client device.
DNS Values This field appears only when you select **Enable** in the **DHCP** field.	
DNS	The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client. Select **DNS Proxy** to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay. Select **Static** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **From ISP** if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).
LAN IPv6 Mode Setup	
IPv6 Active	Use this to enable or disable IPv6 on the Zyxel Device. When IPv6 is used, the following fields need to be set.
DHCPv6 Mode	Select **Enable** to use the DHCPv6 mode. You will need to configure the fields starting from Link Local Address Type. Select **DHCPv6 Relay** to set up DHCPv6 Relay server. Otherwise, select **Disable**. When **DHCPv6 Relay** is selected, You need to configure the DHCPv6 Relay Server Setup fields.
DHCPv6 Relay Server Setup	
Contact Server from WAN	Specifies the interface on which messages to servers are sent. Choices are Cellular WAN1 to Cellular WAN 4.
DHCPv6 Server IP Address	Specifies the DHCPv6 server address to relay packets to.

Table 36 Network Setting > Home Networking > LAN Setup (continued)

<table>
<tr><th>LABEL</th><th>DESCRIPTION</th></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>EUI64</td><td>Select this to have the Zyxel Device generate an interface ID for the LAN interface’s link-local address using the EUI-64 format.</td></tr>
<tr><td>Manual</td><td>Select this to manually enter an interface ID for the LAN interface’s link-local address.</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>
<tr><td>EUI64</td><td>Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address.</td></tr>
<tr><td>Manual</td><td>Select this to manually enter an interface ID for the LAN interface’s global IPv6 address.</td></tr>
<tr><td>LAN IPv6 Prefix Setup</td><td>Select <b>Delegate prefix from WAN</b> to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select <b>Static</b> to configure a fixed IPv6 address for the Zyxel Device’s LAN IPv6 address.</td></tr>
<tr><td>Delegate prefix from WAN</td><td>Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.</td></tr>
<tr><td>Static</td><td>Select this option to configure a fixed IPv6 address for the Zyxel Device’s LAN IPv6 address.</td></tr>
<tr><td>LAN IPv6 Address Assign Setup</td><td>Select how you want to obtain an IPv6 address:
<b>Stateless</b>: 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.
<b>Stateful</b>: 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.</td></tr>
<tr><td>LAN IPv6 DNS Assign Setup</td><td>Select how the Zyxel Device provide DNS server and domain name information to the clients:
<b>From RA & DHCPv6 Server</b>: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.
<b>From DHCPv6 Server</b>: The Zyxel Device provides DNS information through DHCPv6.
<b>From Router Advertisement</b>: The Zyxel Device provides DNS information through router advertisements.</td></tr>
<tr><td colspan="2">DHCPv6 Configuration</td></tr>
<tr><td>DHCPv6 Active</td><td>This shows the status of the DHCPv6. <b>DHCP Server</b> displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.</td></tr>
<tr><td colspan="2">IPv6 Router Advertisement State</td></tr>
<tr><td>RADVD Active</td><td>This shows whether RADVD is enabled or not.</td></tr>
<tr><td colspan="2">IPv6 Address Values</td></tr>
</table>

Table 36 Network Setting > Home Networking > LAN Setup (continued)

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

9.3 Static DHCP

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

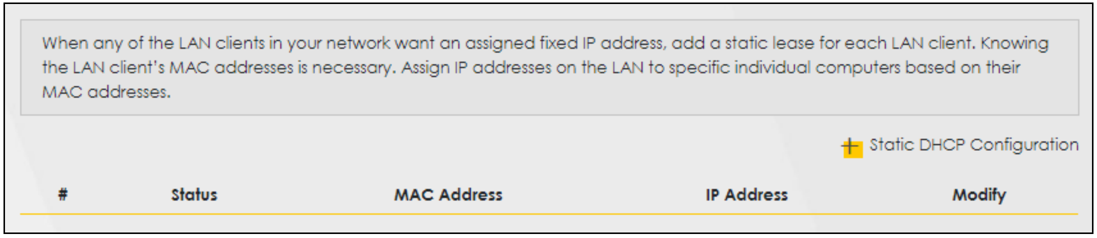
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

9.3.1 Before You Begin

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

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

Figure 77 Network Setting > Home Networking > 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. Assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

#	Status	MAC Address	IP Address	Modify

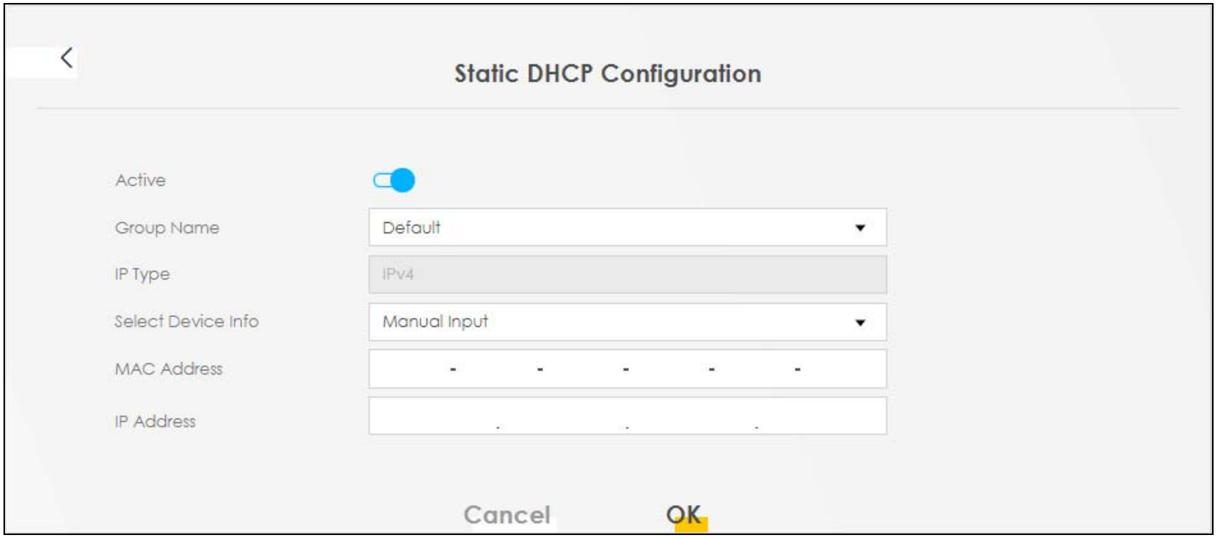
The following table describes the labels in this screen.

Table 37 Network Setting > Home Networking > Static DHCP

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

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

Figure 78 Network Setting > Home Networking > 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 38 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

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

9.4 UPnP

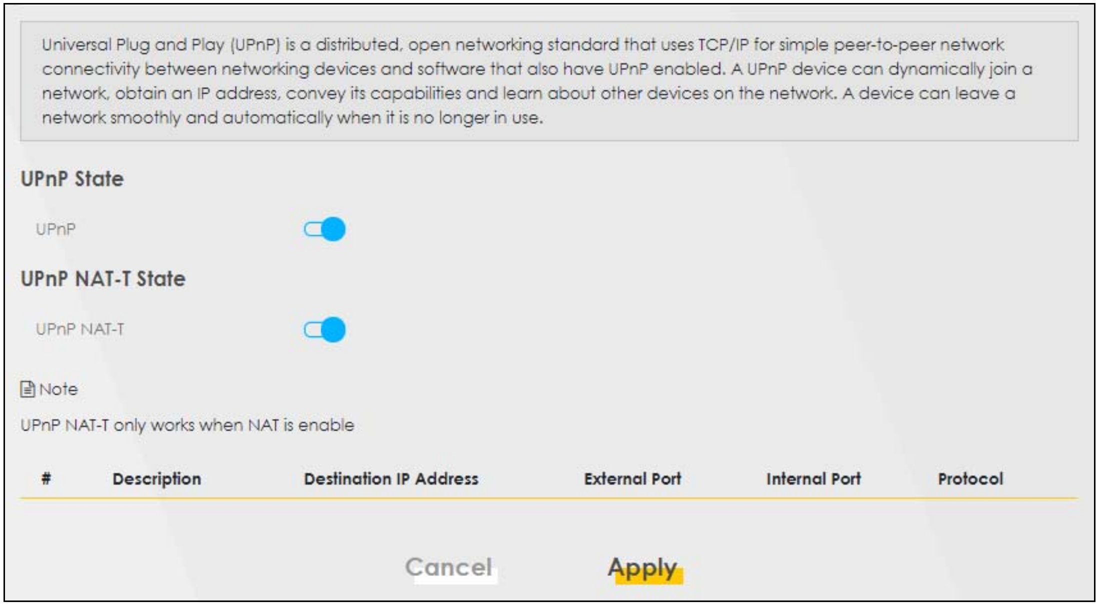
Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn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

See Section 9.8 on page 131 for more information on UPnP.

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

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

Figure 79 Network Setting > Home Networking > UPnP



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

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 39 Network Settings > Home Networking > UPnP

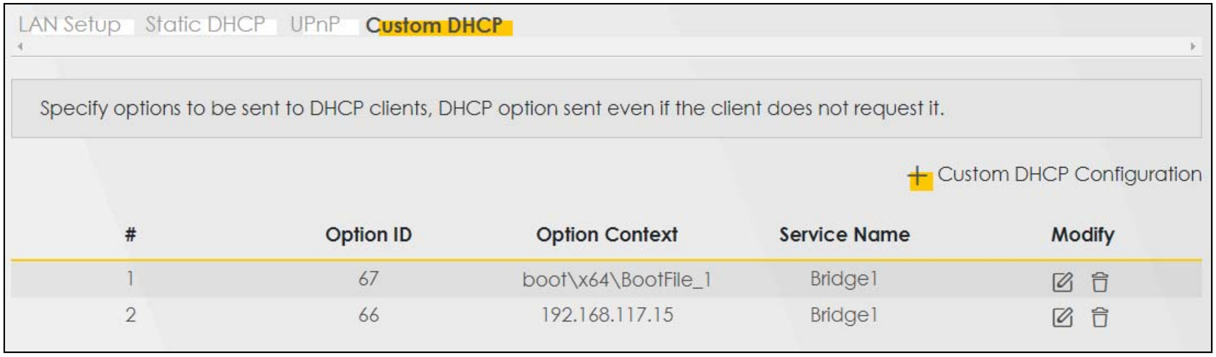
LABEL	DESCRIPTION
UPnP State	
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T State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

9.5 Custom DHCP

DHCP options are additional configurations that DHCP clients can receive from a DHCP server. You can configure the Zyxel Device, as a DHCP server, to send the parameters you configured as DHCP options to your DHCP clients. For example, DHCP option 6 can tell the DHCP client which DNS (Domain Name Server) to use for name resolution along with its IP configuration.

Use the following screen to configure custom DHCP option on your Zyxel Device. Click **Network Setting** > **Home Networking** > **Custom DHCP** to display the screen shown next.

Figure 80 Network Setting > Home Networking > Custom DHCP



Specify options to be sent to DHCP clients, DHCP option sent even if the client does not request it.

#	Option ID	Option Context	Service Name	Modify
1	67	boot\x64\BootFile_1	Bridge1	
2	66	192.168.117.15	Bridge1	

The following table describes the labels in this screen.

Table 40 Network Settings > Home Networking > Custom DHCP

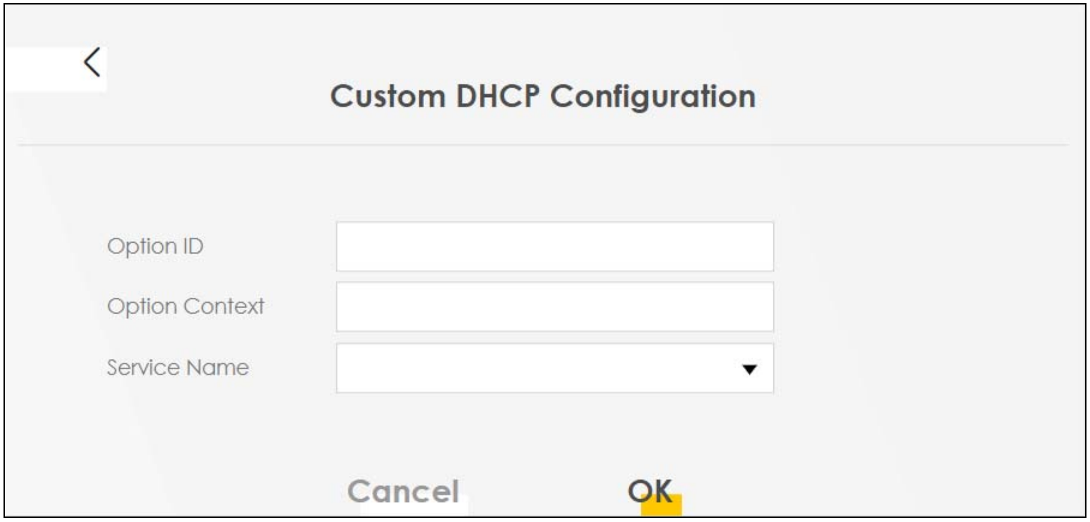
LABEL	DESCRIPTION
Custom DHCP Configuration	Click this to add a DHCP option you want to sent to your DHCP clients.
#	This field displays the index number of the entry.
Option ID	This field displays the DHCP option ID.
Option Context	This field displays the content of the DHCP option.
Service Name	This field displays the interface group that the DHCP option is sent on.
Modify	Click the **Modify** icon to edit an existing entry. Click the **Delete** icon to remove an existing entry.

9.5.1 Custom DHCP Configuration

Use this screen to add a DHCP option, as defined in the RFC protocols, and set its content.

Click **Custom DHCP Configuration** on the **Network Setting** > **Home Networking** > **Custom DHCP** screen to display the following screen.

Figure 81 Network Setting > Home Networking > Custom DHCP



Custom DHCP Configuration

Option ID

Option Context

Service Name

The following table describes the labels in this screen.

Table 41 Network Settings > Home Networking > Custom DHCP

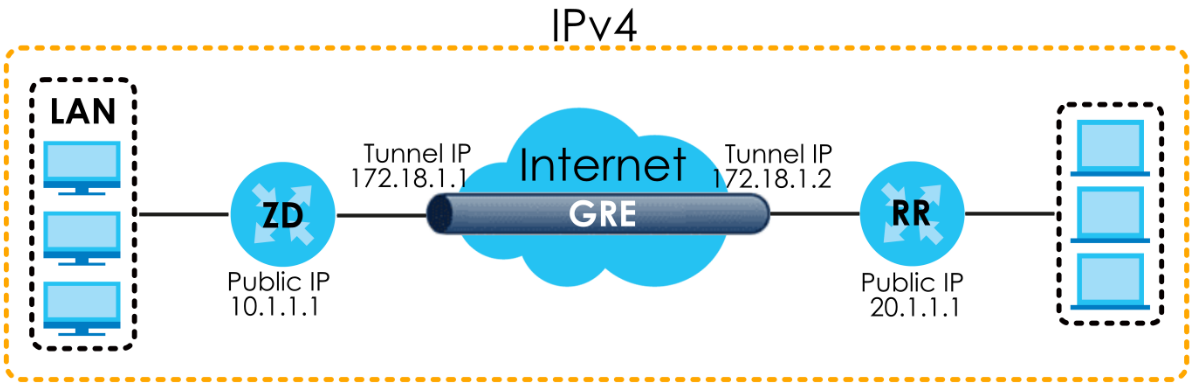
LABEL	DESCRIPTION
Option ID	Enter the option ID for the additional configuration that DHCP clients can receive from a DHCP server. For example, enter ‘6’ for DNS server configuration.
Option Context	Enter additional configuration details. For example, for DHCP option 6, enter the DNS server IP address. You can enter up to 257 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].
Service Name	Select an interface group from the drop-down list. The Zyxel Device will add this DHCP option to DHCP packets sent on the selected service interface group. You can configure interface groups in the **Network Setting** > **Interface Grouping** screen.
Cancel	Click **Cancel** to not save your settings and return to the previous screen.
OK	Click **OK** to save your changes and return to the previous screen.

9.6 GRE Tunnel

GRE (Generic Routing Encapsulation) is a tunneling protocol used to create a virtual point-to-point link between two networks to transport multicast, broadcast and non-IP packets like IPX. In the example below, GRE establishes a private connection between the Zyxel Device (**ZD**) and remote router (**RR**) over an IPv4 network. At the time of writing, the Zyxel Device only supports GRE tunneling in IPv4 networks.

Note: The GRE tunnel must also be configured on the remote router (RR).

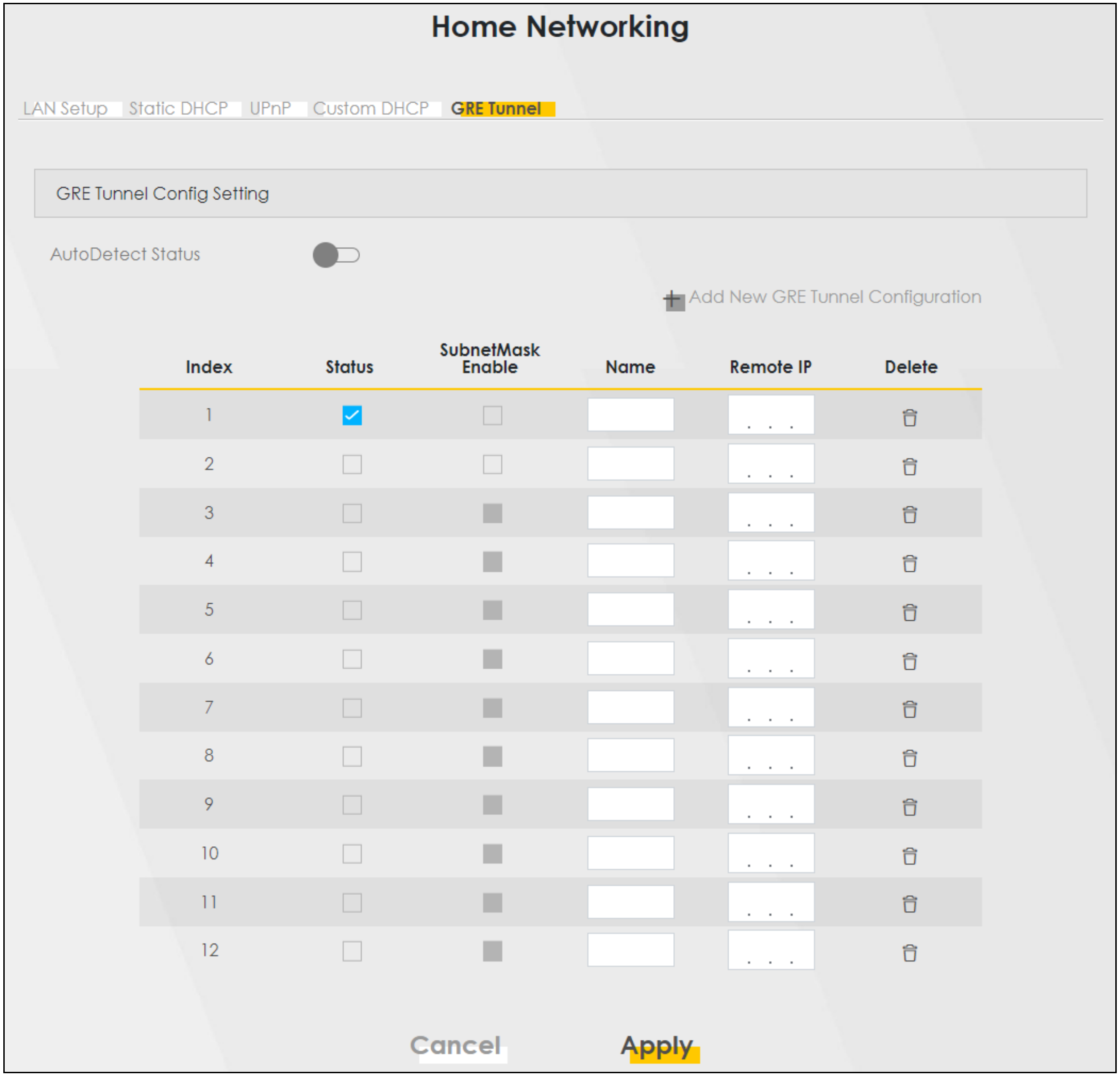
Figure 82 GRE Tunnel Example



Use this screen to configure a GRE tunnel.

Click **Network Setting** > **Home Networking** > **GRE Tunnel** to display the following screen.

Figure 83 Network Setting > Home Networking > GRE Tunnel



Home Networking

GRE Tunnel Config Setting

AutoDetect Status ○

Index	Status	SubnetMask Enable	Name	Remote IP	Delete
1	☑	□		. . .	🗑
2	□	□		. . .	🗑
3	□	■		. . .	🗑
4	□	■		. . .	🗑
5	□	■		. . .	🗑
6	□	■		. . .	🗑
7	□	■		. . .	🗑
8	□	■		. . .	🗑
9	□	■		. . .	🗑
10	□	■		. . .	🗑
11	□	■		. . .	🗑
12	□	■		. . .	🗑

The following table describes the labels in this screen.

Table 42 Network Settings > Home Networking > GRE Tunnel

LABEL	DESCRIPTION
Auto Detect Status	Click this switch to the right to enable the Zyxel Device to automatically detect and connect to remote devices through a GRE tunnel. Alternatively, click this switch to the left to configure/enable/remove/add GRE tunnels.
Note: These fields are available only when **Auto Detect Status** is disabled.	
Add New GRE Tunnel Configuration	Click this if you want to create a new GRE tunnel.
Index	This is the index number of the entry.
Status	Select this to enable the GRE tunnel. Alternatively, disable the GRE tunnel.
Subnet Mask Enable	Select this to allow the Zyxel Device to tunnel local traffic to **Remote IP**s that are within the remote device IP's subnet mask. Note: Due to hardware limitation, you can only enable subnet mask for two **Remote IP** addresses.
Name	Enter a descriptive name for this tunnel. You can enter up to 64 alphanumeric and special characters including spaces and 2-byte characters.
Remote IP	Enter the remote device's IP address for this tunnel. If the tunnel is active and connected, the Zyxel Device tunnels local traffic to this IP address.
Delete	Click this icon to remove a tunnel. The Zyxel Device confirms you want to remove it before doing so.
Cancel	Click **Cancel** to not save your settings and return to the previous screen.
Apply	Click **Apply** to save your changes and return to the previous screen.

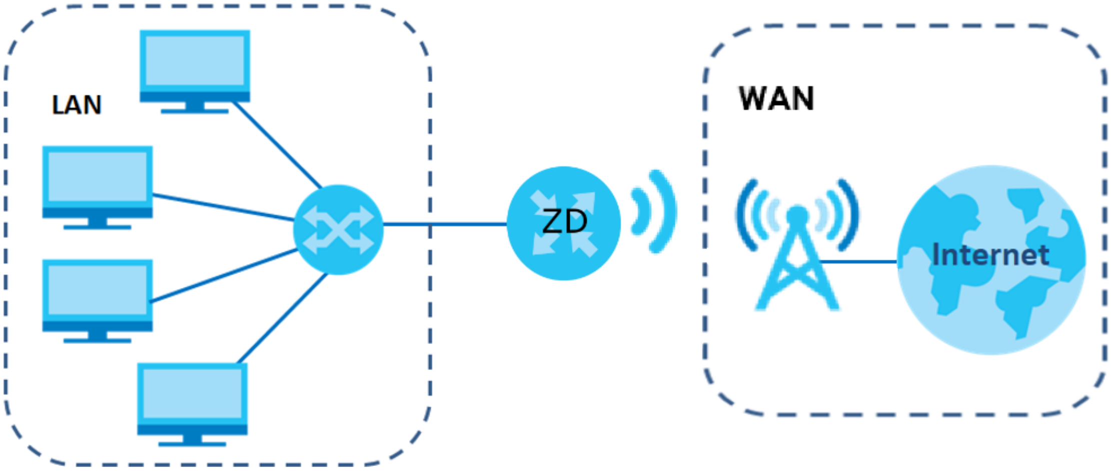
9.7 Technical Reference

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 84 LAN and WAN IP Addresses



9.7.1 DHCP Setup

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

IP Pool Setup

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

9.7.2 DNS Server Addresses

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

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Zyxel Device supports the IPCP DNS server extensions through the DNS proxy feature.

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

9.7.3 LAN TCP/IP

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

IP Address and Subnet Mask

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

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

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

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

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

Private IP Addresses

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

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

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

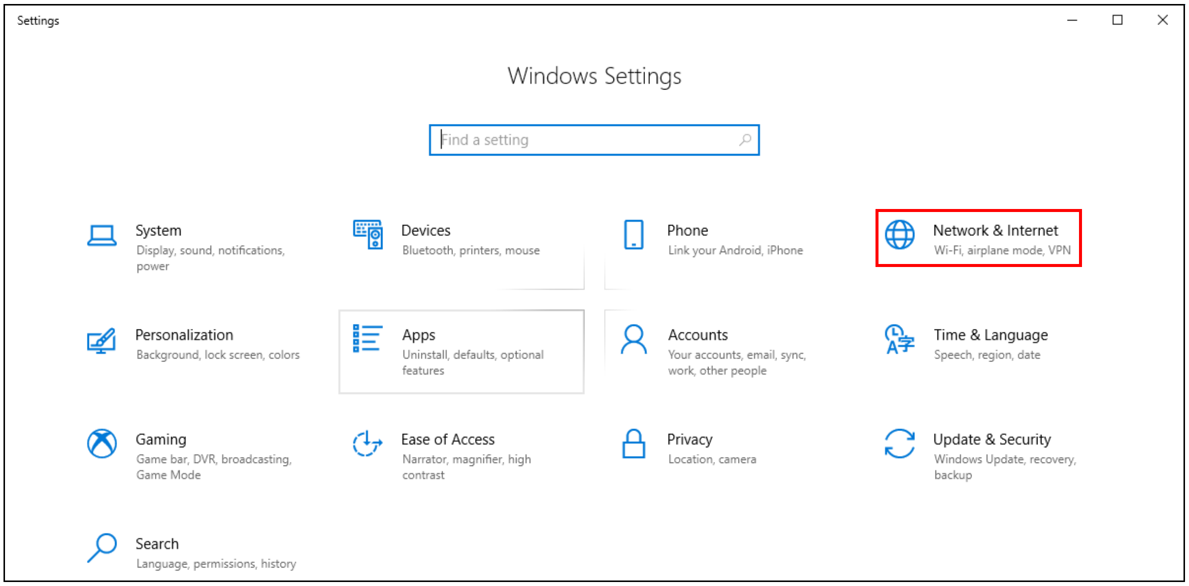
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

9.8 Turn on UPnP in Windows 10 Example

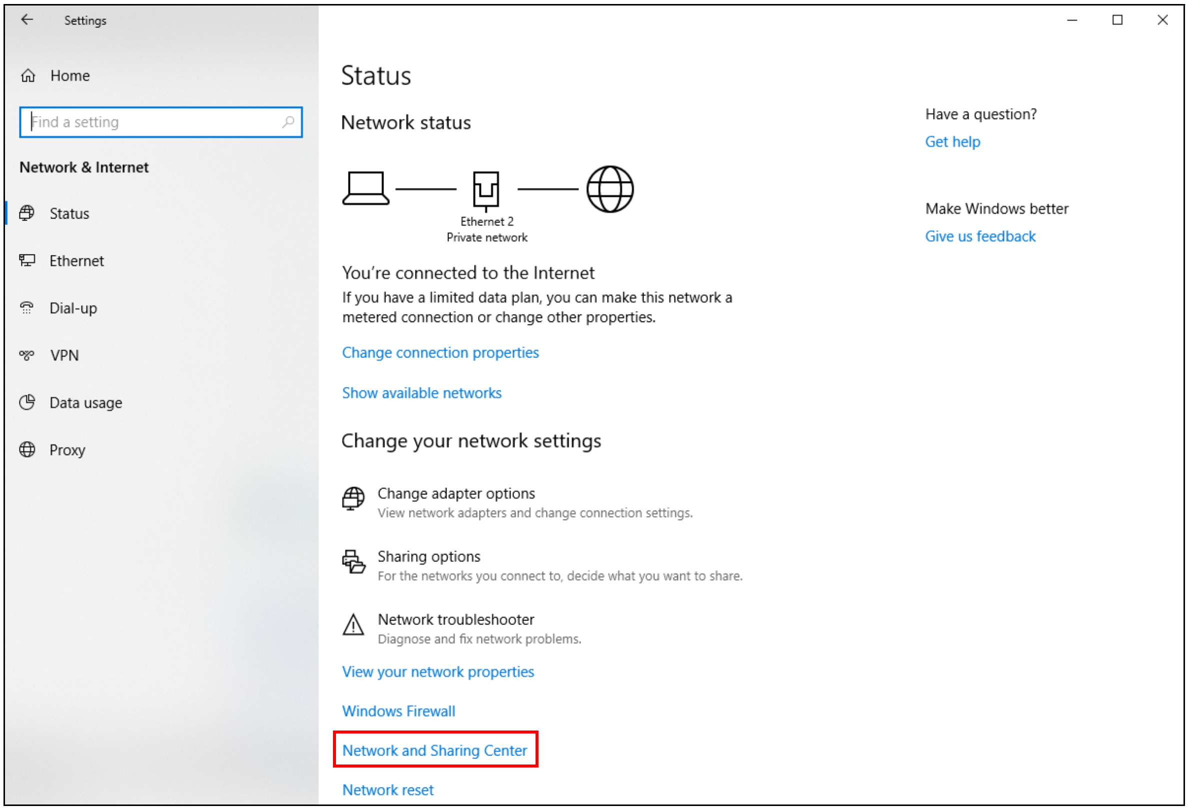
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting** > **Home Networking** > **UPnP**.

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**.



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

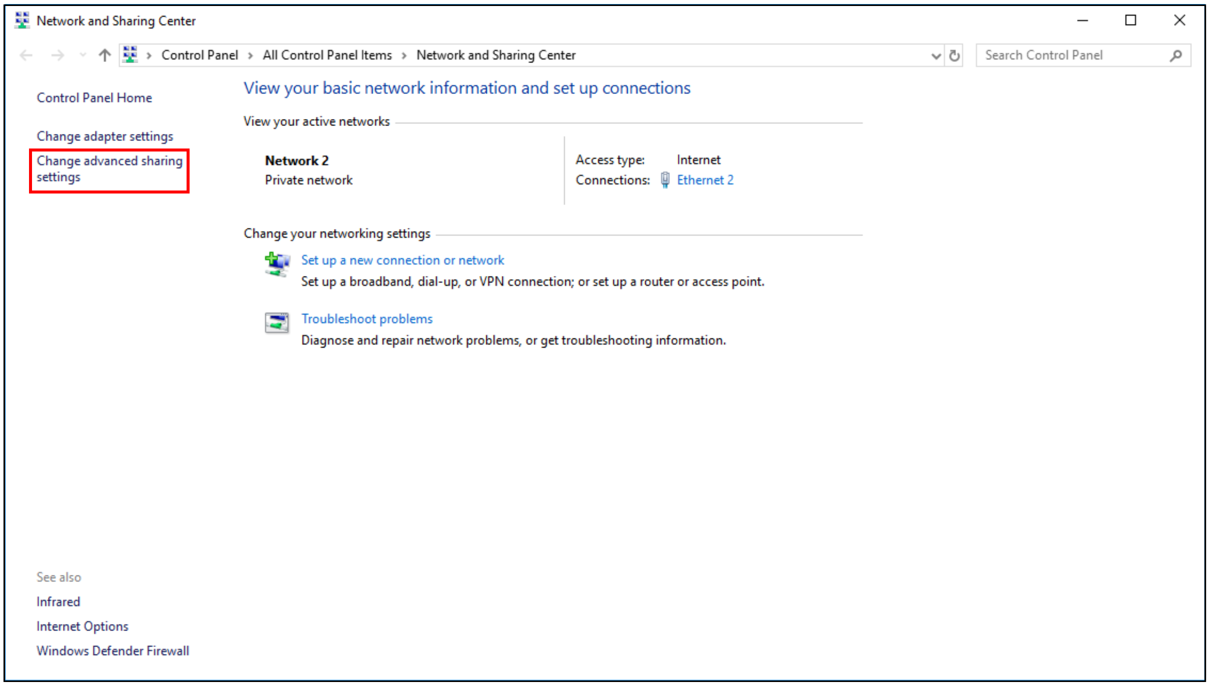
Network and Sharing Center

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

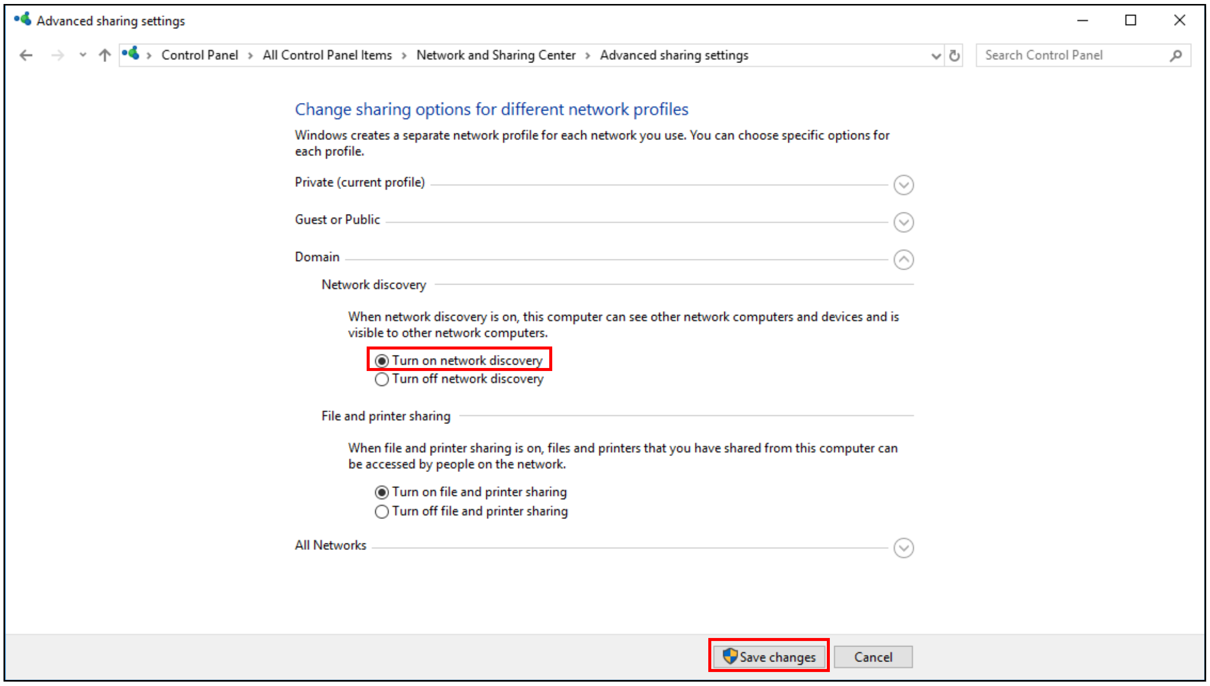
Access type: Internet
Connections: Ethernet 2

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

9.8.1 Auto-discover Your UPnP-enabled Network Device

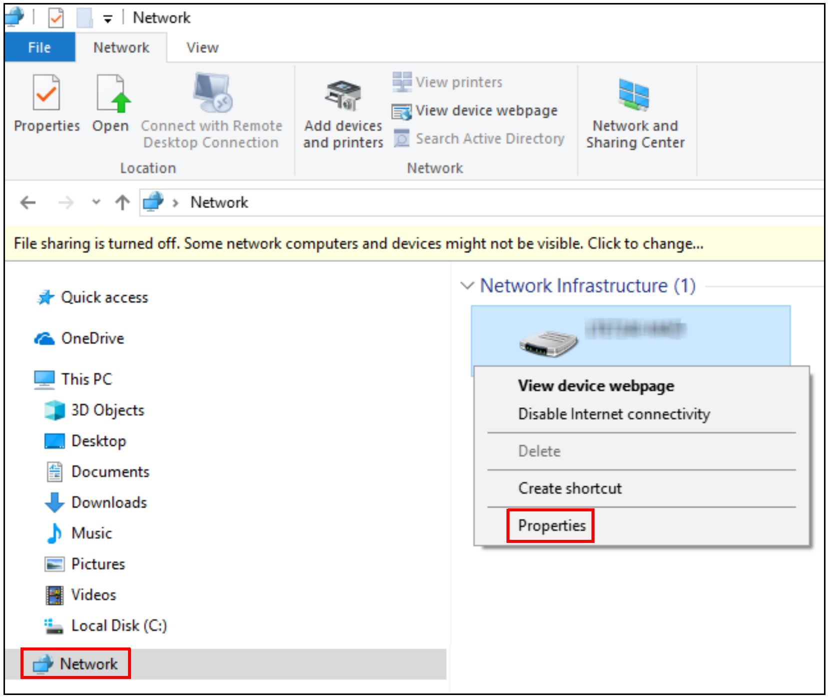
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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**.

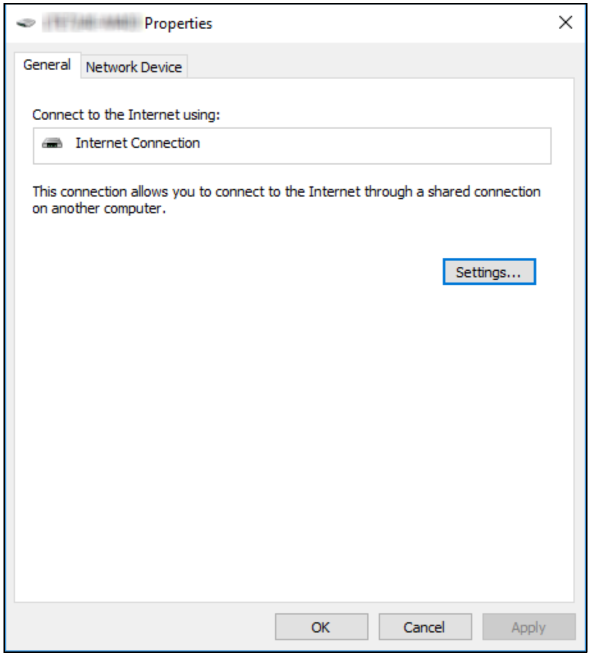
Figure 85 Network Connections



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

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

Figure 86 Internet Connection Properties



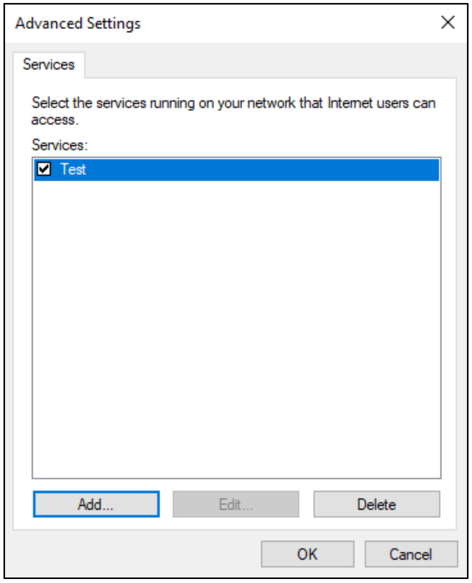
Connect to the Internet using:

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 87 Internet Connection Properties: Advanced Settings

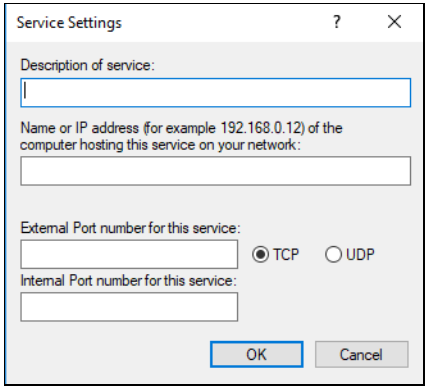


Select the services running on your network that Internet users can access.

Services:

☑ Test

Figure 88 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:

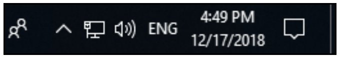
External Port number for this service: ● TCP ○ UDP

Internal Port number for this service:

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

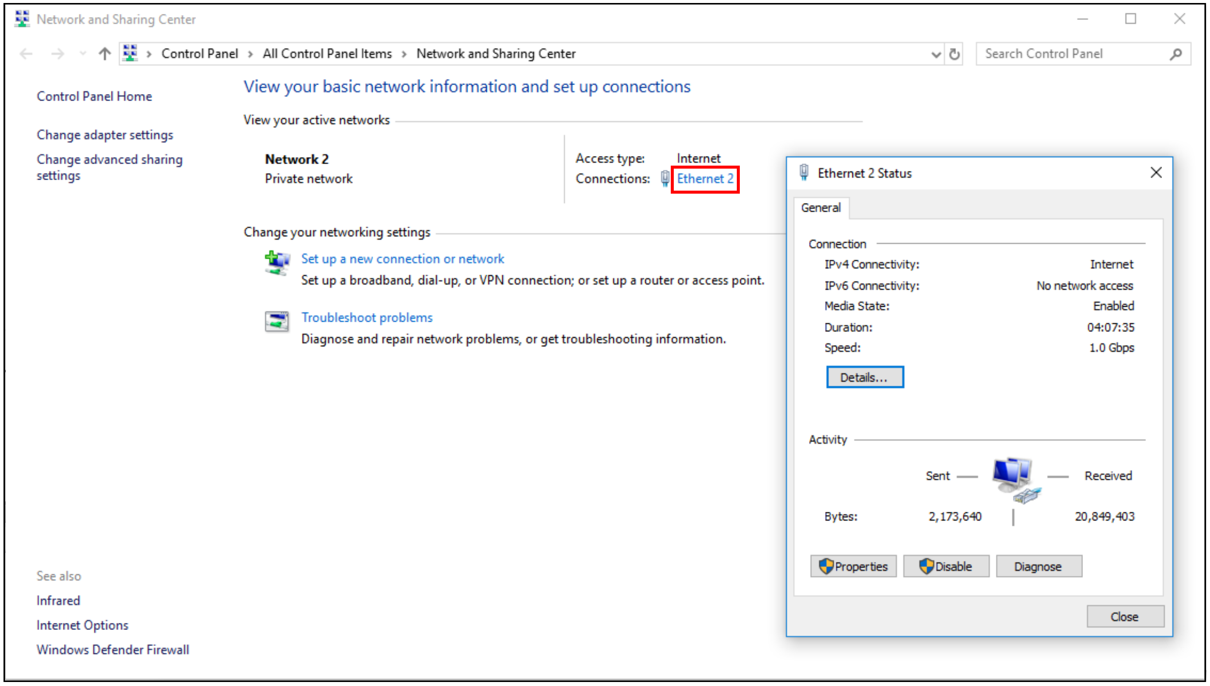
5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 89 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 90 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
See also
Infrared
Internet Options
Windows Defender Firewall
General
Details...
Properties
Disable
Diagnose
Close

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.

Ethernet 2 Status

Connection

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

Activity

Sent — Received

Bytes: 2,173,640 | 20,849,403

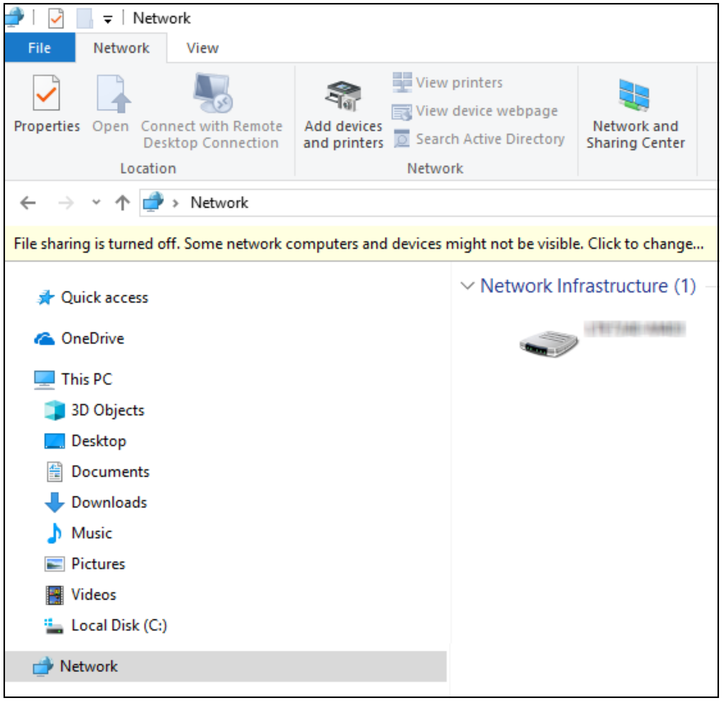
9.9 Web Configurator Access with UPNP in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

Figure 91 Network Connections

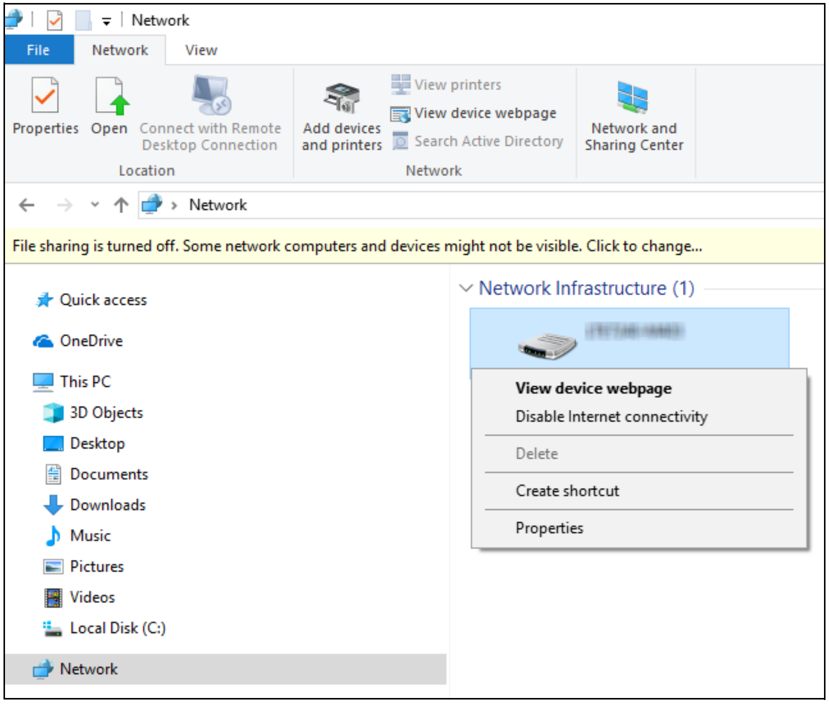


File sharing is turned off. Some network computers and devices might not be visible. Click to change...

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.

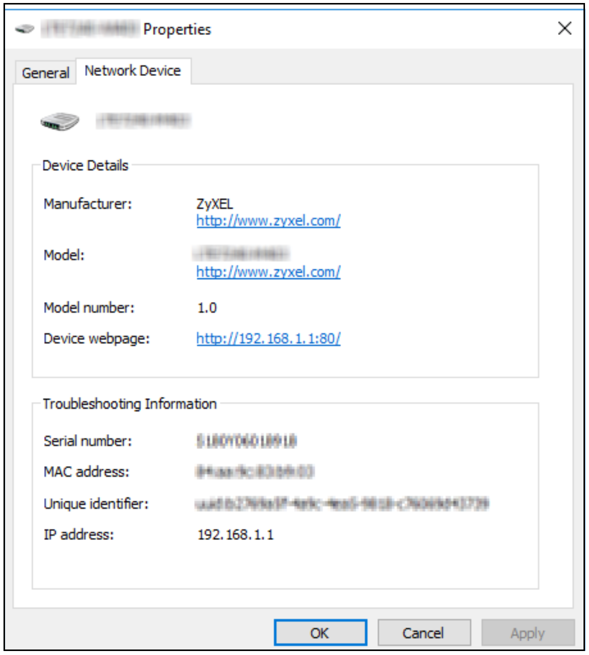
Figure 92 Network Connections: Network Infrastructure



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 93 Network Connections: Network Infrastructure: Properties: Example



[redacted] Properties

[redacted]

Device Details

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

Model: [redacted]
http://www.zyxel.com/

Model number: 1.0

Device webpage: http://192.168.1.1:80/

Troubleshooting Information

Serial number: [redacted]

MAC address: [redacted]

Unique identifier: [redacted]

IP address: 192.168.1.1

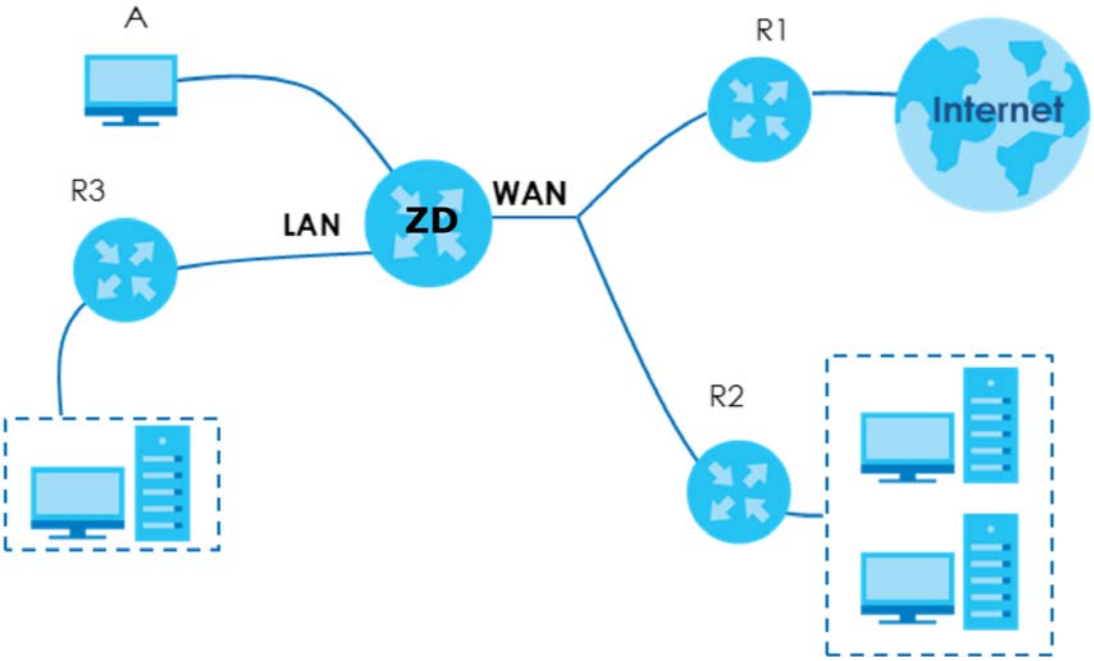
CHAPTER 10 Routing

10.1 Routing Overview

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

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

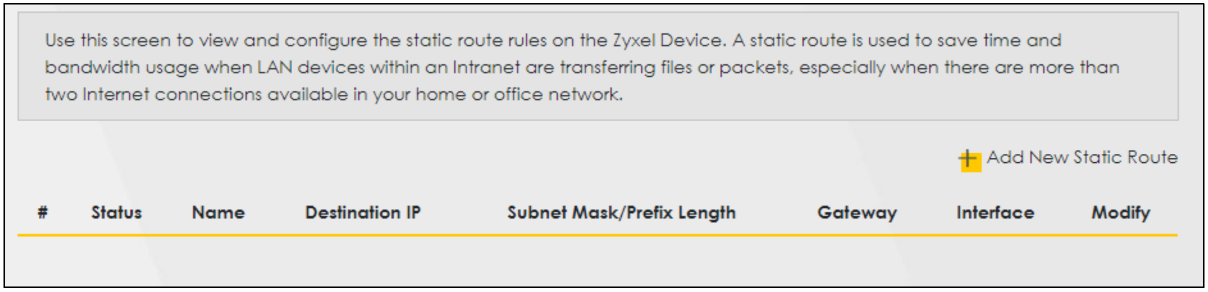
Figure 94 Example of Static Routing Topology



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 95 Network Setting > Routing > Static Route



Use this screen to view and configure the 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 available 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 43

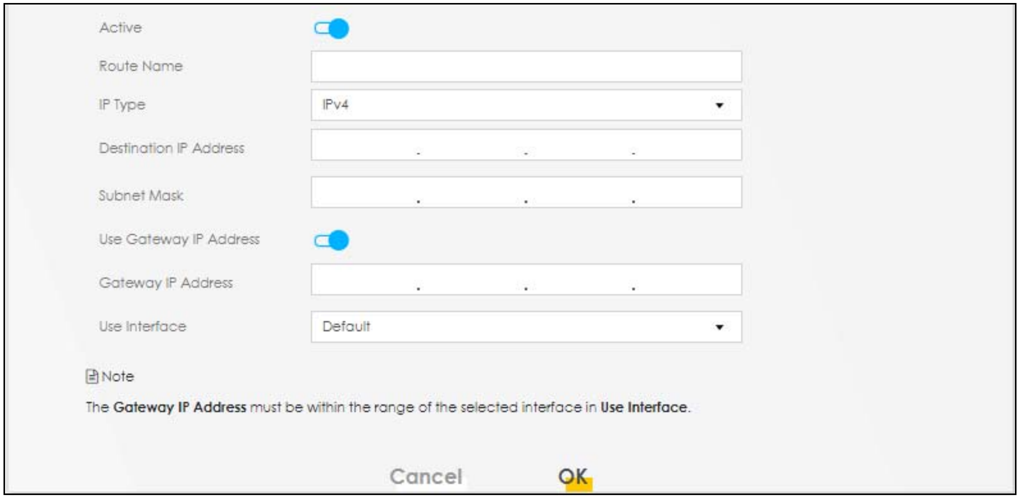
LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Zyxel Device.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This is the name of the static route.
Destination IP	This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

10.2.1 Add or Edit Static Route

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

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

Figure 96 Network Setting > Routing > Static Route > Add New 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 **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

The following table describes the labels in this screen.

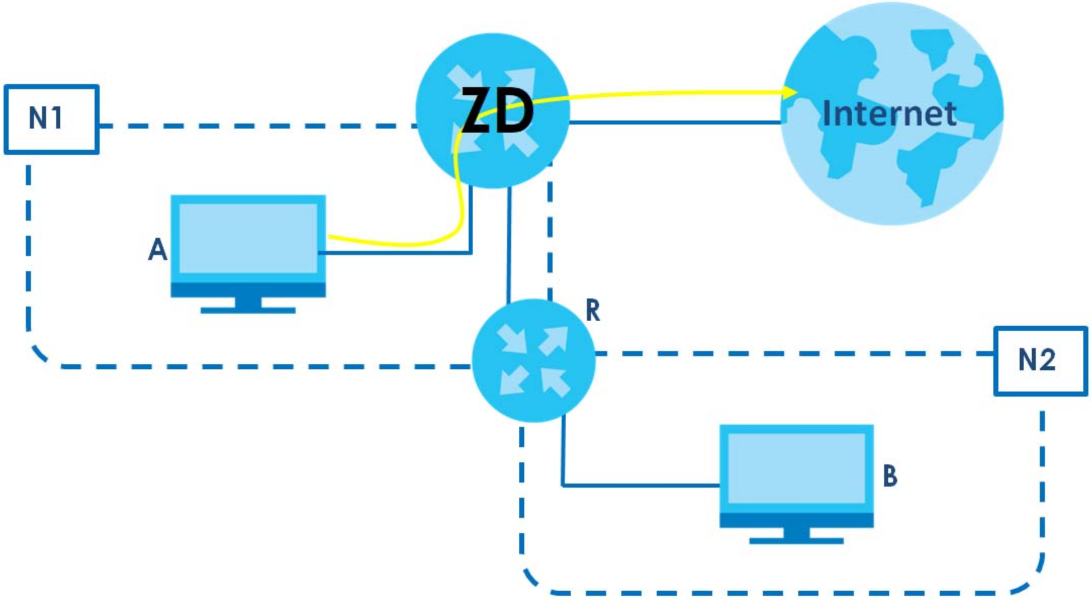
Table 44

LABEL	DESCRIPTION
Active	Click this switch to activate static route. Otherwise, click to disable.
Route Name	Enter a name for your static route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
IP Type	Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4**/**IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD).
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Gateway IP Address	Enter the IP address of the gateway.
User 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.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

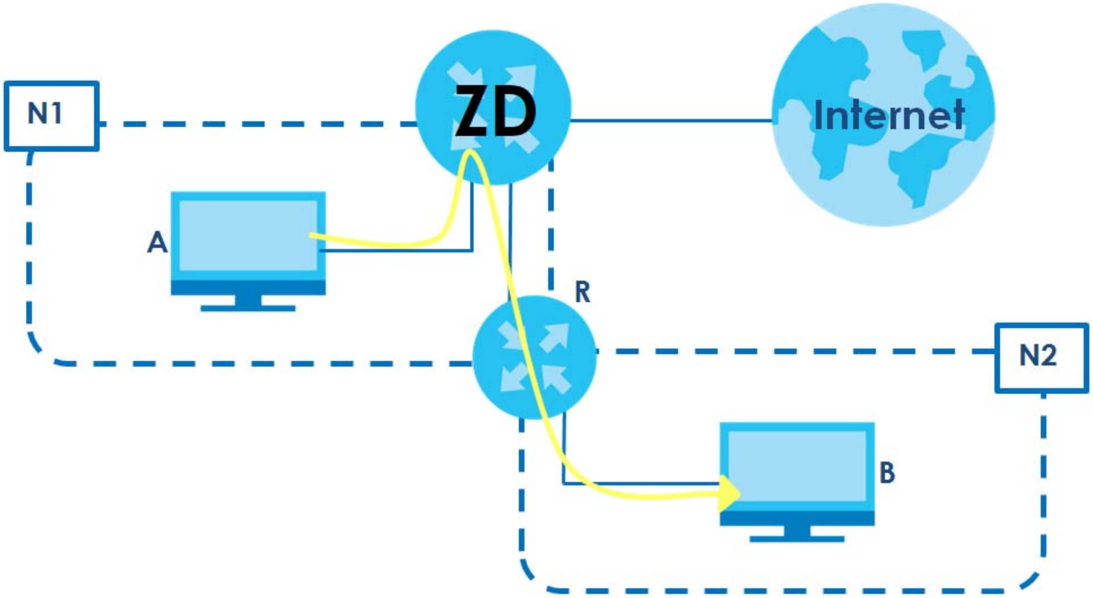
10.2.1.1 An Example of Adding a Static Route

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

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



You need to specify a static routing rule on the Zyxel Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Zyxel Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 45 IP Settings in this Tutorial

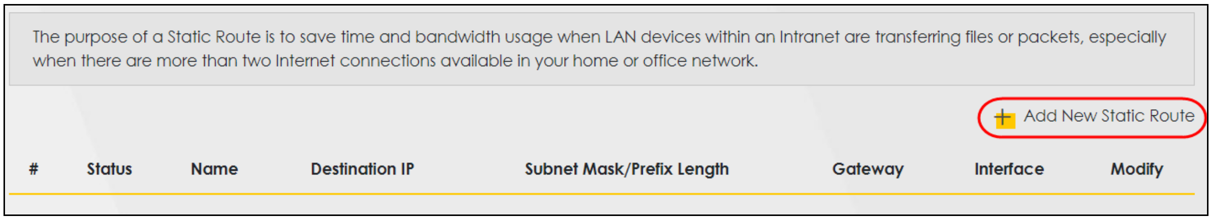
DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	
IP Type	IPv4
Use Interface	Default
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Log into the Zyxel Device's Web Configurator.

2 Click **Network Setting** > **Routing**.

3 Click **Add new Static Route** in the **Static Route** screen.



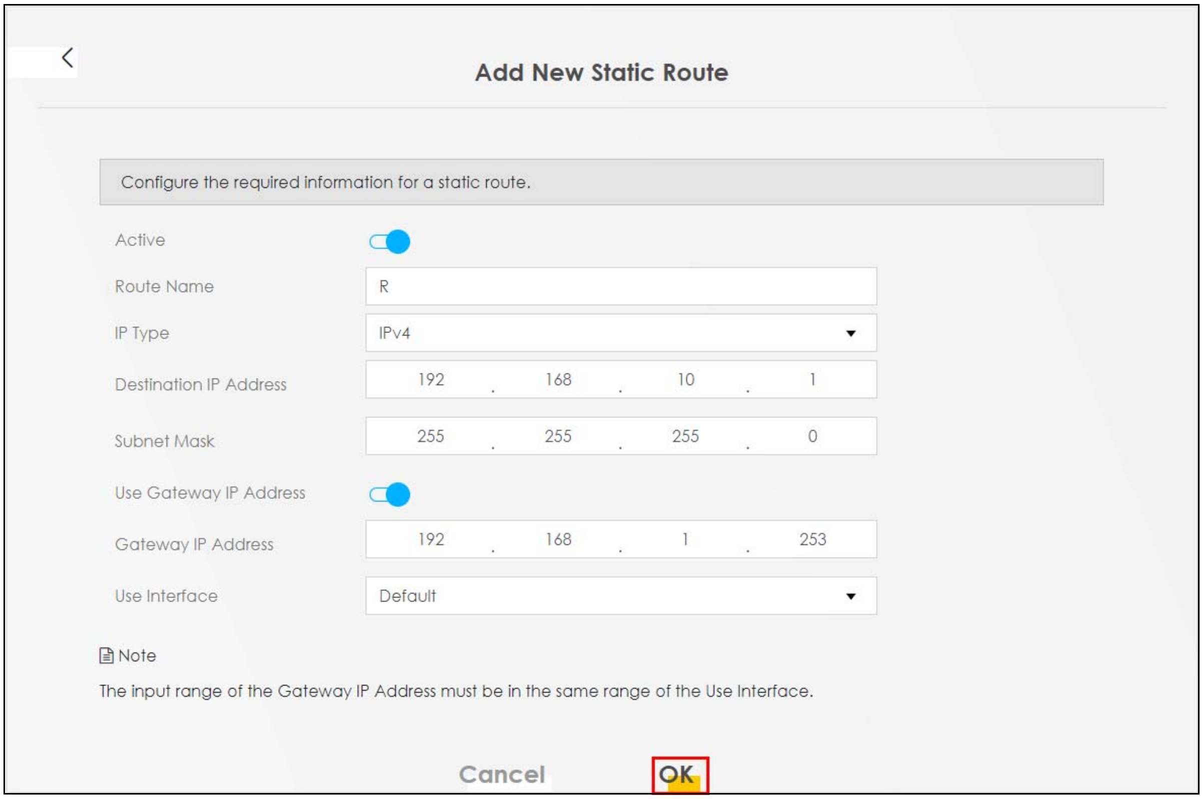
The purpose of a Static Route is to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

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

4 Configure the **Static Route Setup** screen using the following settings:

- Click the **Active** button to enable this static route. When the switch goes to the right, the function is enabled. Enter the **Route Name** as **R**.
- Set **IP Type** to **IPv4**.
- Enter the **Destination IP Address 192.168.10.1** and **IP Subnet Mask 255.255.255.0** for the destination, **N2**.
- Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right, the function is enabled. Enter **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
- Select **Default** as the **Use Interface**.
- Click **OK**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.



Configure the required information for a static route.

Active	●
Route Name	R
IP Type	IPv4
Destination IP Address	192 . 168 . 10 . 1
Subnet Mask	255 . 255 . 255 . 0
Use Gateway IP Address	●
Gateway IP Address	192 . 168 . 1 . 253
Use Interface	Default

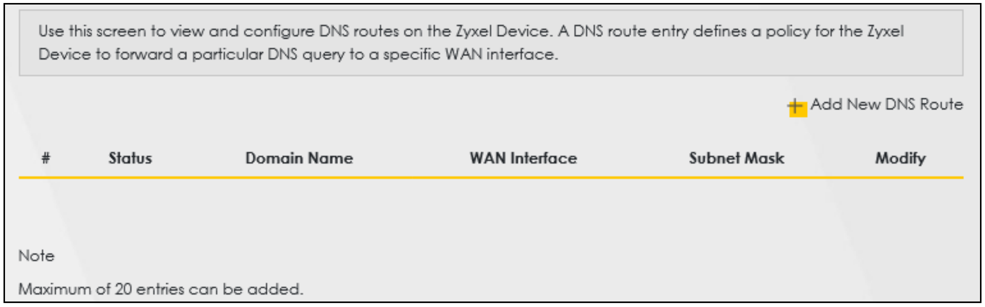
Note

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

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 97 Network Setting > Routing > 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.

#	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 46 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.

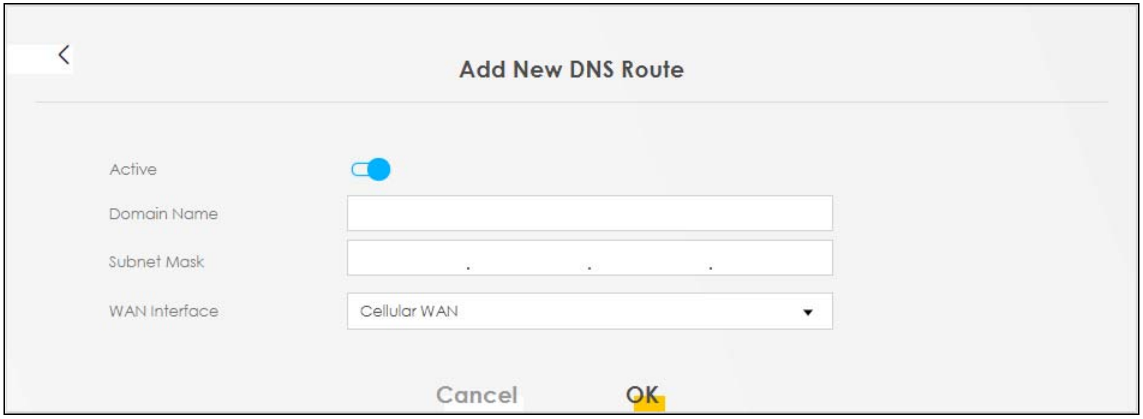
Table 46 Network Setting > Routing > DNS Route (continued)

LABEL	DESCRIPTION
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Subnet Mask	This parameter specifies the IP network subnet mask.
Modify	Click the **Edit** icon to configure a DNS route on the Zyxel Device. Click the **Delete** icon to remove a DNS route from the Zyxel Device.

10.3.1 Add or Edit DNS Route

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **DNS Route** screen, use this screen to configure the required information for a DNS route.

Figure 98 Network Setting > Routing > DNS Route > Add New DNS Route



The following table describes the labels in this screen.

Table 47 Network Setting > Routing > DNS Route > Add New DNS Route

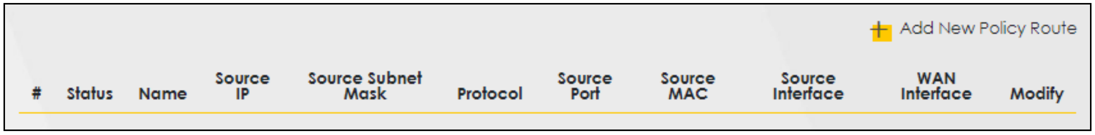
LABEL	DESCRIPTION
Active	Enable DNS route in your Zyxel Device.
Domain Name	Enter the domain name you want to resolve. You can use up to 64 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Zyxel Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
Subnet Mask	Enter the subnet mask of the network for which to use the DNS route in dotted decimal notation, for example 255.255.255.255.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interfaces already configured in the **Broadband** screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

10.4 Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address. For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.

The **Policy Route** screen let you view and configure routing policies on the Zyxel Device. Click **Network Setting** > **Routing** > **Policy Route** to open the following screen.

Figure 99 Network Setting > Routing > Policy Route



The following table describes the labels in this screen.

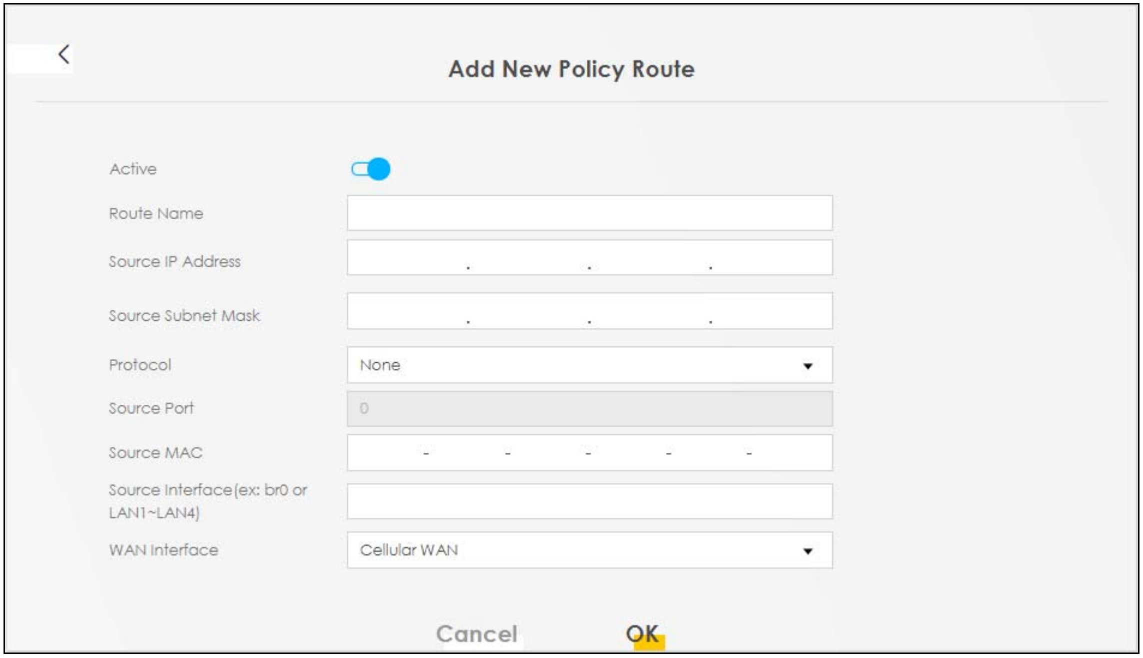
Table 48 Network Setting > Routing > Policy Route

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 or Edit Policy Route

Click **Add New Policy Route** in the **Policy Route** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 100 Network Setting > Routing > Policy Route: Add or 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

The following table describes the labels in this screen.

Table 49 Network Setting > Routing > Policy Route: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this policy route. Otherwise, click to disable.
Route Name	Enter a descriptive name of this policy route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP**, **UDP, or None**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (example: br0 or LAN1 – LAN4)	Enter the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interfaces already configured in the **Broadband** screens.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

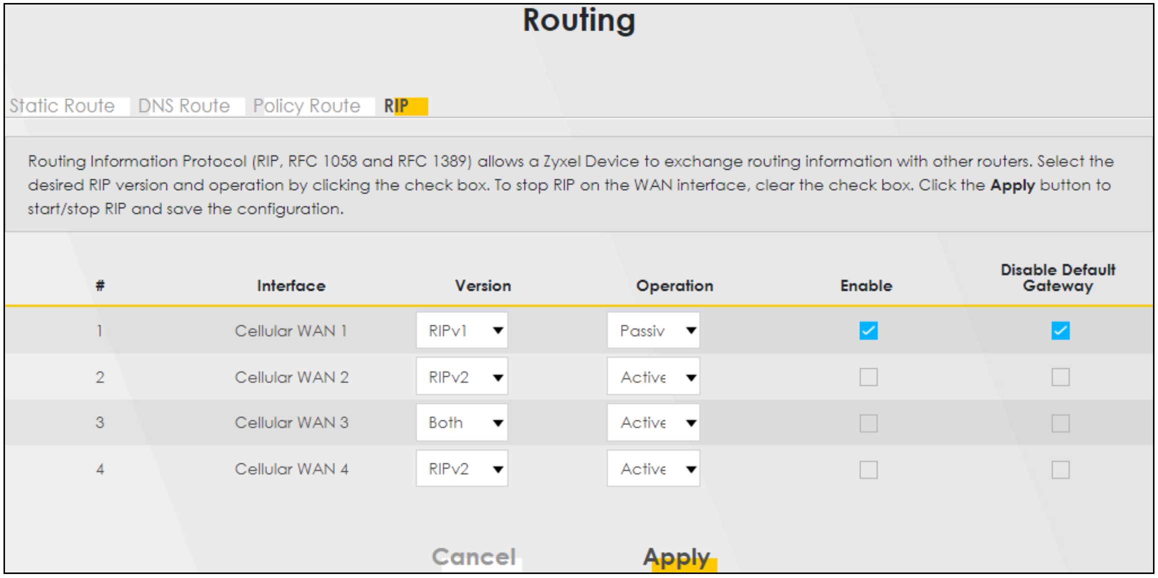
10.5 RIP Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows the Zyxel Device to exchange routing information with other routers. To activate RIP for the WAN interface, select the supported RIP version and operation.

10.5.1 RIP

Click **Network Setting** > **Routing** > **RIP** to open the **RIP** screen. Select the desired RIP version and operation by clicking the check box. To stop RIP on the WAN interface, clear the check box. Click the **Apply** button to start or stop RIP and save the configuration.

Figure 101 Network Setting > Routing > 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	□	□

The following table describes the labels in this screen.

Table 50 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). **RIPv1** is universally supported but **RIPv2** carries more information. **RIPv1** is probably adequate for most networks, unless you have an unusual network topology. When set to **Both**, the Zyxel Device will broadcast its routing table periodically and incorporate the RIP information that it receives
Operation	Select **Passive** to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the 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 NAT Overview

NAT (Network Address Translation – NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

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 150).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings (Section 11.3 on page 153).
- Use the **DMZ** screen to configure a default server (Section 11.4 on page 156).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 11.5 on page 157).

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

Use **Port Forwarding** to forward incoming service requests from the Internet to the servers on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

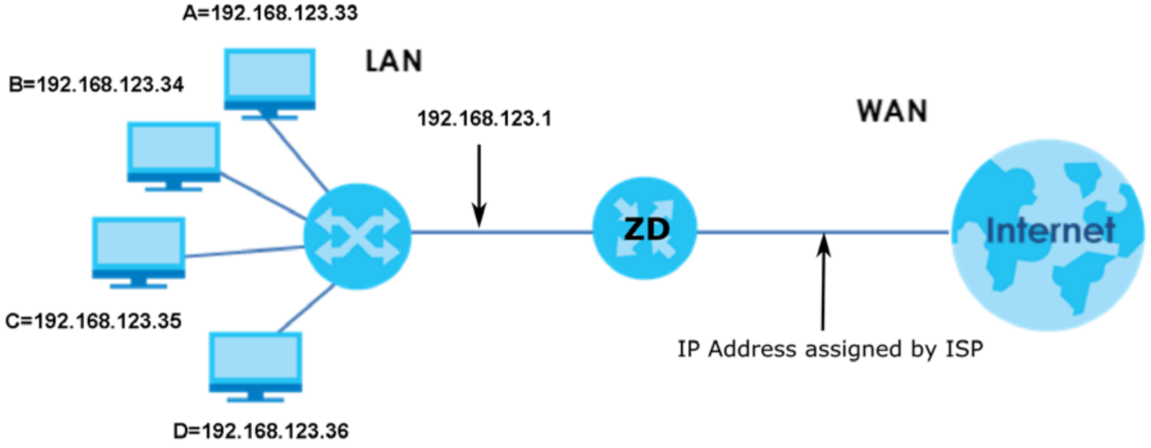
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more 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's 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 102 Multiple Servers Behind NAT Example

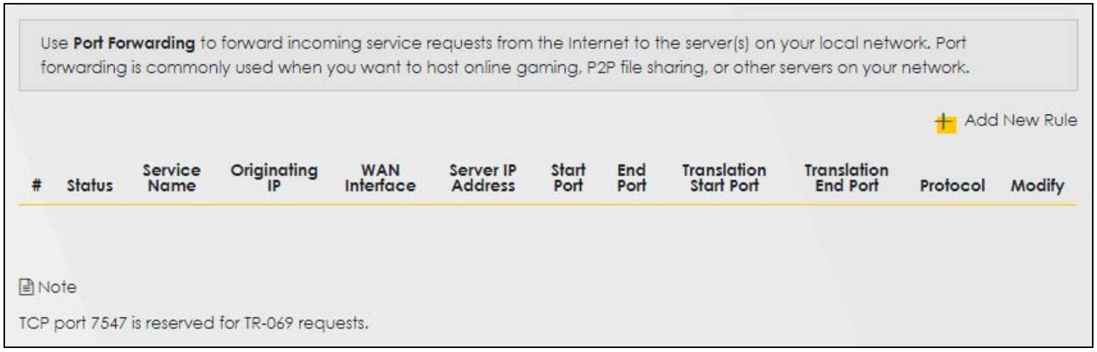


11.2.1 Port Forwarding

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

Note: TCP port 7547 is reserved for system use.

Figure 103 Network Setting > NAT > Port Forwarding


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.

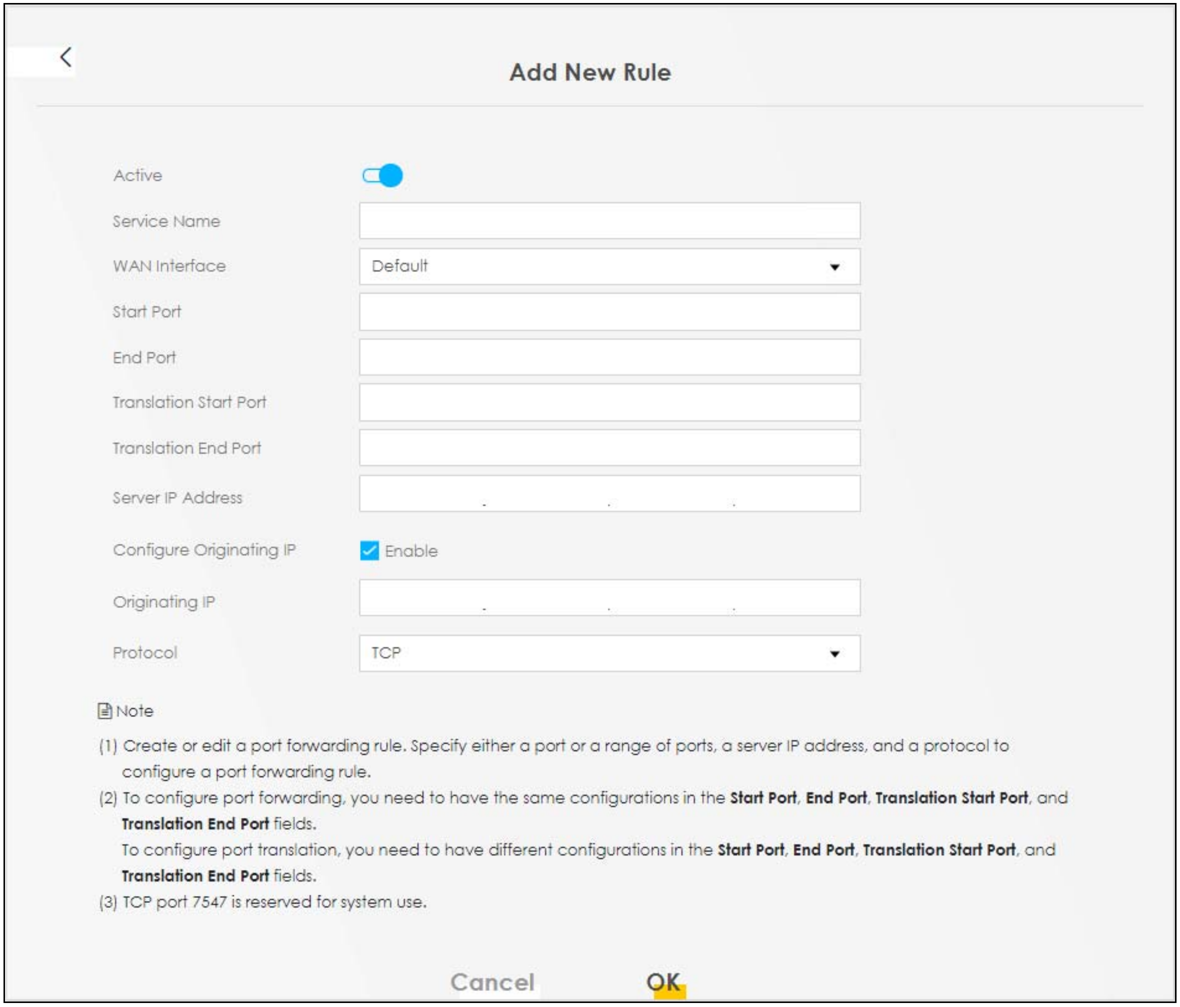
Table 51 Network Setting > NAT > Port Forwarding

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 or Edit Port Forwarding

Create or edit a port forwarding rule. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule. Click **Add New Rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 104 Network Setting > NAT > Port Forwarding: Add or 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
Originating IP	. . .
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.
Here is an example to configure port translation. Configure **Start Port** to 100, **End Port** to 120, **Translation Start Port** to 200, and **Translation End Port** to 220.

Note: TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 52 Network Setting > NAT > Port Forwarding: Add or Edit

LABEL	DESCRIPTION
Active	Click to turn the port forwarding rule on or off.
Service Name	Enter a name for the service to forward. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.

Table 52 Network Setting > NAT > Port Forwarding: Add or Edit (continued)

LABEL	DESCRIPTION
Start Port	Configure this for a user-defined entry. Enter the original destination port for the packets. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Configure this for a user-defined entry. Enter the last port of the original destination port range. To forward only one port, enter the port number in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Translation Start Port	Configure this for a user-defined entry. This shows the port number to which you want the Zyxel Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	Configure this for a user-defined entry. This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Configure Originating IP	Click the **Enable** check box to enter the source IP in the next field.
Originating IP	Enter the source IP address here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

11.3 Port Triggering

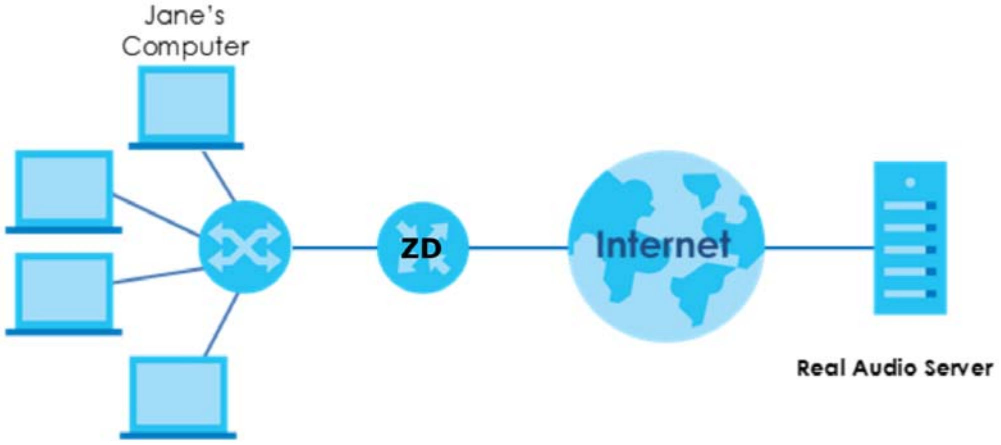
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem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

For example:

Figure 105 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970 – 7170.

3 The Real Audio server responds using a port number ranging between 6970 – 7170.

4 The Zyxel Device forwards the traffic to Jane's computer IP address.

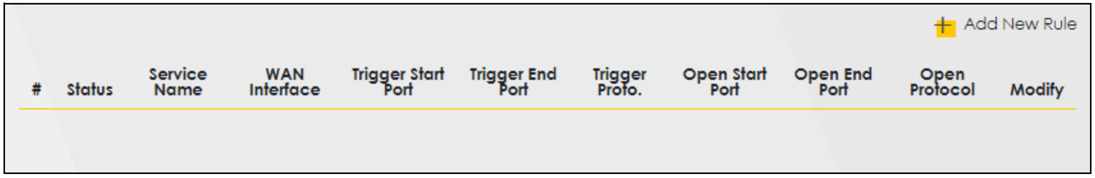
5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in 3 minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting** > **NAT** > **Port Triggering** to open the following screen. Use this screen to view your Zyxel Device's trigger port settings.

Note: TCP port 7547 is reserved for system use.

Note: The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.

Figure 106 Network Setting > NAT > Port Triggering



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

The following table describes the labels in this screen.

Table 53 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.

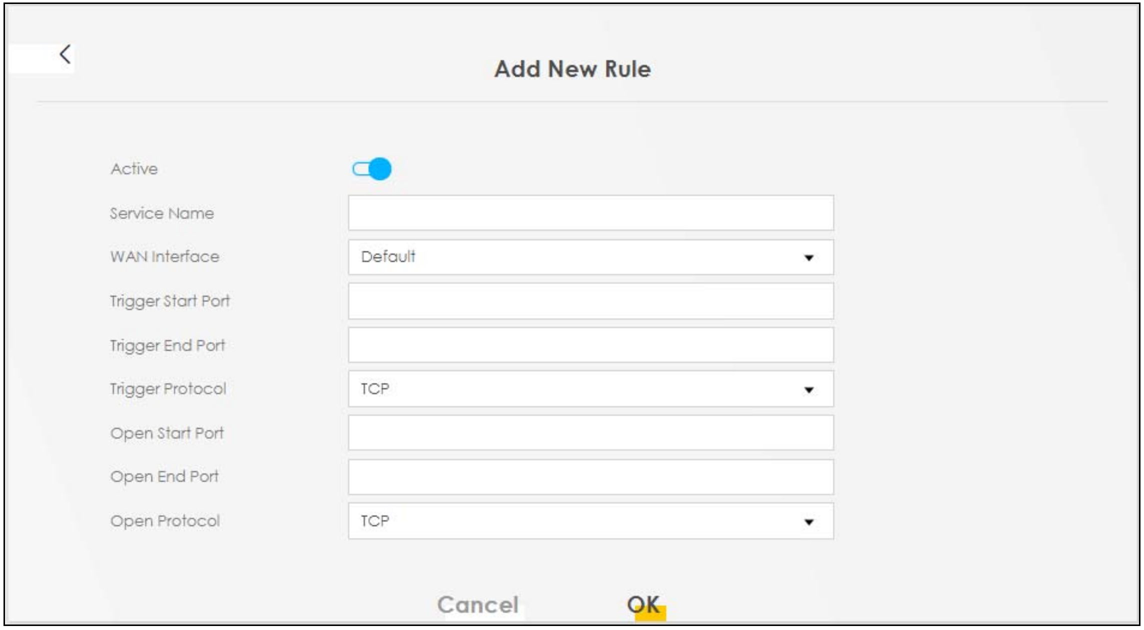
Table 53 Network Setting > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
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 or Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add New Rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen. Use this screen to configure a port or range of ports and protocols for sending out requests and for receiving responses.

Figure 107 Network Setting > NAT > Port Triggering: Add or 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 54 Network Setting > NAT > Port Triggering: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this rule.
Service Name	Enter a name to identify this rule. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter a port number or the starting port number in a range of port numbers.
Trigger End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Enter a port number or the starting port number in a range of port numbers.
Open End Port	Enter a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

11.4 DMZ

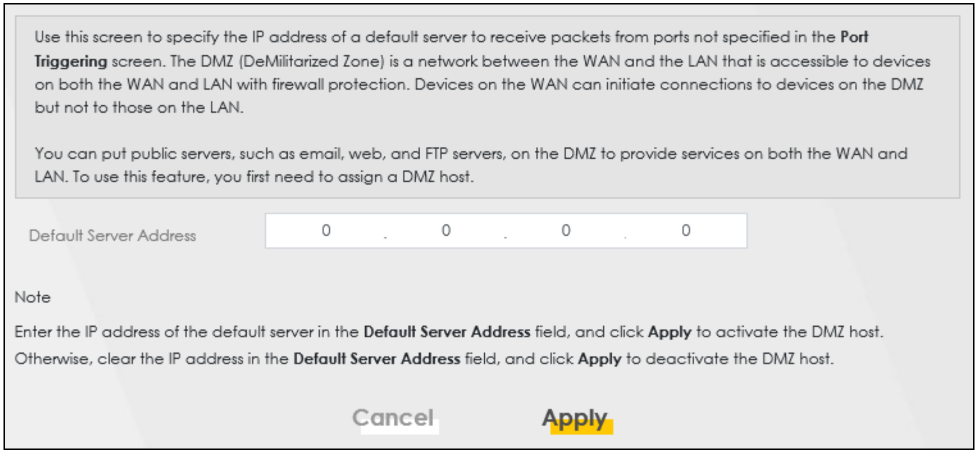
Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (DeMilitarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on 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. 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 108 Network Setting > NAT > 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.

Default Server Address: 0 . 0 . 0 . 0

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.

The following table describes the fields in this screen.

Table 55 Network Setting > NAT > DMZ

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

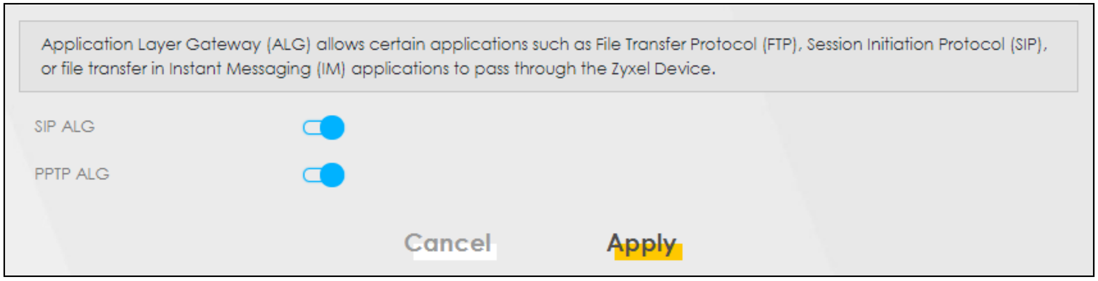
11.5 ALG

Application Layer Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain applications such as File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications. It allows SIP calls to pass through the Zyxel Device. When the Zyxel Device registers with the SIP register server, the SIP ALG translates the Zyxel Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Zyxel Device is behind a SIP ALG.

Click **Network Setting** > **NAT** > **ALG** to open the **ALG** screen. Use this screen to enable and disable the NAT Application Layer Gateway (ALG) in the Zyxel Device.

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

Figure 109 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.

The following table describes the fields in this screen.

Table 56 Network Setting > NAT > ALG

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

11.6 Technical Reference

This part contains more information regarding NAT.

11.6.1 NAT Definitions

Inside or outside denotes where a host is located relative to the Zyxel Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global or local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside or outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 57 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

11.6.2 What NAT Does

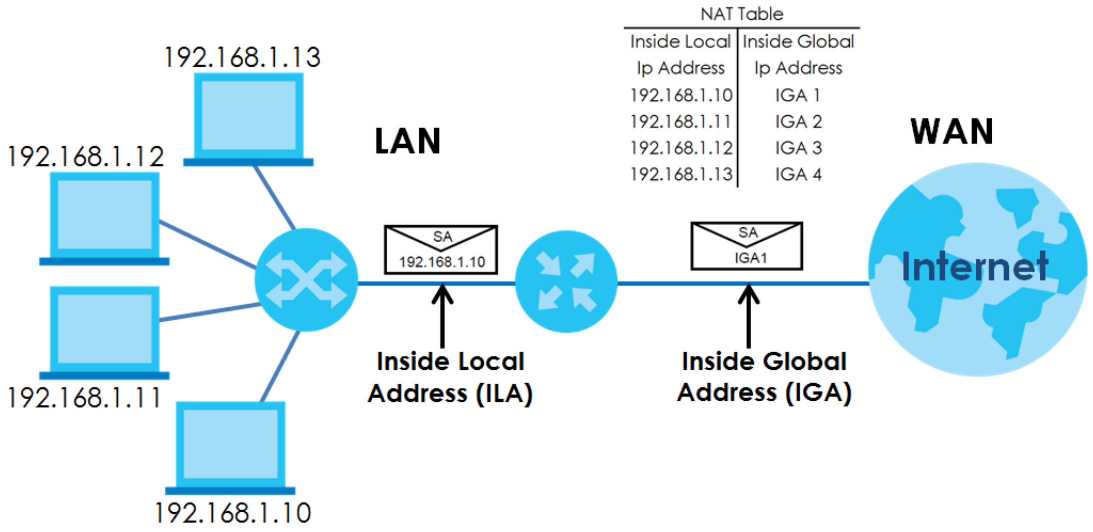
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Zyxel Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

11.6.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Zyxel Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 110 How NAT Works



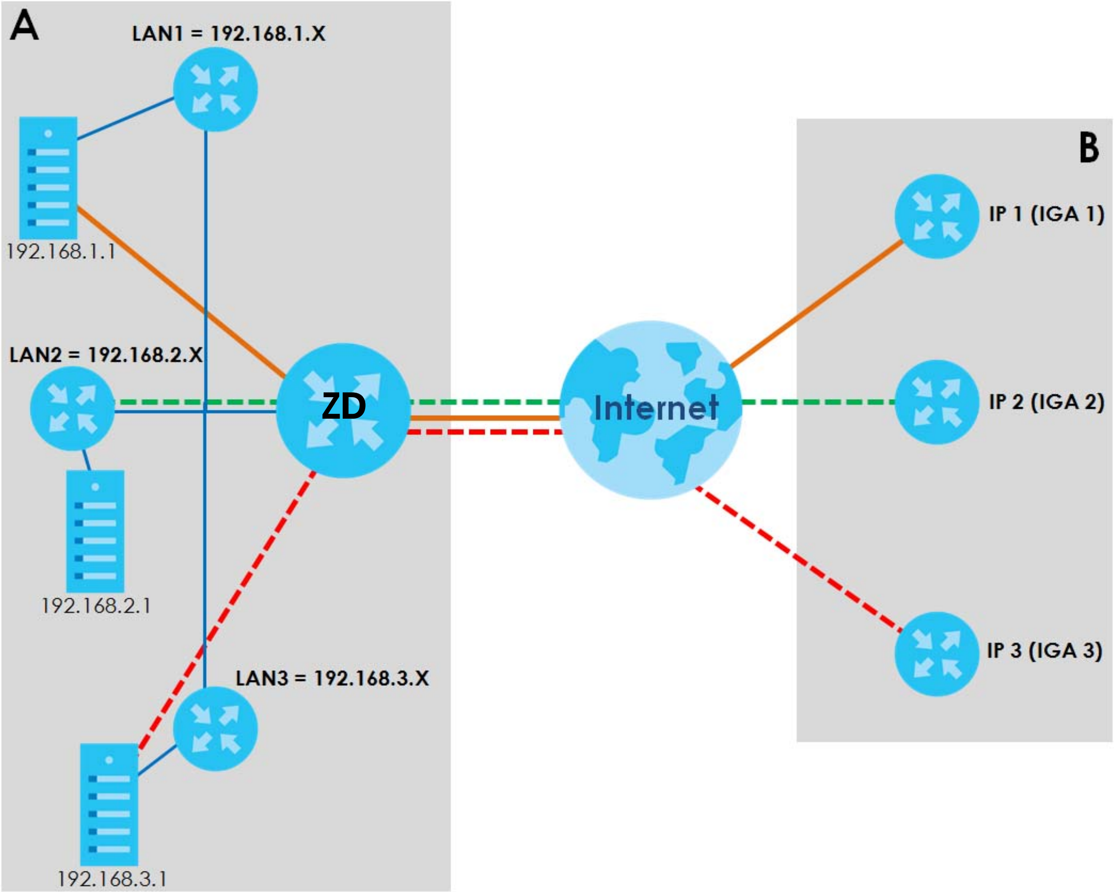
NAT Table

Inside Local Ip Address	Inside Global Ip Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

11.6.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the Zyxel Device can communicate with three distinct WAN networks.

Figure 111 NAT Application With IP Alias



Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 58 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110

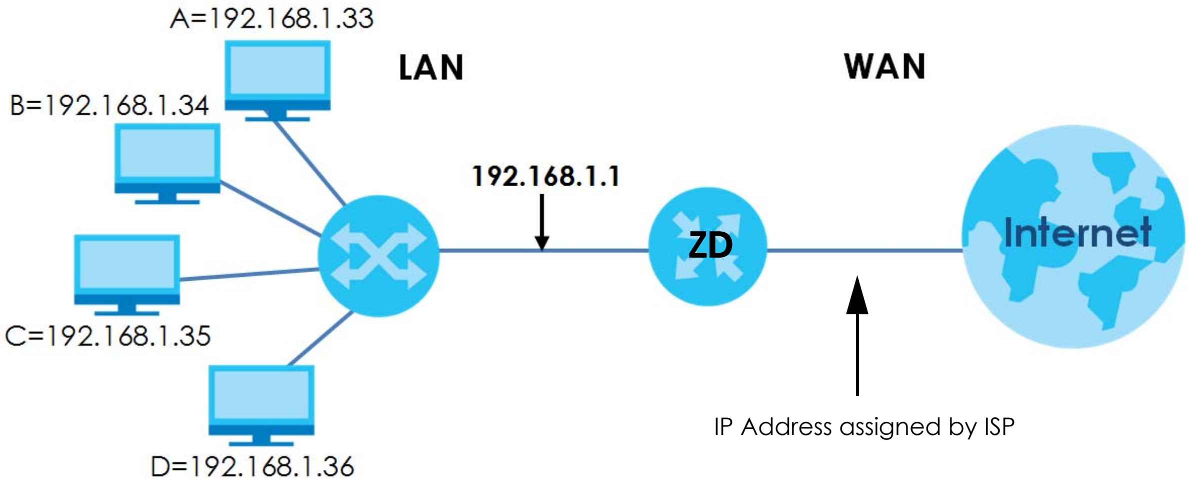
Table 58 Services and Port Numbers (continued)

SERVICES	PORT NUMBER
NNTP (Network News Transport Protocol)	119
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21 – 25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 112 Multiple Servers Behind NAT Example



CHAPTER 12
DNS

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 servers, each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. The Zyxel Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Zyxel Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). 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 163).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device (Section 12.3 on page 164).

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.

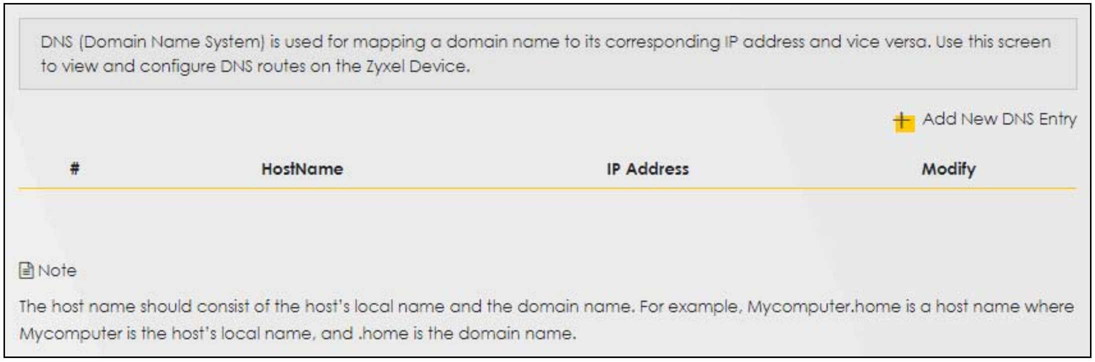
If you have a private WAN IP address, then you cannot use Dynamic DNS.

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 manual DNS entires on the Zyxel Device. Click **Network Setting** > **DNS** to open the **DNS Entry** screen.

Note: The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.

Figure 113 Network Setting > DNS > 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.

#	HostName	IP Address	Modify

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.

The following table describes the fields in this screen.

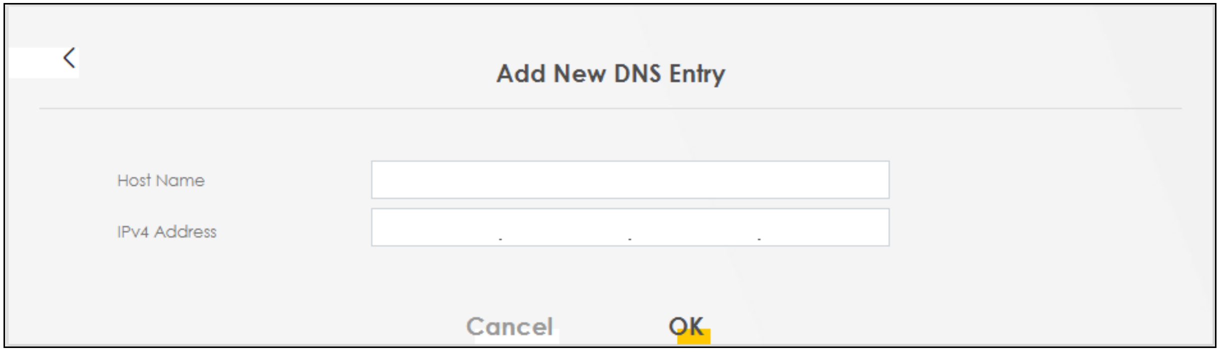
Table 59 Network Setting > DNS > DNS Entry

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 or Edit DNS Entry

You can manually add or edit the Zyxel Device's DNS name and IP address entry. Click **Add New DNS Entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 114 Network Setting > DNS > DNS Entry: Add or Edit



The following table describes the labels in this screen.

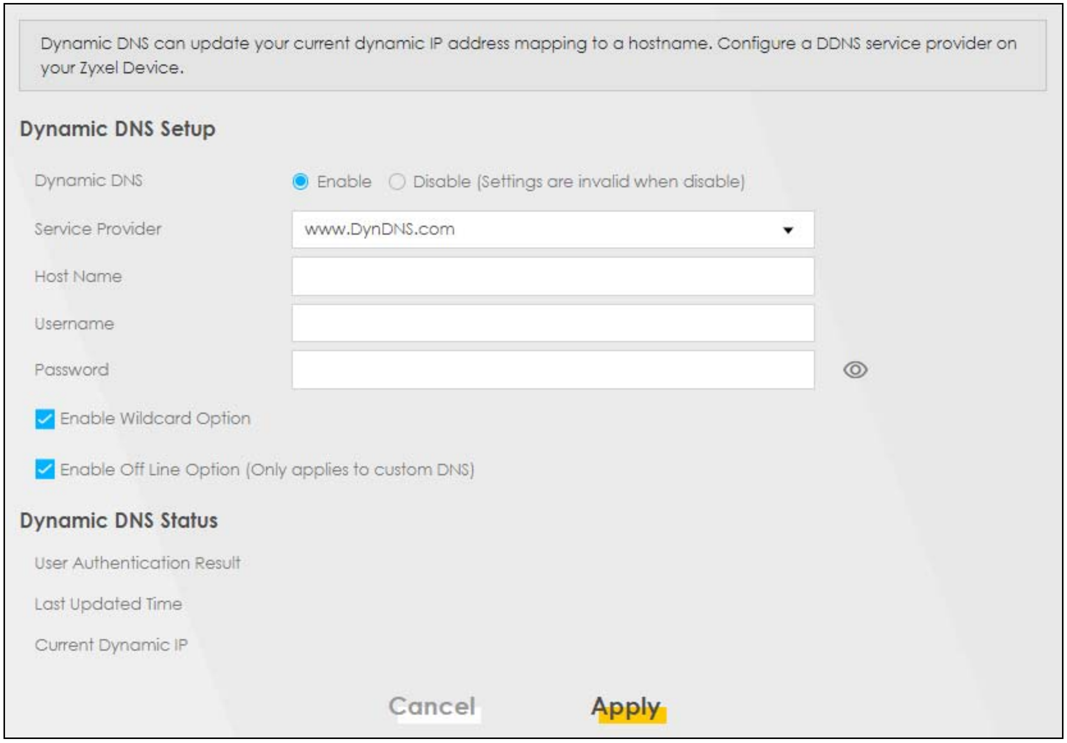
Table 60 Network Setting > DNS > DNS Entry: Add or Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com.
IPv4 Address	Enter the IPv4 address of the DNS entry.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

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 115 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 61 Network Setting > DNS > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Enter the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the 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.

Table 61 Network Setting > DNS > Dynamic DNS (continued)

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

CHAPTER 13 VLAN Group

13.1 VLAN Group Overview

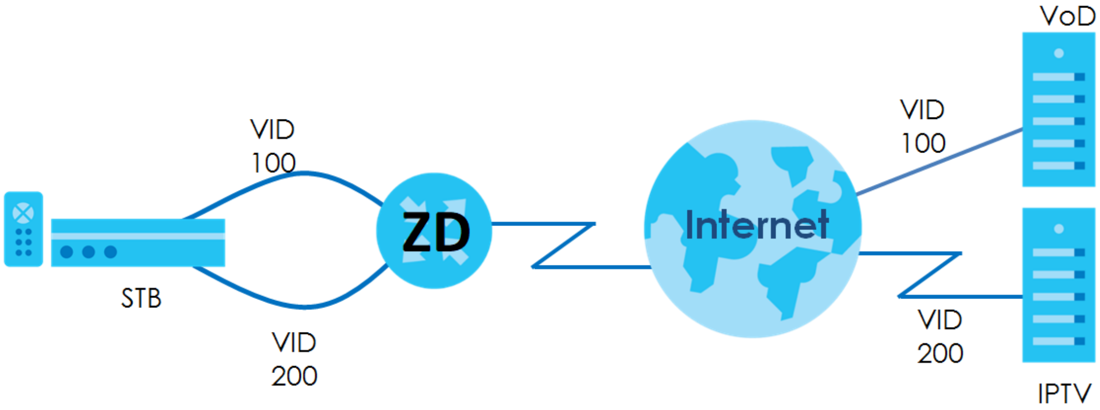
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same groups;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

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. Shared resources such as a server can be used by all ports in the same VLAN as the server. Ports can belong to other VLAN groups too. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges. The VLAN ID associates a frame with a specific VLAN and provides the information that switches the need to process the frame across the network.

In the following example, VLAN IDs (VIDs) 100 and 200 are added to identify Video-on-Demand and IPTV traffic respectively coming from the VoD and IPTV multicast servers. The Zyxel Device can also tag outgoing requests to the servers with these VLAN IDs.

Figure 116 VLAN Group Example



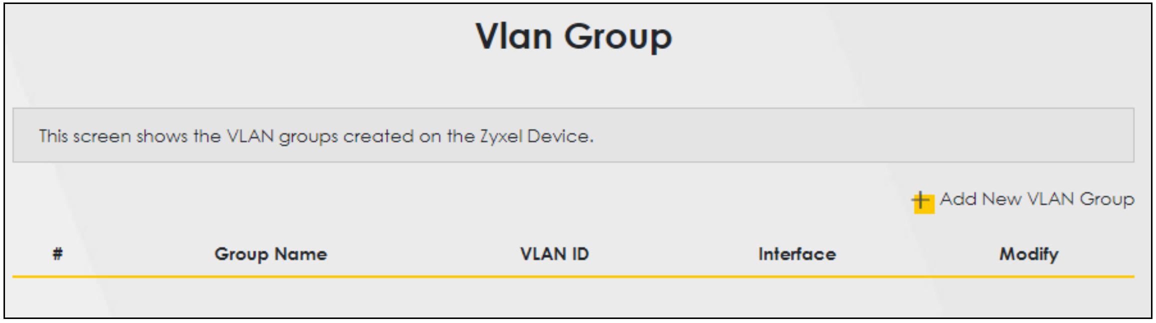
13.1.1 What You Can Do in this Chapter

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 117 Network Setting > VLAN Group



Vlan Group

This screen shows the VLAN groups created on the Zyxel Device.

#	Group Name	VLAN ID	Interface	Modify

The following table describes the fields in this screen.

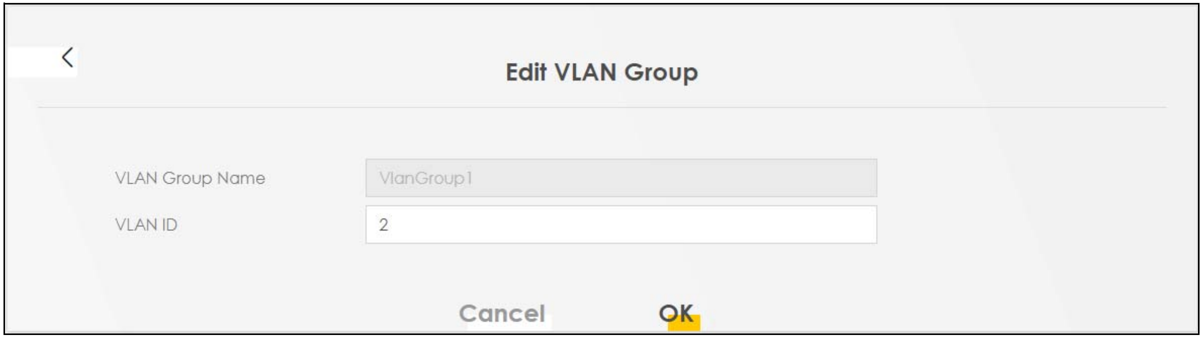
Table 62 Network Setting > VLAN Group

LABEL	DESCRIPTION
Add New VLAN Group	Click this button to create a new VLAN group.
#	This is the index number of the VLAN group.
Group Name	This shows the descriptive name of the VLAN group.
VLAN ID	This shows the unique ID number that identifies the VLAN group.
Interface	This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID.
Modify	Click the **Edit** icon to change an existing VLAN group setting or click the **Delete** icon to remove the VLAN group.

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 118 Network Setting > VLAN Group > Add New VLAN Group/Edit



Edit VLAN Group

VLAN Group Name: VlanGroup1

VLAN ID: 2

The following table describes the fields in this screen.

Table 63 Network Setting > VLAN Group > Add New VLAN Group/Edit

LABEL	DESCRIPTION
VLAN Group Name	Enter a name to identify this group. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify 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 170).

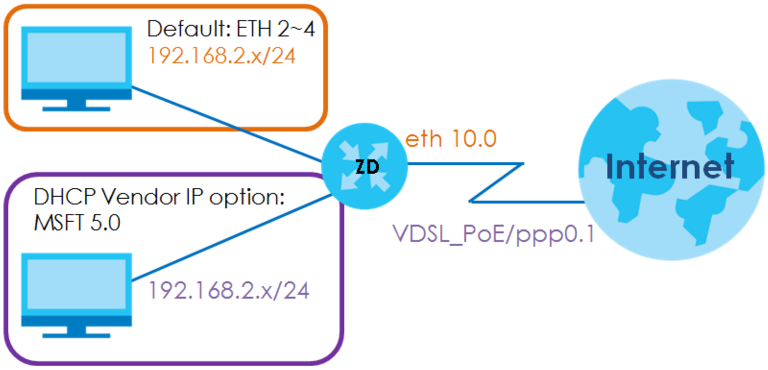
14.2 Interface Grouping

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 Chapter 9 on page 114 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.

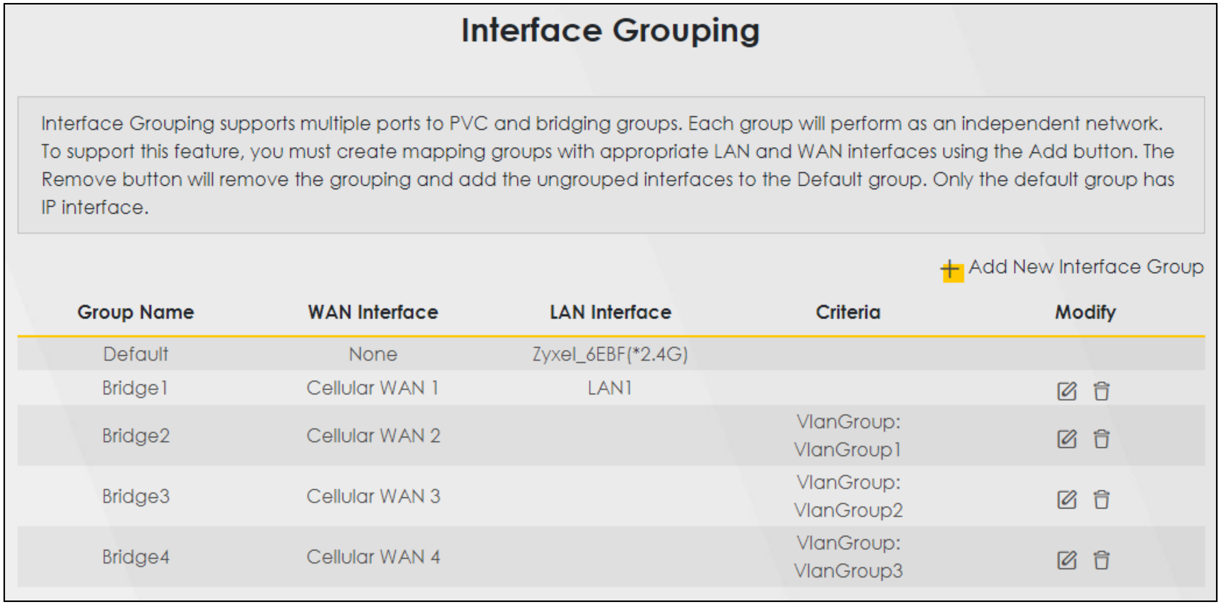
Figure 119 Interface Grouping Application



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 120 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.

+ Add New Interface Group

Group Name	WAN Interface	LAN Interface	Criteria	Modify
Default	None	Zyxel_6EBF(*2.4G)		
Bridge1	Cellular WAN 1	LAN1		✎ 🗑
Bridge2	Cellular WAN 2		VlanGroup: VlanGroup1	✎ 🗑
Bridge3	Cellular WAN 3		VlanGroup: VlanGroup2	✎ 🗑
Bridge4	Cellular WAN 4		VlanGroup: VlanGroup3	✎ 🗑

The following table describes the fields in this screen.

Table 64 Network Setting > Interface Grouping

LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Modify	Click the **Edit** icon to modify an existing Interface group setting or click the **Delete** icon to remove the Interface group.

14.2.1 Interface Group Configuration

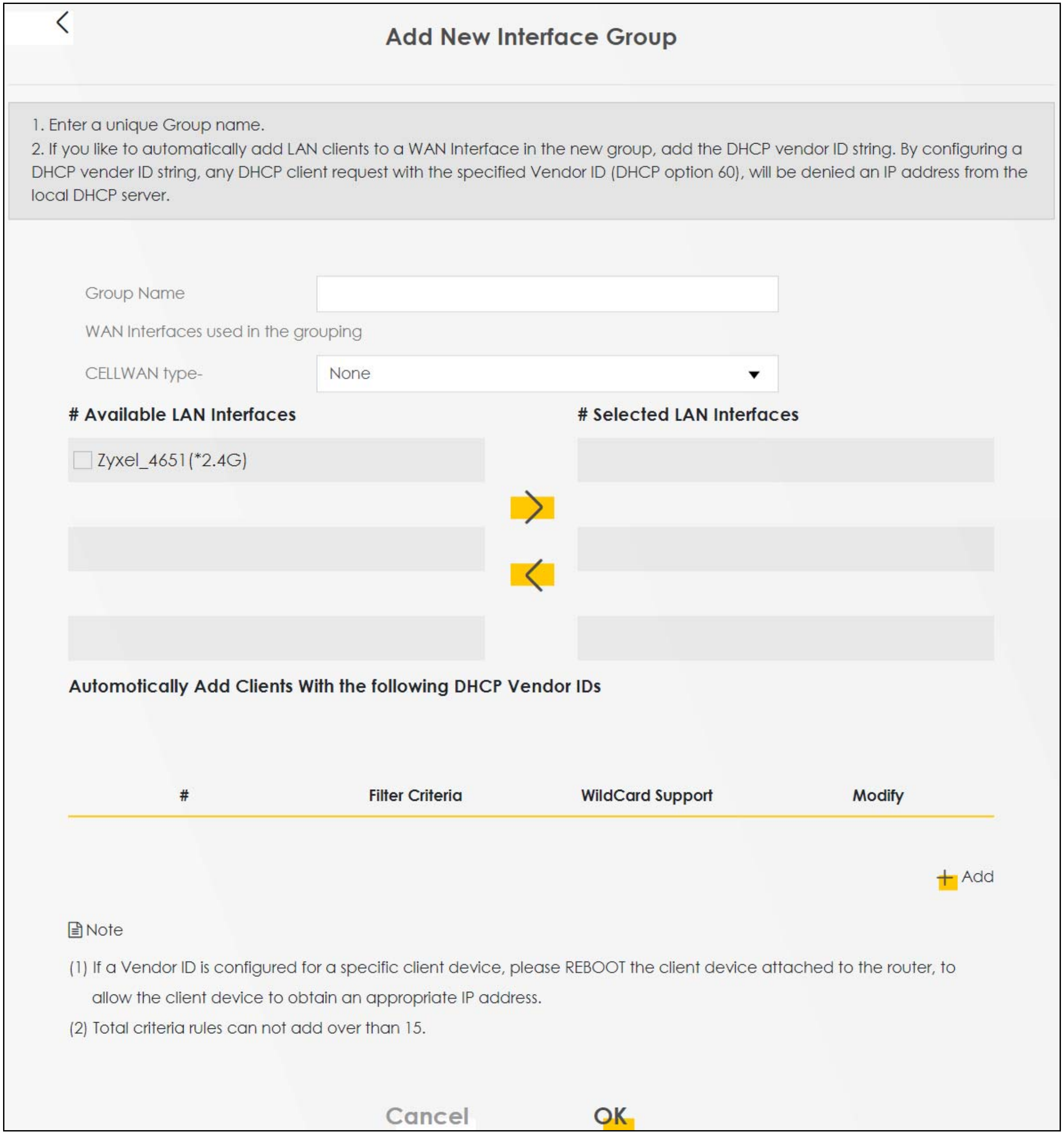
Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group. If you want to automatically add LAN clients to a new group, use filtering criteria.

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 121 Network Setting > Interface Grouping > Add New Interface Group/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

CELLWAN type- None

Available LAN Interfaces

□ Zyxel_4651(*2.4G)

Selected LAN Interfaces

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 65 Network Setting > Interface Grouping > Add New Interface Group/Edit

LABEL	DESCRIPTION
Group Name	Enter a descriptive name for this interface group. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface. Select **None** to not add a WAN interface to this group.

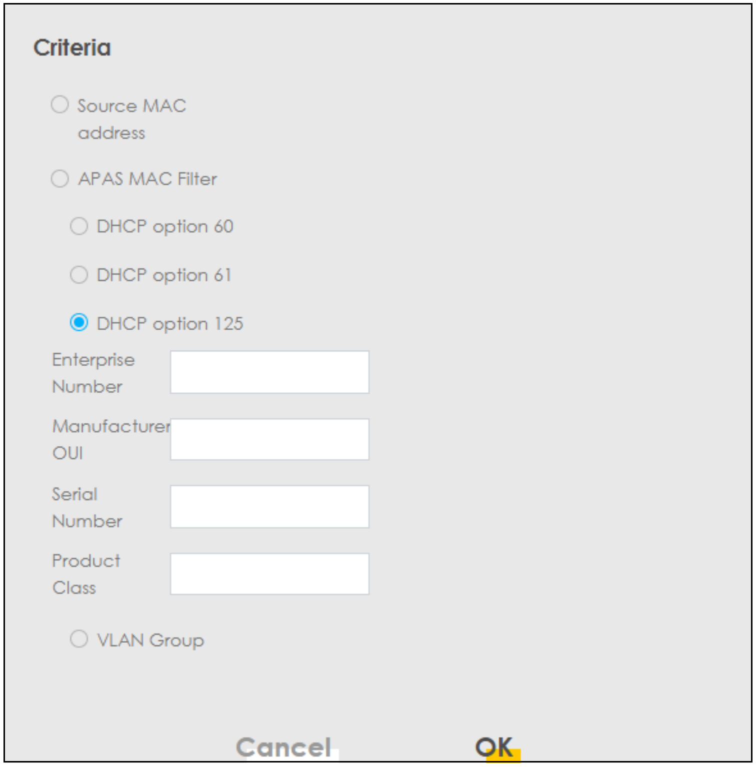
Table 65 Network Setting > Interface Grouping > Add New Interface Group/Edit (continued)

LABEL	DESCRIPTION
CELLWAN type	Use **Available LAN Interfaces** to group LAN interfaces with the WAN interface you select here: **Cellular WAN 1** (APN 1), **Cellular WAN 2** (APN 2), **Cellular WAN 3** (APN 3) or **Cellular WAN 4** (APN 4). A LAN interface can only be grouped with a single WAN interface. The **Cellular WAN** interfaces are configured in the **Network Setting** > **Broadband** screen.
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 173 for more information.
#	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 122 Network Setting > Interface Grouping > Interface Group Configuration: Add



Criteria

○ Source MAC address

○ APAS MAC Filter

○ DHCP option 60

○ DHCP option 61

● DHCP option 125

Enterprise Number

Manufacturer OUI

Serial Number

Product Class

○ VLAN Group

The following table describes the fields in this screen.

Table 66 Network Setting > Interface Grouping > Interface Group Configuration: Add

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 Firewall Overview

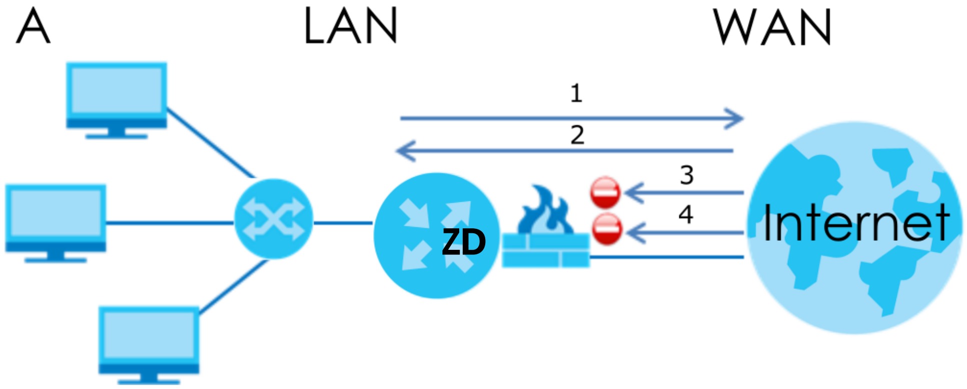
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

By default, the Zyxel Device blocks DoS attacks whether the firewall is enabled or disabled.

The following figure illustrates the firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 123 Default Firewall Action



15.1.1 What You Need to Know About Firewall

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denial-of-Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Zyxel Device is pre-configured to automatically detect and thwart all known DoS attacks.

DoS Thresholds

For DoS attacks, the Zyxel Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

DDoS

A Distributed Denial-of-Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a ‘ping’ utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

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

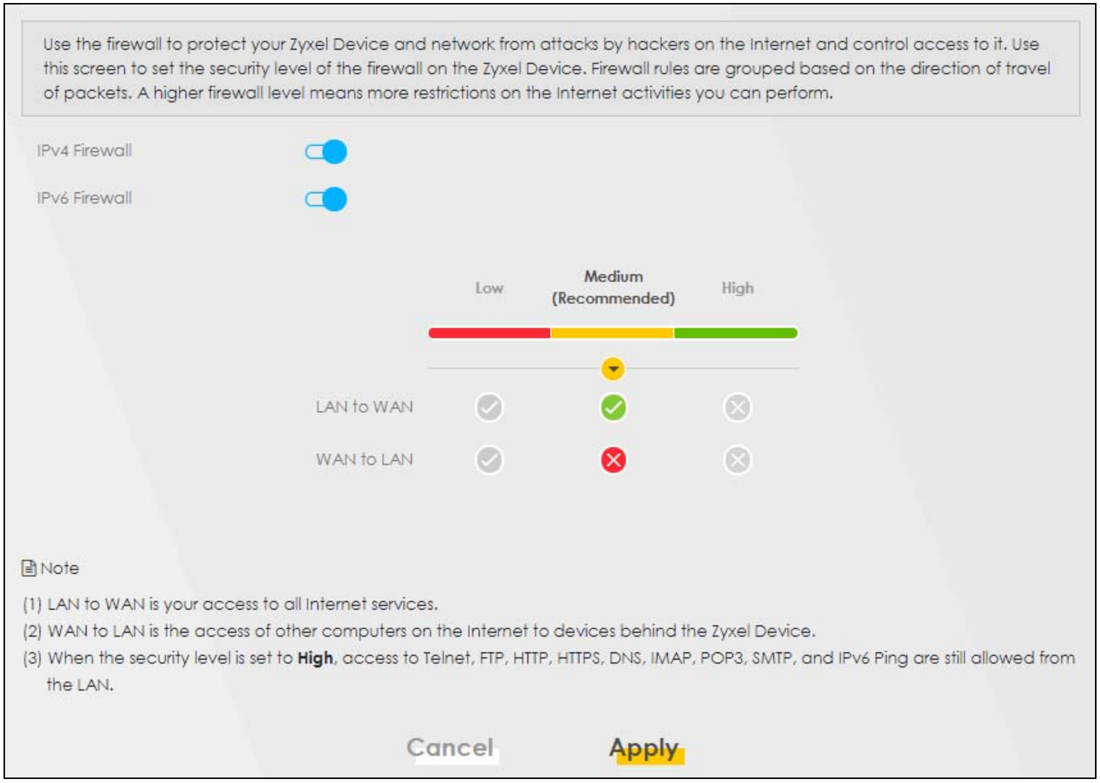
- Use the **General** screen to configure the security level of the firewall on the Zyxel Device (Section 15.3 on page 177).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 15.4 on page 178).

- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules (Section 15.5 on page 179).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 15.6 on page 182).

15.3 Firewall General Settings

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets. A higher firewall level means more restrictions on the Internet activities you can perform. Click **Security** > **Firewall** > **General** to display the following screen. Use the slider to select the level of firewall protection.

Figure 124 Security > Firewall > General



Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets. A higher firewall level means more restrictions on the Internet activities you can perform.

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 67 Security > Firewall > General

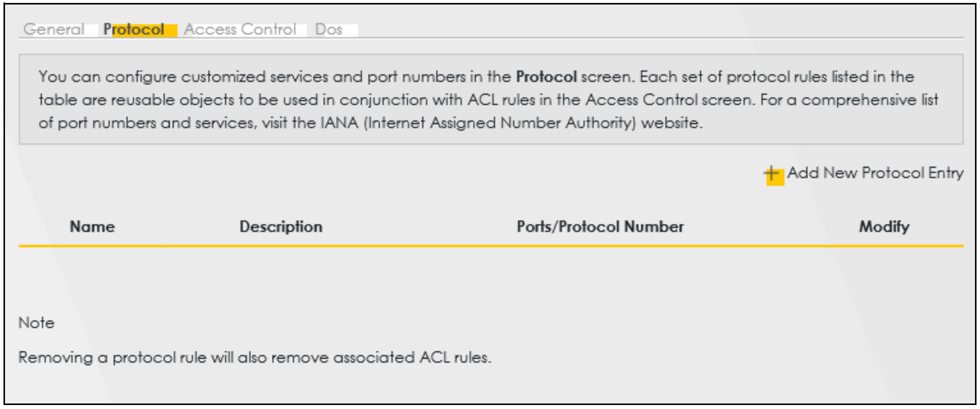
LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using **IPv4** (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using **IPv6** (Internet Protocol version 6).
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, FTP, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.
Medium	This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.
Low	This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

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 125 Security > Firewall > Protocol



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.

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 68 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to configure a customized service.
Name	This is the name of your customized service.
Description	This is a description of your customized service.

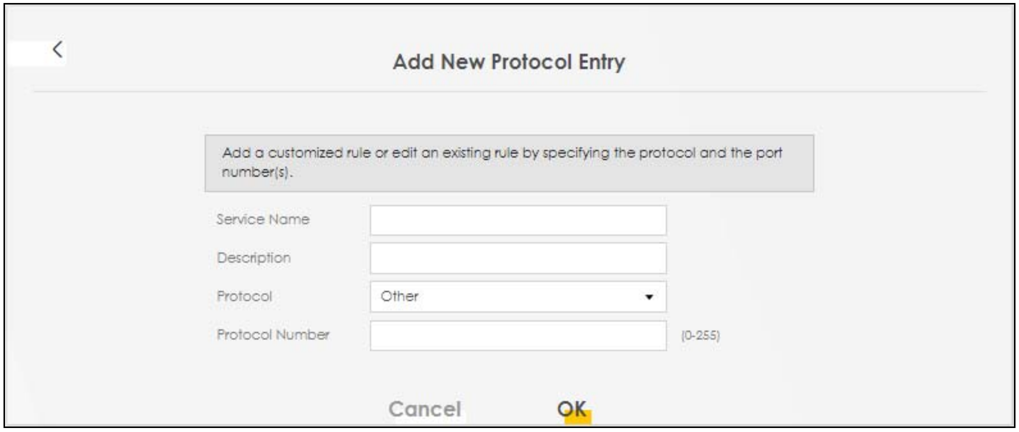
Table 68 Security > Firewall > Protocol (continued)

LABEL	DESCRIPTION
Ports/Protocol Number	This shows the port number or range and the IP protocol (**TCP** or **UDP**) that defines your customized service.
Modify	Click this to edit a customized service.

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 126 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 69 Security > Firewall > Protocol: Add New Protocol Entry

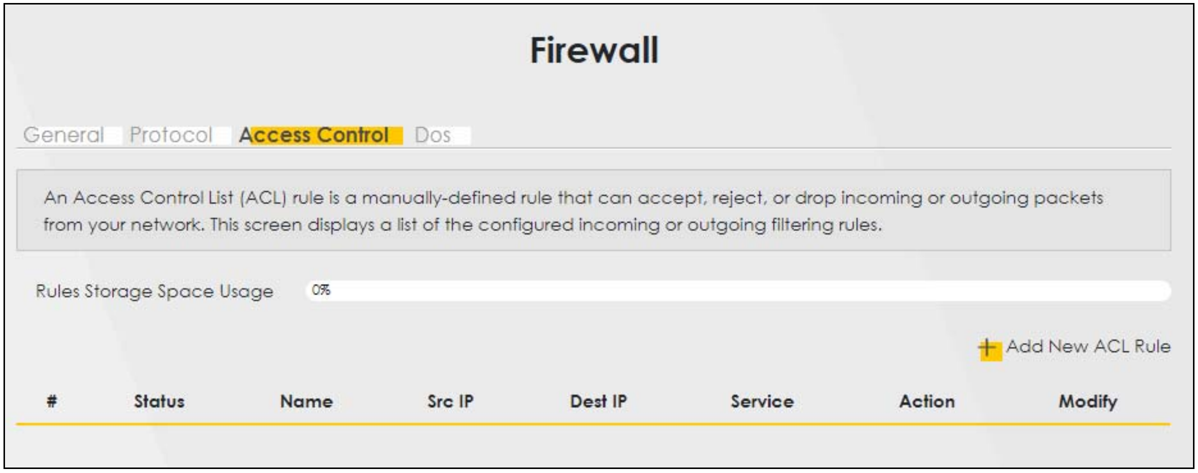
LABEL	DESCRIPTION
Service Name	Enter a descriptive name for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Description	Enter a description for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Protocol	Select the protocol (**TCP**, **UDP**, **ICMP**, **ICMPv6**, or **Other**) that defines your customized port from the drop down list box.
Protocol Number	Enter a single port number or the range of port numbers (**0** – **255**) that define your customized service.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

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 127 Security > Firewall > Access Control



Firewall

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.

Rules Storage Space Usage 0%

#	Status	Name	Src IP	Dest IP	Service	Action	Modify

The following table describes the labels in this screen.

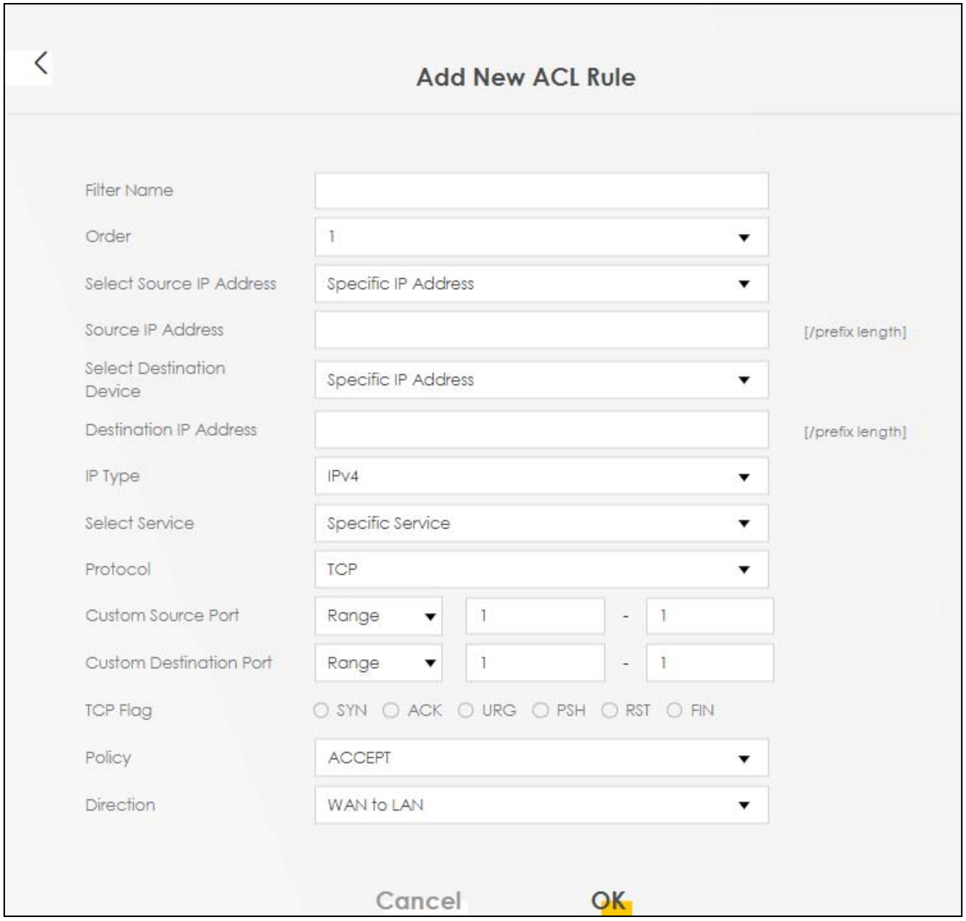
Table 70 Security > Firewall > Access Control

LABEL	DESCRIPTION
Rules Storage Space Usage	This read-only bar shows how much of the Zyxel Device's memory is in use for recording firewall rules. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Add New ACL Rule	Select an index number and click **Add New ACL Rule** to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
#	This field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Name	This field displays the rule name.
Src IP	This field displays the source IP addresses to which this rule applies.
Dest IP	This field displays the destination IP addresses to which this rule applies.
Service	This field displays the protocol (All, TCP, UDP, TCP/UDP, ICMP, ICMPv6, or any) used to transport the packets for which you want to apply the rule.
Action	Displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule.
Modify	Click the **Edit** icon to edit the firewall rule. Click the **Delete** icon to delete an existing firewall rule.

15.5.1 Add New ACL Rule

Click **Add new ACL** rule or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays. Use this screen to accept, reject, or drop packets based on specified parameters, such as source and destination IP address, IP Type, service, and direction. You can also specify a limit as to how many packets this rule applies to at a certain period of time or specify a schedule for this rule.

Figure 128 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	TCP ▼	
Custom Source Port	Range ▼ 1 - 1	
Custom Destination Port	Range ▼ 1 - 1	
TCP Flag	○ SYN ○ ACK ○ URG ○ PSH ○ RST ○ FIN	
Policy	ACCEPT ▼	
Direction	WAN to LAN ▼	

The following table describes the labels in this screen.

Table 71 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name for your filter rule. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Order	Assign the order of your rules as rules are applied in turn.
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**, or **ICMPv6**) used to transport the packets for which you want to apply the rule.

Table 71 Security > Firewall > Access Control > Add New ACL Rule (continued)

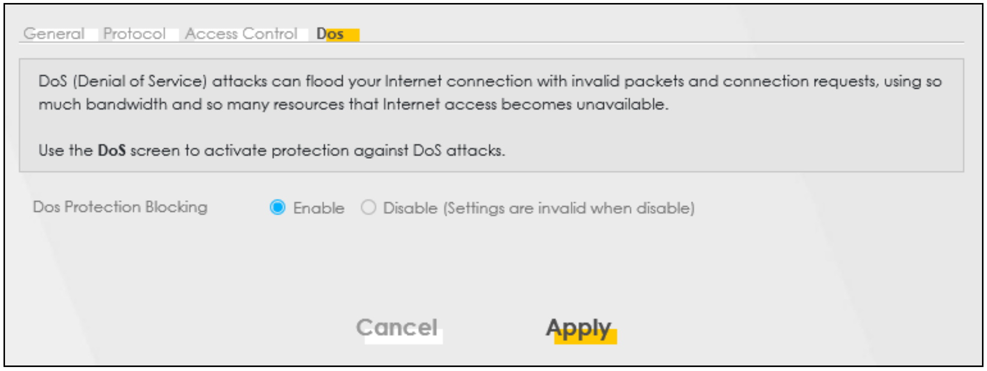
LABEL	DESCRIPTION
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN). This appears when you select **TCP/UDP** or **TCP** in the **Protocol** field.
Policy	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule.
Direction	Select **WAN to LAN** to apply the rule to traffic from WAN to LAN. Select **LAN to WAN** to apply the rule to traffic from LAN to WAN. Select **WAN to Router** to apply the rule to traffic from WAN to router. Select **LAN to Router** to apply the rule to traffic from LAN to router.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

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 129 Security > Firewall > 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.

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

The following table describes the labels in this screen.

Table 72 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Enable this to protect against DoS attacks. The Zyxel Device will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

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 through the Web Configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your router.
4. Don't enable any local service (such as telnet or FTP) that you do not use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

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

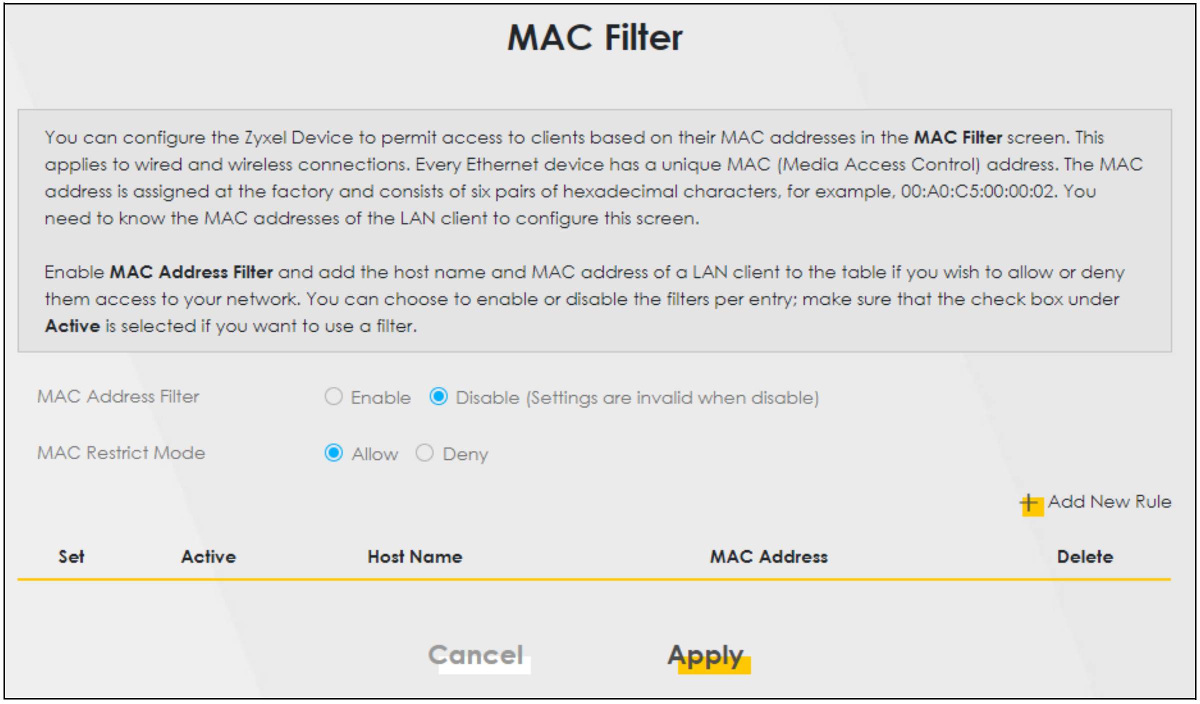
16.1 MAC Filter Overview

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 connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of wired LAN client to configure this screen.

16.2 MAC Filter

Enable **MAC Address Filter** and add the host name and MAC address of a wired LAN client to the table if you wish to allow or deny them access to your network. You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter. Select **Security** > **MAC Filter**. The screen appears as shown.

Figure 130 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 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.

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.

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

MAC Restrict Mode ● Allow ○ Deny

Set	Active	Host Name	MAC Address	Delete

The following table describes the labels in this screen.

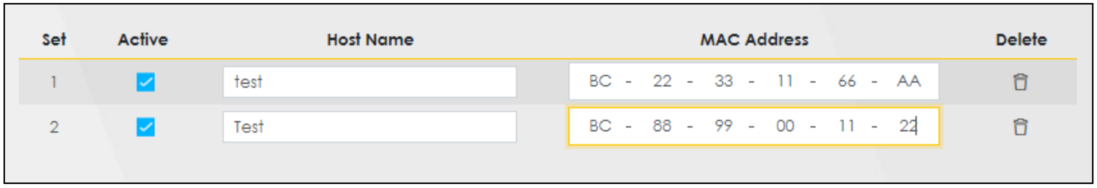
Table 73 Security > MAC Filter

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 the **Add** 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 a wired LAN client that you want to allow access to the Zyxel Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC address of a wired LAN client that you want to allow access to the Zyxel Device. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the **Delete** icon to delete an existing rule.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

16.2.1 Add New Rule

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. Select **Security** > **MAC Filter** > **Add New Rule**. The screen appears as shown.

Figure 131 Security > MAC Filter > Add New Rule



Set	Active	Host Name	MAC Address	Delete
1	☑	test	BC - 22 - 33 - 11 - 66 - AA	🗑
2	☑	Test	BC - 88 - 99 - 00 - 11 - 22	🗑

The following table describes the labels in this screen.

Table 74 Security > MAC Filter > Add New Rule

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
Active	Select **Active** to enable the MAC filter rule. The rule will not be applied if **Allow** is not selected under **MAC Restrict Mode**.
Host Name	Enter the host name of a wired LAN client that you want to allow access to the Zyxel Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC addresses of a wired LAN client that you want to allow access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the **Delete** icon to delete an existing rule.

Table 74   Security > MAC Filter > Add New Rule (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 17 Certificates

17.1 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.

17.1.1 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 17.3 on page 189).
- 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 17.4 on page 193).

17.2 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.

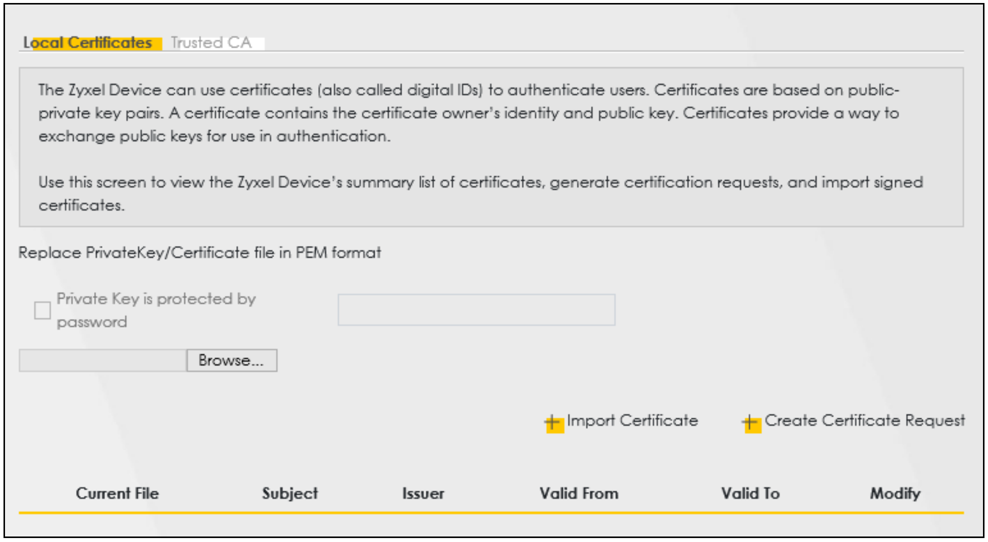
17.3 Local Certificates

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

- Web Server – This certificate secures HTTP connections.
- SSH – This certificate secures remote connections.

Click **Security** > **Certificates** to open the **Local Certificates** screen.

Figure 132 Security > Certificates > Local Certificates



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.

Replace PrivateKey/Certificate file in PEM format

□ Private Key is protected by password

Current File	Subject	Issuer	Valid From	Valid To	Modify

The following table describes the labels in this screen.

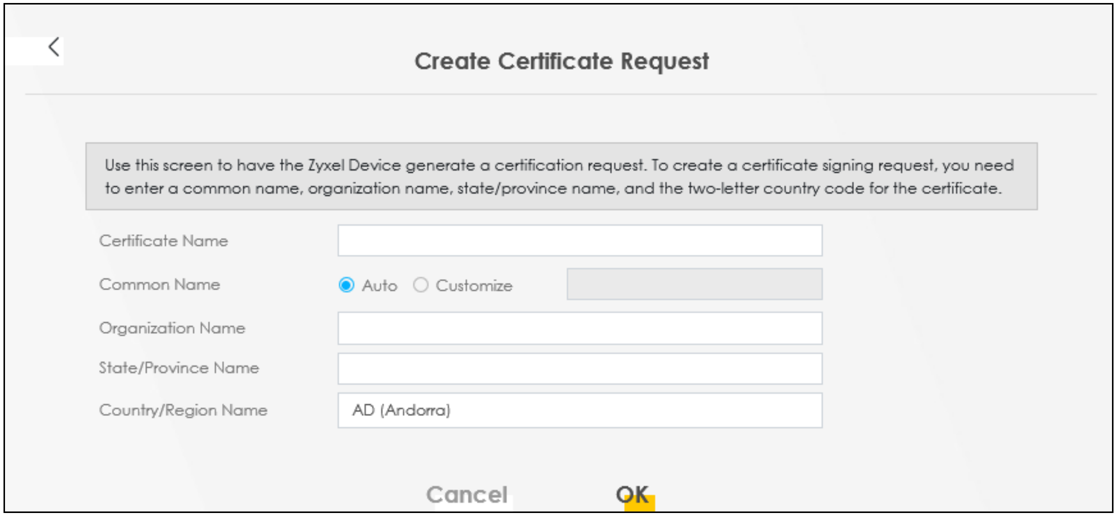
Table 75 Security > Certificates > Local Certificates

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. You can use up to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
Choose File/ Browse	Click this button to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Zyxel Device.
Create Certificate Request	Click this button to go to the screen where you can have the Zyxel Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have a unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate. For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

17.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state or province name, and the default US two-letter country code (The US country code is by default and not changeable when sold in the U.S.) for the certificate.

Figure 133 Security > Certificates > Local Certificates: Create Certificate Request



Create Certificate Request

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.

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 76 Security > Certificates > Local Certificates: Create Certificate Request

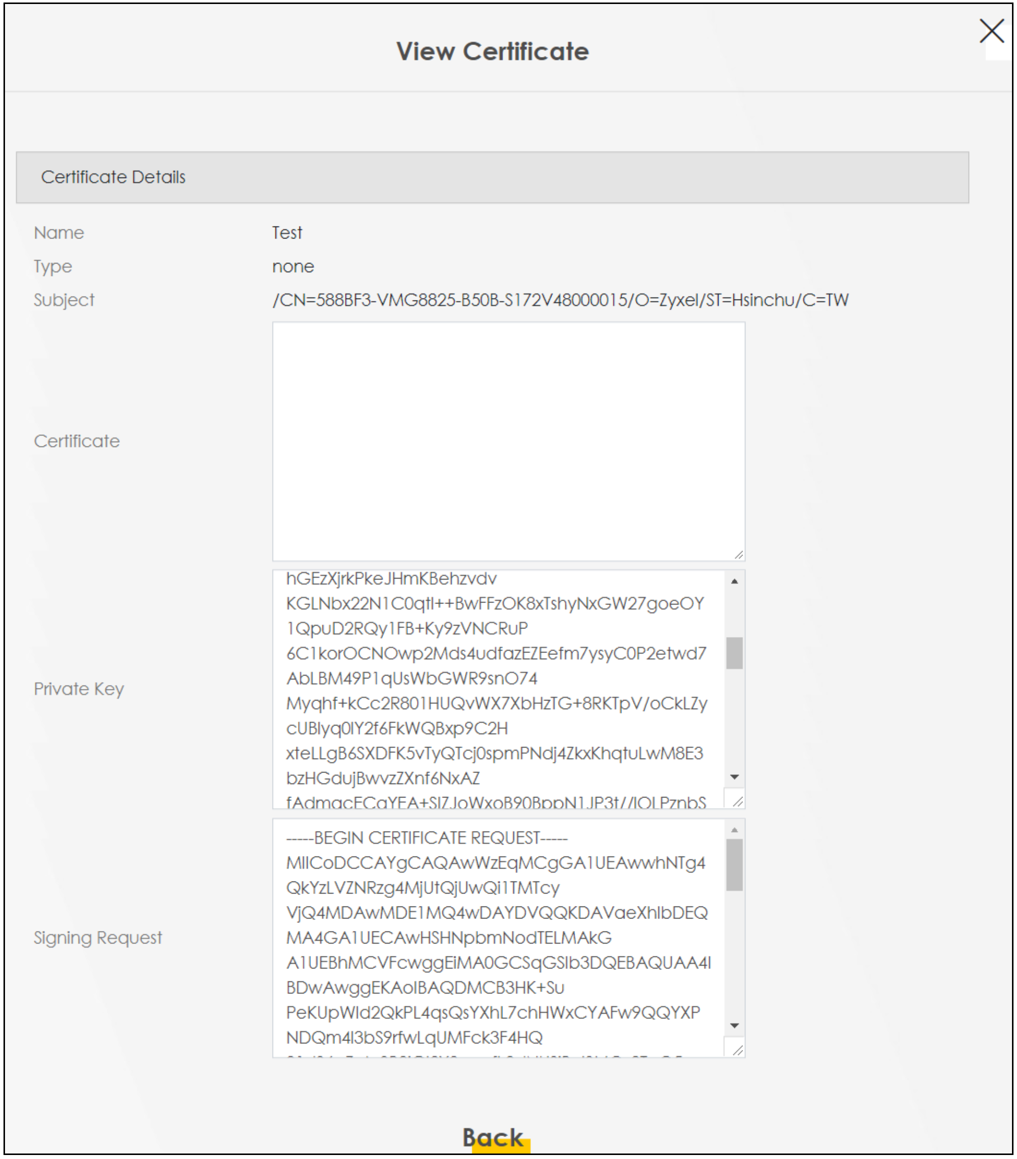
LABEL	DESCRIPTION
Certificate Name	Enter a descriptive name to identify this certificate. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Common Name	Select **Auto** to have the Zyxel Device configure this field automatically. Or select **Customize** to enter it manually. Enter the IP address (in dotted decimal notation), domain name or email address in the field provided. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Enter a descriptive name to identify the company or group to which the certificate owner belongs. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
State/Province Name	Enter a descriptive name to identify the state or province where the certificate owner is located. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

17.3.2 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 134 Security > Certificates > Local Certificates: View Certificate



View Certificate

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
PeKUpWId2QkPL4qsQsYXhL7chHWxCYAFw9QQYXP
NDQm4l3bS9rfwLqUMFck3F4HQ
```

The following table describes the fields in this screen.

Table 77 Security > Certificates > Local Certificates: View Certificates

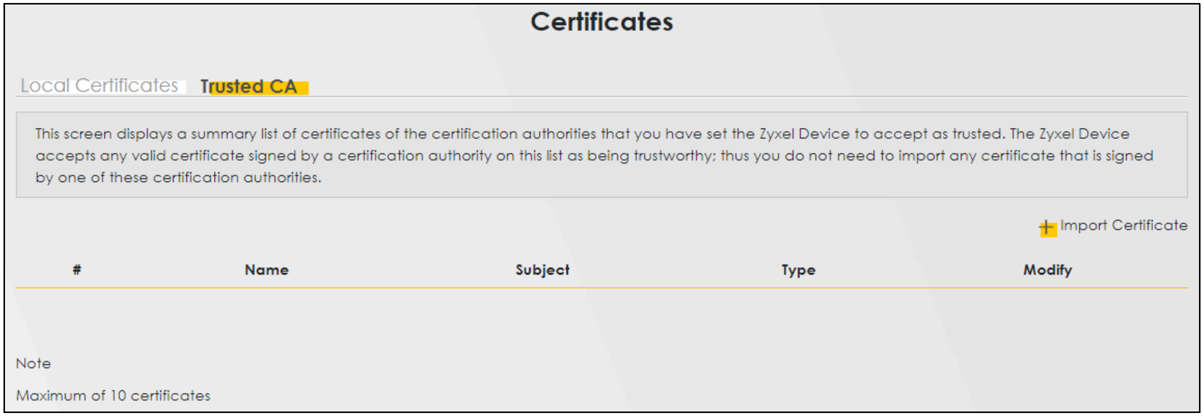
LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an 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.

17.4 Trusted CA

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

Note: A maximum of ten certificates can be added.

Figure 135 Security > Certificates > Trusted CA



Certificates

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; thus you do not need to import any certificate that is signed by one of these certification authorities.

#	Name	Subject	Type	Modify

Note

Maximum of 10 certificates

The following table describes the labels in this screen.

Table 78 Security > Certificates > Trusted CA

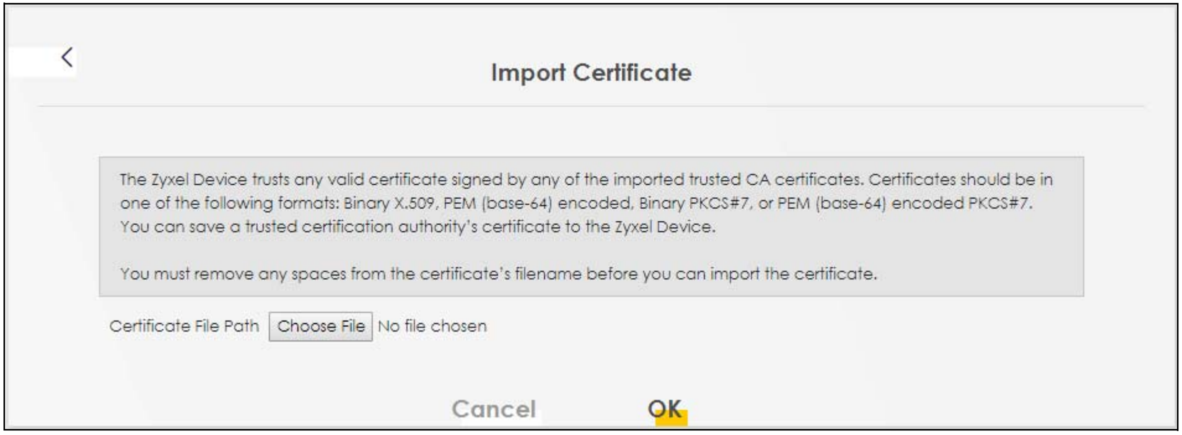
LABEL	DESCRIPTION
Import Certificate	Click this to open a screen where you can save the certificate of a certification authority that you trust to the Zyxel Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have a unique subject information.
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.

17.5 Import Trusted CA Certificate

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

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

Figure 136 Security > Certificates > Trusted CA > Import Certificate



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 [Choose File] No file chosen

The following table describes the labels in this screen.

Table 79 Security > Certificates > Trusted CA > Import Certificate

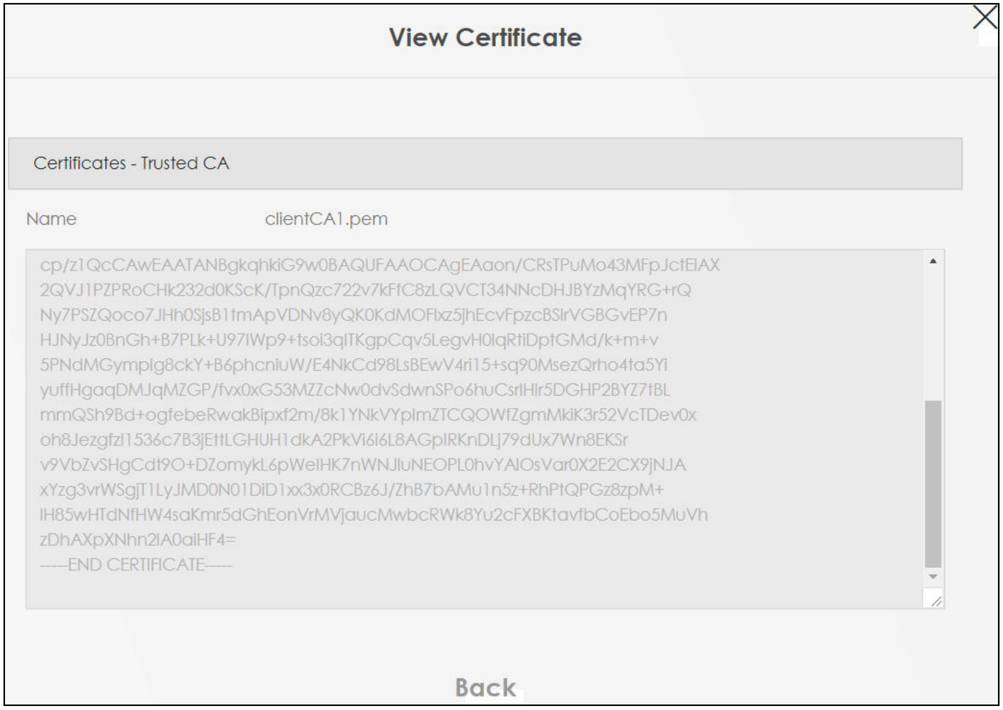
LABEL	DESCRIPTION
Certificate File Path	Enter the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it.
Choose File/ Browse	Click this to find the certificate file you want to upload.
OK	Click this to save the certificate on the Zyxel Device.
Cancel	Click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

17.6 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 137 Security > Certificates > Trusted CA > View Certificate



Name clientCA1.pem

```
cp/z1QcCAwEAATANBgkqhkiG9w0BAQUFAAOCAgEAaon/CRsTPuMo43MFpJctEiAX
2QVJ1PZPRoCHk232d0KScK/TpnQzc722v7kFfC8zLQVCT34NNcDHJBYzMqYRG+rQ
Ny7PSZQoco7JHh0SjsB1tmApVDNv8yQK0KdMOFlxz5jhEcvFpzcBSlrVGBGvEP7n
HJNyJz0BnGh+B7PLk+U97IWp9+tsoi3qlTKgpCqv5LegvH0lqRtiDptGMd/k+m+v
5PNdMGymplg8ckY+B6phcniuW/E4NkCd98LsBEwV4ri15+sq90MsezQrho4ta5Yi
yuffHgaqDMJqMZGP/fvx0xG53MZZcNw0dvSdwnSPo6huCsrlHlr5DGHP2BYZ7tBL
mmQSh9Bd+ogfebeRwakBipxf2m/8k1YNkVYplmZTCQOWfZgmMkiK3r52VcTDev0x
oh8Jezgfzl1536c7B3jEttLGHUH1dkA2PkVi6i6L8AGplRKnDLj79dUx7Wn8EKSr
v9VbZvSHgCdt9O+DZomykL6pWelHK7nWNJluNEOPL0hvYAlOsVar0X2E2CX9jNJA
xYzg3vrWSgjT1LyJMD0N01DiD1xx3x0RCBz6J/ZhB7bAMu1n5z+RhPtQPGz8zpM+
lH85wHTdNfHW4saKmr5dGhEonVrMVjaucMwbcRWk8Yu2cFXBKtavfbCoEbo5MuVh
zDhAXpXNhn2lA0aiHF4=
-----END CERTIFICATE-----
```

The following table describes the labels in this screen.

Table 80 Security > Certificates > Trusted CA > View Certificate

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through USB thumb drive for example).
Back	Click this to return to the previous screen.

17.7 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.

17.7.1 Verify a Certificate

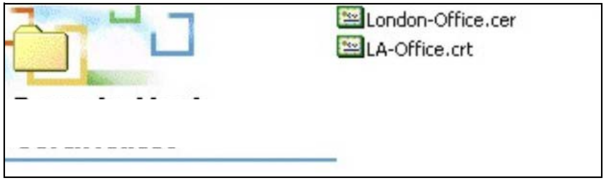
Before you import a trusted CA or trusted remote host certificate into the Zyxel Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the Zyxel Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

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.

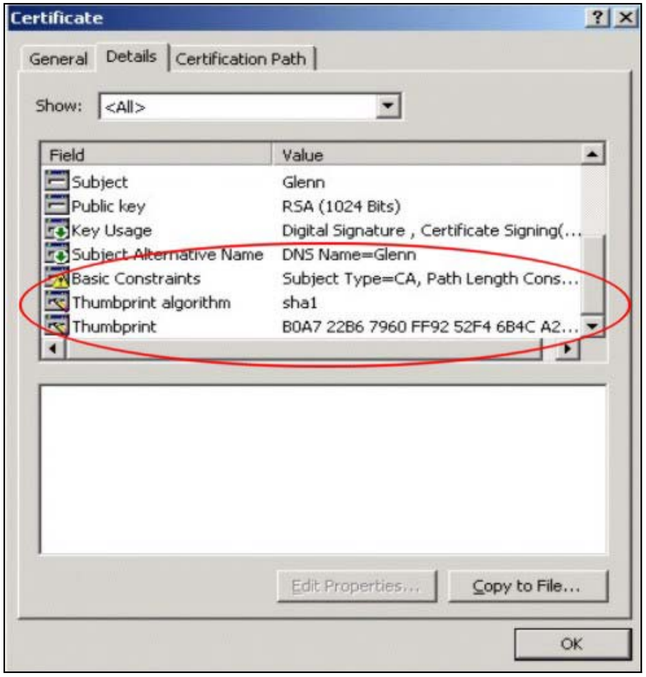
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 138 Certificates on Your Computer



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

Figure 139 Certificate Details



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 18 Log

18.1 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.

18.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 18.2 on page 200).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 18.3 on page 201).

18.1.2 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 81 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.

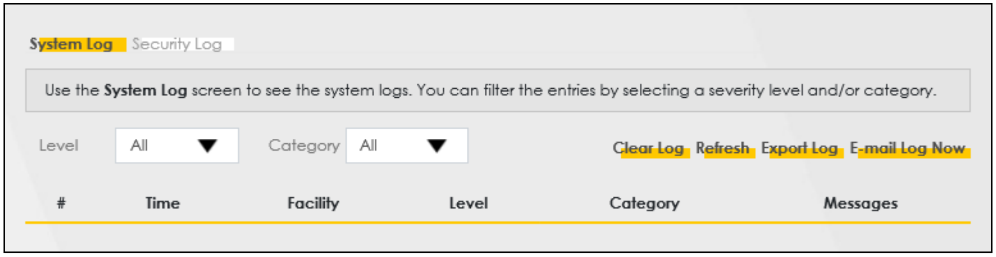
Table 81 Syslog Severity Levels (continued)

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

18.2 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 140 System Monitor > Log > 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.

The following table describes the fields in this screen.

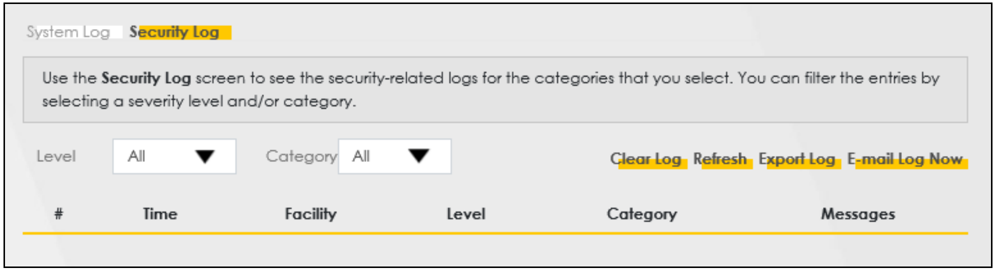
Table 82 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the Zyxel Device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

18.3 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 141 System Monitor > Log > Security Log



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

#	Time	Facility	Level	Category	Messages

The following table describes the fields in this screen.

Table 83 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the Zyxel Device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

CHAPTER 19
Traffic Status

19.1 Traffic Status Overview

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

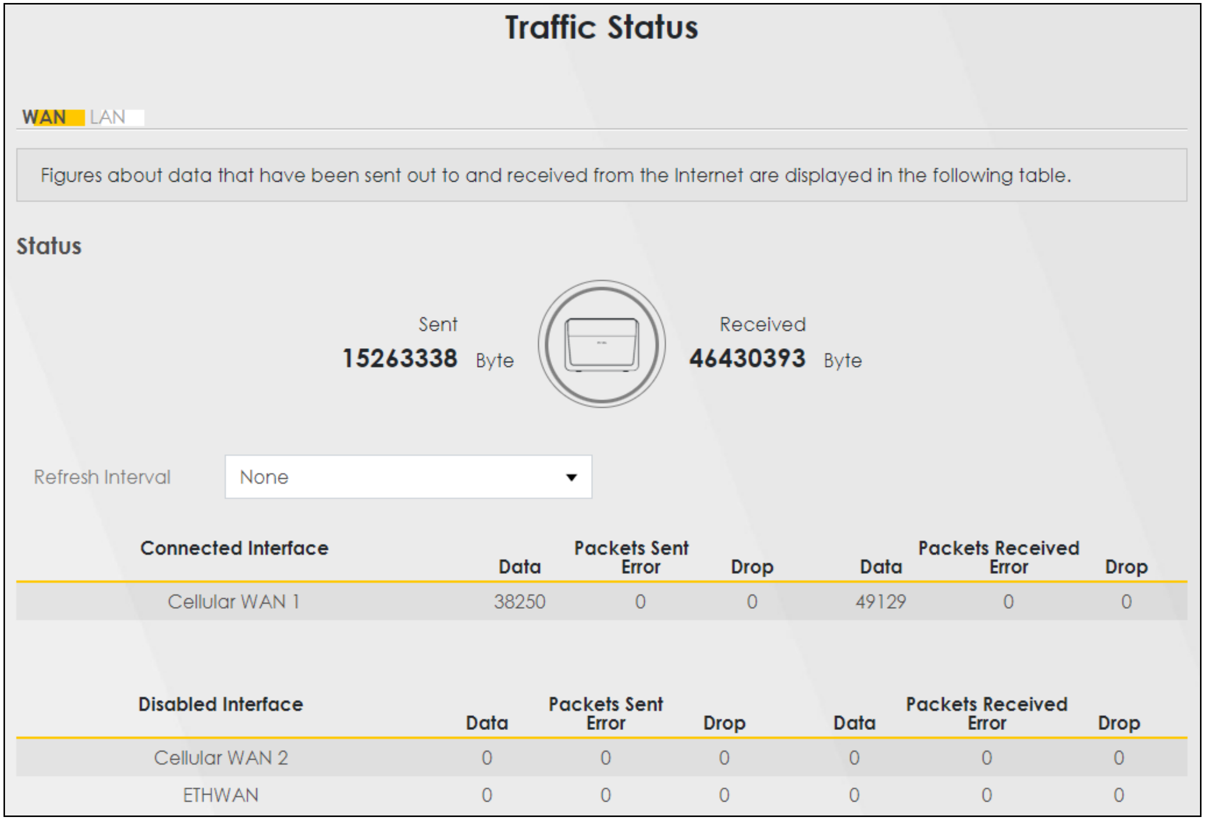
19.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 19.2 on page 202).
- Use the **LAN** screen to view the LAN traffic statistics (Section 19.3 on page 204).

19.2 WAN Status

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

Figure 142 System Monitor > Traffic Status > WAN



Traffic Status

Figures about data that have been sent out to and received from the Internet are displayed in the following table.

Status

Sent 15263338 Byte

Received 46430393 Byte

Refresh Interval: None

Connected Interface	Packets Sent Data	Packets Sent Error	Packets Sent Drop	Packets Received Data	Packets Received Error	Packets Received Drop
Cellular WAN 1	38250	0	0	49129	0	0

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

The following table describes the fields in this screen.

Table 84 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	

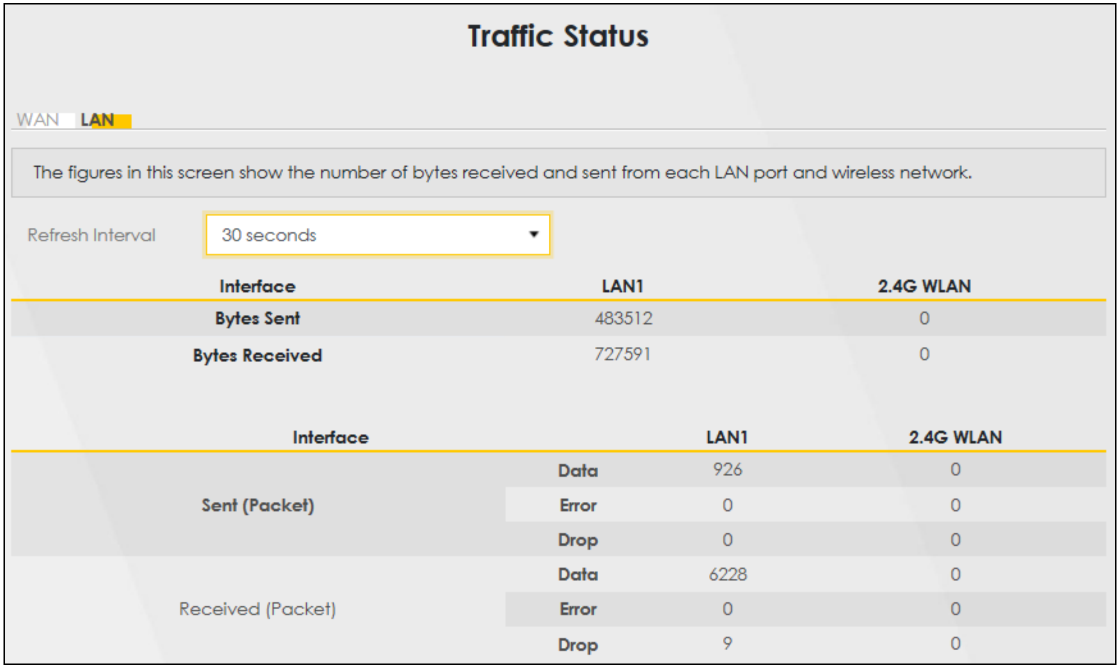
Table 84   System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
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.

19.3 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 143   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 85   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)	

Table 85 System Monitor > Traffic Status > LAN (continued)

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

CHAPTER 20
ARP Table

20.1 ARP Table Overview

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

An IP version 4 address is 32 bits long. MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

20.1.1 How ARP Works

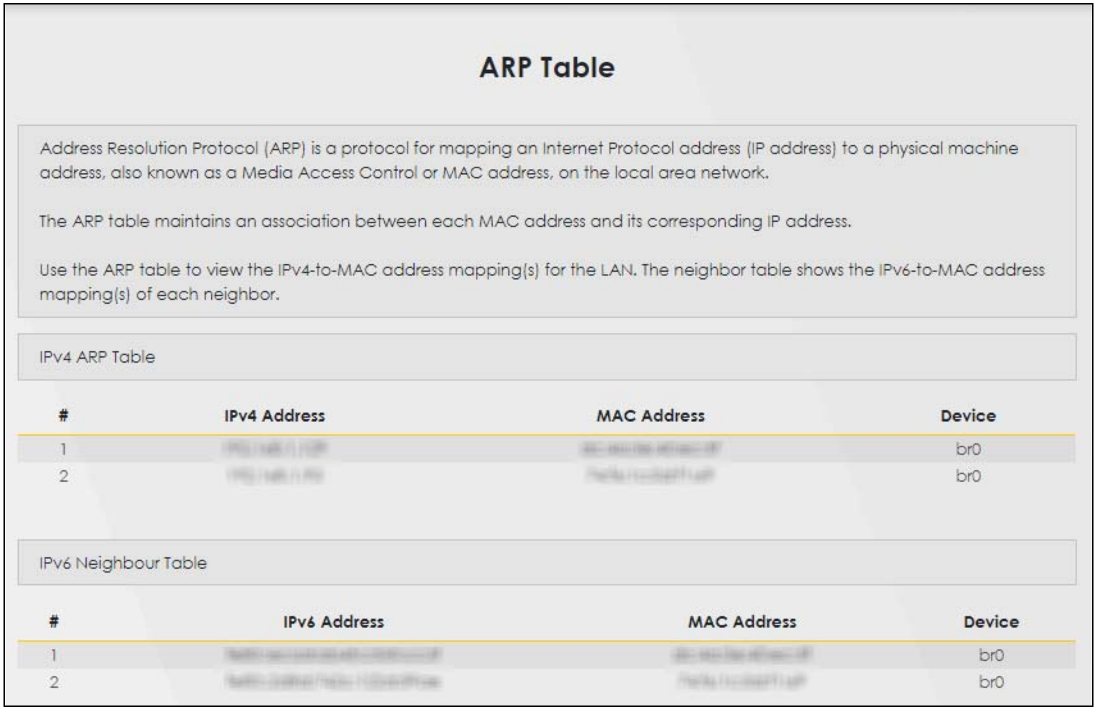
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

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.

20.2 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 144 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	[redacted]	[redacted]	br0
2	[redacted]	[redacted]	br0

IPv6 Neighbour Table

#	IPv6 Address	MAC Address	Device
1	[redacted]	[redacted]	br0
2	[redacted]	[redacted]	br0

The following table describes the labels in this screen.

Table 86 System Monitor > ARP Table

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

CHAPTER 21 Routing Table

21.1 Routing Table Overview

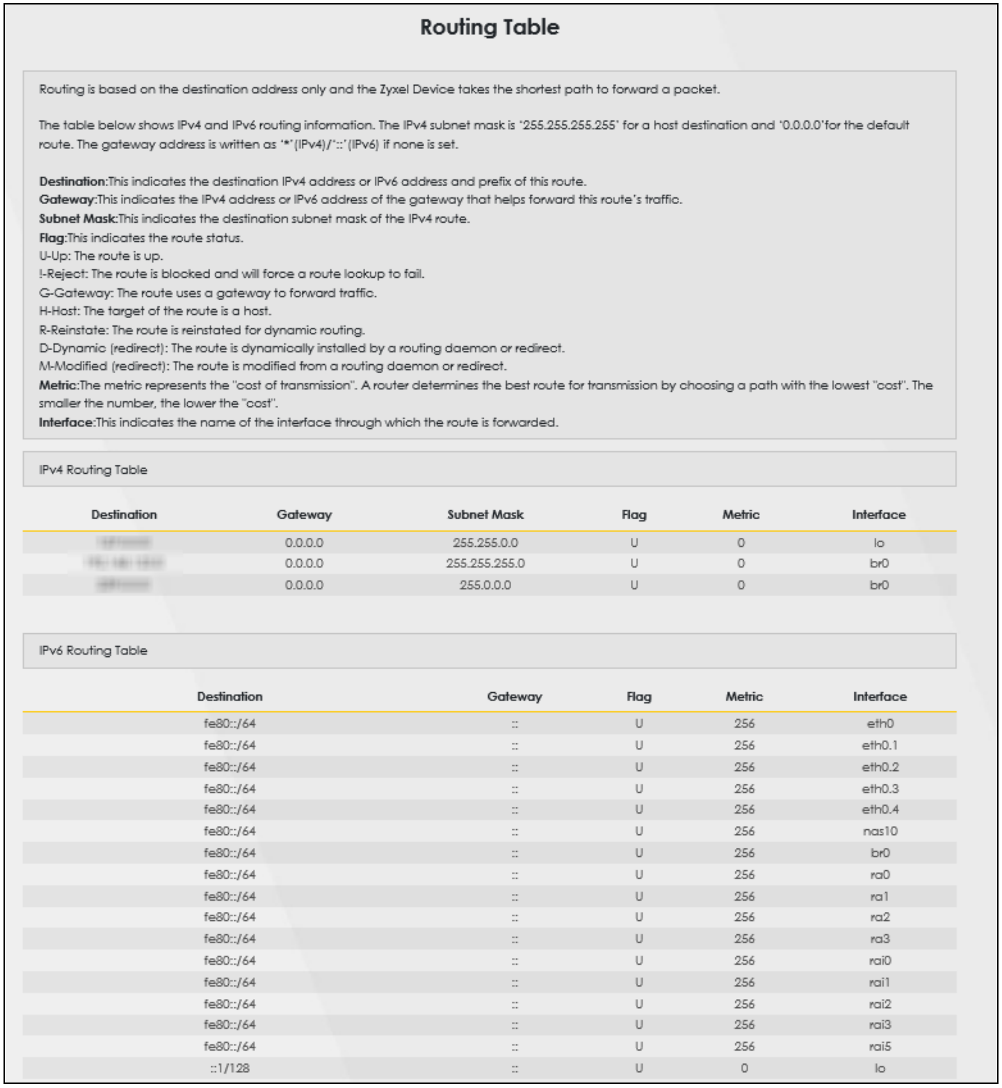
Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

21.2 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 145 System Monitor > Routing Table



Routing Table

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

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0'for the default route. The gateway address is written as '*'(IPv4)/'::'(IPv6) if none is set.

Destination: This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway: This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask: This indicates the destination subnet mask of the IPv4 route.
Flag: This indicates the route status.
U-Up: The route is up.
!-Reject: The route is blocked and will force a route lookup to fail.
G-Gateway: The route uses a gateway to forward traffic.
H-Host: The target of the route is a host.
R-Reinstate: The route is reinstated for dynamic routing.
D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.
M-Modified (redirect): The route is modified from a routing daemon or redirect.
Metric: The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Interface: This indicates the name of the interface through which the route is forwarded.

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
[redacted]	0.0.0.0	255.255.0.0	U	0	lo
[redacted]	0.0.0.0	255.255.255.0	U	0	br0
[redacted]	0.0.0.0	255.0.0.0	U	0	br0

IPv6 Routing Table

Destination	Gateway	Flag	Metric	Interface
fe80::/64	::	U	256	eth0
fe80::/64	::	U	256	eth0.1
fe80::/64	::	U	256	eth0.2
fe80::/64	::	U	256	eth0.3
fe80::/64	::	U	256	eth0.4
fe80::/64	::	U	256	nas10
fe80::/64	::	U	256	br0
fe80::/64	::	U	256	ra0
fe80::/64	::	U	256	ra1
fe80::/64	::	U	256	ra2
fe80::/64	::	U	256	ra3
fe80::/64	::	U	256	rai0
fe80::/64	::	U	256	rai1
fe80::/64	::	U	256	rai2
fe80::/64	::	U	256	rai3
fe80::/64	::	U	256	rai5
::1/128	::	U	0	lo

The following table describes the labels in this screen.

Table 87 System Monitor > Routing Table

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

Table 87 System Monitor > Routing Table (continued)

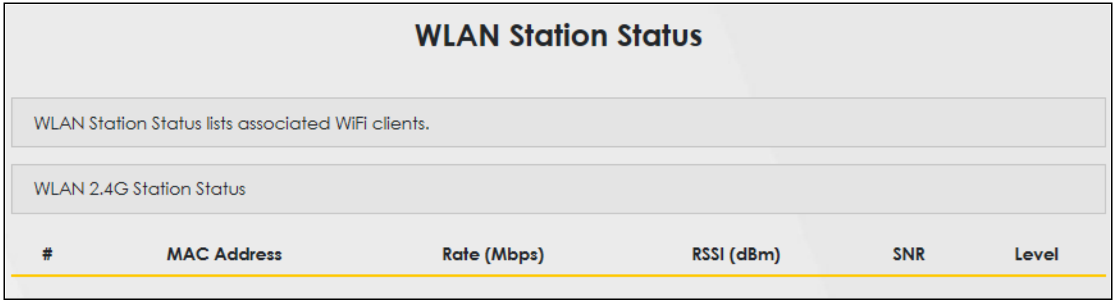
LABEL	DESCRIPTION
Flag	This indicates the route status. **U–Up:** The route is up. **!–Reject:** The route is blocked and will force a route lookup to fail. **G–Gateway:** The route uses a gateway to forward traffic. **H–Host:** The target of the route is a host. **R–Reinstate:** The route is reinstated for dynamic routing. **D–Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect. **M–Modified (redirect):** The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission." A router determines the best route for transmission by choosing a path with the lowest "cost." The smaller the number, the lower the "cost."
Interface	This indicates the name of the interface through which the route is forwarded. • **brx** indicates a LAN interface where x can be 0 – 3 to represent LAN1 to LAN4 respectively.

CHAPTER 22
WLAN Station Status

22.1 WLAN Station Status Overview

Click **System Monitor** > **WLAN Station Status** to open the following screen. Use this screen to view information and status of the WiFi stations (WiFi clients) that are currently associated with the Zyxel Device. Being associated means that a WiFi client (for example, your computer with a WiFi network card installed) has connected successfully to an AP (or WiFi router) using the same SSID, channel, and WiFi security settings.

Figure 146 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 88 System Monitor > WLAN Station Status

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

Table 88 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 greater the number, the better the quality of WiFi. The normal range is 15 to 40. If the value drops below 15, try moving the associated WiFi station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated WiFi station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the Zyxel Device is receiving an excellent WiFi signal. **4** means the Zyxel Device is receiving a very good WiFi signal. **3** means the Zyxel Device is receiving a weak WiFi signal, **2** means the Zyxel Device is receiving a very weak WiFi signal. **1** means the Zyxel Device is not receiving a WiFi signal.

CHAPTER 23
Cellular WAN Status

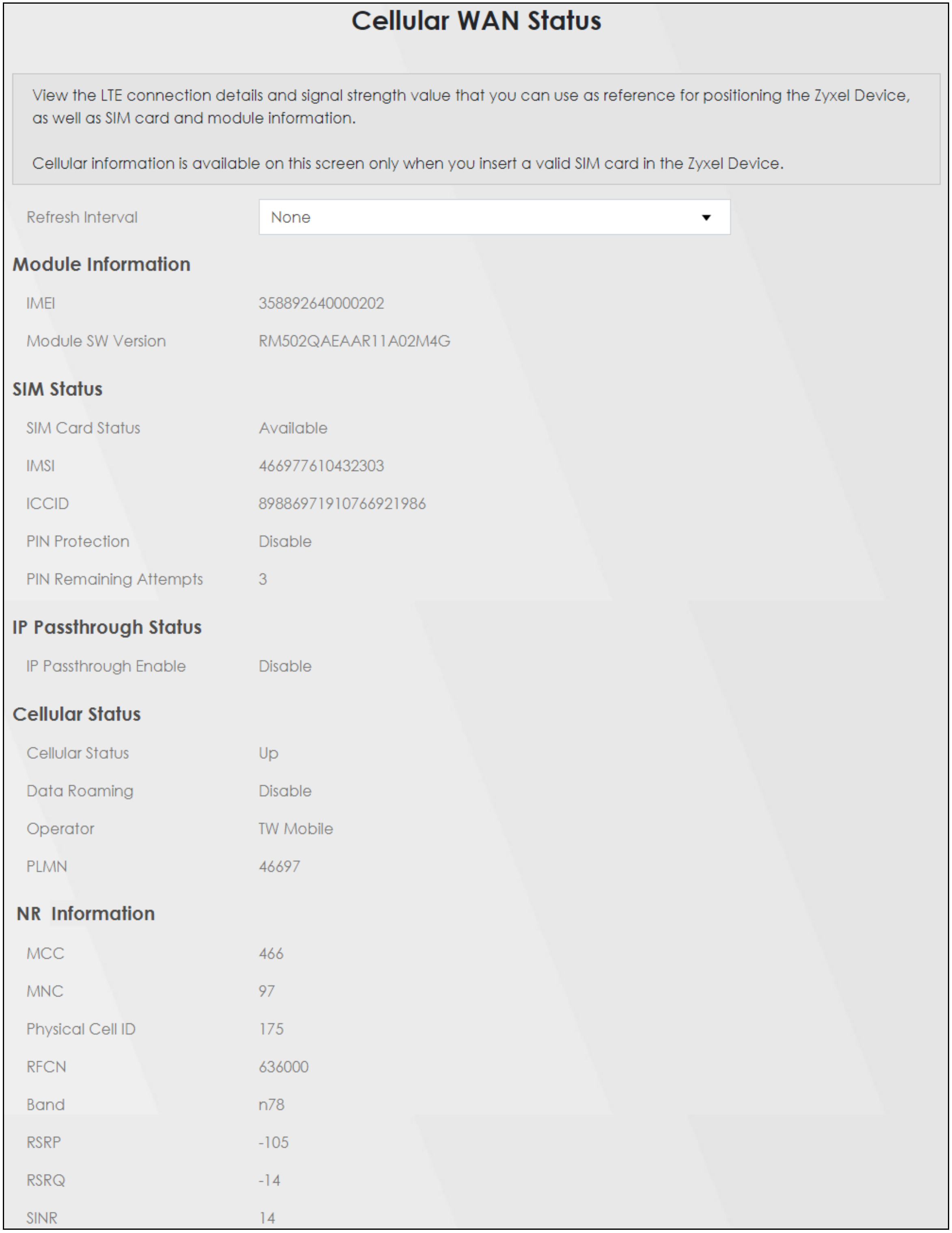
23.1 Cellular WAN Status Overview

View the cellular 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.

23.2 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 147 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

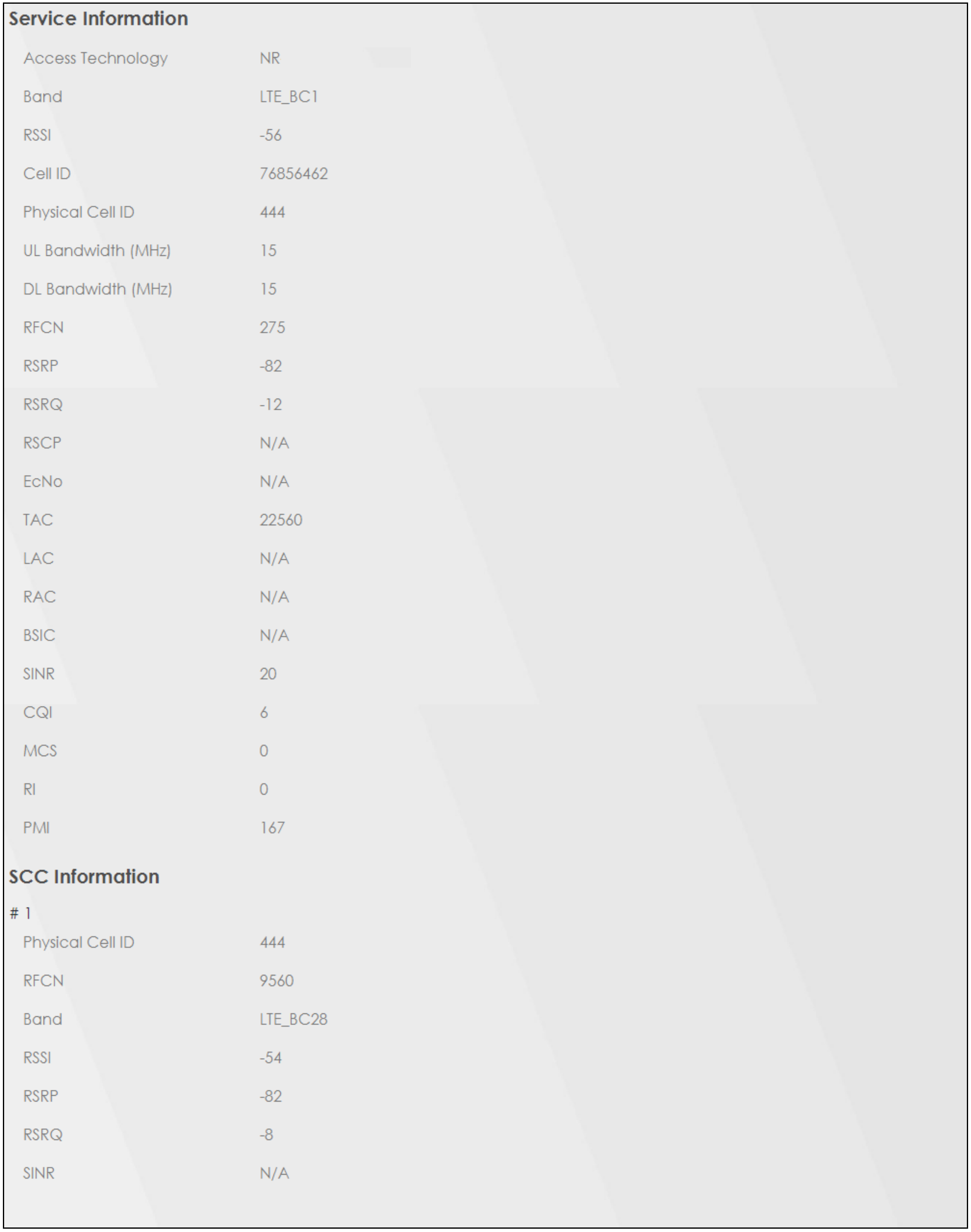
Cellular Status

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 148 System Monitor > Cellular WAN Status (continued)



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 89 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 cellular 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 doesn't 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. Without the PIN code, you cannot use the SIM card. Shows **Enable** if the service provider requires you to enter a PIN to use the SIM card and **PIN Protection** is enabled. Shows **Disable** if the service provider lets you use the SIM without inputting a PIN.
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 first LAN computer on the local network and will not go through NAT.
IP Passthrough Mode	This displays the IP Passthrough mode. This displays **Dynamic** and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device. This displays **Fixed** and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.

Table 89 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
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.
PLMN	This displays the PLMN number.
Antenna Status	This displays **Internal** when the **INT EXT** switch is set to **INT**. Use the Zyxel Device's internal antenna to get cellular signal. This displays **External** when the **INT EXT** switch is set to **EXT**. Connect external antennas to the Zyxel Device's to strengthen the cellular signal. See Section 2.4 on page 33 for more information.
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.
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 the mobile network to which the Zyxel Device is connecting.
Band	This displays the current cellular band of your Zyxel Device.
RSSI (dBm)	This displays the strength of the WiFi signal between an associated wireless station and an AP. The normal range is –30 dBm to –79 dBm. If the value drops below –80 dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.
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, 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 connecting to. The normal range is 1 to 504.
UL Bandwidth (MHz)	This shows the cellular channel bandwidth from the Zyxel Device to the 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 cellular channel bandwidth from the 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).

Table 89 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
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, for 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.
SINR (dB)	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.
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, for example, –240 dB.
Primary Scrambling Code	This displays a unique scrambling code used by the Nebula Device to identify a base station in a cellular network. A primary scrambling code is the product of the scrambling code and 16. Therefore, the primary scrambling code set contains all multiples of 16 from 0 through 8176. Note: This only appears in UMTS mode. Otherwise, this field is blank.
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, it uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and use 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.
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.
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.

Table 89 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
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 the downlink rate.
NR SINR (dBm)	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 5G network. A negative value means more noise than signal.

CHAPTER 24
System

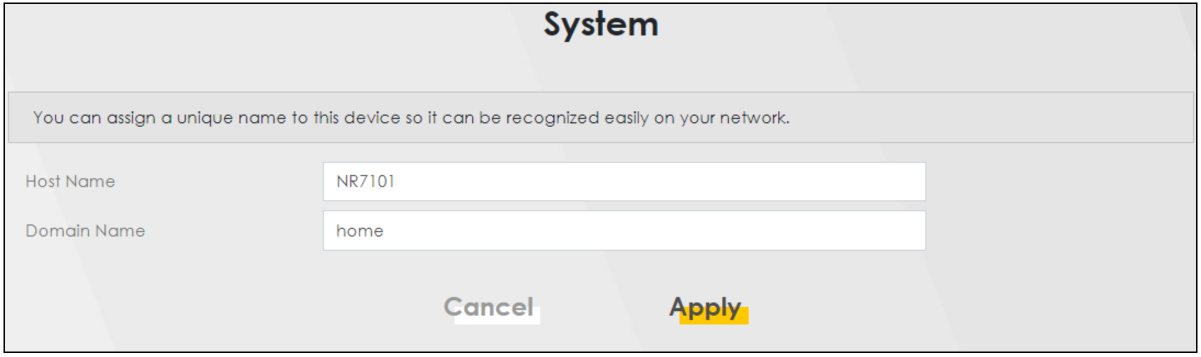
24.1 System Overview

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

24.2 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 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.

Figure 149 Maintenance > System



System

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

Host Name: NR7101

Domain Name: home

The following table describes the labels in this screen.

Table 90 Maintenance > System

LABEL	DESCRIPTION
Host Name	Enter a descriptive host name for your Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. For some models, the supported maximum input length is 16 alphanumeric characters.
Domain Name	Enter a domain name for your host Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Cancel	Click **Cancel** to abandon this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 25
User Account

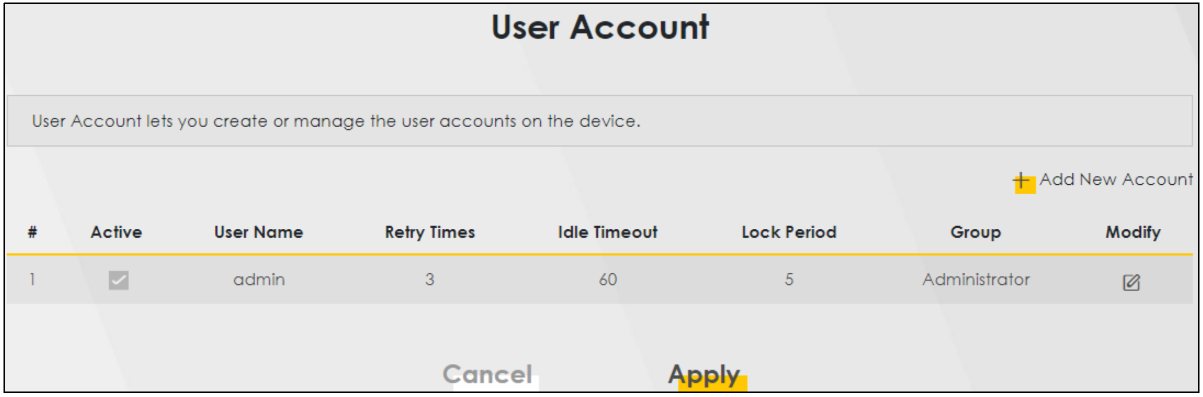
25.1 User Account Overview

In the **User Account** screen, you can view the settings of the “admin” that you use to log into the Zyxel Device to manage it.

25.2 User Account

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

Figure 150 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 91 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account (up to four **Administrator** accounts and four **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**.

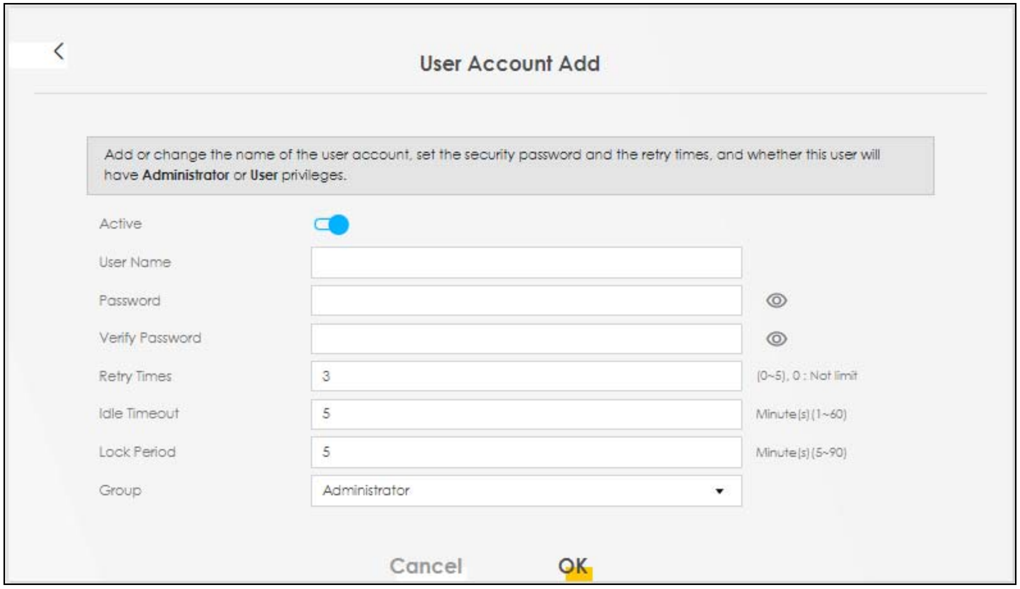
Table 91 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Group	This field displays this user has **Administrator** privileges.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

25.2.1 User Account Add or Edit

Add or change the name of the user account, set the security password and the retry times, and whether this user will have **Administrator** or **User** privileges. Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance** > **User Account** to open the following screen.

Figure 151 Maintenance > User Account > Add



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 92 Maintenance > User Account > User Account Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (switch turns blue) or disable (switch turns gray) to activate or deactivate the user account.
User Name	Enter a name for this account. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Password	Enter your new system password (from 8-64 characters long, and must contain at least one upper case letter, one lower case letter and one number). Note that as you enter 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. If you are changing your existing password, you have to first enter your **Old Password** then enter your **New Password**.
Verify Password	Enter the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.

Table 92 Maintenance > User Account > 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 26 Remote Management

26.1 Remote Management Overview

Remote management controls through which interfaces, 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.

26.1.1 What You Can Do in this Chapter

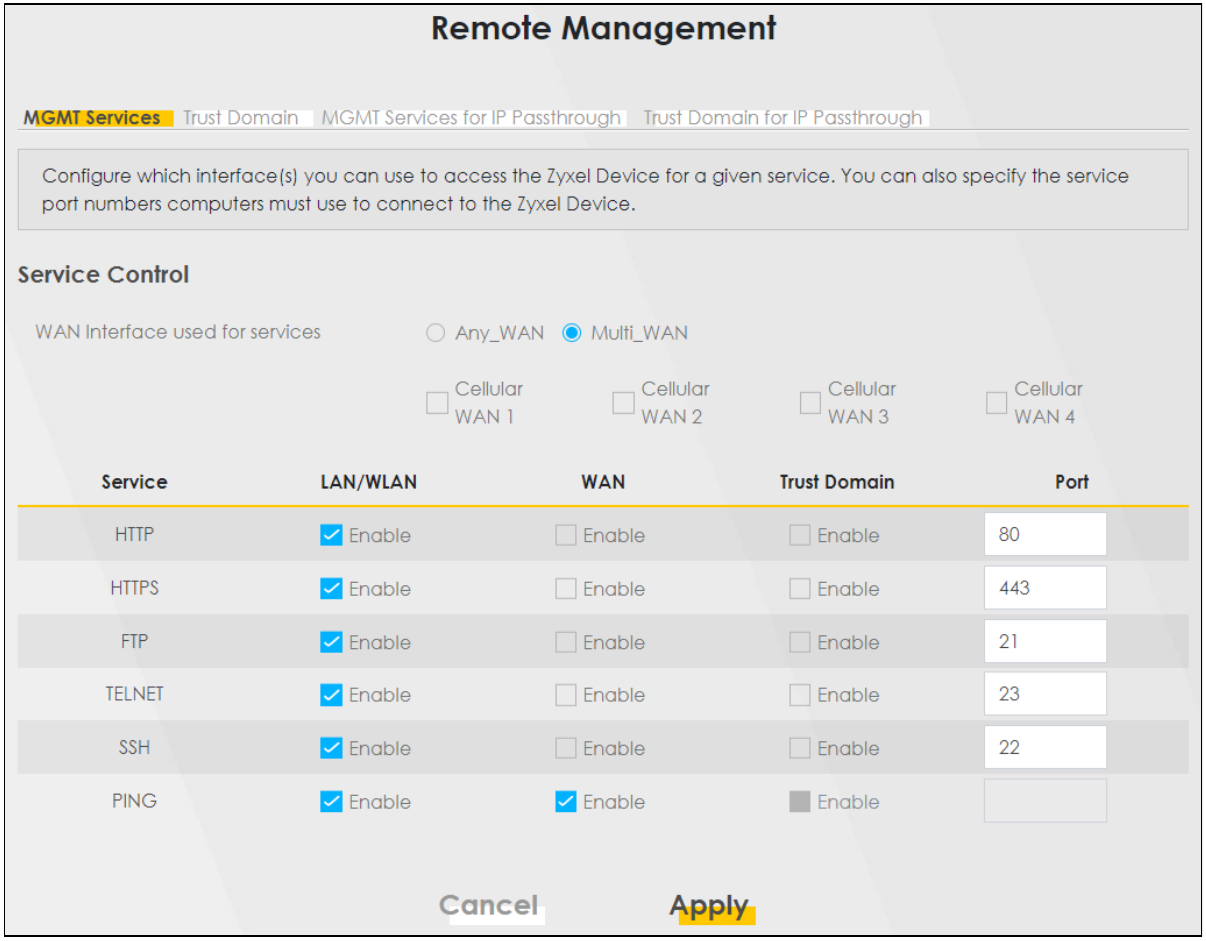
- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 26.2 on page 224).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 26.3 on page 226).
- Use **MGMT Services for IP Passthrough** to configure which interfaces you can use to access the Zyxel Device for a given service (Section 26.4 on page 227).
- Use **Trust Domain for IP Passthrough** to view a list of public IP addresses and complete domain names which are allowed to access the Zyxel Device (Section 26.5 on page 228),

26.2 MGMT Services

Note: The **MGMT Services** screen will be hidden if you enable the **IP Passthrough** function in **Network Setting** > **Broadband** > **Cellular IP Passthrough** screen.

Use this screen to configure the interfaces through which services can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance** > **Remote Management** > **MGMT Services** to open the following screen.

Figure 152 Maintenance > Remote Management > MGMT Services



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 for a given service. You can also specify the service port numbers computers must use to connect to the Zyxel Device.

Service Control

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 93 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
Service Control	
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Cellular WAN	Enable the cellular WAN connection configured in **Network Setting** > **Broadband** > **Cellular WAN** to access the service on the Zyxel Device. If there are multiple cellular WANs configured on the Zyxel Device, you can select which to use for the Zyxel Device management.
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 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.

Table 93 Maintenance > Remote Management > MGMT Services (continued)

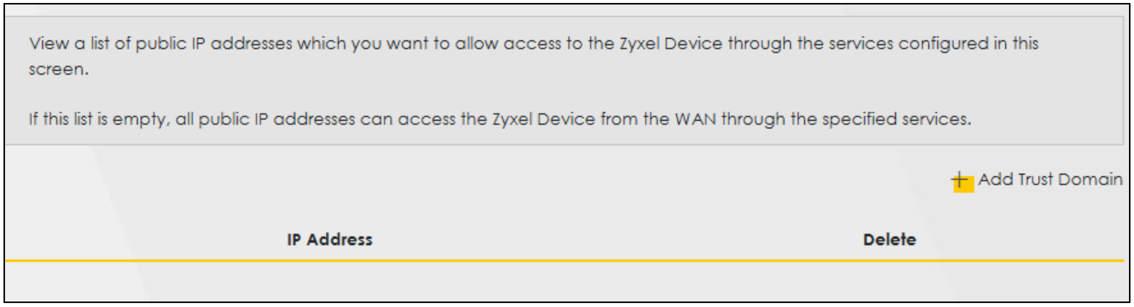
LABEL	DESCRIPTION
Redirect HTTP to HTTPS	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server. For example, if you enter http://192.168.1.1 in your browser to access the Web Configurator, then the Zyxel Device will automatically change this to the more secure https://192.168.1.1 for access.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

26.3 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 153 Maintenance > Remote Management > Trust Domain



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.

The following table describes the fields in this screen.

Table 94 Maintenance > Remote Management > Trust Domain

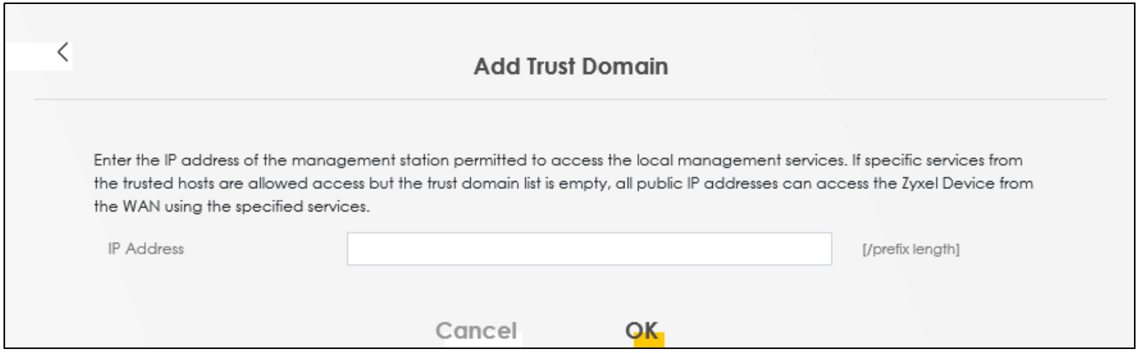
LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon to remove the trusted host IP address.

26.3.1 Add Trust Domain

Use this screen to add a public IP addresses or a complete domain name of a device which is allowed to access the Zyxel Device. Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted-hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Click the **Add Trust Domain** button in the **Maintenance** > **Remote Management** > **Trust Domain** screen to open the following screen.

Figure 154 Maintenance > Remote Management > Trust Domain > Add Trust Domain



Add Trust Domain

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.

IP Address [/prefix length]

The following table describes the fields in this screen.

Table 95 Maintenance > Remote Management > Trust Domain > Add Trust Domain

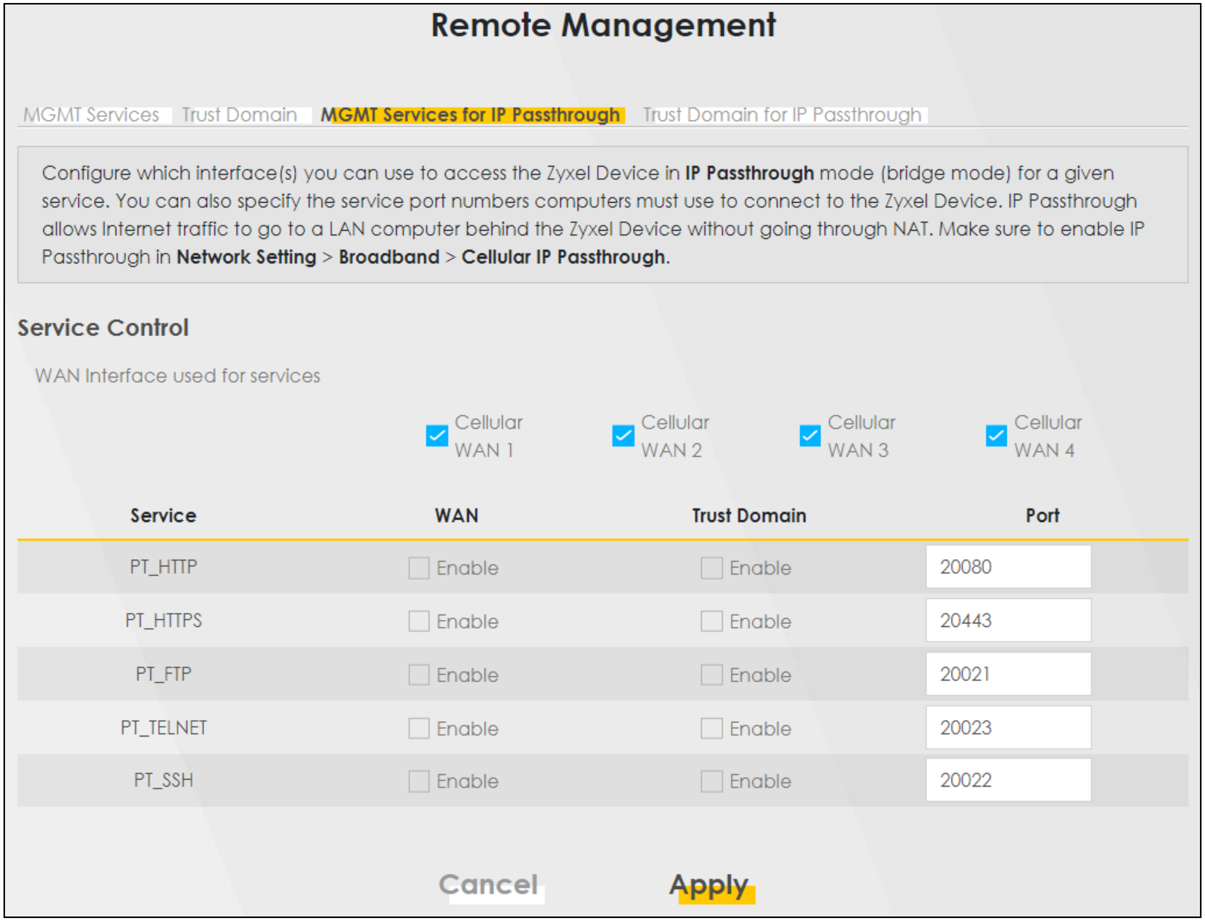
LABEL	DESCRIPTION
IP Address	Enter a public IPv4/IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

26.4 MGMT Services for IP Passthrough

Configure which interfaces you can use to access the Zyxel Device when **IP Passthrough** is enabled 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**.

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

Figure 155 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

WAN Interface used for services

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

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 96 Maintenance > Remote Management

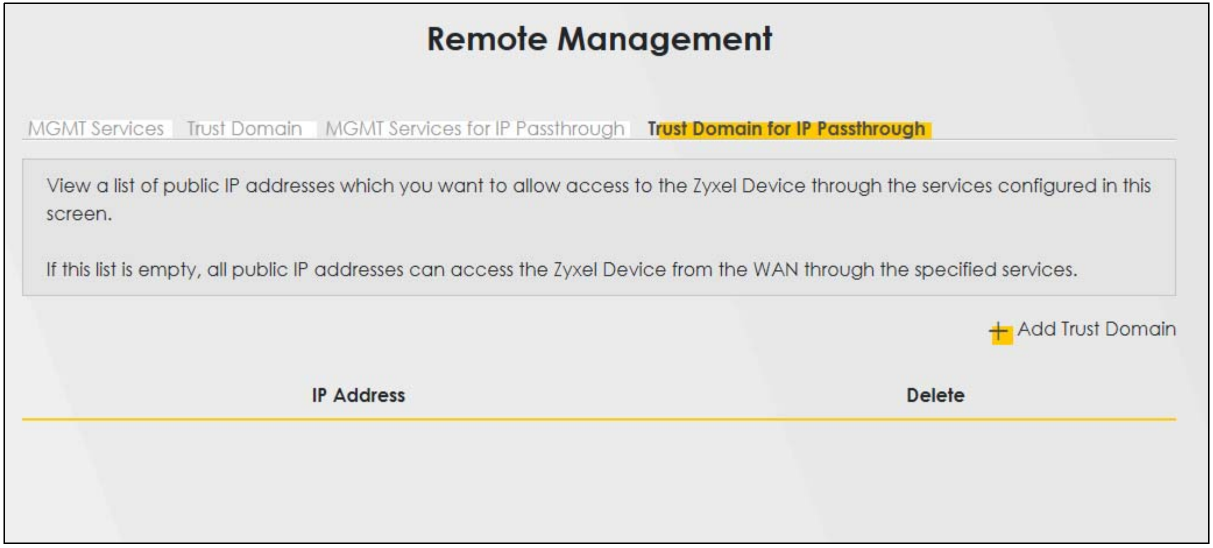
LABEL	DESCRIPTION
Service	This is the service you may use to access the Zyxel Device.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** check box for the corresponding services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

26.5 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 when **IP Passthrough** is enabled. 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**.

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

Figure 156 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.

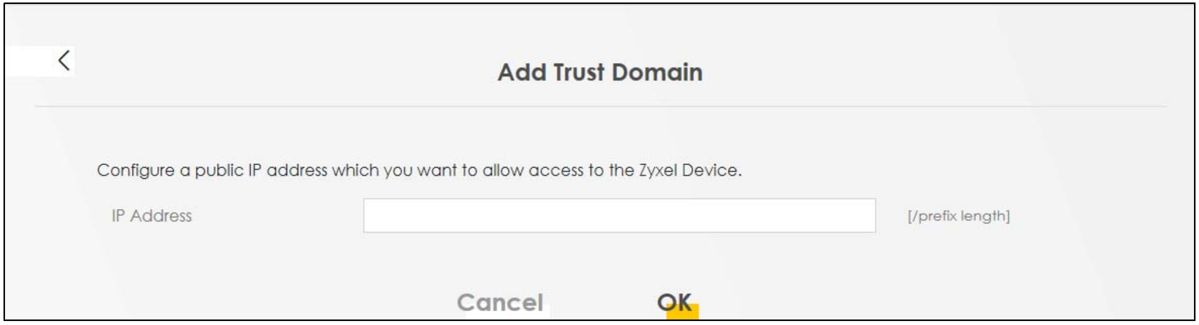
Table 97 Maintenance > Remote Management > Trust Domain for IP Passthrough

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.

26.5.1 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 157 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 98 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 from the WAN.
Cancel	Click **Cancel** to restore your previously saved settings.
OK	Click **OK** to save your changes.

CHAPTER 27
TR-069 Client

27.1 TR-069 Overview

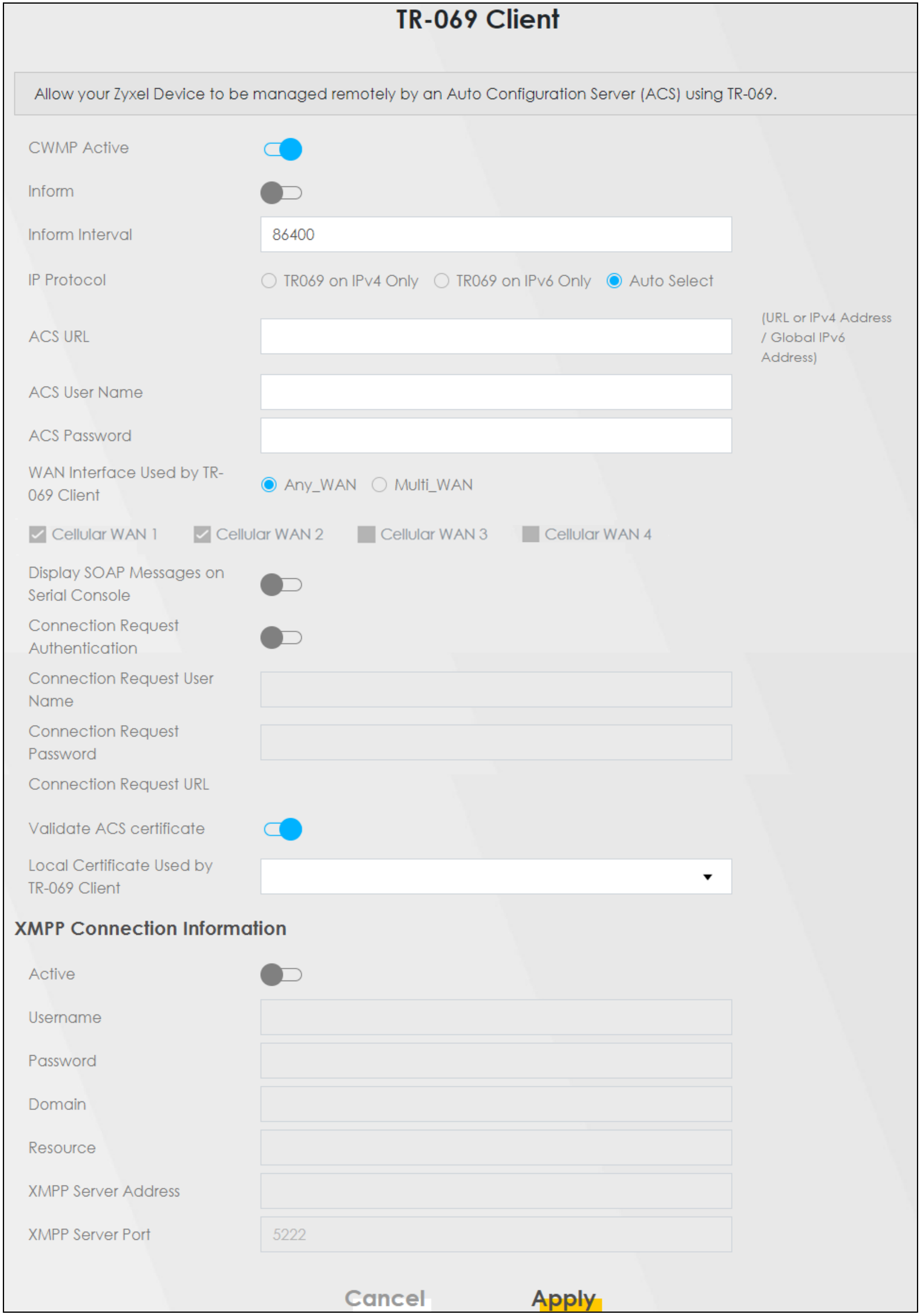
This chapter explains how to configure the Zyxel Device's TR-069 auto-configuration settings.

27.2 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.

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

Figure 158 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	●	
Inform	○	
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	○
Connection Request Authentication	○
Connection Request User Name	
Connection Request Password	
Connection Request URL	
Validate ACS certificate	●
Local Certificate Used by TR-069 Client	▾

XMPP Connection Information

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

The following table describes the fields in this screen.

Table 99 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP Active	CPE WAN Management Protocol (CWMP) enables the Zyxel Device to be remotely configured through 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 through 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.
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 CPE.
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 99 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)
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore the screen's last saved settings.

CHAPTER 28 TR-369

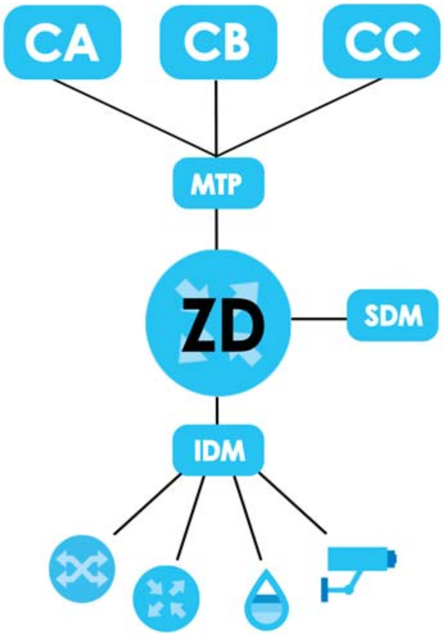
28.1 TR-369 Overview

TR-369 or USP (User Services Platform) is a standardized protocol for managing, monitoring, upgrading, and controlling connected network devices. It can manage WiFi, mesh networks, or IoT devices in smart homes. The TR-369 agent collects and analyzes data from network devices to identify potential problems and generate reports and alerts and sends them to a controller.

A service element refers to the set of objects, commands, events, and parameters that represent a specific set of functionality that can be modified by a controller on an agent. An agent, the Zyxel Device, **ZD** in the following example figure, exposes service elements to one or more controllers (**CA**, **CB**, **CC** in the example figure below). A controller manipulates service elements through one or more agents. The Instantiated Data Model (IDM) of an agent represents the current status of service elements that are exposed to one or more controllers. The Supported Data Model (SDM) of an agent represents the complete set of service elements it is capable of exposing to a controller.

A message refers to the contents of a TR-369 communication. A Message Transfer Protocol (**MTP**) is the protocol that carries a message. The endpoint must be identified by a locally or globally unique endpoint identifier depending on the scheme used for assignment.

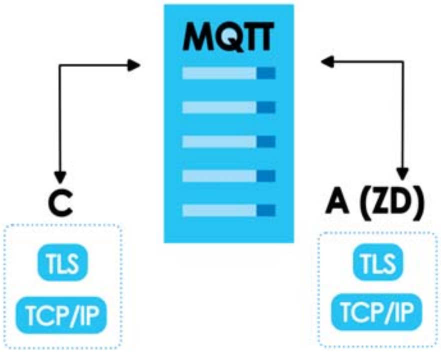
Figure 159 Example TR-369 Topology



28.1.1 MQTT

The Zyxel Device supports MQ Telemetry Transport (MQTT) to send messages for always-on, direct communications between an agent (**A,** the Zyxel Device, **ZD**), controller (**C**), the MQTT broker (**MQTT**) and other clients. The MQTT broker (**MQTT**) routes and delivers messages between the controller and agent. Messages can be encrypted with TLS (Transport Layer Security) for end-to-end message security and integrity.

Figure 160 MQTT Broker



28.1.2 Topics

An agent exposes a service element to a controller by publishing a topic. Controllers use topic filters to subscribe to specific published topics that they can manage.

A topic uses a hierarchical structure with forward slash "/" characters for organizing topics and to identify the exact location of a service element. For example, “myhome/livingroom/temperature”, “myhome/bedroom/temperature”, “myoffice/meetingroom/temperature”.

Note: **Response Topic** in the **Agent** screen is a topic filter where you can subscribe to multiple topics at once using wildcards.

Topic in the **Controller** screen is a topic name used to publish a topic. It must not contain wildcards.

28.1.2.1 Topic Filter Wildcards

Wildcard characters can be used in topic filters, but not in topic names. [MQTT-4.7.1-1].

The number sign (‘#’ U+0023) is a wildcard character that matches any number of levels within a topic. The multi-level wildcard represents the parent and any number of child levels. The multi-level wildcard character must be specified either on its own or following a topic level separator. In either case it must be the last character specified in the topic filter [MQTT-4.7.1-2]

For example, if a client subscribes to “sport/tennis/player1/#”, it would receive messages published using these topic names:

- “sport/tennis/player1”
- “sport/tennis/player1/ranking”
- “sport/tennis/player1/score/wimbledon”

- “sport/#” also matches the singular “sport”, since # includes the parent level.
- “#” is valid and will receive every Application Message
- “sport/tennis/#” is valid
- “sport/tennis#” is not valid
- “sport/tennis/#/ranking” is not valid

The plus sign (‘+’ U+002B) is a wildcard character that matches only one topic level. The single-level wildcard can be used at any level in the topic filter, including first and last levels. Where it is used it must occupy an entire level of the filter [MQTT-4.7.1-3]. It can be used at more than one level in the topic filter and can be used in conjunction with the multilevel wildcard.

For example, “sport/tennis/+” matches “sport/tennis/player1” and “sport/tennis/player2”, but not “sport/tennis/player1/ranking”. Also, because the single-level wildcard matches only a single level, “sport/+” does not match “sport” but it does match “sport/”.

- “+” is valid
- “+/tennis/#” is valid
- “sport+” is not valid
- “sport/+/player1” is valid
- “/finance” matches “+/+” and “/+”, but not “+”

28.1.2.2 Rules for Topic Names and Topic Filters

- All topic names and topic filters must be at least one character long.
- Topic names and topic filters are case sensitive.
- Topic names and topic filters can include the space character.
- A topic name or topic filter can have just the ‘/’ character, but you should make the topic as clear as possible.
- Topic names and topic filters must not include the null character (Unicode U+0000).
- Topic names and topic filters are UTF-8 encoded strings, and must not encode to more than 65,535 bytes.
- There is no limit to the number of levels in a topic name but the total length must be under 65,535 bytes.

28.2 Configuration Overview

Make sure the below prerequisites are done before configuring TR-369 on the Zyxel Device.

28.2.1 Prerequisites

Register with an MQTT broker. You may need to configure the following items.

Table 100 MQTT Broker Registration

ITEM	DESCRIPTION
Username	If this is required, note it and enter the same on the Zyxel Device.
Password	If this is required, note it and enter the same on the Zyxel Device.

Table 100 MQTT Broker Registration (continued)

ITEM	DESCRIPTION
Port	The default port is 1883. If the broker uses a different port, you must enter that different port number on the Zyxel Device.
TLS	If this is configured on the broker, you must also configure it on the Zyxel Device.
QoS	Note whether the broker uses QoS 0, 1 or 2, and select the same on the Zyxel Device.
Protocol Version	Note whether the broker uses version 3.11 or 5.0, then select the same on the Zyxel Device.

28.2.2 Configuring TR-369 on the Zyxel Device

1. First, configure the **MQTT** screen. Each client connecting to the same MQTT broker must have a unique **Client ID**.

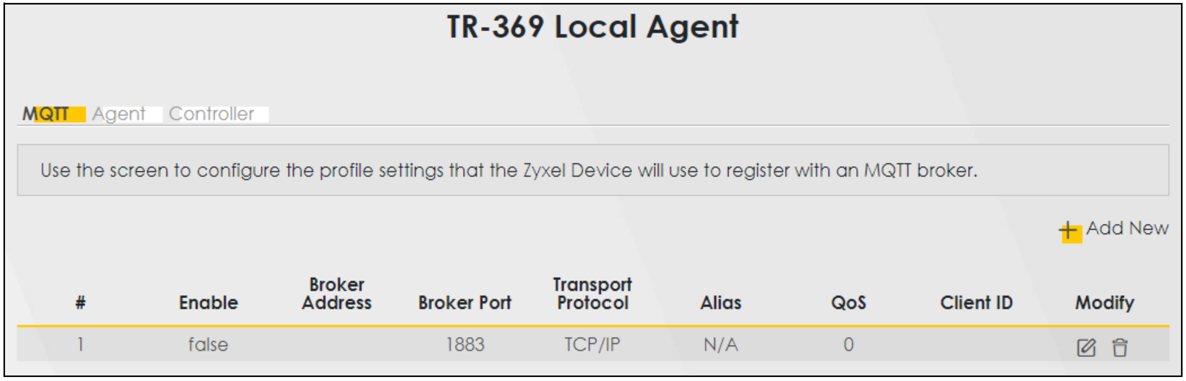
2. Then, configure the **Agent** screen. This **Endpoint ID** should identify the Zyxel Device acting as an agent. The **Alias** is a friendly name for the Zyxel Device. Set the **Response Topic** as the topic name for the Zyxel Device to receive USP messages from controllers. Select the **Reference** to be the MQTT client you configured in the **MQTT** screen. For example, Device.MQTT.Client.1.

3. Finally, configure the **Controller** screen. This **Endpoint ID** should identify the controller. The **Alias** is a friendly name for the controller. Set the **Topic** as the topic name for the Zyxel Device to publish USP messages to the controller. For example, /usp/controller/Zyxel.

28.3 MQTT

Click **Maintenance** > **TR-369 Local Agent** > **MQTT** to open the following screen. Use the screen to manage the profile settings that the Zyxel Device will use to register with an MQTT broker.

Figure 161 Maintenance > TR-369 Local Agent > MQTT



TR-369 Local Agent

Use the screen to configure the profile settings that the Zyxel Device will use to register with an MQTT broker.

#	Enable	Broker Address	Broker Port	Transport Protocol	Alias	QoS	Client ID	Modify
1	false		1883	TCP/IP	N/A	0		✎ 🗑

The following table describes the fields in this screen.

Table 101 Maintenance > TR-369 Local Agent > MQTT

LABEL	DESCRIPTION
Add New	Click this button to add a new MQTT client. Note: At the time of writing, you can add up to 128 MQTT clients.
#	This displays the index number of the MQTT client.

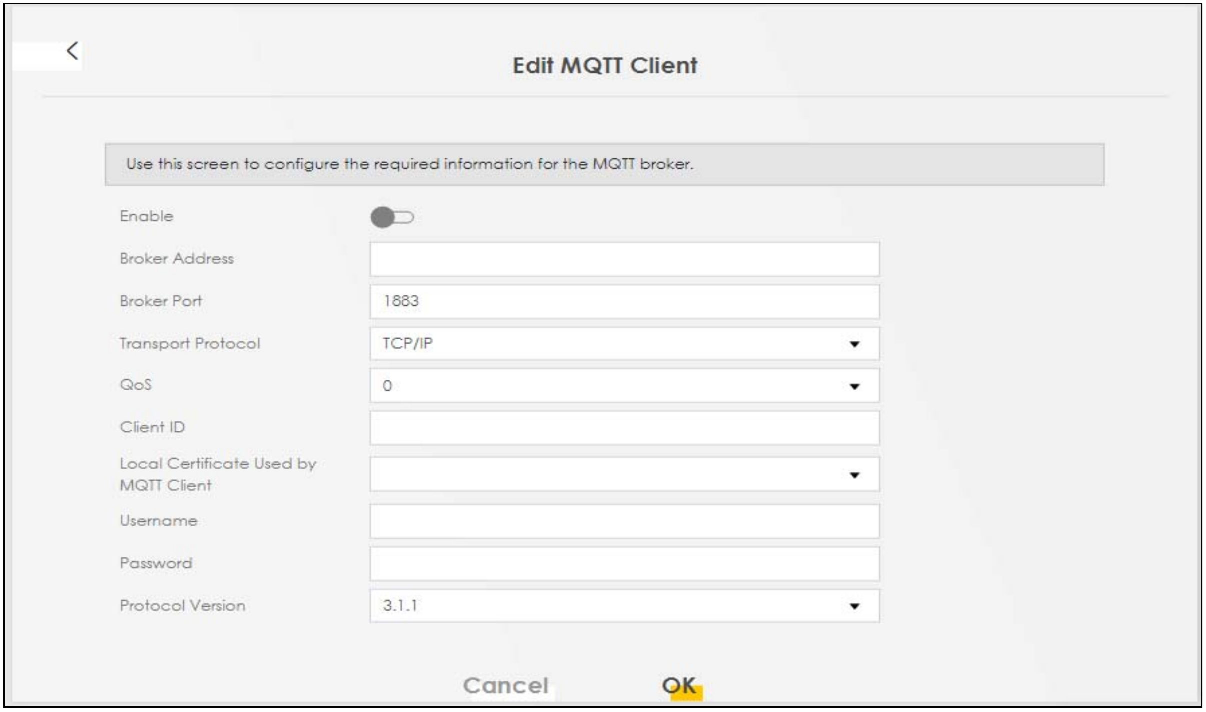
Table 101 Maintenance > TR-369 Local Agent > MQTT (continued)

LABEL	DESCRIPTION
Enable	This displays if the MQTT client is enabled.
Broker Address	This displays the URL of the MQTT broker.
Broker Port	This displays the port used for registration with the broker.
Transport Protocol	This displays the transport protocol (**TCP/IP** or **TLS**) for the Zyxel Device to send messages to the broker.
Alias	This displays a friendly name to identify the MQTT client.
QoS	This displays the Quality of Service transmission between the Zyxel Device and the broker.
Client ID	This field displays the unique **Client ID** of the client connecting to the MQTT broker.
Modify	Click the **Edit** icon to configure an entry. Click the **Delete** icon to remove an entry.

28.3.1 Add or Edit MQTT

Click **Add New** in the **MQTT** screen or click the **Edit** icon next to a controller. Use this screen to configure the required information for the MQTT broker.

Figure 162 Maintenance > TR-369 Local Agent > MQTT: Add or Edit



Edit MQTT Client

Use this screen to configure the required information for the MQTT broker.

Enable	○
Broker Address	
Broker Port	1883
Transport Protocol	TCP/IP ▾
QoS	0 ▾
Client ID	
Local Certificate Used by MQTT Client	▾
Username	
Password	
Protocol Version	3.1.1 ▾

The following table describes the fields in this screen.

Table 102 Maintenance > TR-369 Local Agent > MQTT: Add or Edit

LABEL	DESCRIPTION
Enable	Slide this to the right to enable this MQTT client.
Broker Address	Enter the URL of the MQTT broker. Make sure the broker is reachable from the Zyxel Device.
Broker Port	Enter the port used for registration with the broker. The default port is shown here. If the broker is using a different port, enter that port number here.

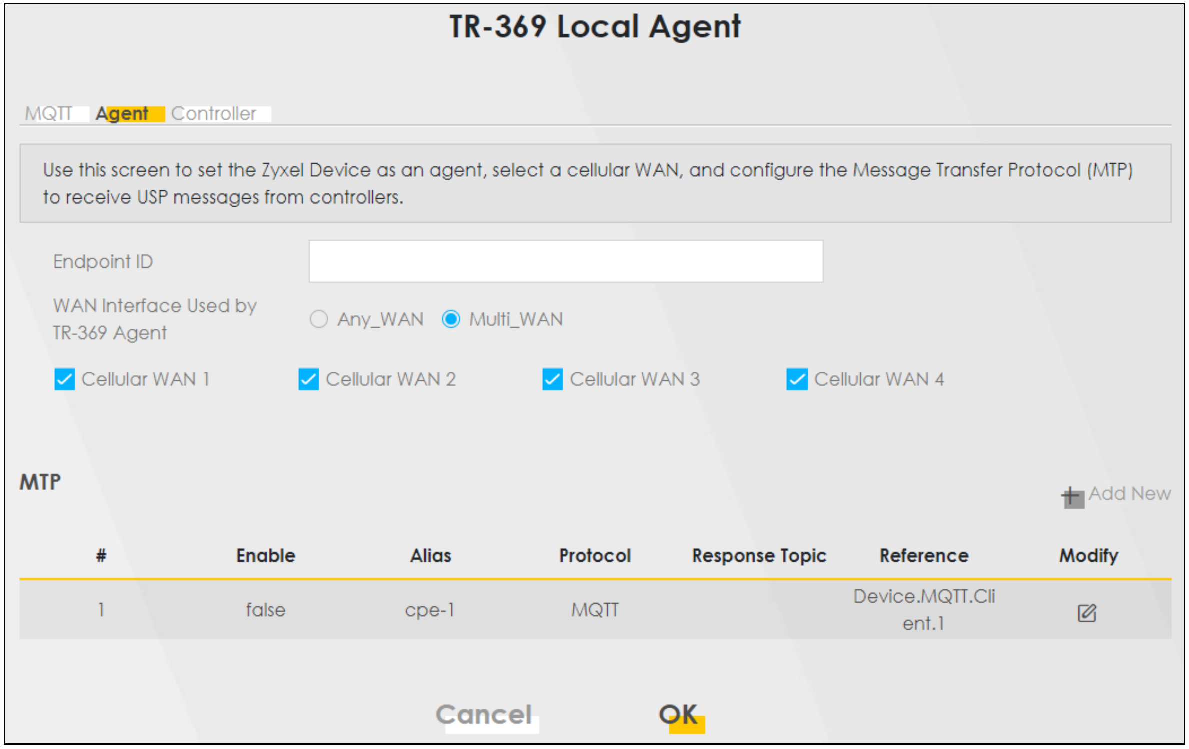
Table 102 Maintenance > TR-369 Local Agent > MQTT: Add or Edit (continued)

LABEL	DESCRIPTION
Transport Protocol	Select the transport protocol (**TCP/IP** or **TLS**) for the Zyxel Device to send messages. Select **TLS** is you want MTP message encryption using a certificate in TLS. Make sure the broker also supports TLS.
QoS	Select the Quality of Service transmission for messages sent from the Zyxel Device to the MQTT broker. Make sure the same settings were configured on the broker when you registered. **0** – At most once. When a message is sent, there is no guarantee that the message is delivered. The message may not be sent or sent just once. **1** – At least once. When a message is sent, the receiver will confirm that the message has been received. The message will be resent multiple times until confirmation is received. If the sender does not receive a response after a certain period of time, it will assume that the message was not delivered and resend the message. However, if the agent receives a message, but the response is missed due to a connection failure, the receiver will wrongly think that the sender has not received the reply message and send it again, resulting in the receiver receiving the same message repeatedly. **2** – Exactly once. This is used to avoid the receiver receiving the same message repeatedly. When a message is sent, the receiver will confirm that the message has been received and it will also send the same identification code that the sender sent. This is to make sure the reply message will not be sent again.
Client ID	Enter the unique **Client ID** of the MQTT client connecting to the MQTT broker. Enter between 1 and 23 UTF-8 encoded case-sensitive alpha-numeric characters. The MQTT broker determines the characters allowed for the Client ID.
Local Certificate Used by MQTT Client	Select the certificate if the **Transport Protocol** is using **TLS**. First, upload the certificate to the Zyxel Device in **Security** > **Certificates** > **Local Certificates**.
Username	Enter the user name if the MQTT broker requires it for login. Enter 0-255 printable characters including special characters and spaces.
Password	Enter the password if the MQTT broker requires it for login. Enter 0-255 printable characters including special characters and spaces.
Protocol Version	The Protocol Version must be the same version that you used to register with the broker. Select **3.1.1** or **5.0**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to restore the screen’s last saved settings.

28.4 TR-369 Local Agent

Click **Maintenance** > **TR-369 Local Agent** > **Agent** to open the following screen. Use this screen to set the Zyxel Device as an agent, select a cellular WAN, and configure the Message Transfer Protocol (MTP) to receive USP messages from controllers.

Figure 163 Maintenance > TR-369 Local Agent > Agent



TR-369 Local Agent

Use this screen to set the Zyxel Device as an agent, select a cellular WAN, and configure the Message Transfer Protocol (MTP) to receive USP messages from controllers.

Endpoint ID

WAN Interface Used by TR-369 Agent ○ Any_WAN ● Multi_WAN

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

MTP

#	Enable	Alias	Protocol	Response Topic	Reference	Modify
1	false	cpe-1	MQTT		Device.MQTT.Client.1	

The following table describes the fields in this screen.

Table 103 Maintenance > TR-369 Local Agent > Agent

LABEL	DESCRIPTION
Endpoint ID	This identifies the Zyxel Device acting as an agent. The Endpoint Identifier (ID) is used in the USP Record and various Parameters in a USP Message to uniquely identify agent endpoints. It can be globally or locally unique, either among all endpoints or among all controllers or all agents, depending on the scheme used for assignment. It has two mandatory and one optional components: authority-scheme, authority-id, and instance-id. These three components are combined as: authority-scheme ":" [authority-id] ":" instance-id The format of the authority-id is dictated by the authority-scheme. The format of the instance-id is dictated either by the authority-scheme or by the entity identified by the authority-id. When used in a certificate, an Endpoint ID is expressed as a urn in the bbf namespace as: "urn:bbf:usp:id:" authority-scheme ":" [authority-id] ":" instance-id When used anywhere else (e.g. in the to_id and from_id of a USP Record), the namespace information is omitted, and the Endpoint ID is expressed as: authority-scheme ":" [authority-id] ":" instance-id.
WAN Interface Used by TR-369 Agent	Select **Any WAN** to have the Zyxel Device use any cellular WAN that is available (the APN you enabled in **Network Setting** > **Broadband** > **Cellular APN**) to send TR-369 messages. Select **Multiple WAN** and then choose a specific WAN that you configured in **Network Setting** > **Broadband** > **Cellular APN** to send TR-369 messages.
MTP	The Message Transfer Protocol (MTP) is the protocol that carries a message.
Add New	At the time of writing, you can only have one agent MTP entry, so you can only edit the existing entry.
#	This displays the index number of the MTP (Message Transfer Protocol).

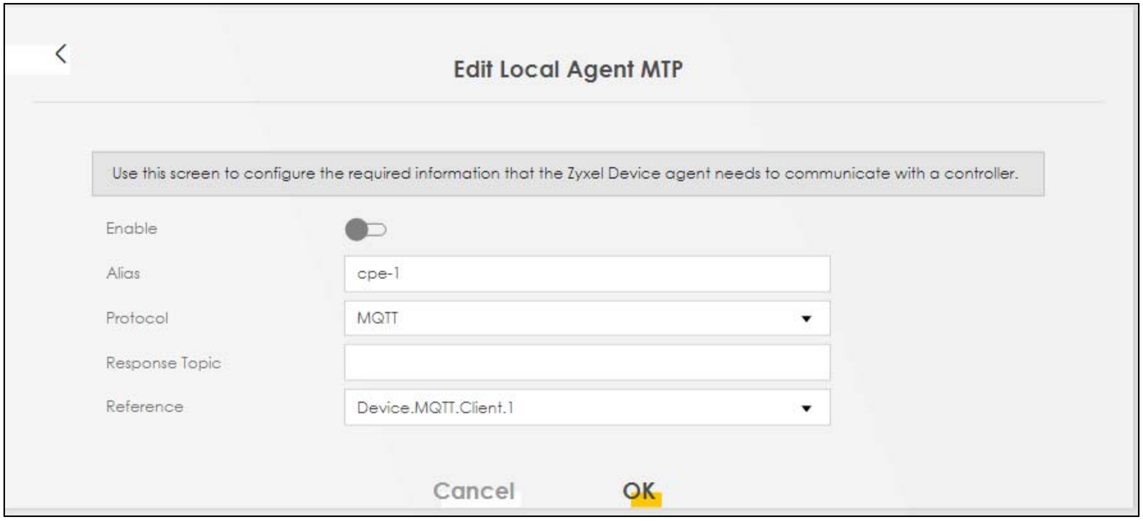
Table 103 Maintenance > TR-369 Local Agent > Agent (continued)

LABEL	DESCRIPTION
Enable	This displays if the Zyxel Device is enabled as an agent.
Alias	This is a friendly name for the Zyxel Device.
Protocol	The Zyxel Device supports the MQ Telemetry Transport (**MQTT**) protocol to send messages.
Response Topic	This displays the topic name for the Zyxel Device to receive USP messages.
Reference	This displays the MQTT client you configured in the MQTT screen. For example, Device.MQTT.Client.1.
Modify	Click the **Edit** icon to configure an entry.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to restore the screen's last saved settings.

28.4.1 Edit Agent

Click the **Edit** icon next to an agent in **Maintenance** > **TR-369 Local Agent** > **Agent**. Use this screen to configure the required information that the Zyxel Device agent needs to communicate with a controller.

Figure 164 Maintenance > TR-369 Local Agent > Agent: Edit



Edit Local Agent MTP

Use this screen to configure the required information that the Zyxel Device agent needs to communicate with a controller.

Enable

Alias: cpe-1

Protocol: MQTT

Response Topic:

Reference: Device.MQTT.Client.1

The following table describes the fields in this screen.

Table 104 Maintenance > TR-369 Local Agent > Agent: Edit

LABEL	DESCRIPTION
Enable	Slide this to the right to enable the Zyxel Device as a TR-369 agent.
Alias	Enter a unique name to identify the Zyxel Device acting as an agent to the controller. Please note the following: • The value must not be empty. • The value must start with a letter. • If the value is not assigned by the controller at creation time, you must assign a value with a "cpe-" prefix. • If the value is not assigned by the controller on creation, you must choose an initial value that doesn't conflict with any existing entries.
Protocol	At the time of writing, just the MQ Telemetry Transport (**MQTT**) protocol is used by the Zyxel Deviceto send messages.

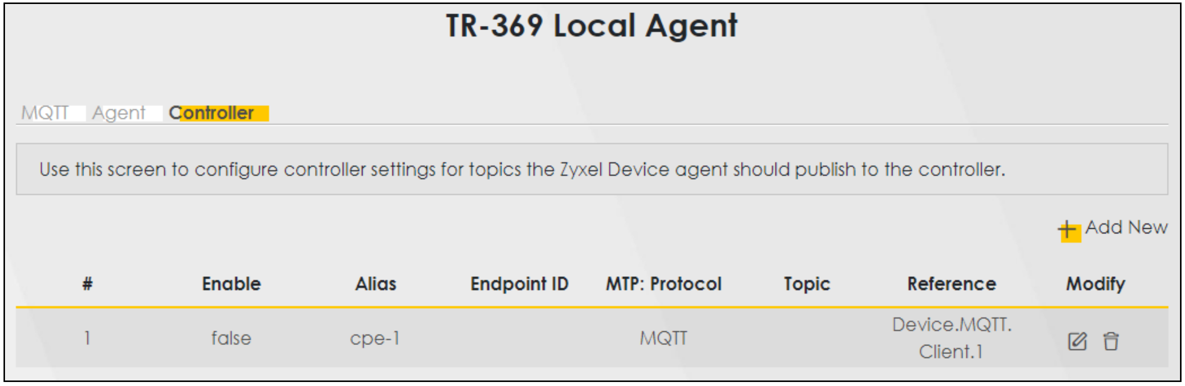
Table 104 Maintenance > TR-369 Local Agent > Agent: Edit (continued)

LABEL	DESCRIPTION
Response Topic	Set this as the topic name for the Zyxel Device to receive USP messages from controllers.You can subscribe to multiple topics at once using wildcards. See Section 28.1.2.1 on page 236.
Reference	Select the entry that is one of the MQTT clients you configured in the **MQTT** screen. For example, Device.MQTT.Client.1.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to restore the screen's last saved settings.

28.5 Controller

Click **Maintenance** > **TR-369 Local Agent** > **Controller** to open the following screen. Use this screen to configure controller settings for topics the Zyxel Device agent should publish to this controller.

Figure 165 Maintenance > TR-369 Local Agent > Controller



TR-369 Local Agent

Use this screen to configure controller settings for topics the Zyxel Device agent should publish to the controller.

#	Enable	Alias	Endpoint ID	MTP: Protocol	Topic	Reference	Modify
1	false	cpe-1		MQTT		Device.MQTT. Client.1	

The following table describes the fields in this screen.

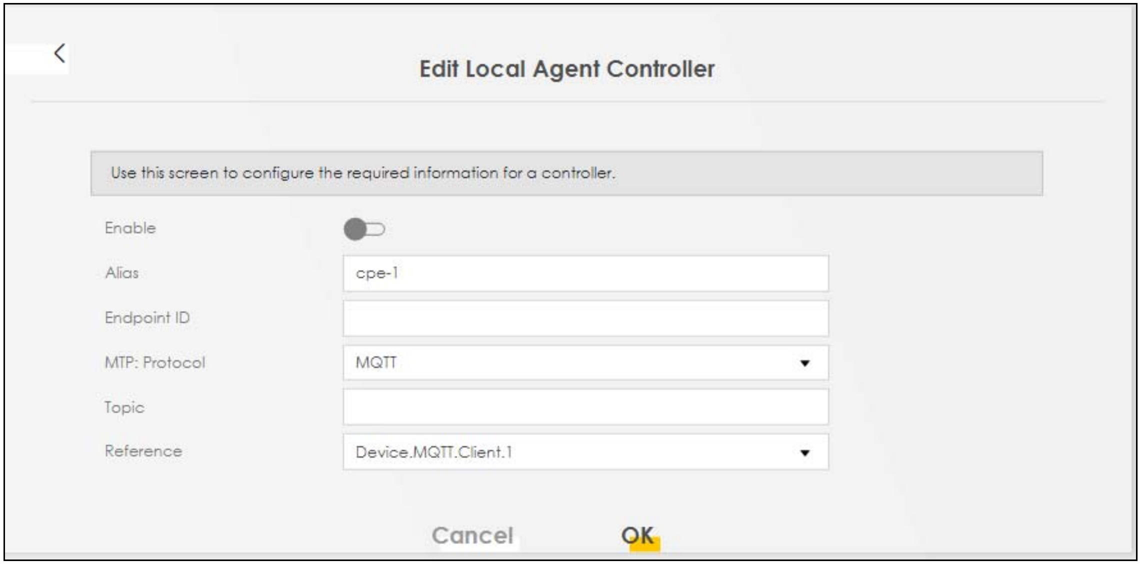
Table 105 Maintenance > TR-369 Local Agent > Controller

LABEL	DESCRIPTION
Add New	Click this button to add a new controller entry. Note: At the time of writing, you can add up to 8 controller entries.
#	The displays the index number of the controller entry.
Enable	This displays if the controller is enabled.
Alias	This displays a friendly name for the controller.
Endpoint ID	This identifies the controller.
MTP: Protocol	The Zyxel Device supports the MQ Telemetry Transport (**MQTT**) protocol to send and receive messages.
Topic	This displays the topic name for the Zyxel Device to publish USP messages to the controller.
Reference	This displays the MQTT client you configured in the **MQTT** screen.
Modify	Click the **Edit** icon to configure an entry. Click the **Delete** icon to remove an entry.

28.5.1 Add or Edit Controller

Click **Add New** in the **Controller** screen or click the **Edit** icon next to a controller. Use this screen to configure the required information for a controller.

Figure 166 Maintenance > TR-369 Local Agent > Controller: Add or Edit



Edit Local Agent Controller

Use this screen to configure the required information for a controller.

Enable

Alias: cpe-1

Endpoint ID

MTP: Protocol: MQTT

Topic

Reference: Device.MQTT.Client.1

The following table describes the fields in this screen.

Table 106 Maintenance > TR-369 Local Agent > Controller: Add or Edit

LABEL	DESCRIPTION
Enable	Slide this to the right to enable the controller.
Alias	Enter a unique name to identify the device acting as the controller. Please note the following: • The value must not be empty. • The value must start with a letter. • If the value is not assigned by the controller at creation time, you must assign a value with a "cpe-" prefix. If the value isn't assigned by the controller on creation, you must choose an initial value that doesn't conflict with any existing entries.
Endpoint ID	This identifies the device acting as a controller. The Endpoint Identifier (ID) is used in the USP Record and various parameters in a USP Message to uniquely identify Controller Endpoints. It can be globally or locally unique, either among all Endpoints or among all controllers or all agents, depending on the scheme used for assignment. It has two mandatory and one optional components: authority-scheme, authority-id, and instance-id. These three components are combined as: authority-scheme ":" [authority-id] ":" instance-id. The format of the authority-id is dictated by the authority-scheme. The format of the instance-id is dictated either by the authority-scheme or by the entity identified by the authority-id. When used in a certificate, an Endpoint ID is expressed as a urn in the bbf namespace as: "urn:bbf:usp:id:" authority-scheme ":" [authority-id] ":" instance-id When used anywhere else (for example, in the to_id and from_id of a USP Record), the namespace information is omitted, and the Endpoint ID is expressed as: authority-scheme ":" [authority-id] ":"instance-id.

Table 106   Maintenance > TR-369 Local Agent > Controller: Add or Edit (continued)

LABEL	DESCRIPTION
MTP: Protocol	Note: At the time of writing, the Zyxel Device just uses the MQ Telemetry Transport (**MQTT**) protocol to send messages
Topic	Set this as the topic name for the Zyxel Device to publish USP messages to the controller. It must not contain wildcards. See Section 28.1.2.2 on page 237. For example, /usp/controller/Zyxel.
Reference	Select this to be the MQTT client you configured in the **MQTT** screen. For example, Device.MQTT.Client.1.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to restore the screen's last saved settings.

CHAPTER 29
Time Settings

29.1 Time Settings Overview

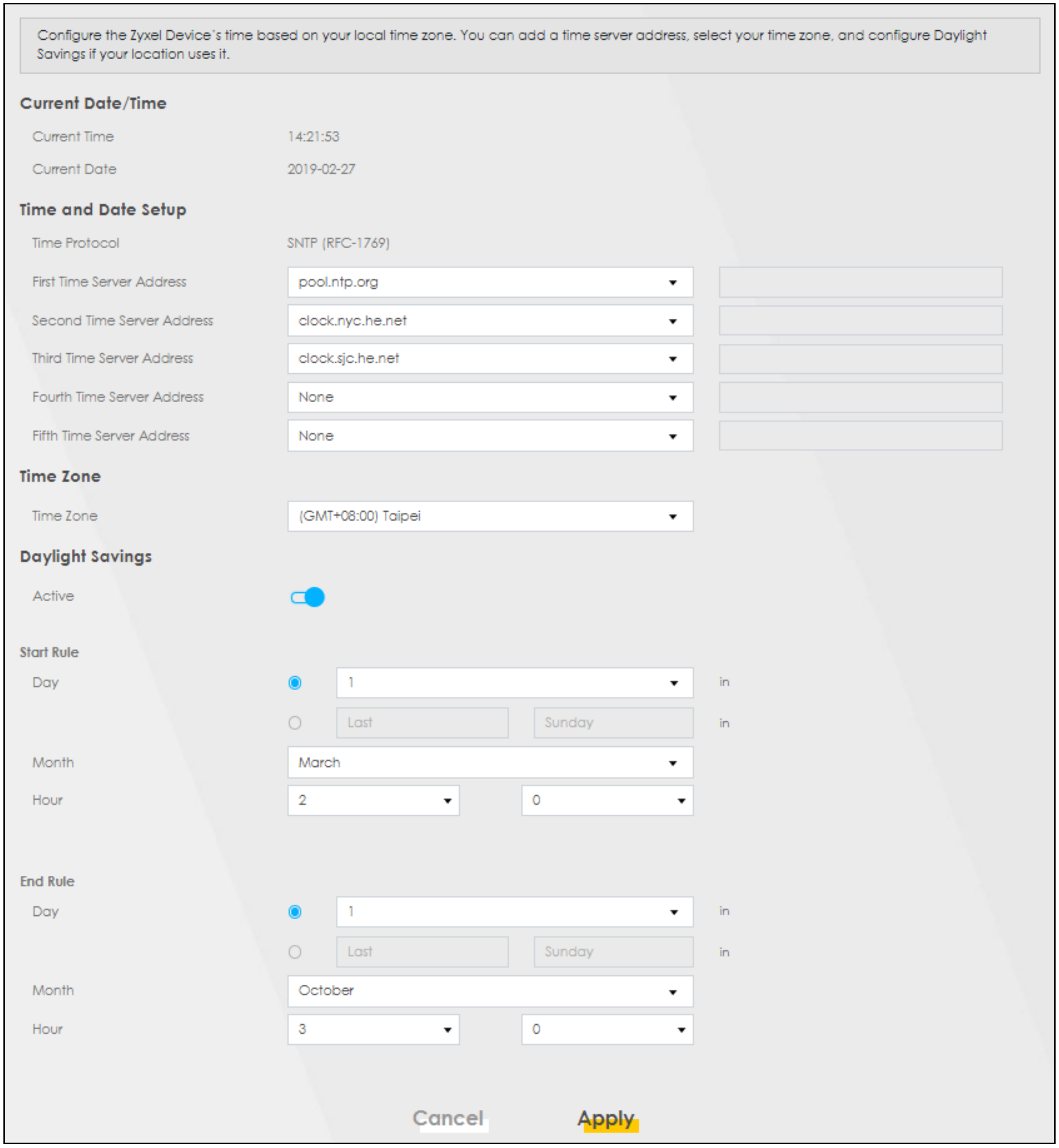
This chapter shows you how to configure system related settings, such as system date and time.

29.2 Time

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

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

Figure 167 Maintenance > 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 14:21:53

Current Date 2019-02-27

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 107 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This displays the time of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the time with the time server.
Current Date	This displays the date of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the date with the time server.
Time and Date Setup	
Time Protocol	This displays the time protocol used by your Zyxel Device.

Table 107 Maintenance > Time (continued)

LABEL	DESCRIPTION
First – Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 printable characters in length) of your time server. Select **None** if you do not want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.	
Active	Click this switch to enable or disable Daylight Saving Time. When the switch turns blue, the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 30 Email Notification

30.1 Email Notification Overview

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

To have the Zyxel Device send reports, logs or notifications through email, you must specify an email server and the email addresses of the sender and receiver.

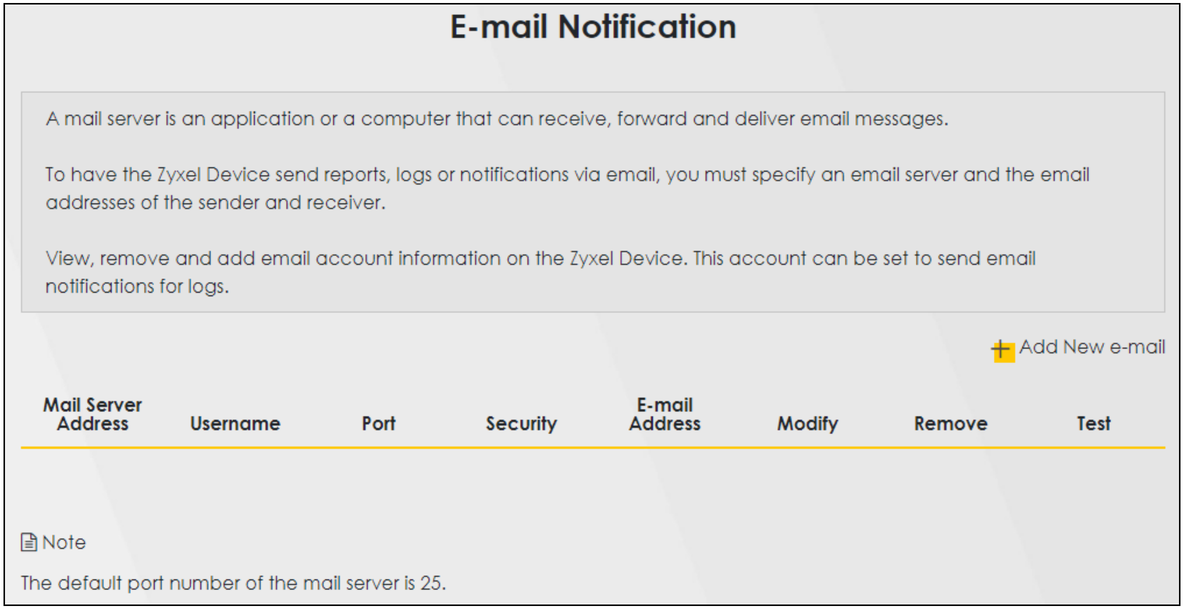
30.2 Email Notification

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

Click **Maintenance** > **E-mail Notification** to open the **E-mail Notification** screen.

Note: The default port number of the mail server is 25.

Figure 168 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.

Mail Server Address	Username	Port	Security	E-mail Address	Modify	Remove	Test

Note

The default port number of the mail server is 25.

The following table describes the labels in this screen.

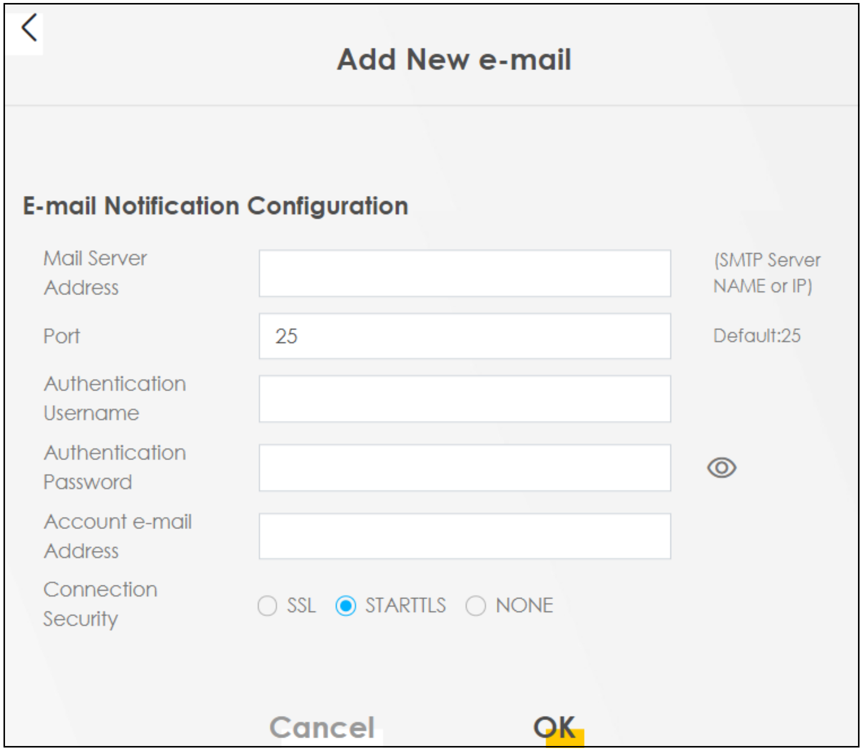
Table 108 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry (up to 32 can be created).
Mail Server Address	This displays the server name or the IP address of the mail server.
Username	This displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the email address that you want to be in the from or sender line of the email that the Zyxel Device sends.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Remove	Click this button to delete the selected entries.
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 email through a mail server.

Figure 169 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 109 Maintenance > E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the email address specified in the **Account e-mail Address** field. If this field is left blank, reports, logs or notifications will not be sent through email.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. This is usually the user name of a mail account you specified in the **Account email Address** field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the email address that you want to be in the from or sender line of the email notification that the Zyxel Device sends. If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well.
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

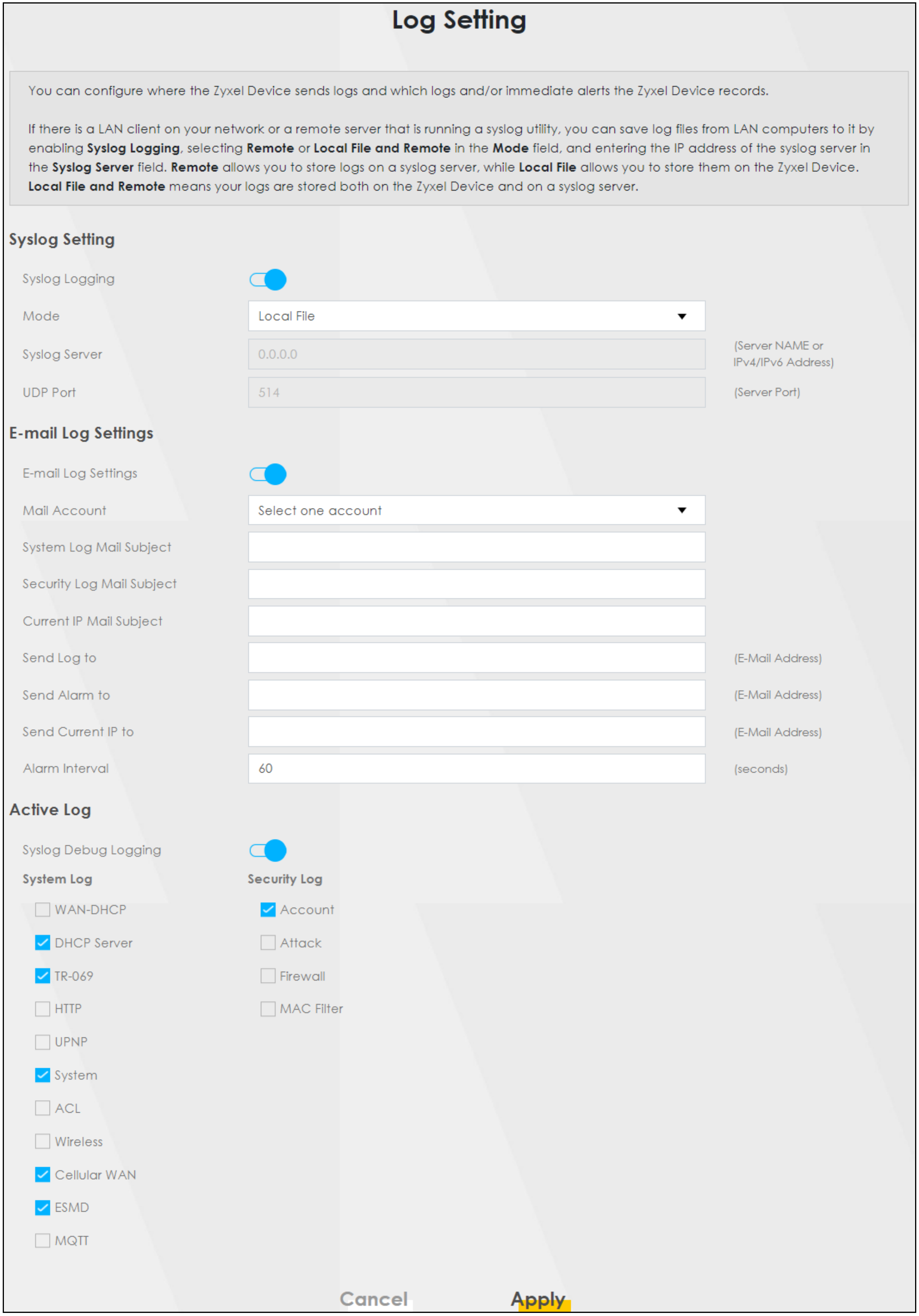
You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the **Logs Setting** screen.

31.2 Log Setting

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

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging**, and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the Zyxel Device. Select **Local File and Remote** to store logs on both the Zyxel Device and the syslog server. To change your Zyxel Device's log settings, click **Maintenance** > **Log Setting**. The screen appears as shown.

Figure 170 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	Security Log
□ WAN-DHCP	☑ Account
☑ DHCP Server	□ Attack
☑ TR-069	□ Firewall
□ HTTP	□ MAC Filter
□ UPNP	
☑ System	
□ ACL	
□ Wireless	
☑ Cellular WAN	
☑ ESMD	
□ MQTT	

The following table describes the fields in this screen.

Table 110 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Slide the switch to the right to enable syslog logging.
Mode	Select **Remote** to have the Zyxel Device send it to an external syslog server. Select **Local File** to have the Zyxel Device save the log file on the Zyxel Device itself. Select **Local File and Remote** to have the Zyxel Device save the log file on the Zyxel Device itself and send it to an external syslog server. Note: A warning appears upon selecting **Remote** or **Local File and Remote**. Just click **OK** to continue.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
E-mail Log Settings	Slide the switch to the right to allow the sending through email the system and security logs to the email address specified in **Send Log to**. Note: Make sure that the **Mail Server Address** field is not left blank in the **Maintenance** > **E-mail Notifications** screen.
Mail Account	Select a server specified in **Maintenance** > **E-mail Notifications** to send the logs to.
System Log Mail Subject	This field allows you to enter a descriptive name for the system log email (for example Zyxel System Log). Up to 127 printable characters are allowed for the **System Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Security Log Mail Subject	This field allows you to enter a descriptive name for the security log email (for example Zyxel Security Log). Up to 127 printable characters are allowed for the **Security Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Send Log to	This field allows you to enter the log's designated email recipient. The log's format is plain text file sent as an email attachment.
Send Alarm to	This field allows you to enter the alarm's designated e-mail recipient. The alarm's format is plain text file sent as an email attachment.
Alarm Interval	Select the frequency of showing of the alarm.
Active Log	
Syslog Debug Logging	Slide the switch to the right 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.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

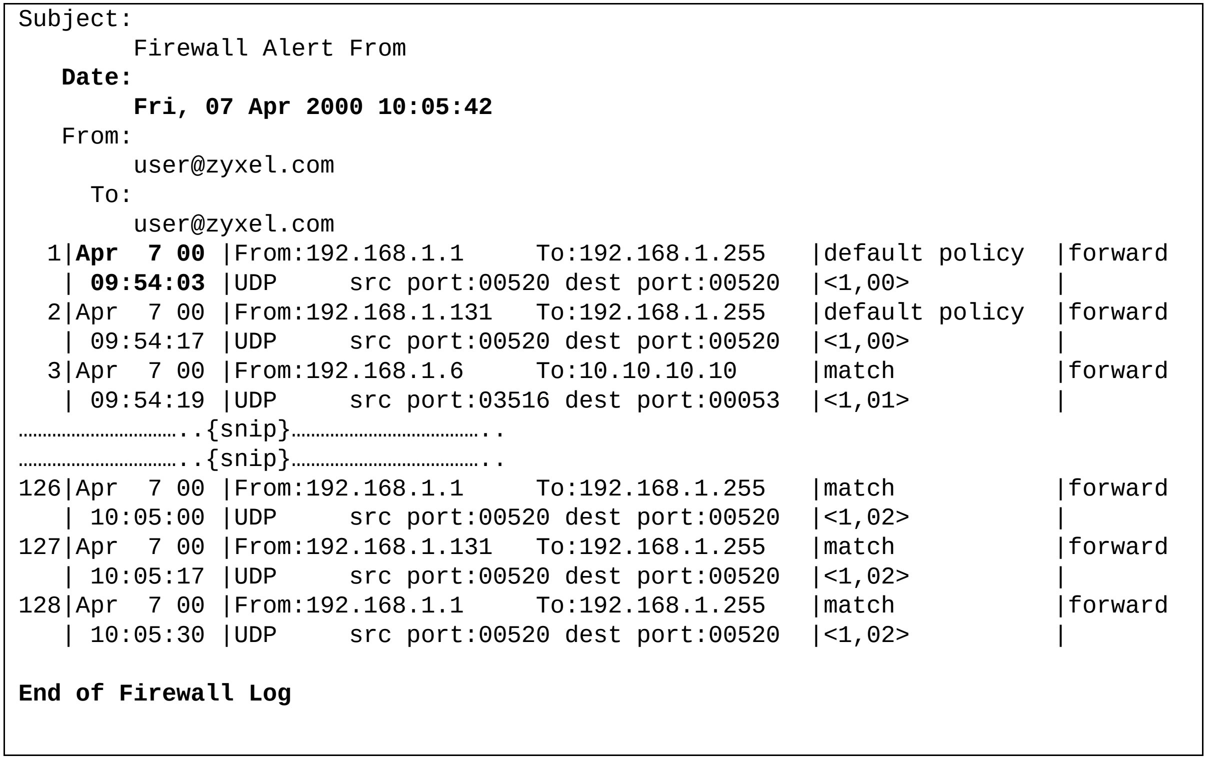
31.2.1 Example Email Log

An 'End of Log' message displays for each mail in which a complete log has been sent. The following is an example of a log sent by email.

- You may edit the subject title.
- The date format here is Day-Month-Year.

- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- ‘`End of Log`’ message shows that a complete log has been sent.

Figure 171 Email Log Example



```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
...............................{snip}.....................................
...............................{snip}.....................................
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

CHAPTER 32 Firmware Upgrade

32.1 Firmware Upgrade Overview

This chapter explains how to upload new firmware to your Zyxel Device if you get new firmware releases from your service provider.

32.2 Firmware Upgrade

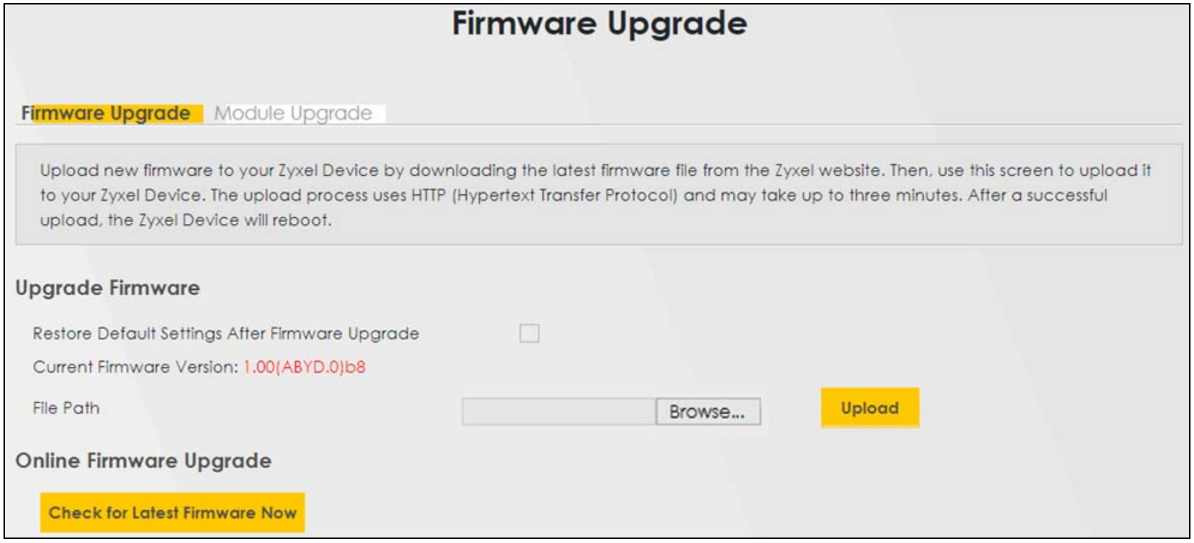
This screen lets you upload new firmware to your Zyxel Device.

Get the latest firmware from your service provider. Then upload the firmware file to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol). The upload may take up to 3 minutes. After a successful upload, the Zyxel Device will reboot.

Click **Maintenance** > **Firmware Upgrade** to open the **following** screen.

Do NOT turn off the Zyxel Device while firmware upload is in progress!

Figure 172 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

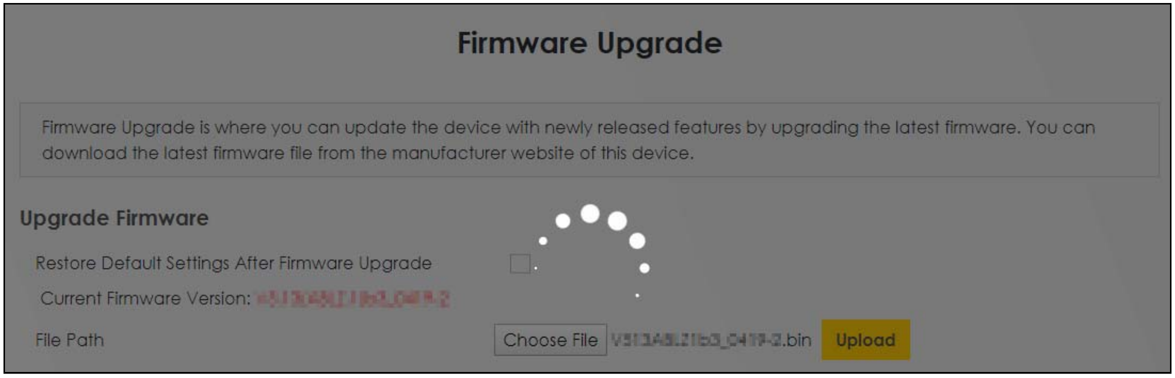
The following table describes the labels in this screen.

Table 111 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select this to reset all your configurations, including Mesh WiFi settings, to the factory defaults after firmware upgrade. Otherwise, make sure this is cleared if you do not want the Zyxel Device to lose all its current configurations and return to the factory defaults. Note: Make sure to back up the Zyxel Device's configuration settings first in case the reset all settings process is not successful.
Current Firmware Version	This is the current firmware version.
File Path	Enter the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it.
Choose File/ Browse	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to 3 minutes. Note: Only use firmware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device. For example, if the Zyxel Device's current firmware version is V5.70(ACDZ.0)B4, you must upload the firmware file containing "ACDZ".
Online Firmware Upgrade	
Do Online Firmware Upgrade	
Check for Latest Firmware Now	With the Zyxel Device connected to the Internet, click this 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.

Figure 173 Firmware Uploading



Firmware Upgrade

Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this device.

Upgrade Firmware

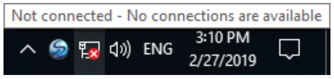
Restore Default Settings After Firmware Upgrade □

Current Firmware Version: [redacted]

File Path Choose File [redacted].bin Upload

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 174 Network Temporarily Disconnected

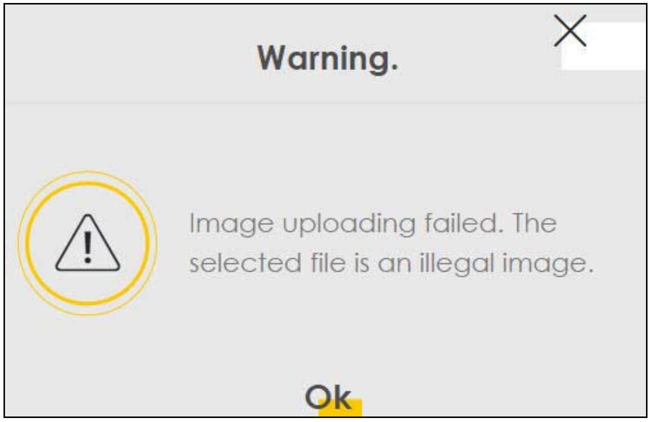


Not connected - No connections are available

After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

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

Figure 175 Error Message



Warning.

Image uploading failed. The selected file is an illegal image.

32.3 Module Upgrade

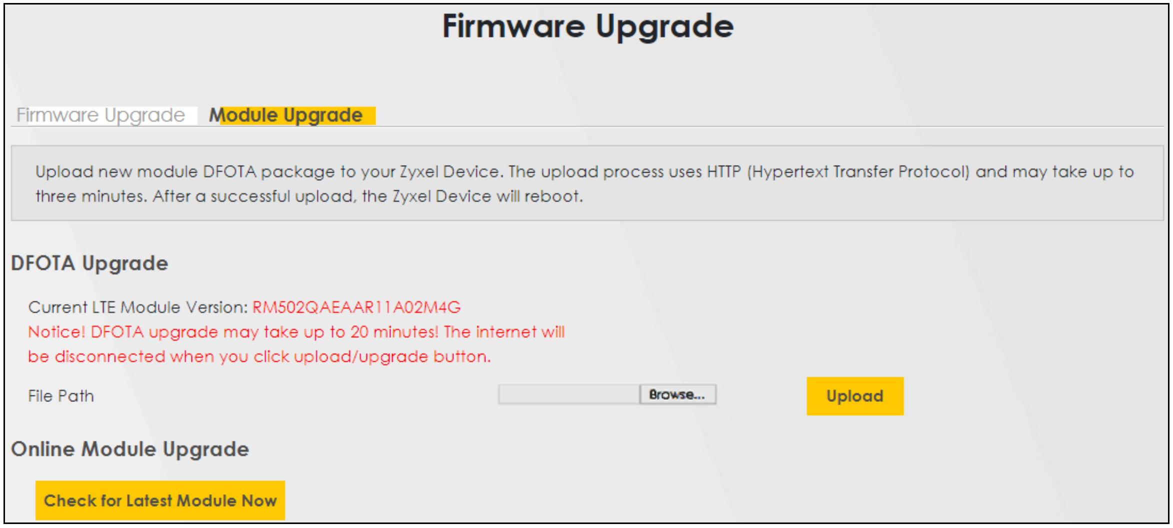
This screen lets you upload new firmware specific to the built-in LTE module in order to improve the LTE module's reliability and performance. The upload process uses HTTP (Hypertext Transfer Protocol) and may take more than 3 minutes. After a successful upload, the Zyxel Device will reboot.

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 module firmware upload is in progress!

Figure 176 Maintenance > Firmware Upgrade > Module Upgrade



Firmware 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.

DFOTA Upgrade

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

Online Module Upgrade

The following table describes the labels in this screen.

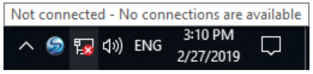
Table 112   Maintenance > Firmware Upgrade > Module Upgrade

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. 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 177   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

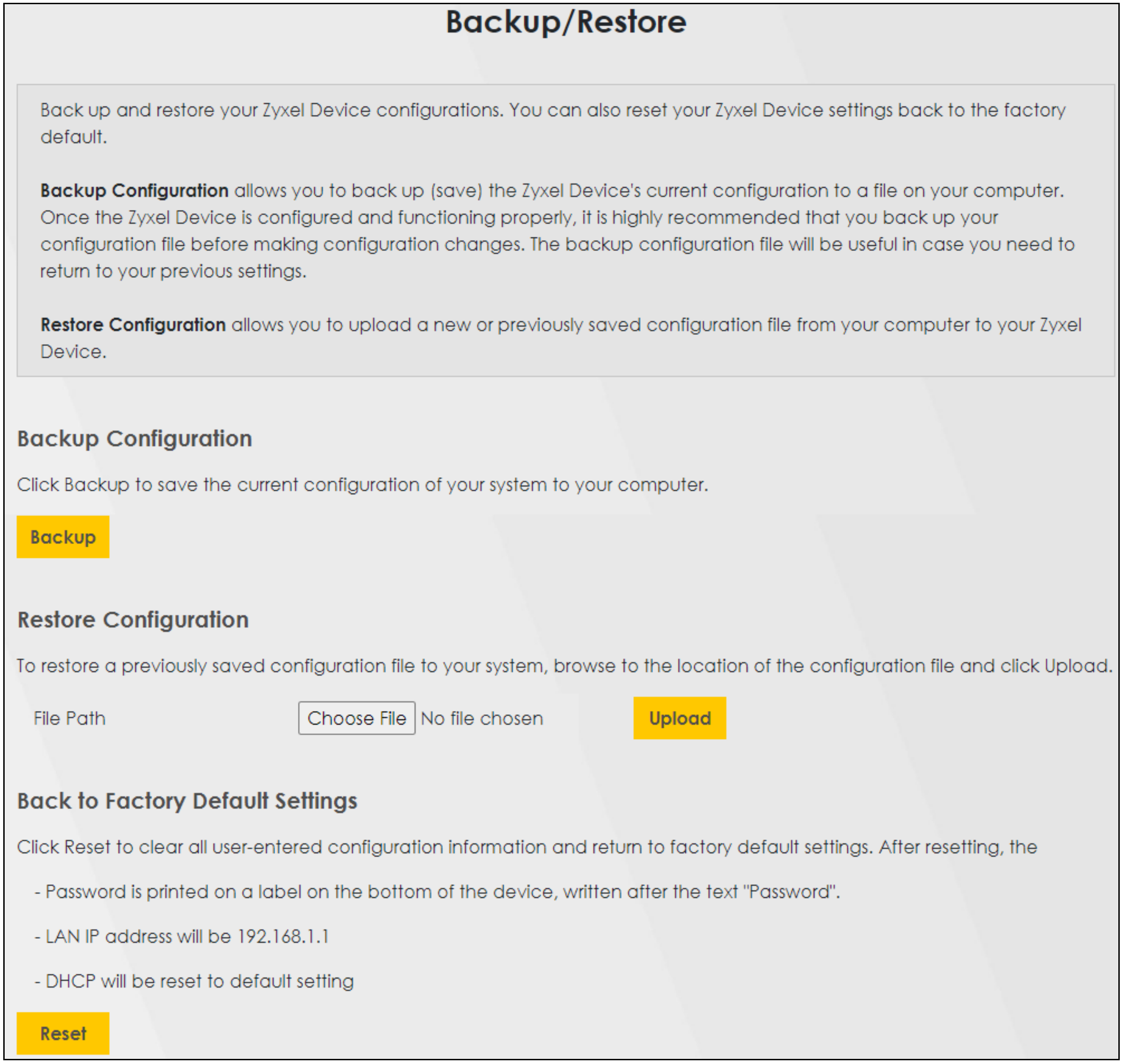
33.1 Backup/Restore Overview

Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore Zyxel Device's previous 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 178 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 chosen

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 113 Maintenance > Backup/Restore: Restore Configuration

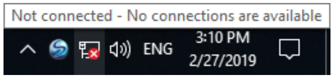
LABEL	DESCRIPTION
File Path	Enter in the location of the file you want to upload in this field or click **Choose File** / **Browse** to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your 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 179 Network Temporarily Disconnected

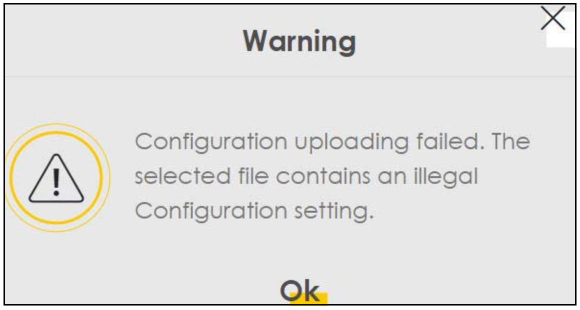


Not connected - No connections are available

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 (192.168.1.1-192.168.225.225).

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

Figure 180 Configuration Upload Error



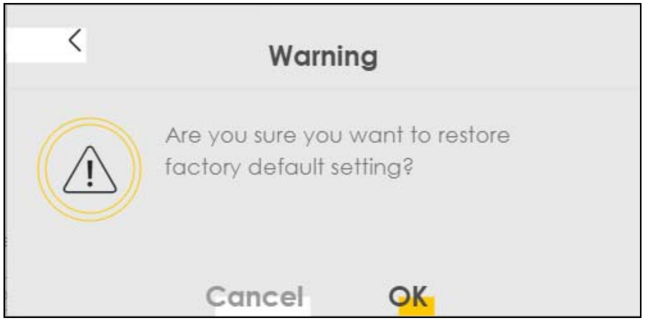
Warning

Configuration uploading failed. The selected file contains an illegal Configuration setting.

Reset All Settings

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

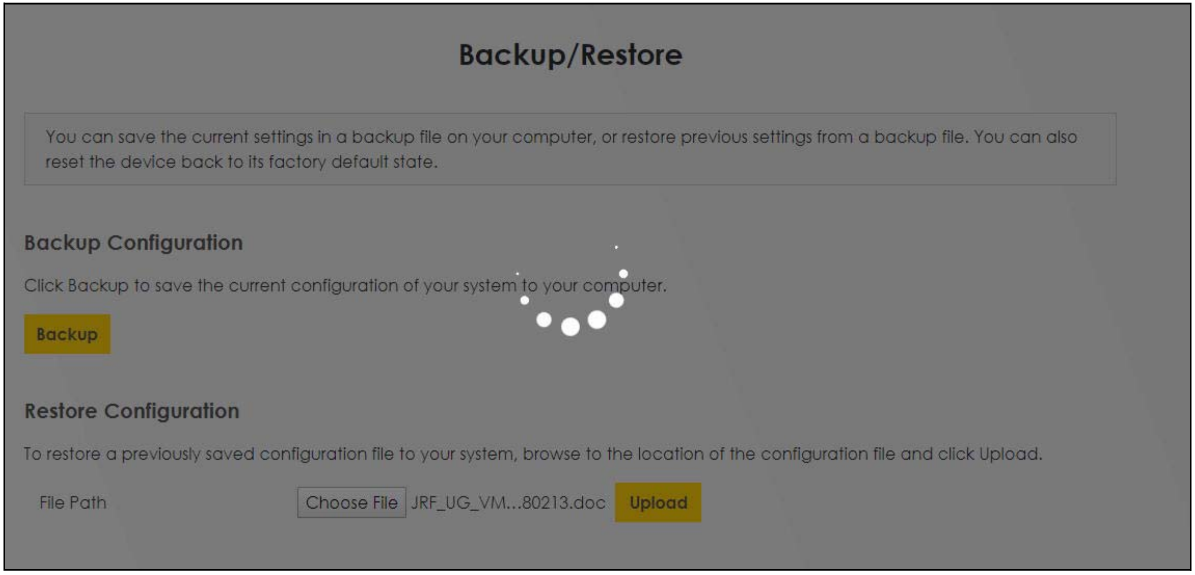
Figure 181 Reset Warning Message



Warning

Are you sure you want to restore factory default setting?

Figure 182 Reset In Progress



Backup/Restore

You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.

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 Choose File JRF_UG_VM...80213.doc

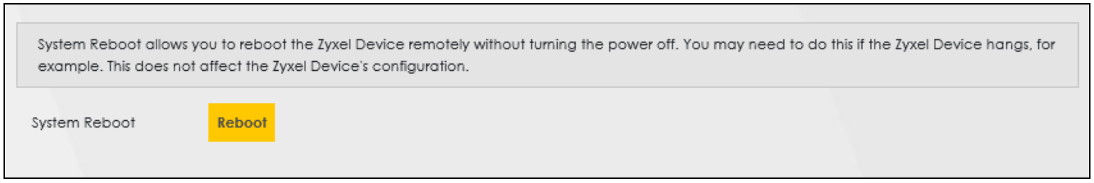
You can also press the **RESET** button on the panel to reset the factory defaults of your Zyxel Device.

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 183 Maintenance > 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.

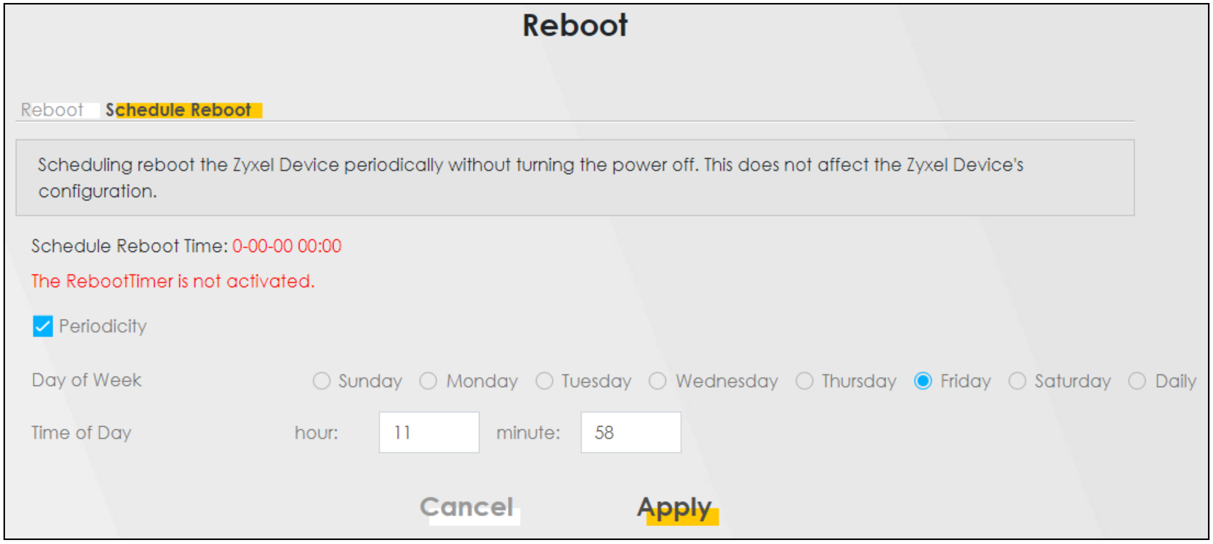
System Reboot

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** to open the following screen.

Figure 184 Maintenance > Reboot > Schedule Reboot



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

Day of Week ○ Sunday ○ Monday ○ Tuesday ○ Wednesday ○ Thursday ● Friday ○ Saturday ○ Daily

Time of Day hour: 11 minute: 58

The following table describes the labels in this screen.

Table 114 Maintenance > Reboot > Schedule Reboot

LABEL	DESCRIPTION
Periodicity	Select this to have 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	Select 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

The **Diagnostic** screen displays information to help you identify Internet connection problems with the Zyxel Device.

34.1.1 What You Can Do in this Chapter

- The **Diagnostic** screen lets you select different methods to test an Internet connection (Section 34.2 on page 265).

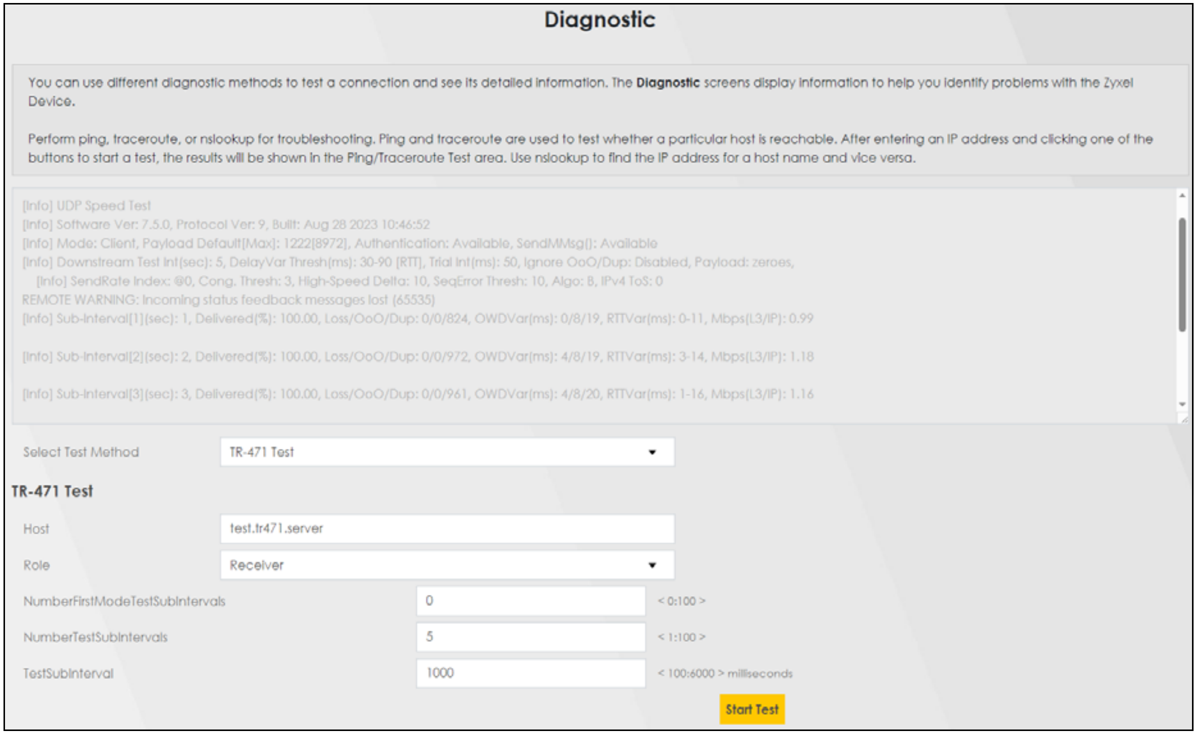
34.2 Diagnostic

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 screen. Use nslookup to find the IP address for a host name and vice versa. Use speed test to perform an upload and download throughput test for applications such as file transfer, web browsing and email. Use TR-471 test to perform an Internet connection quality test through a TR-471 test server for applications such as live streaming, online games and VoIP.

Note: Not all Zyxel Devices support speed test.

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

Figure 185 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.

```
[Info] UDP Speed Test
[Info] Software Ver: 7.5.0, Protocol Ver: 9, Built: Aug 28 2023 10:46:52
[Info] Mode: Client, Payload Default[Max]: 1222[8972], Authentication: Available, SendMMsg(): Available
[Info] Downstream Test Int(sec): 5, DelayVar Thresh(ms): 30-90 [RTT], Trial Int(ms): 50, Ignore OoO/Dup: Disabled, Payload: zeroes,
  [Info] SendRate Index: @0, Cong. Thresh: 3, High-Speed Delta: 10, SeqError Thresh: 10, Algo: B, IPv4 ToS: 0
REMOTE WARNING: Incoming status feedback messages lost (65535)
[Info] Sub-Interval[1](sec): 1, Delivered(%): 100.00, Loss/OoO/Dup: 0/0/824, OWDVar(ms): 0/8/19, RTTVar(ms): 0-11, Mbps(L3/IP): 0.99

[Info] Sub-Interval[2](sec): 2, Delivered(%): 100.00, Loss/OoO/Dup: 0/0/972, OWDVar(ms): 4/8/19, RTTVar(ms): 3-14, Mbps(L3/IP): 1.18

[Info] Sub-Interval[3](sec): 3, Delivered(%): 100.00, Loss/OoO/Dup: 0/0/961, OWDVar(ms): 4/8/20, RTTVar(ms): 1-16, Mbps(L3/IP): 1.16
```

Select Test Method: TR-471 Test

TR-471 Test

Host: test.tr471.server

Role: Receiver

NumberFirstModeTestSubIntervals: 0 < 0:100 >

NumberTestSubIntervals: 5 < 1:100 >

TestSubInterval: 1000 < 100:6000 > milliseconds

The following table describes the fields in this screen.

Table 115 Maintenance > Diagnostic

LABEL	DESCRIPTION
	The result of tests is shown here in the info area.
Select Test Method	
Ping	Select this to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area.
Ping 6	Select this to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area.
Trace Route	Select this to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Select this to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Select this to perform a DNS lookup on the IP address or host name.
Speed Test	Select this to perform an upload and download throughput test based on the TCP (Transmission Control Protocol). TCP ensures the successful delivery of messages and data across networks. Use this when you need to test applications such as file transfer, web browsing and email.
TR-471 Test	Select this to perform an Internet connection quality test by connecting to a TR-471 test server. The UDP-based (User Datagram Protocol) **TR-471 Test** prioritizes speed and efficiency. Use this when you need to test applications such as live streaming, online games and VoIP.
TCP/IP	
Address	Enter the IP address of a computer that you want to perform ping, trace route, nslookup, or speed test in order to test a connection.
TR-471 Test	

Table 115 Maintenance > Diagnostic (continued)

LABEL	DESCRIPTION
Host	Enter the IP address or FQDN (fully qualified domain name) of the TR-471 test server from your SP (service provider). The Zyxel Device will receive or send test packets from/to the test server.
Role	Select **Receiver** to do a download test to the Zyxel Device. Select **Sender** to do an upload test from the Zyxel Device.
Number First Mode Test Sub Intervals	To display two time test intervals (bimodal testing) in the info area, enter the number of measurement intervals (i), where (i) is any whole number from **1** to **100**. • 1 to i (**Number First Mode Test Sub Intervals**) – this is the first time test intervals. • i + 1 to m (where (m) is the value of the next field **Number Test Sub Intervals**) – this is the second time test intervals. Alternatively, enter **0** to display one time test interval only in the info area.
Number Test Sub Intervals	Enter the number of intermediate measurement intervals (m), where (m) is any whole number from **1** to **100**.
Test Sub Interval	Enter the duration in milliseconds of measurement reporting interval, where the interval is any whole number from **100** to **6000**. For example, if the **Number Test Sub Intervals** (m) is 10 and **Test Sub Interval** is 2000 milliseconds, then the test will last 20 seconds where 10 intervals (m) multiplied by 2 seconds (2000 milliseconds) is equal to 20 seconds.

Table 115 Maintenance > Diagnostic (continued)

LABEL	DESCRIPTION
	After clicking **Start Test**, the result for maximum upstream test when the **Role** is **Sender**, or maximum downstream test when the **Role** is **Receiver**, is displayed. Example 1. When the **Role** is **Receiver**, i is 2 intervals, m is 4 intervals and **Test Sub Interval** is 6 seconds, the following example measurement intervals are displayed in the info area. [Info] Sub-Interval[**1**](sec): 6, Delivered(%): 100.00, Loss/OoO/Dup: 0/54/5123, OWDVar(ms): 0/5/39, RTTVar(ms): 0-30, Mbps(L3/IP): 1.04 [Info] Sub-Interval[**2**](sec): 12, Delivered(%): 99.96, Loss/OoO/Dup: 5/3/5887, OWDVar(ms): 0/5/19, RTTVar(ms): 0-20, Mbps(L3/IP): **1.19** [Info] Sub-Interval[3](sec): 18, Delivered(%): 99.97, Loss/OoO/Dup: 4/2/5815, OWDVar(ms): 1/5/27, RTTVar(ms): 0-19, Mbps(L3/IP): 1.18 [Info] Sub-Interval[4](sec): 24, Delivered(%): 99.99, Loss/OoO/Dup: 1/0/5450, OWDVar(ms): 1/6/21, RTTVar(ms): 0-23, Mbps(L3/IP): 1.10 [Info] Downstream Summary Delivered(%): 99.99, Loss/OoO/Dup: 13/105/55831, OWDVar(ms): 0/6/122, RTTVar(ms): 0-111, Mbps(L3/IP): 1.13 [Info] Downstream Minimum One-Way Delay(ms): 9 [w/clock difference], Round-Trip Time(ms): 25 [Info] Downstream Max[**1-2**] Mbps(L3/IP): **1.19**, Mbps(L2/Eth): 1.21, Mbps(L1/Eth): 1.53, Mbps(L1/Eth+VLAN): 1.59 [Info] Downstream Max[3-4] Mbps(L3/IP): 1.18, Mbps(L2/Eth): 1.42, Mbps(L1/Eth): 1.79, Mbps(L1/Eth+VLAN): 1.86 This means that for the first set of two (6 seconds) test interval (1 to i), the best result of the download test is 1.19 Mbps. On the second set of two (6 seconds) test interval (i + 1 to m), the best result of the download test is 1.18 Mbps. Example 2. When the **Role** is **Receiver**, i is 0 interval, m is 2 intervals and **Test Sub Interval** is 5 seconds, the following example measurement interval is displayed in the info area. This means that for a set of two (5 seconds) test interval (i + 1 to m), the best result of the download test is 1.20 Mbps. [Info] Sub-Interval[1](sec): 5, Delivered(%): 99.97, Loss/OoO/Dup: 1/1/1726, OWDVar(ms): 0/4/17, RTTVar(ms): 0-21, Mbps(L3/IP): 1.04 [Info] Sub-Interval[2](sec): 10, Delivered(%): 100.00, Loss/OoO/Dup: 0/1/1982, OWDVar(ms): 0/4/22, RTTVar(ms): 2-24, Mbps(L3/IP): **1.19** [Info] Downstream Summary Delivered(%): 99.98, Loss/OoO/Dup: 7/19/19013, OWDVar(ms): 0/5/22, RTTVar(ms): 0-26, Mbps(L3/IP): 1.15 [Info] Downstream Minimum One-Way Delay(ms): 11 [w/clock difference], Round-Trip Time(ms): 26 [Info] Downstream [Info] Maximum Mbps(L3/IP): **1.19**, Mbps(L2/Eth): 1.41, Mbps(L1/Eth): 1.79, Mbps(L1/Eth+VLAN): 1.85
Start Test	Click this to perform the selected test method.

PART III
Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your Zyxel Device.

CHAPTER 35 Troubleshooting

35.1 Troubleshooting 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.

PoE Devices

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.

The LED does not behave as expected.

1 Make sure you understand the normal behavior of the LED.

2 Check the hardware connections.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the Zyxel Device off and on.

5 If the problem continues, contact the vendor.

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.

I forgot the admin password.

1 See the Zyxel Device label or this document's cover page for the default admin password.

2 If you changed the password from default and cannot remember the new one, you have to reset the Zyxel Device to its factory default settings.

I cannot access the Web Configurator login screen.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten the new address, see the troubleshooting suggestions for I do not know the IP address of the Zyxel Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.

4 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.

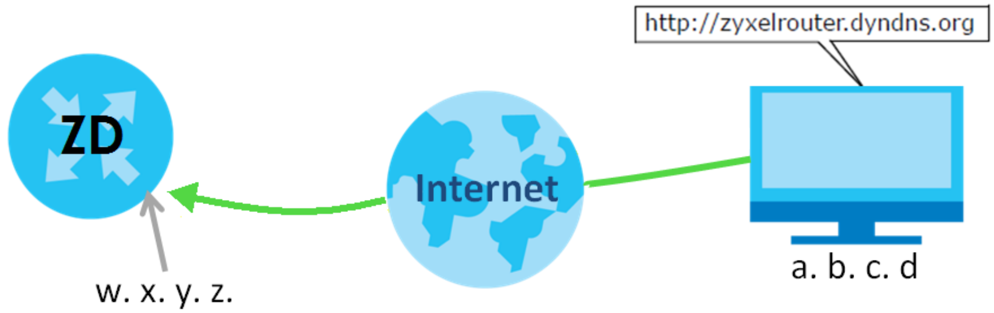
2 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

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 log into the Zyxel Device using DDNS.

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the Zyxel Device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

Note: If you have a private WAN IP address, then you cannot use DDNS.

Here are the three steps to use a domain name to log in the Web Configurator:

Step 1 Register for a DDNS Account on www.dyndns.org

1 Open a browser and enter **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the Zyxel Device later.

Step 2 Configure DDNS on Your Zyxel Device

Configure the following settings in the **Network Setting** > **DNS** > **Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Enter **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**). Click **Apply**.

Step 3 Test the DDNS Setting

Now you should be able to access the Zyxel Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Enter **http://zyxelrouter.dyndns.org** and press [Enter].

3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

I cannot connect to the Zyxel Device using 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.

3 Try the troubleshooting suggestions for I cannot access the Web Configurator login screen. Ignore the suggestions about your browser.

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, the account has expired, it needs to be removed and reinserted (refer to the Quick Start Guide), or it is missing.

3 Make sure you entered your ISP account information correctly on the **Network Setting** > **Broadband** screen. Fields on this screen are case-sensitive, so check if [Caps Lock] is on of off.

4 Disconnect all the cables from your Zyxel 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 (such as microwaves, other wireless networks).

3 Turn the Zyxel Device off and on.

4 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions in I cannot access the Web Configurator login screen.

Note: If your Zyxel Device is an outdoor-type, inclement weather like rain and hot weather may affect cellular signals.

35.6 WiFi Problems

I cannot connect to the Zyxel Device WiFi.

1. Check the WiFi LED status to make sure the Zyxel Device WiFi is on.
2. Make sure your WiFi client is within transmission range of the Zyxel Device.
3. Make sure you entered the correct SSID and password. See the Zyxel Device back label for the default SSID and password.
4. Make sure your WiFi client is using the same WiFi security type (WPA2-PSK or none) as the Zyxel Device.
5. Make sure the WiFi adapter on your WiFi client is working properly. Right-click your computer's network adapter then select **Properties** to check your network adapter status.
6. Make sure the WiFi adapter on your WiFi client is IEEE 802.11-compatible and supports the same WiFi standard as the Zyxel Device radio.

The WiFi has no Internet connection.

The Zyxel Device WiFi is for management only. The Zyxel Device WiFi has no Internet connection and will be automatically turned off 30 minutes after the Zyxel Device boots up.

The WiFi connection is slow and intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your WiFi connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the WiFi client.
- Reduce the number of WiFi clients connecting to the same AP simultaneously, or add additional APs if necessary.

- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Place the Zyxel Device where there are minimum obstacles (such as walls and ceilings) between the Zyxel Device and the WiFi client. Avoid placing the Zyxel Device inside any type of box that might block WiFi signals.

35.7 UPnP Problems

My computer cannot detect UPnP settings from the Zyxel Device.

1. Make sure that UPnP is enabled in your computer.
2. On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings** > **Home Networking** > **UPnP** screen.
3. Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.
4. Reconnect the Ethernet cable.
5. Restart your computer.

35.8 Getting More Troubleshooting Help

Search for support information for your model at *https://service-provider.zyxel.com/global/en/tech-support* and *community.zyxel.com* for more troubleshooting suggestions.

Appendix A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the Zyxel Device.

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

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

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

Korea

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

Malaysia

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Belarus

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

Belgium (Netherlands)

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

Bulgaria

- Zyxel Bulgaria

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

Czech Republic

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

Denmark

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Norway

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

Poland

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

Romania

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

Russian Federation

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

Slovakia

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

Spain

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

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

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

South America

Argentina

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

Brazil

- Zyxel Communications Brasil Ltda.

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

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

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

North America

USA

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

APPENDIX B
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 116 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 117 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 118 Reserved Multicast Address

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

Subnet Masking

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

Interface ID

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

EUI-64

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

Table 119

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

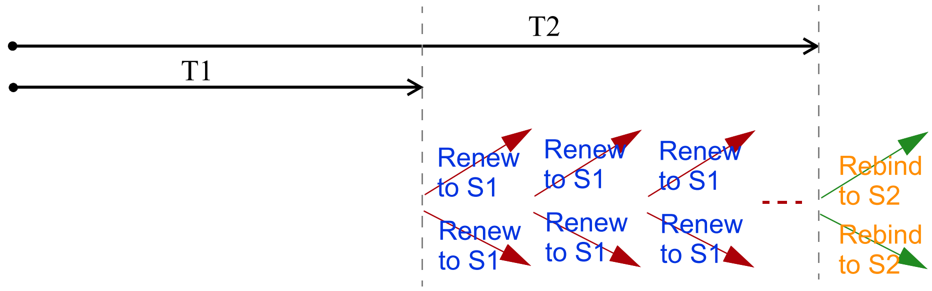
Table 120

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

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

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

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

Prefix Delegation

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

ICMPv6

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

Neighbor Discovery Protocol (NDP)

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

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

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

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

Multicast Listener Discovery

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

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

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

MLD filtering controls which Multicast groups a port can join.

MLD Messages

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

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

Example – Enabling IPv6 on Windows 10

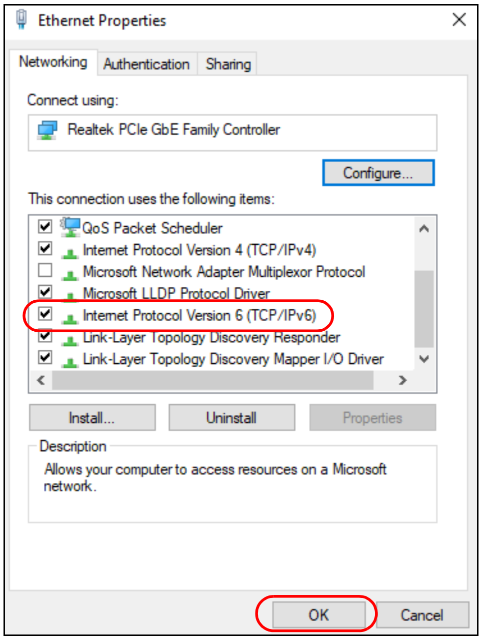
Windows 10 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 10 computer.

To enable IPv6 in Windows 10:

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

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



Connect using:

Realtek PCIe GbE Family Controller

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Description

Allows your computer to access resources on a Microsoft network.

4 Click the Search icon (🔍) and then enter “cmd” in the search box..

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

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

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

APPENDIX C
Legal Information

Copyright

Disclaimer

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

Regulatory Notice and Statement

EUROPEAN UNION and UNITED KINGDOM

CE and UK CA

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Radio Equipment Regulations 2017

- 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/FWA710)

- 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

(NR7302)

- WCDMA Band I/VIII is 24 dBm
- LTE Band 1/3/7/8/20/28/40 is 25 dBm
- LTE Band 38/42/43 is 28 dBm
- NR Band n1/n3/n7/n8/n20/n28/n38/n40 is 25 dBm
- NR Band n77/n78 is 28 dBm
- Wi-Fi The band 2400 – 2483.5 MHz is 19.95 dBm

(NR7303)

- WCDMA Band I/VIII is 24 dBm
- LTE Band 1/3/5/7/8/20/28/32/38/40/41/42/43 is 23 dBm
- NR Band n40/n41/n77/n78 is 26 dBm

- Wi-Fi The band 2400-2483.5 MHz is 99.77mW

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.
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 *https://www.mise.gov.it/it/* for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare *https://www.mise.gov.it/it/* per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
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 store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device. Opening or removing the device covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connected cables carefully so that no one will step on them or stumble over them.
- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect the power adaptor or cord to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove the damaged power adaptor or cord from the device and the power source. Do not try to repair the power adaptor or cord by yourself. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this device, please contact your local city office, your household waste disposal service, or the store where you purchased the device.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device:

  – For a permanently connected device, a readily accessible method to disconnect the device shall be incorporated externally to the device;

  – For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

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.

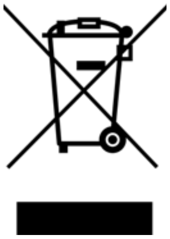
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung 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:

- 請勿將此產品接近火焰或放置在高溫的環境。
- 避免設備接觸:
  – 灰塵及污物 – 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。

- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 （如：台灣供應電壓 110 伏特）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿隨一般垃圾丟棄。
- 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.

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://www.zyxel.com/form/gpl_oss_software_notice.shtml

https://service-provider.zyxel.com/global/en/gpl-oss-software-notice.

Index