ZYXEL
Your Networking Ally

User's Guide

LTE7461-M602

LTE Outdoor Router

Default Login Details

LAN IP Address	http://192.168.1.1
Login	admin
Password	See the Zyxel Device label
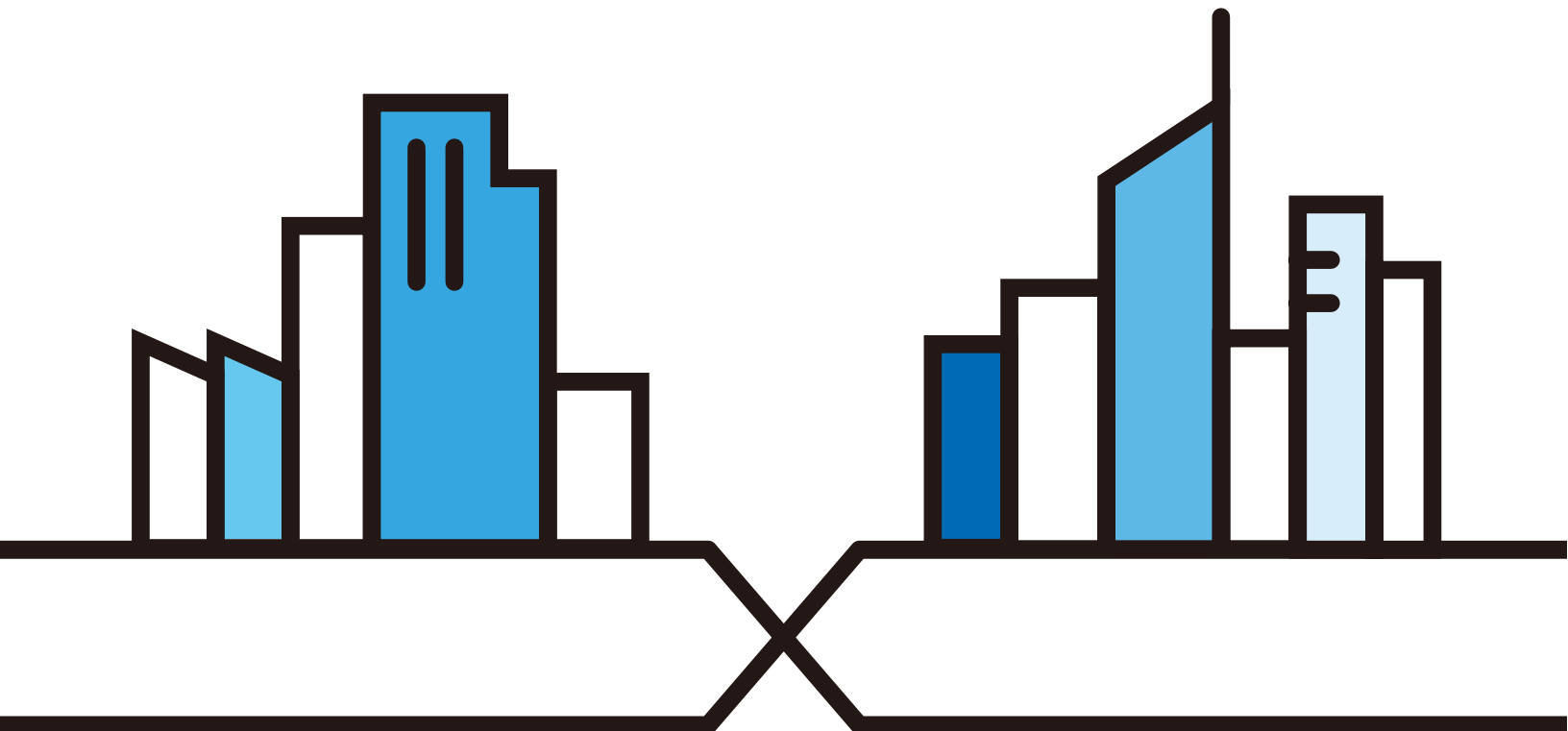
IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for the LTE7461-M602. Screenshots and graphics in this book may differ slightly from what you see due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

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

- More Information

    Go to **support.zyxel.com** to find other information on the Zyxel Device.

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

- The LTE7461-M602 in this user's guide may be referred to as the "Zyxel Device" in this guide.

- Product labels, screen names, field labels and field choices are all in **bold** font.

- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting > Routing > DNS Route** means you first click **Network Setting** in the navigation panel, then the **Routing** sub menu and finally the **DNS Route** tab to get to that screen.

Icons Used in Figures

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

Zyxel Device	Generic Router	Switch
Server	Firewall	USB Storage Device
Printer		

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

The Zyxel Device is an outdoor LTE (Long Term Evolution) router that supports (but not limited to) the following:

- Gigabit Ethernet connection
- DHCP (Dynamic Host Configuration Protocol) server
- NAT (Network Address Translation)
- DMZ (Demilitarized Zone)
- Port Forwarding/Triggering
- ALG (Application Layer Gateway)
- Bridge/Router mode
- Dynamic DNS (Domain Name System) for the first APN (Access Point Name)
- Static/Dynamic Route setting for RIP (Routing Information Protocol)
- Remote Management under Bridge mode
- Address Resolution Protocol (ARP)
- Firewall that uses Stateful Packet Inspection (SPI) technology
- Protects against Denial of Service (DoS) attacks
- Filter of LAN MAC address, LAN IP address and URLs
- Local and remote device management
- Firmware upgrade via TR-069 and Web Configurator

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 mounting, Internet setup and turning on/off WiFi (optional).

1.2 Application for the Zyxel Device

Wireless WAN

The LTE Device can connect to the Internet through a 2G/3G/4G LTE SIM card to access a wireless WAN connection. Just insert a SIM card into the SIM card slot at the bottom of 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 an LTE network. A computer can connect to the Zyxel Device's PoE injector for configuration via the Web Configurator.

Figure 1   Zyxel Device's Internet Access Application
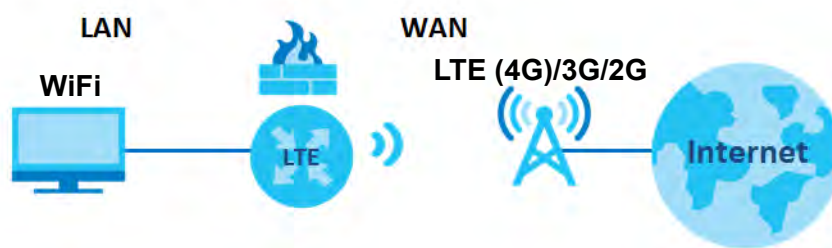
1.3 Managing the Zyxel Device

Use the Web Configurator for management of the Zyxel Device using a (supported) web browser.

1.4 Good Habits for Managing the Zyxel Device

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

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Refer to Section 23.2 on page 147. 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.

1.5 Front and Rear Panels

The LED indicators are located on the front panel. The wall mounting panel is located on the rear.

Figure 2   Front and Rear Panels

1.6 LEDs (Lights)

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

Table 1   LTE7461-M602 LED Descriptions

COLOR	STATUS	DESCRIPTION
Red	On	The Zyxel Device is abnormal status.
	Blinking Slow	The Zyxel Device is booting.
Amber	On	The WiFi network is activated.
	Off	The WiFi network is not activated.
Green	On	The Zyxel Device is registered and successfully connected to a mobile network.
	Blinking (slow)	The Zyxel Device is not connected to Mobile network.
	Blinking (fast)	The Zyxel Device is trying to connect to a 4G/3G network.
	Off	There is no service.

Note: Blinking (slow) means the LED blinks once per second.
Blinking (fast) means the LED blinks once per 0.2 second.

1.7 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button of the Zyxel Device as shown in the following figure to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to **1234** and the IP address will be reset to **192.168.1.1**.

Figure 3   Reset Button and IO ports
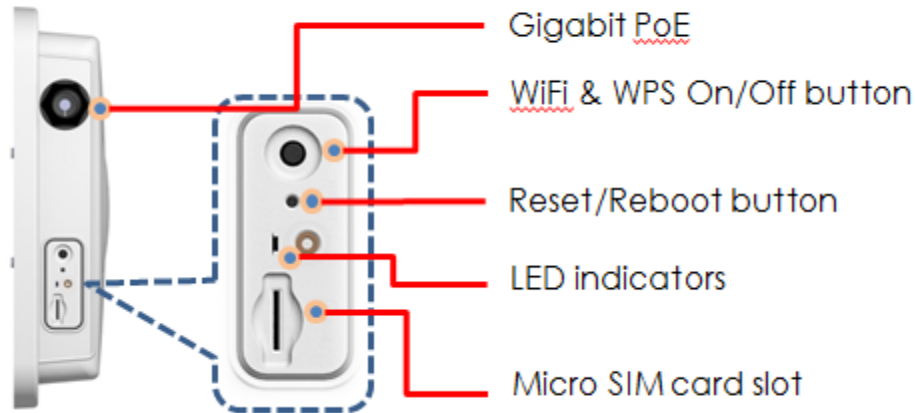
1   Make sure the Zyxel Device is connected to power and LED is on.

2   To set the Zyxel Device back to the factory default settings, press the **RESET** button for 5 seconds.

Note: If you press the **RESET** button for more than 2 seconds but less than 5 seconds, it will cause the system to reboot.

CHAPTER 2
The Web Configurator

2.1 Overview

The Web Configurator is an HTML-based management interface that allows easy Zyxel Device setup and management via Internet browser. Use Internet Explorer 8.0 and later versions or Mozilla Firefox 3 and later versions or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.
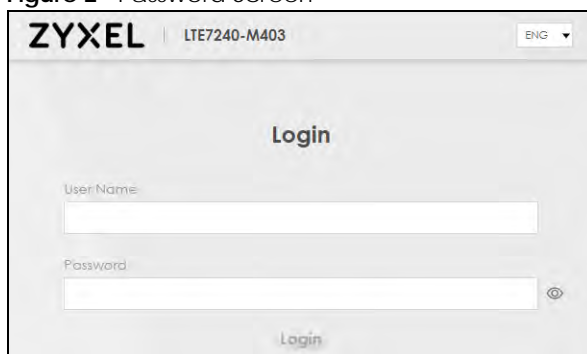
In order to use the Web Configurator you need to allow:

• Web browser pop-up windows from your Zyxel Device. Web pop-up blocking is enabled by default in Windows 10.
• JavaScript (enabled by default).
• Java permissions (enabled by default).

2.1.1 Accessing the Web Configurator

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

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

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

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

Figure 2   Password Screen

Note: The first time you enter the password, you will be asked to change it. Make sure the new password must contain at least one uppercase letter, one lowercase letter and one number.

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

Figure 3 Connection Status
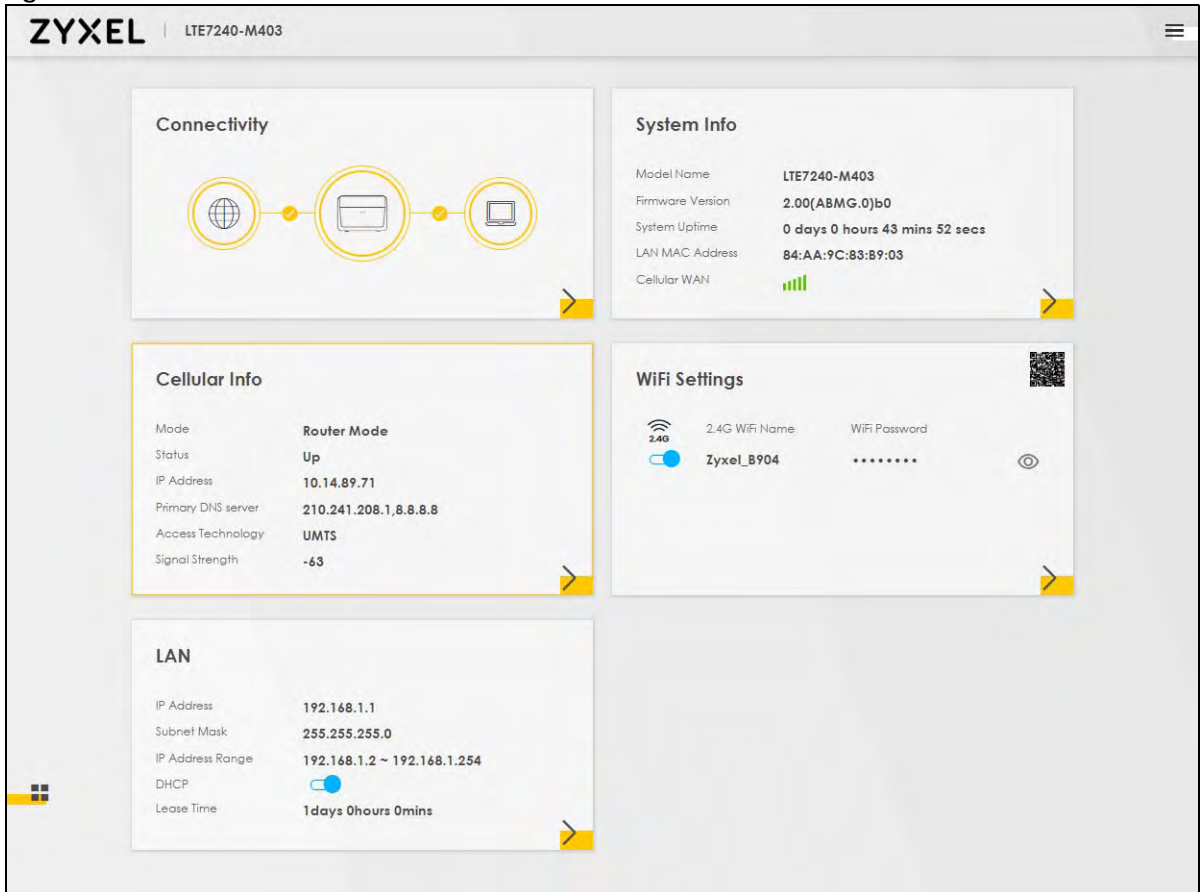
2.2 Web Configurator Layout

Figure 4   Screen Layout
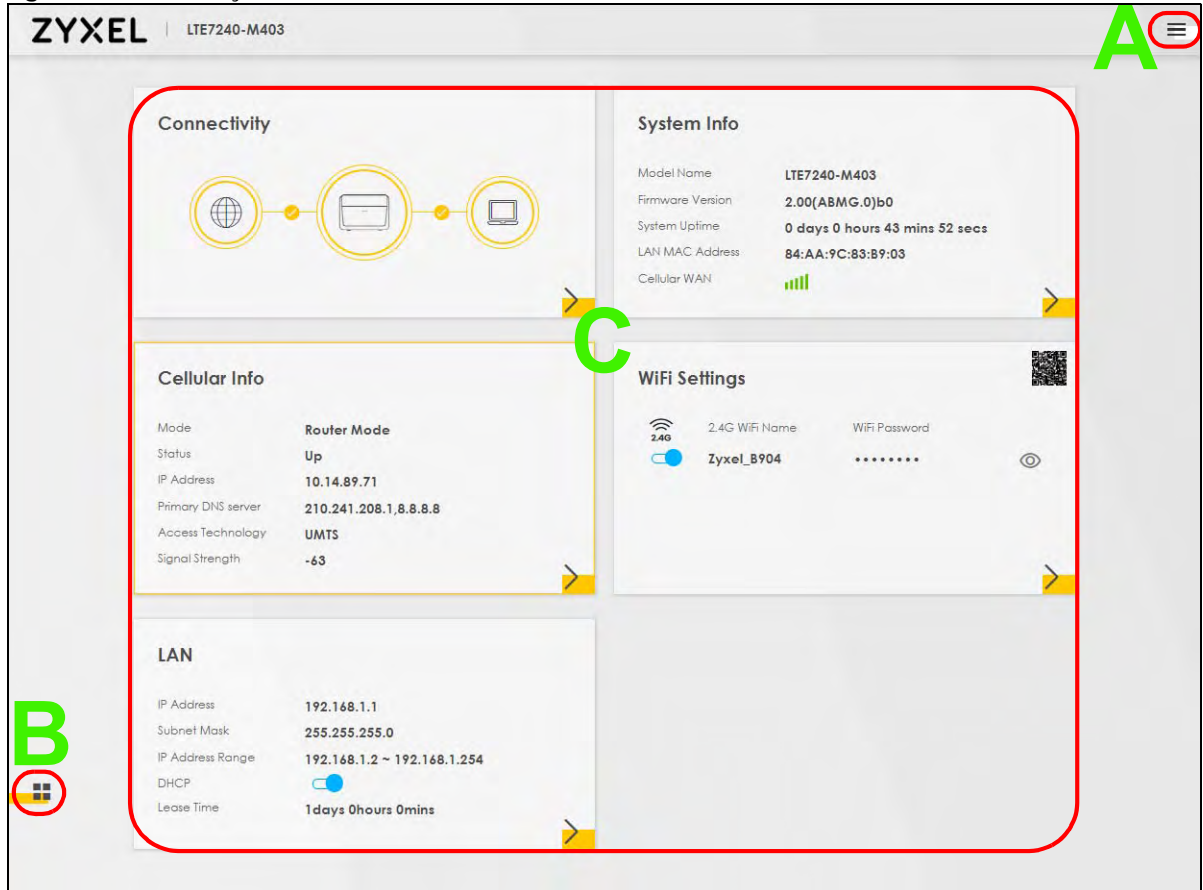
As illustrated above, the main screen is divided into these parts:

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

2.2.1 Settings Icon

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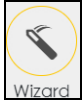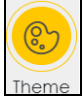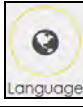
2.2.1.1 Side Bar

The side bar provides some icons on the right hand side.
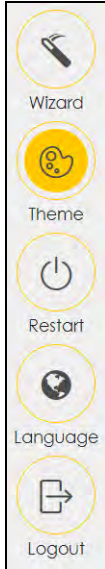
The icons provide the following functions.

Table 2   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 wireless settings. See Chapter 3 on page 23 for more information about the **Wizard** screens.
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.

2.2.1.2 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.

Table 3   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	Cellular WAN	Use this screen to configure an LTE WAN connection that includes the Access Point Name (APN) provided by your service provider.
	Cellular SIM	Use this screen to enter a PIN for your SIM card to prevent others from using it.
	Cellular Band	Use this screen to configure the LTE 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 mode (bridge mode).
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP	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 or disable SIP ALG.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Security		

Table 3   Navigation Panel Summary (continued)
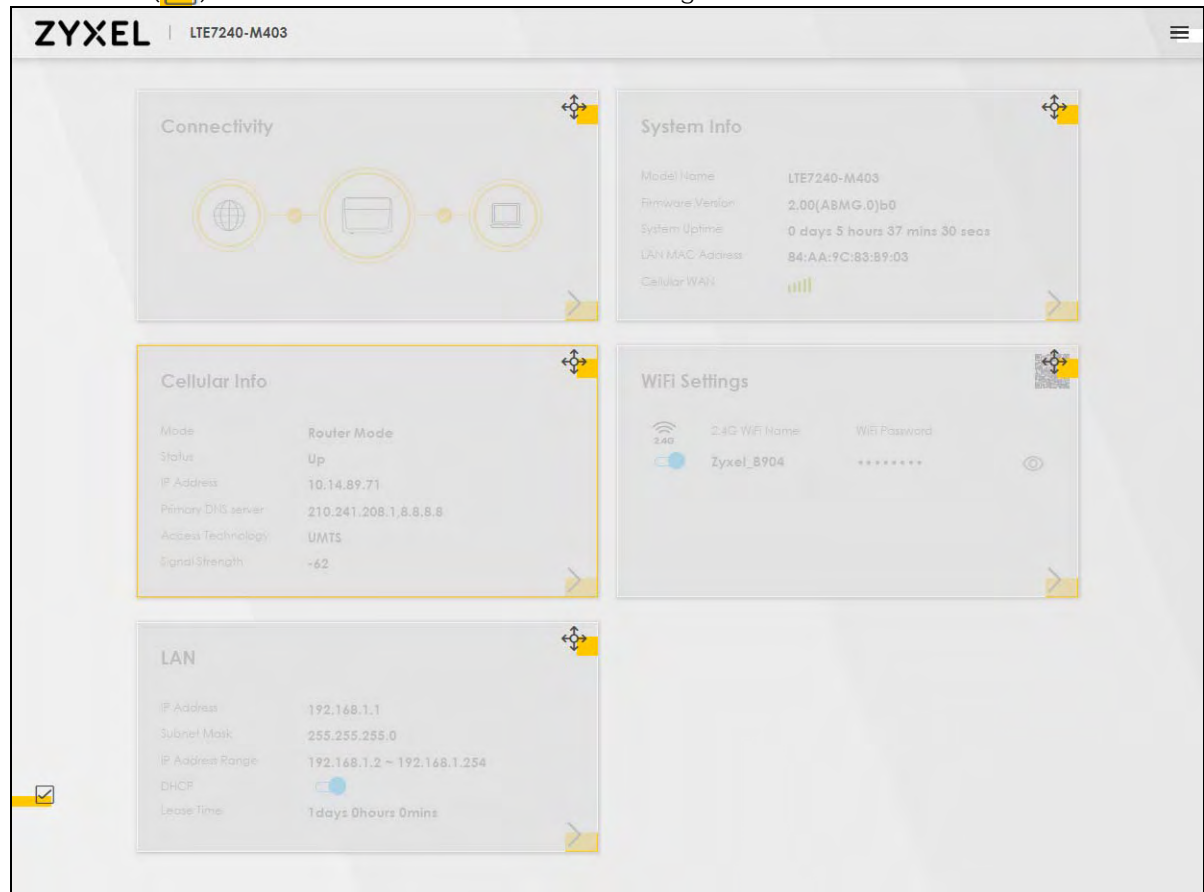
LINK	TAB	FUNCTION
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate 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.
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.
Cellular WAN Status	Cellular Statistics	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.
	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	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.

Table 3   Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
TR-069 Client	TR-069 Client	Use this screen to configure your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.
Time	Time	Use this screen to change your Zyxel Device's time and date.
Email Notification	Email 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.
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.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems.

2.2.2 Widget Icon

Click this icon ( ) to arrange the screen order. Select a block and hold it to move around. Click the Check icon ( ) in the lower left corner to save the changes.

CHAPTER 3
Quick Start

3.1 Overview

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

Note: See the technical reference chapters (starting on Chapter 4 on page 53) for background information on the features in this chapter.

3.2 Quick Start Setup

You can click the **Wizard** icon in the side bar to open the **Wizard** screens. See Section 2.2.1.1 on page 19 for more information about the side bar. After you click the **Wizard** icon, the following screen appears. Click **Let's Go** to proceed with settings on time zone and wireless networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can click **Skip** to leave the **Wizard** screens.

Figure 5 Wizard - Home
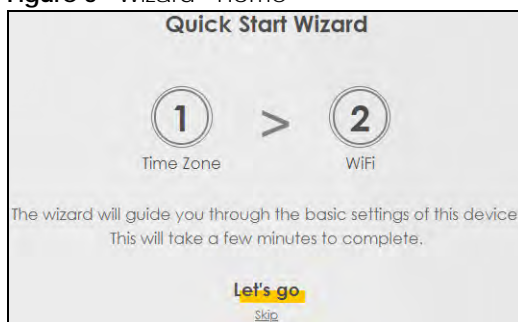
3.3 Time Zone

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

Figure 6 Wizard - Time Zone
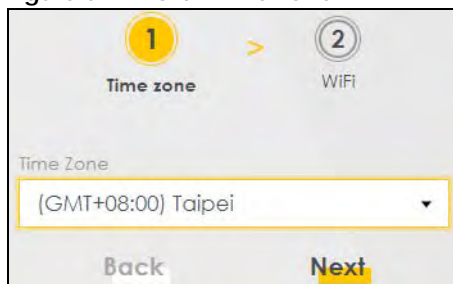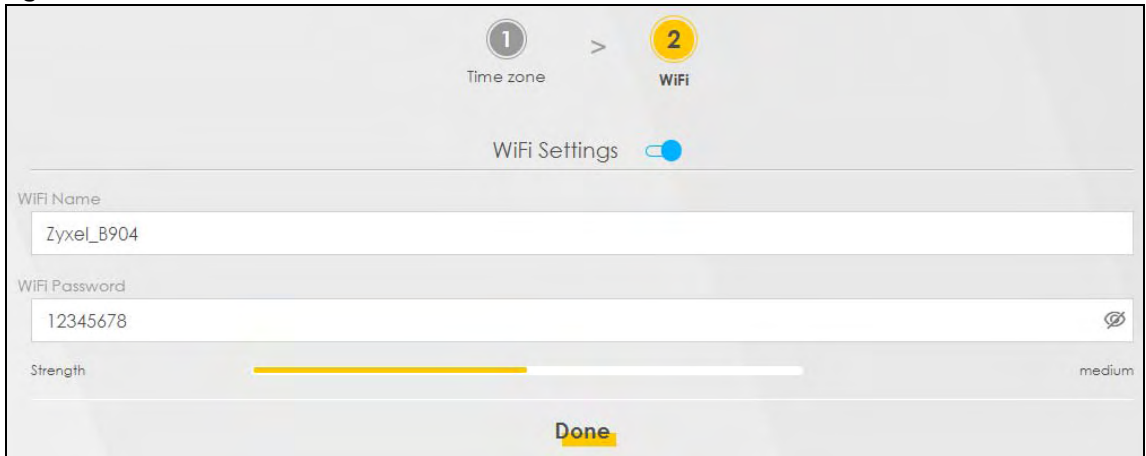
3.4 WiFi Setup

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

Figure 7 Wizard - Wireless

Note: You can also enable the wireless service using any of the following methods:
Click **Network Setting** > **Wireless** to open the **General** screen. Then select **Enable** in the **Wireless** field. Or,
Press the **WiFi** button located under the **RESET** button (see Section 1.6 on page 14 for the location) for one second.

3.5 Quick Start Setup-Finish

Your Zyxel Device saves your settings and attempts to connect to the Internet.

PART II
Technical Reference

Connection Status Screens

4.1 The Connection Status Screen

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

4.1.1 The Connectivity Screen

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

Figure 8 Connectivity
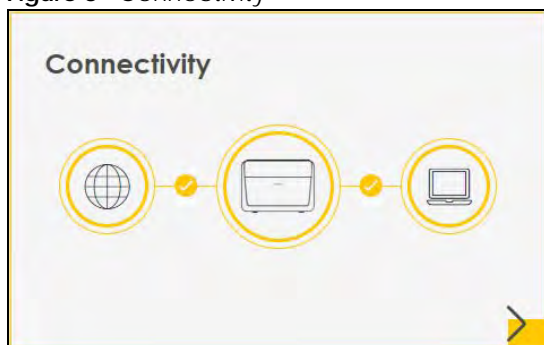
Click the Arrow icon ( ) to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

Figure 9 Connectivity: Connected Devices

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. Click **Save** to save your changes.

Figure 10   Connectivity: Edit
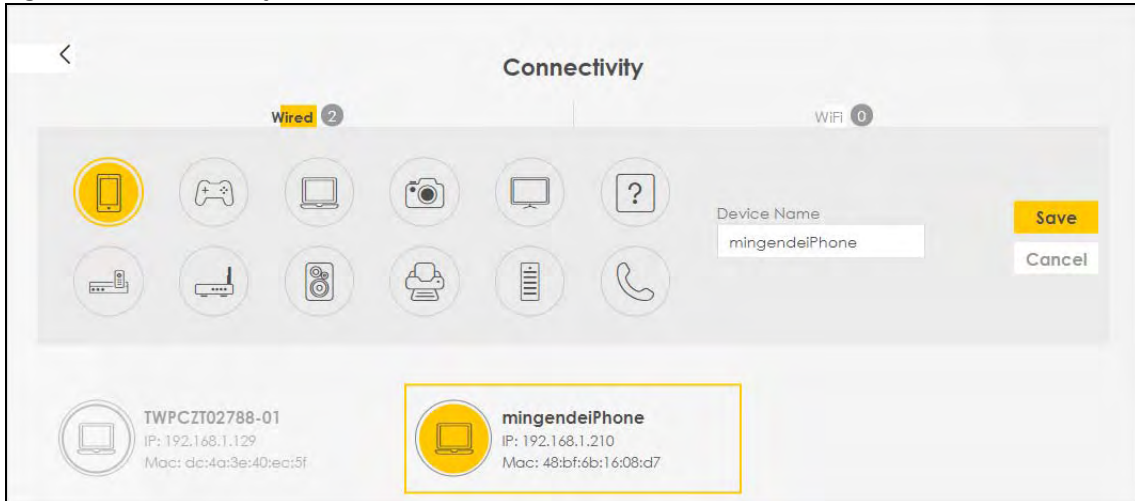
4.1.2 The System Info Screen

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

Figure 11   System Info
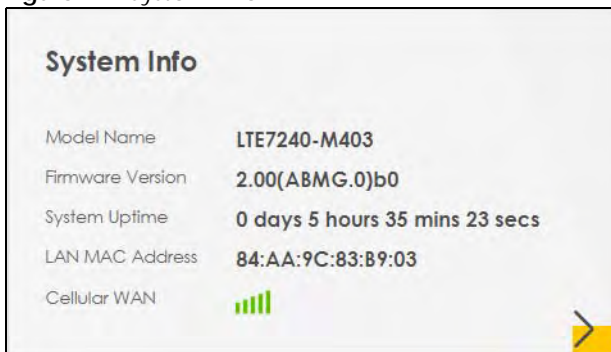
Click the Arrow icon ( ) to view the more information on the status of your firewall and interfaces (WAN, LAN, and WLAN).

Figure 12 System Info: Detailed Information
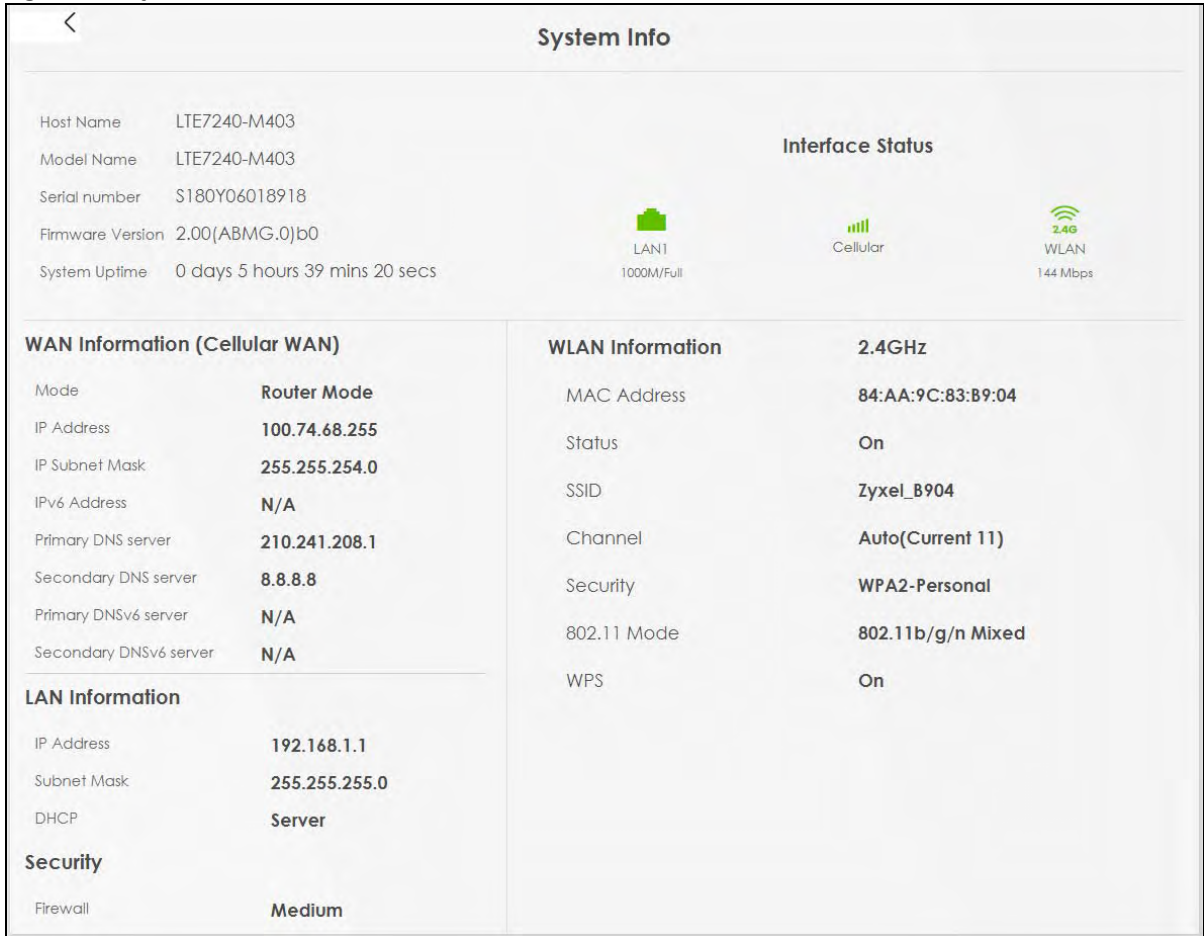
Each field is described in the following table.

Table 4   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 Up Time	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Interface Status Virtual ports are shown here. You can see the ports in use and their transmission rate.	
WAN Information (These fields display when you have a WAN connection.)	
Mode	This field displays the current mode of your Zyxel Device.
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.

Table 4   System Info: Detailed Information (continued)

LABEL	DESCRIPTION
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.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are:
	Server - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.
	Relay - The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
	None - The Zyxel Device is not providing any DHCP services to the LAN.
Security	
Firewall	This displays the firewall's current security level.
WLAN Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of the wireless interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a wireless LAN.
Channel	This is the channel number currently used by the wireless interface.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.

4.1.3 The WiFi Settings Screen

Use this screen to enable or disable the main 2.4 GHz wireless network. When the switch turns blue ( ), the function is enabled. Otherwise, it's not. 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 wireless networks. If you want to show or hide your WiFi passwords, click the Eye icon ( ).

Figure 13 WiFi Settings
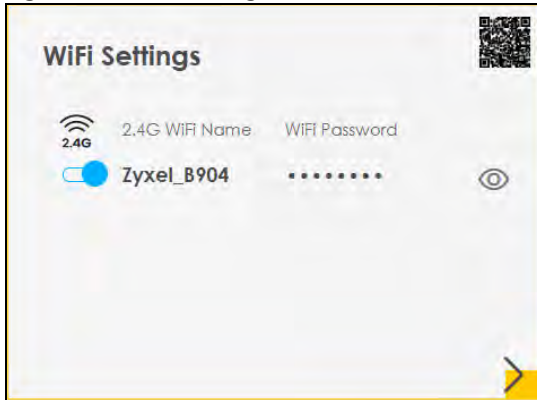
Click the Arrow icon ( ) to configure the SSIDs and/or passwords for your main wireless networks. Click the Eye icon ( ) to display the characters as you enter the WiFi Password.

Figure 14 WiFi Settings: Configuration
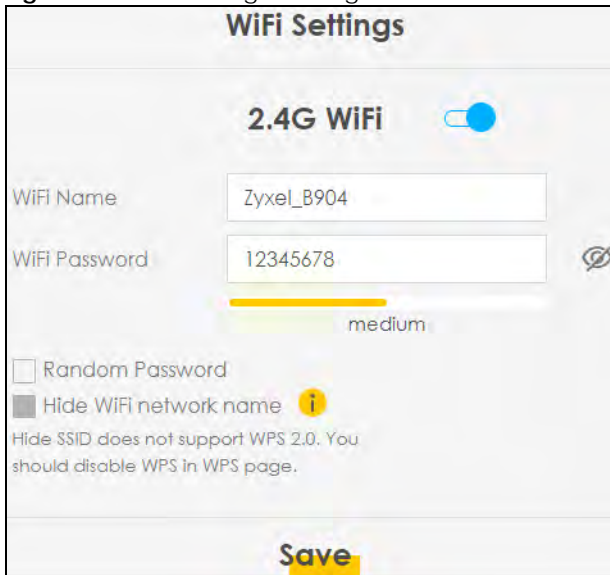
Each field is described in the following table.

Table 5   WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4G WiFi	Click this switch to enable or disable the 2.4 GHz wireless network. When the switch turns blue , the function is enabled. Otherwise, it's not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it's hidden.

LABEL	DESCRIPTION
Random Password	Select this option to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this 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. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

4.1.4 The LAN Screen

Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device.

Figure 15   LAN
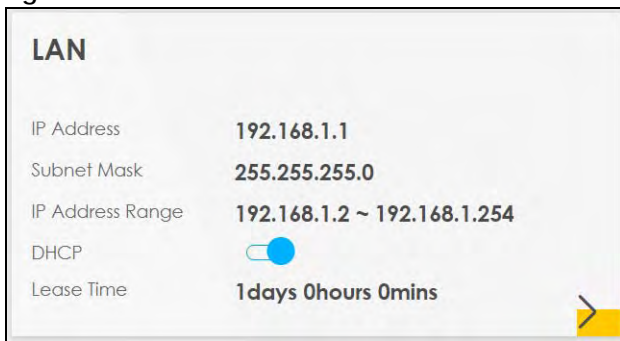
Click the Arrow icon ( ) to configure the LAN IP settings and DHCP setting for your Zyxel Device.

Figure 16   LAN Setup
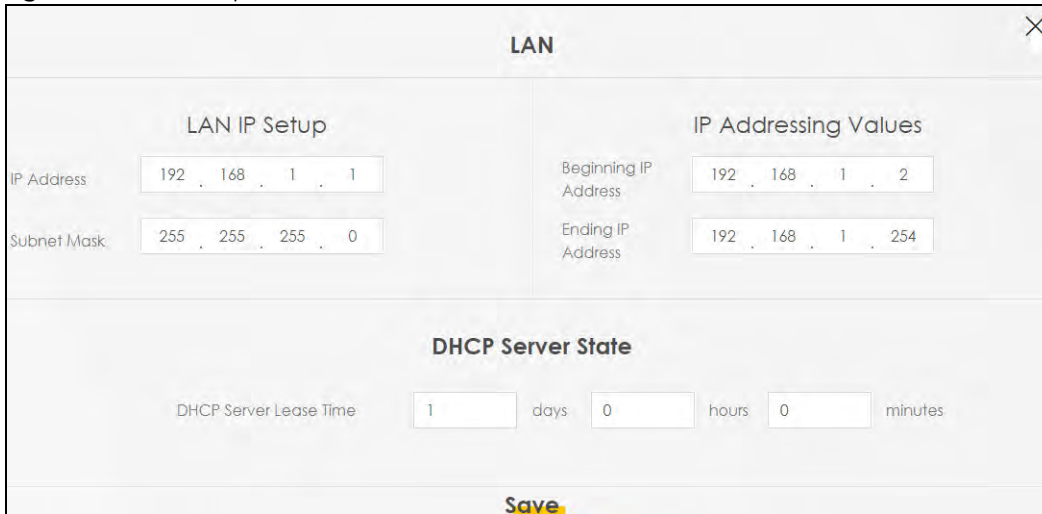
Each field is described in the following table.

Table 6   Status Screen

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
DHCP Server State	
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
Save	Click **Save** to save your changes.

Broadband

5.1 Overview

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

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

Figure 17   LAN and WAN
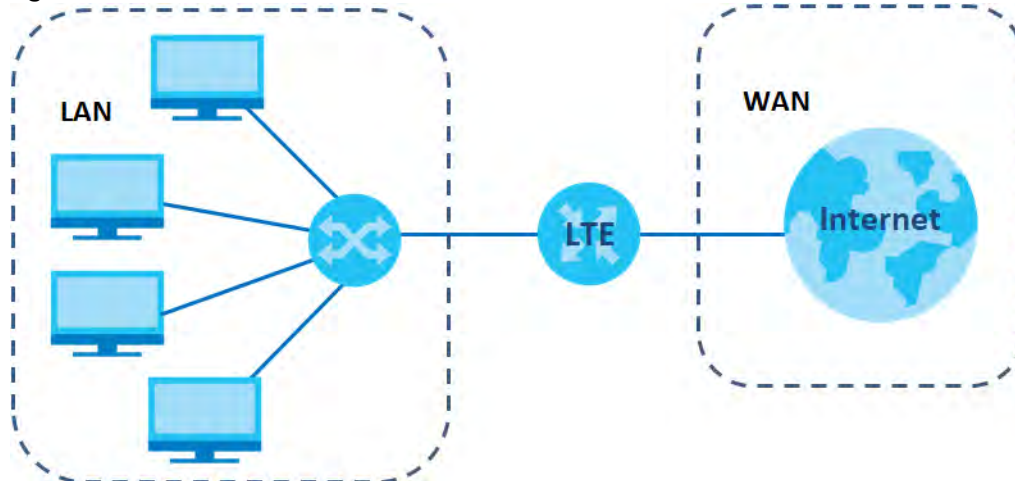
5.1.1 What You Can Do in this Chapter

- Use the **Cellular WAN** screen to configure an LTE WAN connection (Section 5.2 on page 34).
- Use the **Cellular SIM** screen to enter the PIN of your SIM card (Section 5.3 on page 36).
- Use the **Cellular Band** screen to view or edit an LTE WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 5.4 on page 37).
- Use the **Cellular PLMN** screen to display available Public Land Mobile Networks (Section 5.5 on page 38).
- Use the **Cellular IP Passthrough** screen to configure an LTE WAN connection (Section 5.6 on page 40).

5.1.2 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 an LTE network. An APN is required for LTE stations to enter the LTE network and then the Internet.

5.1.3 Before You Begin

You may need to know your Internet access settings such as LTE APN, WAN IP address and SIM card's PIN code if the **INTERNET** light on your Zyxel Device is off. Get this information from your service provider.

5.2 The Cellular WAN Screen

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

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

Figure 18   Network Setting > Broadband > Cellular WAN

Note: Roaming charges may apply when **Data Roaming** is enabled.
       Automatic APN Mode is not supported when operating in 3G only mode.

The following table describes the fields in this screen.

Table 7   Network Setting > Broadband > Cellular WAN

LABEL	DESCRIPTION
Roaming	
Data Roaming	Click this to enable ( ) data roaming on the Zyxel Device.
	4G 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.
APN Settings	
APN Manual Mode	Disable this to have the Zyxel Device configure the APN (Access Point Name) of an LTE network automatically. Otherwise, Click this to enable ( ) and enter the APN manually in the field below.
APN	This field allows you to display the Access Point Name (APN) in the profile.
	Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method.
	You can enter up to 30 printable ASCII characters. Spaces are allowed.

Table 7   Network Setting > Broadband > Cellular WAN (continued)

LABEL	DESCRIPTION
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.
Authentication Type	Select the type of authentication method peers use to connect to the Zyxel Device in LTE 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 **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.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

5.3 The Cellular SIM Configuration Screen

Enter a 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 19   Network Setting > Broadband > Cellular SIM

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 8   Network Setting > Broadband > Cellular SIM

LABEL	DESCRIPTION
PIN Management	
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.
	Click to enable (⬤) if the service provider requires you to enter a PIN to use the SIM card.
	Click to disable if the service provider lets you use the SIM without inputting a PIN.
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.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previous screen without saving.

5.4 The Cellular Band Configuration Screen

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 (**4G**, **3G**, or **2G**) to which you want the Zyxel Device to connect.

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

Figure 20   Network Setting > Broadband > Cellular Band
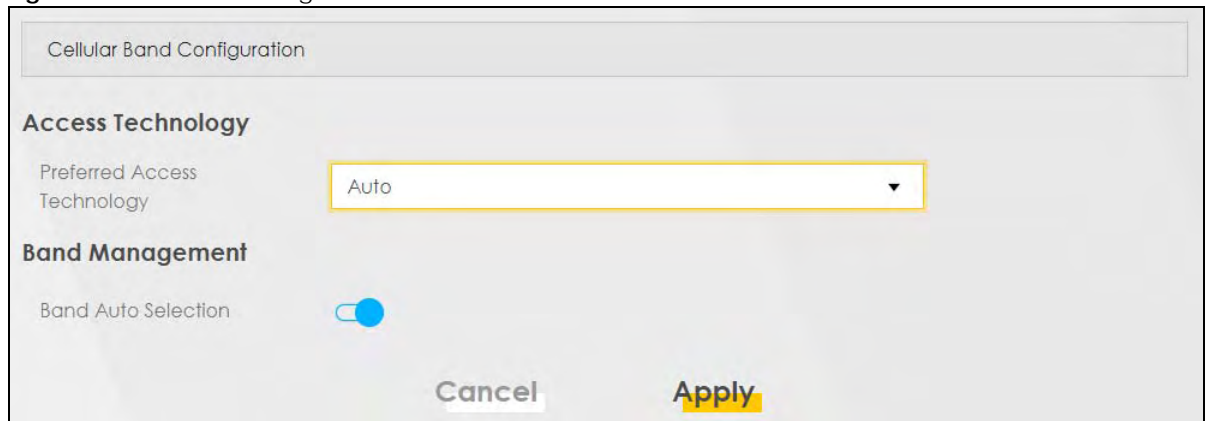
The following table describes the fields in this screen.

Table 9   Network Setting > Broadband > Cellular Band

LABEL	DESCRIPTION
Access Technology	
Preferred Access Technology	Select the type of the network (**4G**, **3G**, or **2G**) to which you want the Zyxel Device to connect 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.
Band Management	
Band Auto Selection	Select the LTE bands to use for the Zyxel Device's WAN connection. Click to enable ( ) automatic LTE frequency band selection as provided by your service provider. Otherwise, select disabled.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

5.5 PLMN Configuration Screen

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 21   Network Setting > Broadband > Cellular PLMN
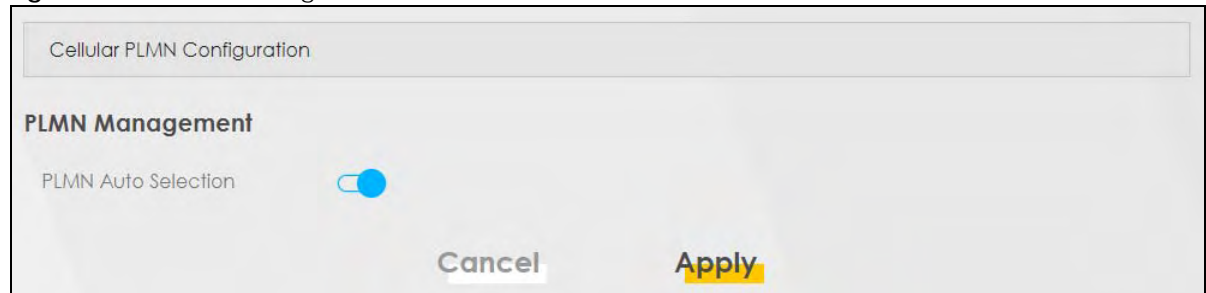
The following table describes the labels in this screen.

Table 10   Network Setting > Broadband > Cellular PLMN

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

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

Figure 22   Network Setting > Broadband > Cellular PLMN > Manual Scan Warning
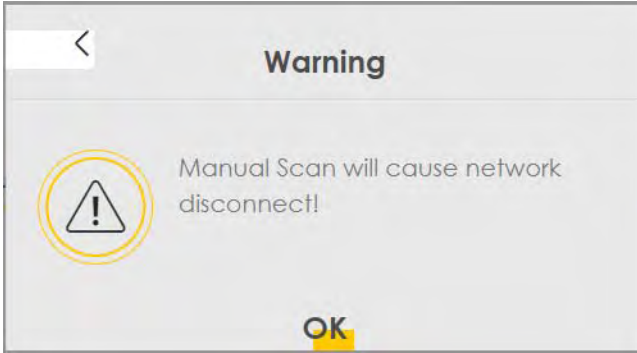
When the next screen appears, clicking **Scan** will allow the Zyxel Device to check for available PLMNs in its surroundings and display the network list.

Figure 23   Network Setting > Broadband > Cellular PLMN > Manual Scan
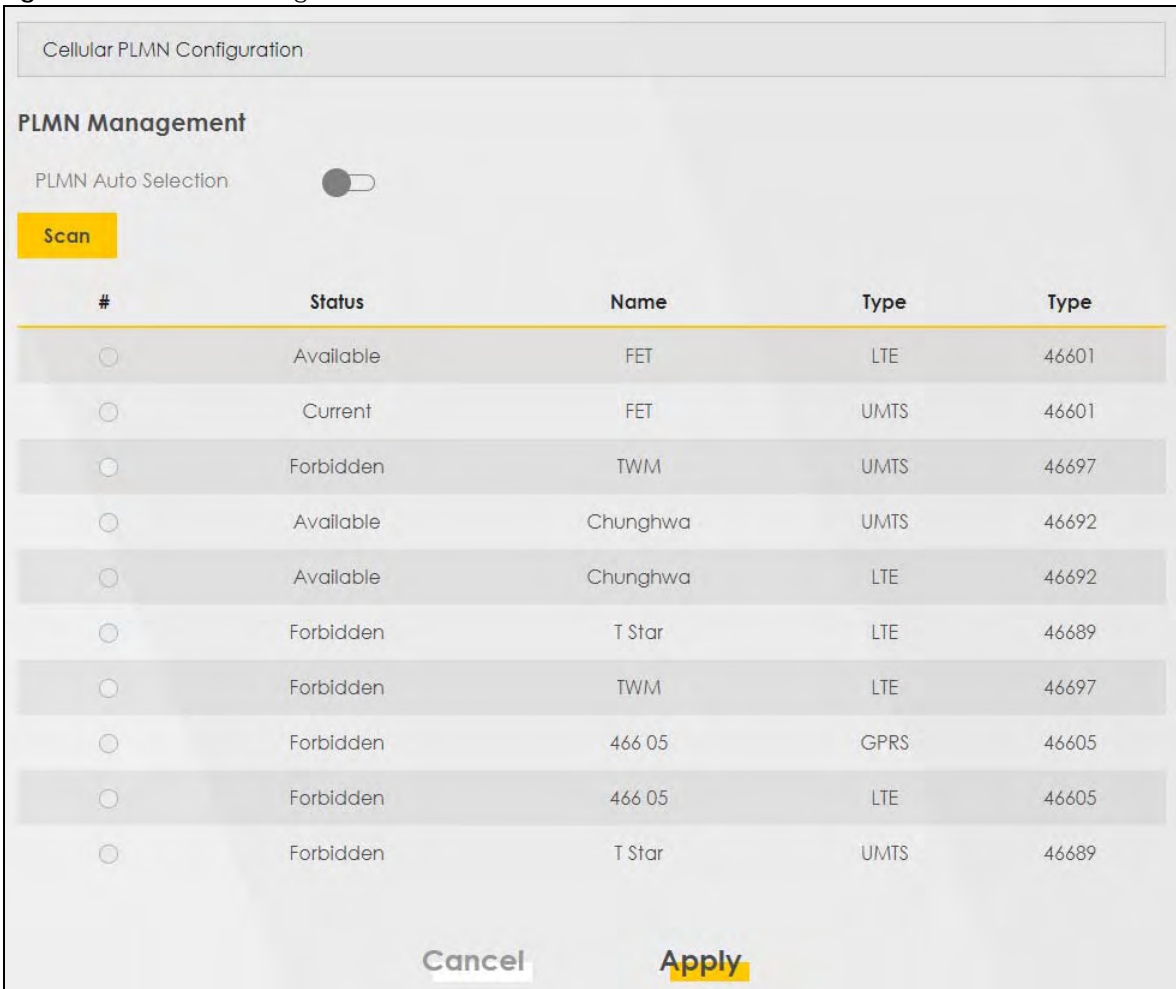
The following table describes the labels in this screen.

Table 11   Network Setting > Broadband > Cellular PLMN > Manual 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**.

5.6 IP Passthrough Screen

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

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

Figure 24   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 25 Network Setting > Broadband > Cellular IP Passthrough > Enable Warning
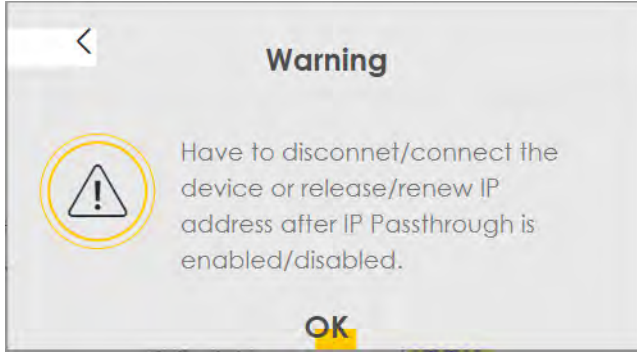
The following table describes the fields in this screen.

Table 12   Network Setting > Broadband > IP Passthrough

LABEL	DESCRIPTION
IP Passthrough Management	
IP Passthrough	IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
Passthrough Mode	Select **Dynamic** to allow traffic to be forwarded to any LAN computer on the local network of the Zyxel Device. Select **Fixed** to allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device. 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.

CHAPTER 6
Wireless

6.1 Overview

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

6.1.1 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 6.2 on page 43).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device (Section 6.3 on page 46).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 6.4 on page 48).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 6.5 on page 49).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 6.6 on page 50).

6.1.2 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 6.7 on page 52 for advanced technical information on WiFi networks.

6.2 The General Screen

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

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

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

Figure 26   Network Setting > Wireless > General

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

Table 13   Network Setting > Wireless > General

LABEL	DESCRIPTION
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 while **5GHz** is used by IEEE 802.11a/ac WiFi clients.
WiFi	Click **Enable** to enable the wireless LAN in this field.
Channel	Use **Auto** to have the Zyxel Device automatically determine a channel to use.
Bandwidth	Select whether the Zyxel Device uses a WiFi channel width of **20MHz**, **40MHz** or **20/40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40MHz. It is often better to use the 20MHz setting in a location where the environment hinders the WiFi signal. Select **20MHz** if you want to lessen radio interference with other WiFi devices in your neighborhood or the WiFi clients do not support channel bonding.
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
WiFi Network Settings	
WiFi Network Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This check box is grayed out if the WPS function is enabled in the **Network** > **Wireless** > **WPS** screen.
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled.
Security Level	
Security Mode	Select **More Secure (WPA2-PSK)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate with this network without any data encryption or authentication. See the following sections for more details about this field.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

6.2.1 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 27   Wireless > General: No Security
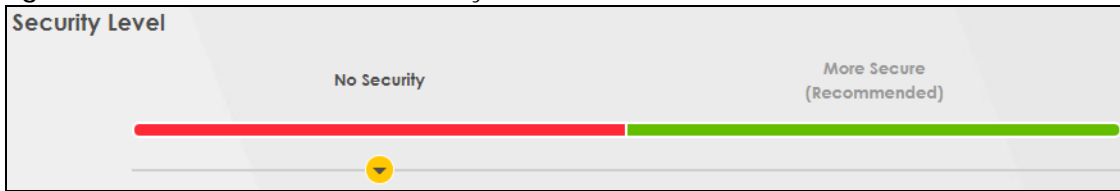
The following table describes the labels in this screen.

Table 14   Wireless > General: No Security

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

6.2.2 More Secure (WPA2-PSK)

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

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

Figure 28   Wireless > General: More Secure: WPA2-PSK
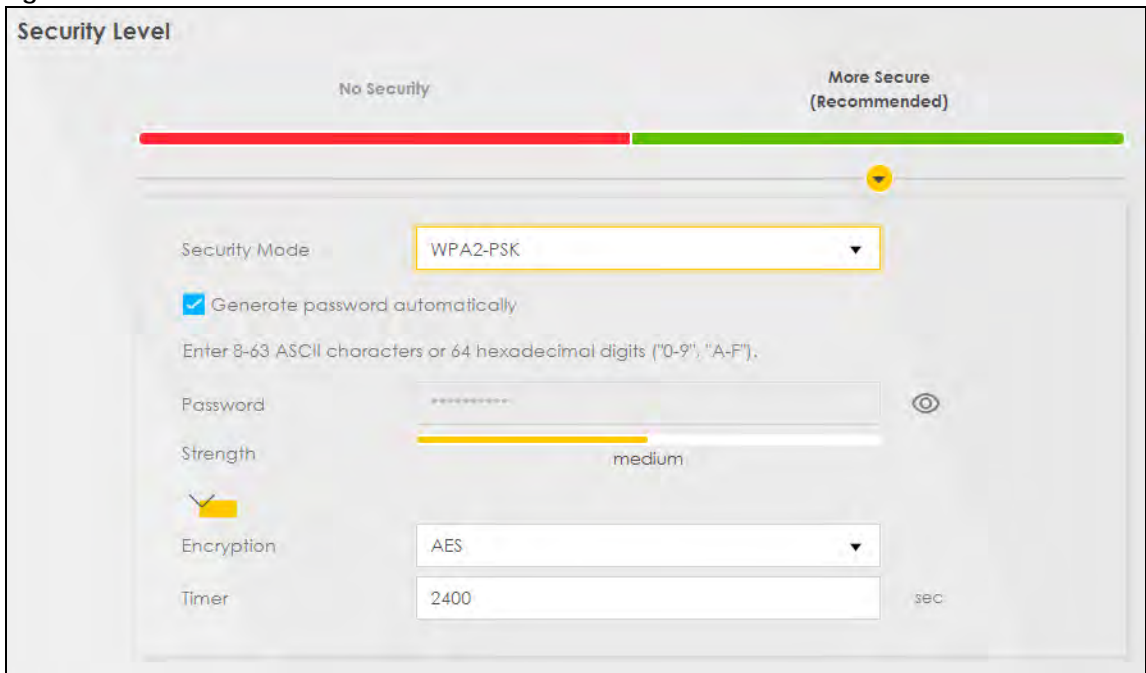
The following table describes the labels in this screen.

Table 15   Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA2-PSK data encryption.
Security Mode	**WPA2-PSK** is the default security mode.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	Select **Generate password automatically** or enter a **Password**. The password has two uses. 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: Enter 8-63 ASCII characters only. 64 hexadecimal characters are not accepted for WPS. Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed ⌀, you'll see the password in plain text. Otherwise, it's hidden.
more...	Click this to show more fields in this section. Click this to hide them.
Encryption	**AES** is the default data encryption type, which uses a 128-bit key.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

6.3 MAC Authentication

Configure the Zyxel Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Zyxel Device **(Deny)** based on the device(s) MAC address. Every Ethernet device has a unique MAC (Media Access Control) address. It 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 device(s) you want to allow/deny to configure this screen. Edit the list in the table to decide the rule of access on device(s).

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 29 Network Setting> Wireless > MAC Authentication
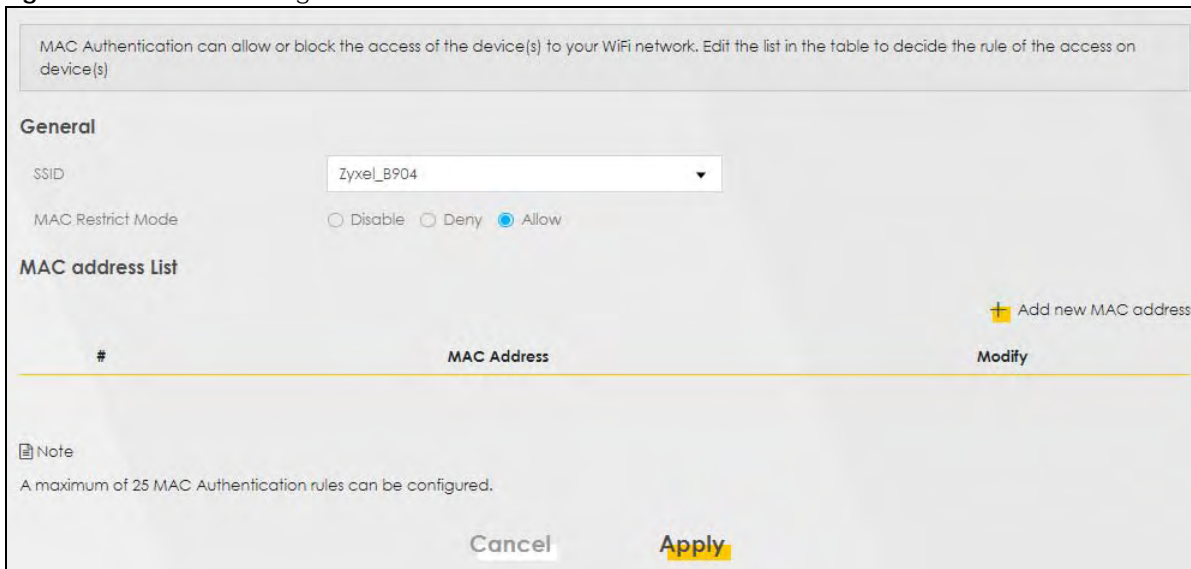
The following table describes the labels in this screen.

Table 16   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.
#	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.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

6.4 The WPS Screen

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

WiFi Protected Setup (WPS) allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your WiFi client supports it. See for more information about WPS.

Note: The Zyxel Device uses the security settings of the **SSID1** profile (see). The WPS button will gray-out when wireless LAN or WPS is disabled.

Note: If WPS is enabled, UPnP will automatically be turned on.

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

Figure 30 Network Setting > Wireless > WPS

The following table describes the labels in this screen.

Table 17   Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Click to enable (⬤) and have the Zyxel Device activate WPS. Otherwise, it is disabled.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS WiFi network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click **Apply** to activate WPS method 1 on the Zyxel Device.
WPS	Click this button to add another WPS-enabled WiFi device (within WiFi range of the Zyxel Device) to your WiFi network. This button may either be a physical button on the outside of a device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other WiFi device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS WiFi network by entering the PIN of the client into the Zyxel Device. Click this switch to make it turn blue. Click **Apply** to activate WPS method 2 on the Zyxel Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the WiFi device to your WiFi network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Zyxel Device.
Method 3	Use this section to set up a WPS WiFi network by entering the PIN of the Zyxel Device into the client. Click this switch to make it turn blue. Click **Apply** to activate WPS method 3 on the Zyxel Device.
Release Configuration	The default WPS status is configured. Click this button to remove all configured WiFi and WiFi security settings for WPS connections on the Zyxel Device.
Generate New PIN	If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use the WPS push-button method. Click the **Generate New PIN** button to have the Zyxel Device create a new PIN.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

6.5 The WMM Screen

Enable Wi-Fi 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.

Click **Network Setting > Wireless > WMM** to display the following screen.
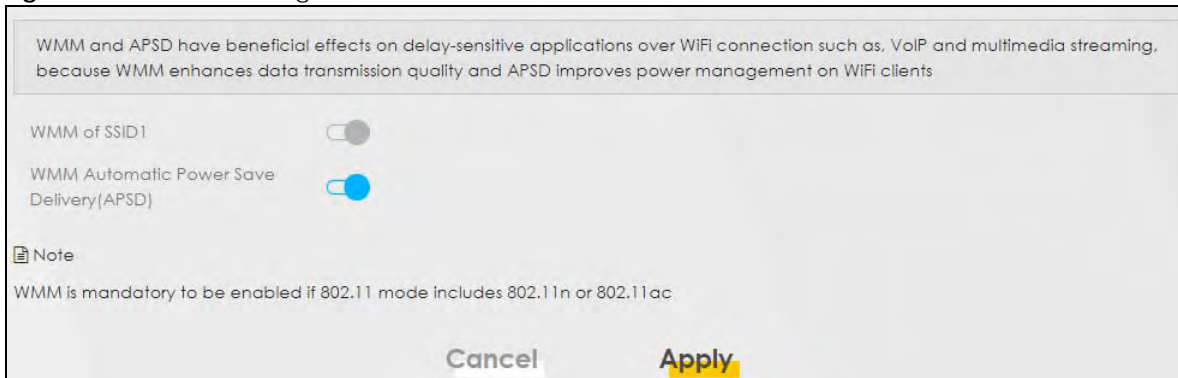
Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

The following table describes the labels in this screen.

Table 18   Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM of SSID1~4	Select **On** to have the Zyxel Device automatically give the WiFi network (SSIDx) 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 or 802.11ac, 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.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

6.6 The Others Screen

Use this screen to change the default advanced WiFi settings. See the User's Guide for field details. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See Section 6.7.2 on page 54 for detailed definitions of the terms listed here.

Figure 32   Network Setting > Wireless > Others

The following table describes the labels in this screen.

Table 19   Network Setting > Wireless > Others

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

Table 19   Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Mode	For 2.4GHz frequency WLAN devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the Zyxel Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. For 5GHz frequency WLAN devices: • Select **802.11a Only** to allow only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. • Select **802.11ac Only** to allow only IEEE 802.11ac compliant WLAN devices to associate with the Zyxel Device. • Select **802.11a/n Mixed** to allow either IEEE 802.11a or IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11n/ac Mixed** to allow either IEEE 802.11n or IEEE 802.11ac compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac Mixed** to allow IEEE 802.11a, IEEE 802.11n or IEEE802.11ac compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network. 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 6.7.6 on page 57 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Protected Management Frames	Wi-Fi 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**.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

6.7 Technical Reference

This section discusses wireless LANs in depth.

6.7.1 WiFi Network Overview

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

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

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

The following figure provides an example of a WiFi network.

Figure 33   Example of a WiFi Network
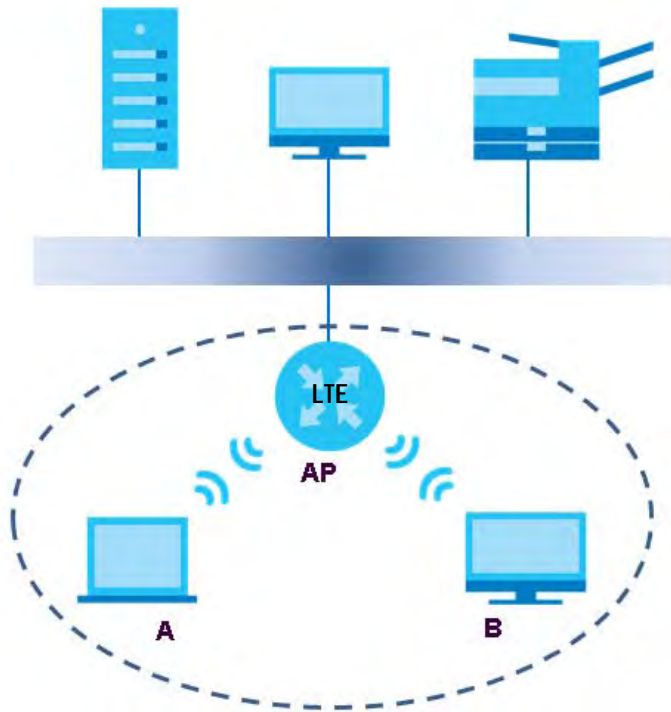
The WiFi network is the part in the blue circle. In this WiFi network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

Every WiFi network must follow these basic guidelines.

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

  The SSID is the name of the WiFi network. It stands for Service Set IDentifier.

- If two WiFi networks overlap, they should use a different channel.

  Like radio stations or television channels, each WiFi network uses a specific channel, or frequency, to send and receive information.

- Every device in the same WiFi network must use security compatible with the AP.

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

Radio Channels

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

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

6.7.2 Additional Wireless Terms

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

Table 20   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 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.

6.7.3 WiFi Security Overview

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

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

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

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

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

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

6.7.3.1 SSID

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

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

6.7.3.2 MAC Address Filter

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

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

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

---

1. Some 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.

6.7.3.3 User Authentication

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

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

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

6.7.3.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 6.7.3.3 on page 56 for information about this.)

Table 21   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.

6.7.4 Signal Problems

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

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

6.7.5 BSS

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

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

Figure 34   Basic Service Set
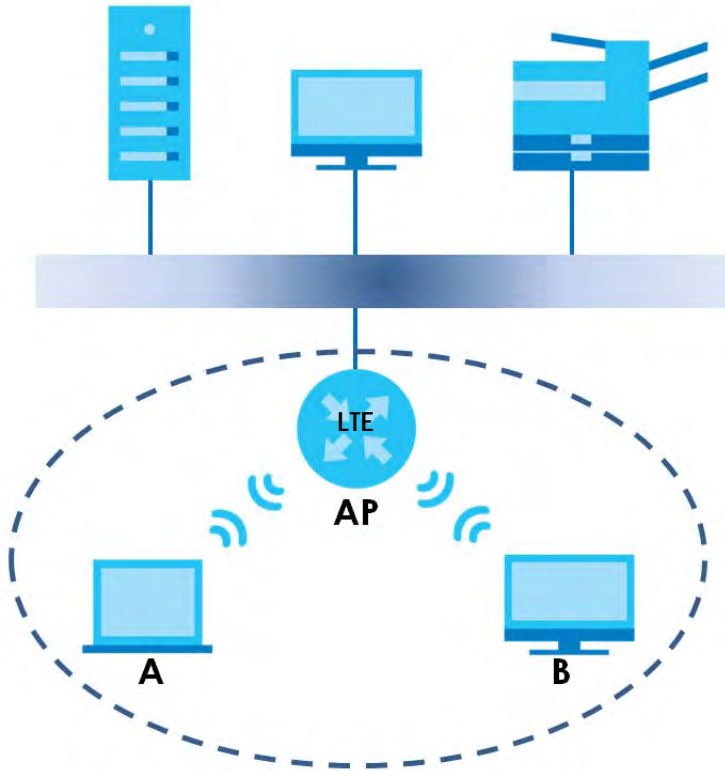
6.7.6 Preamble Type

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

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

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

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

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

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

6.7.7 WiFi Protected Setup (WPS)

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

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

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

6.7.7.1 Push Button Configuration

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

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

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

1 Ensure that the two devices you want to set up are within wireless range of one another.

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

3 Press the button on one of the devices (it doesn't matter which). For the Zyxel Device you must press the **WiFi** button for more than five seconds.

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

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

6.7.7.2 PIN Configuration

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

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

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

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

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide on how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide on how to find the WPS PIN - for the Zyxel Device, see Section 6.4 on page 48).

4 Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within two minutes.

7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the WiFi client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated WiFi clients in the AP's configuration utility. If you see the WiFi client in the list, WPS was successful.

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

Figure 35   Example WPS Process: PIN Method
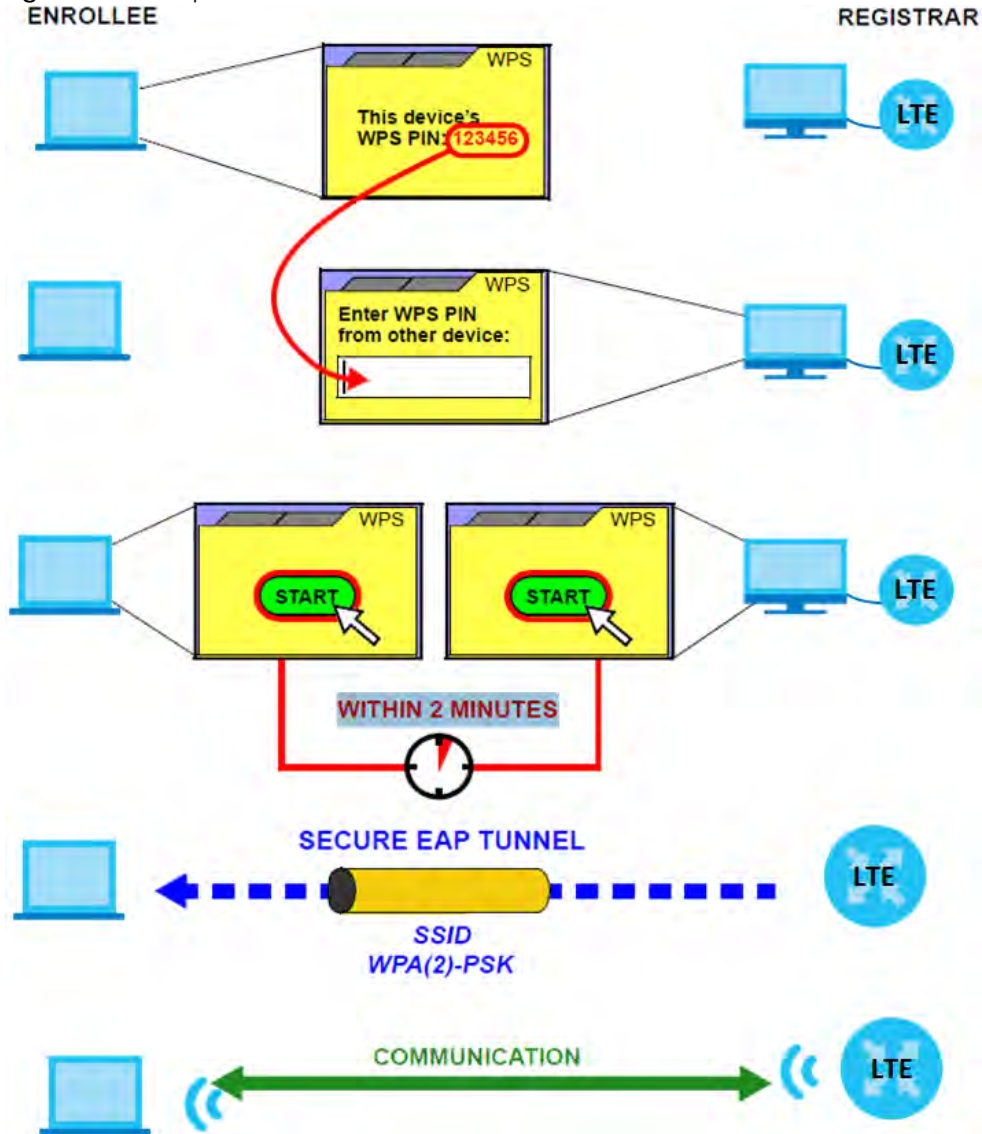
6.7.7.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

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

Figure 36 How WPS works
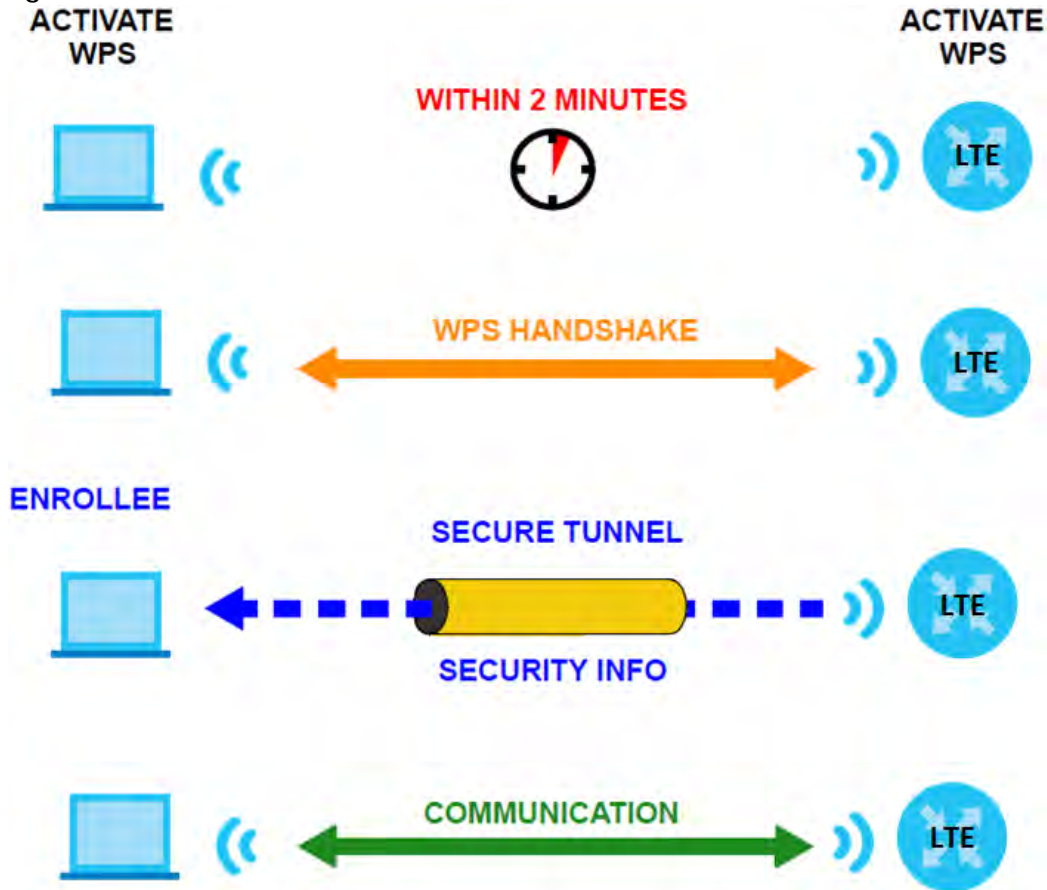
The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

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

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

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

6.7.7.4 Example WPS Network Setup

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

The following figure shows a sample network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1**

is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 37 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 38 WPS: Example Network Step 2
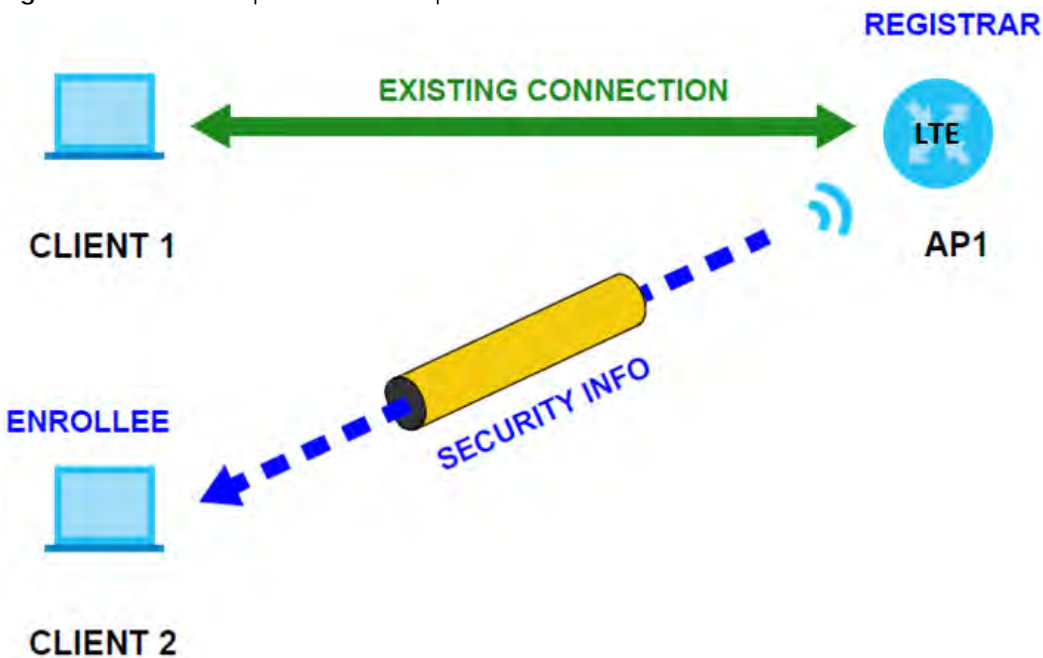
In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 39   WPS: Example Network Step 3
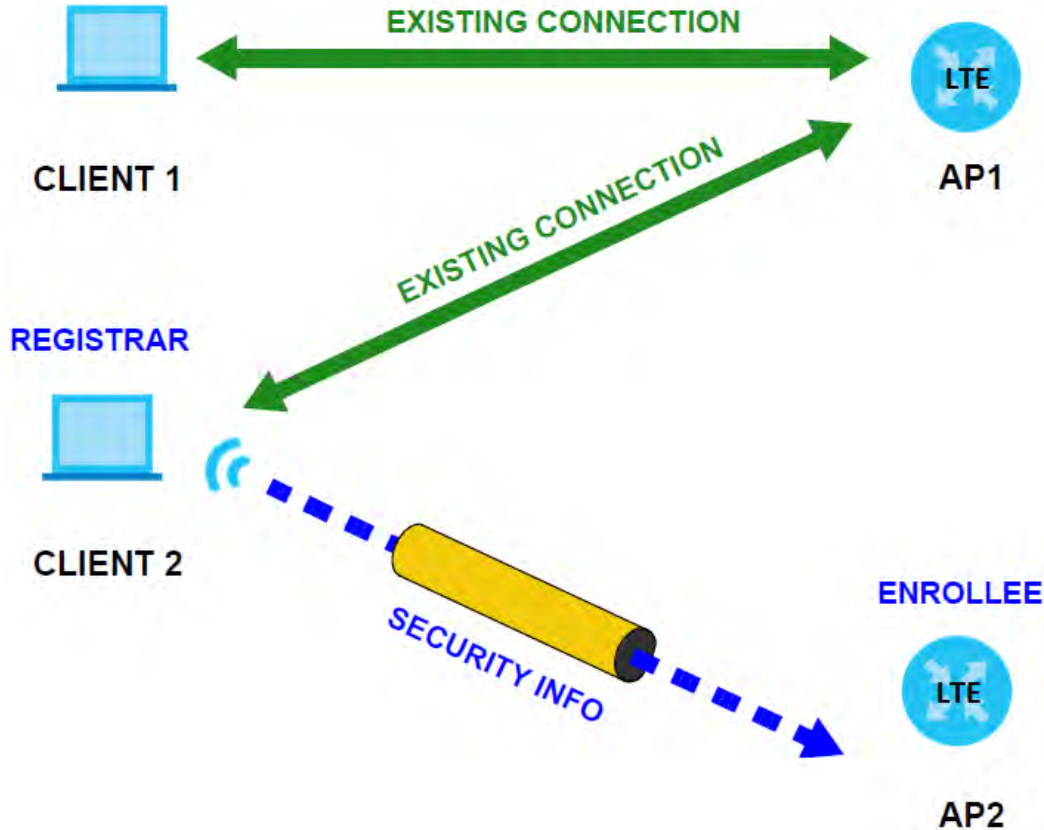
6.7.7.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

You can easily check to see if this has happened. WPS only works simultaneously between two devices, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point

is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your WiFi clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

Home Networking

7.1 Overview

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

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.
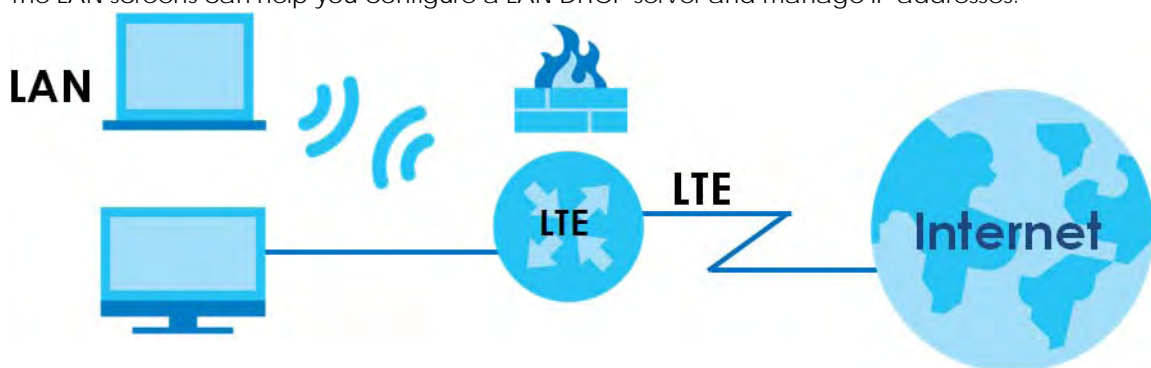
7.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 7.2 on page 66).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 7.3 on page 70).
- Use the **UPnP** screen to enable UPnP (Section 7.4 on page 72).

7.1.2 What You Need To Know

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

7.1.2.1 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 don't 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.

7.1.2.2 About UPnP

How do I know if I'm using UPnP?

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

Cautions with UPnP

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

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

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

UPnP and Zyxel

Zyxel has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Zyxel's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See for examples on installing and using UPnP.

7.2 The LAN Setup Screen

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

Figure 40 Network Setting > Home Networking > LAN Setup

The following table describes the fields in this screen.

Table 22   Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	This displays the name of the group that your Zyxel Device belongs to.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select **Enable** to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.
	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.
	When DHCP is used, the following fields need to be set:
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.
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	
Days/Hours/Minutes	DHCP server leases an address to a new device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different device.
DNS Values	
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 **From ISP** if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).
	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 **DNS Proxy** to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.
LAN IPv6 Mode Setup	
IPv6 Active	Use this field to **Enable** or **Disable** IPv6 activation on the Zyxel Device.
	When IPv6 activation is used, the following fields need to be set:

Table 22   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
Link Local Address Type	A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows. Select **EUI64** to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select **Manual**. Link-local Unicast Address Format <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>
LAN Global Identifier Type	Select **EUI64** to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select **Manual** to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Prefix Setup	Select **Delegate prefix from WAN** to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select **Static** to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: **Stateless**: The Zyxel Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. **Stateful**: The Zyxel Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: **From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements. **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.
DHCPv6 Configuration	**DHCPv6 Active** shows the status of the DHCPv6. **DHCPv6 Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	**RADVD Active** shows whether RADVD is enabled or not.
IPv6 DNS Values	
IPv6 DNS Server 1~3	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **User Defined** - Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. **From ISP** - Select this if your ISP dynamically assigns IPv6 DNS server information. **Proxy** - Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay. Otherwise, select **None** if you do not want to configure IPv6 DNS servers.

Table 22   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Query Scenario	Select how the Zyxel Device handles clients' DNS information requests. **IPv4/IPv6 DNS Server**: The Zyxel Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. **IPv6 DNS Server Only**: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. **IPv4 DNS Server Only**: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. **IPv6 DNS Server First**: The Zyxel Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. **IPv4 DNS Server First**: The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.3 The Static DHCP Screen

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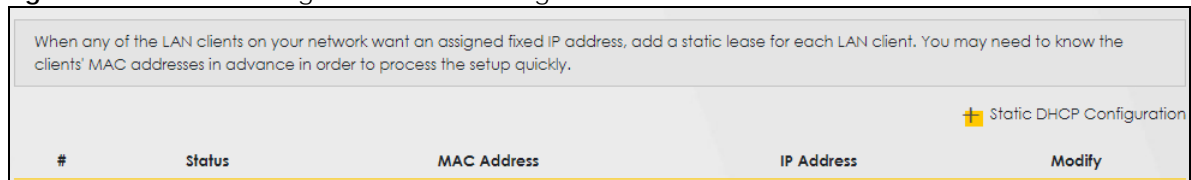
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

7.3.1 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 41   Network Setting > Home Networking > Static DHCP

The following table describes the labels in this screen.

Table 23   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.

Table 23   Network Setting > Home Networking > Static DHCP (continued)

LABEL	DESCRIPTION
Status	Active
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.

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

Figure 42   Static DHCP: Static DHCP Configuration

The following table describes the labels in this screen.

Table 24   Static DHCP: Configuration

LABEL	DESCRIPTION
Active	Enable static DHCP in your Zyxel Device.
Group Name	This displays the **Group Name**, usually **Default**.
IP Type	The **IP Type** is normally **IPv4** (non-configurable).
Select Device Info	Select between **Manual Input** which allows you to enter the next two fields (**MAC Address** and **IP Address**); or selecting an existing device would 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.

7.4 The UPnP Screen

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.

See Section 7.6 on page 74 for more information on UPnP.

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

Figure 43   Network Setting > Home Networking > UPnP

The following table describes the labels in this screen.

Table 25   Network Settings > Home Networking > UPnP

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

Table 25   Network Settings > Home Networking > UPnP

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

7.5 Technical Reference

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

LANs, WANs and the Zyxel Device

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

Figure 44   LAN and WAN IP Addresses
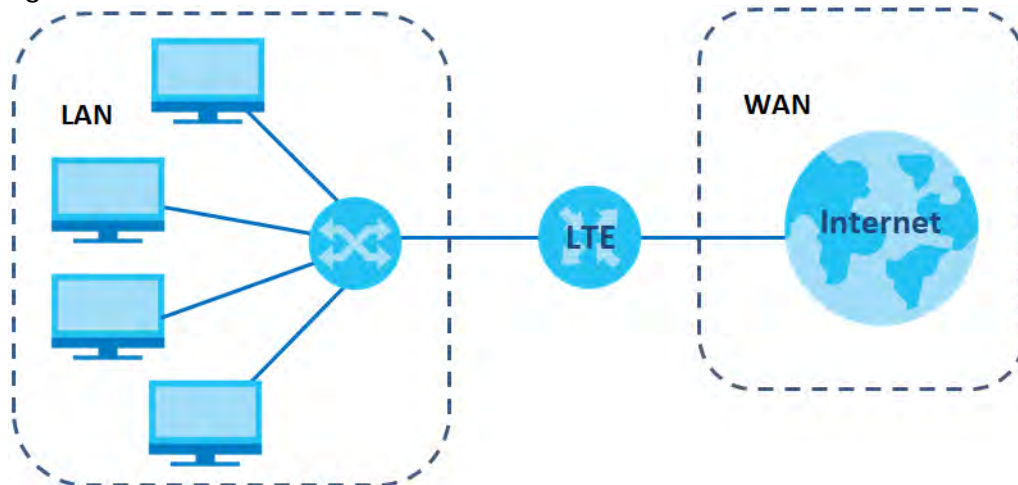
Private IP Addresses

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

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

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

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

7.6 Turning on UPnP in Windows 7 Example

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

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

1   Click the start icon, **Control Panel** and then the **Network and Sharing Center.**
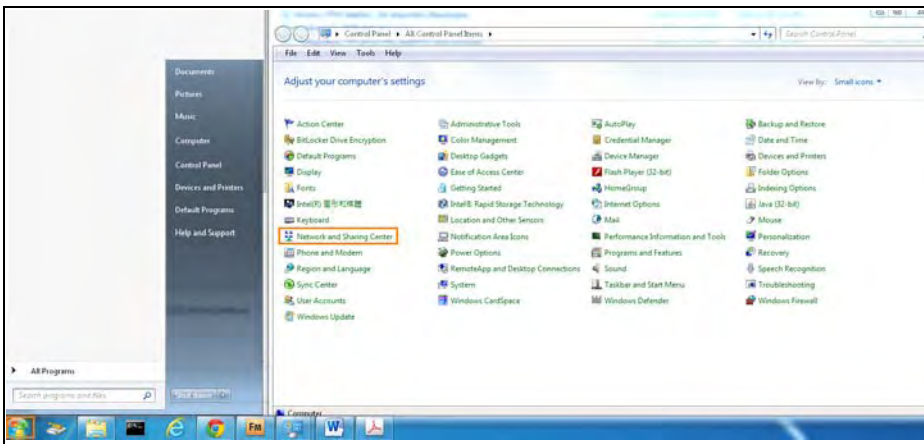
2   Click **Change Advanced Sharing Settings**.
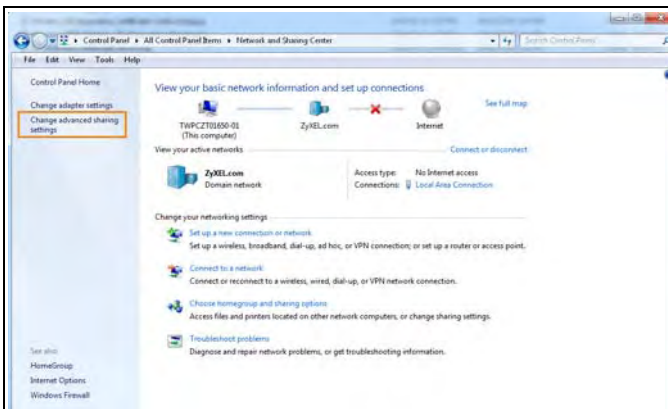
3   Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.
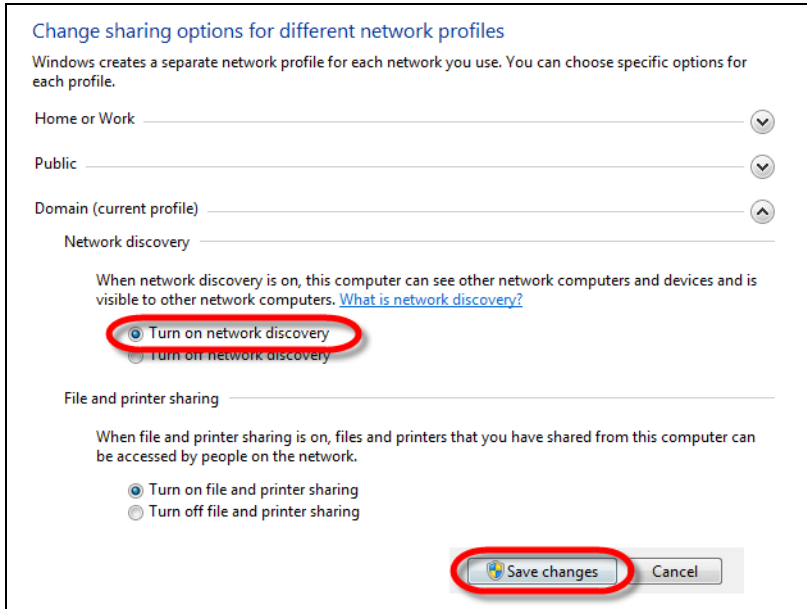
7.6.1 Auto-discover Your UPnP-enabled Network Device

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

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

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

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

Figure 45   Network Connections
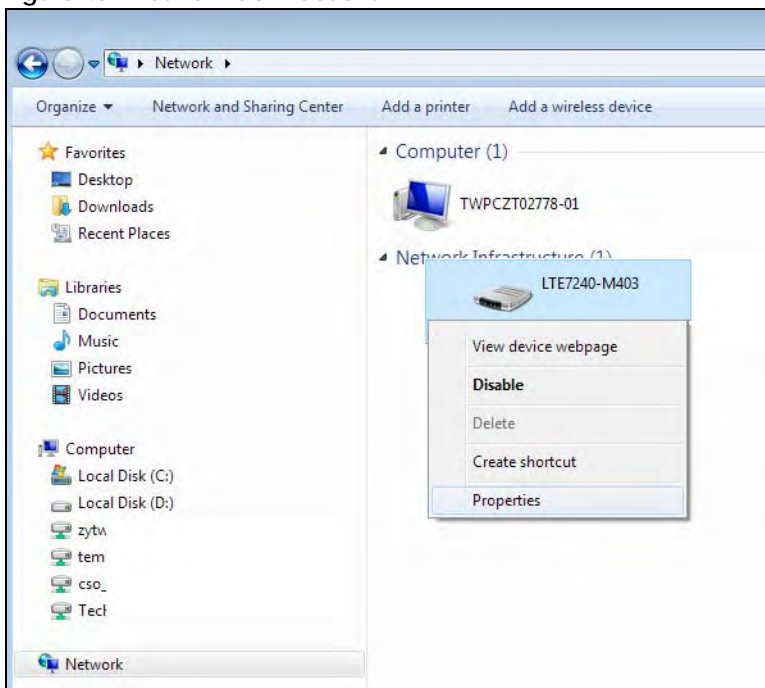
3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 46 Internet Connection Properties

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

Figure 47 Internet Connection Properties: Advanced Settings
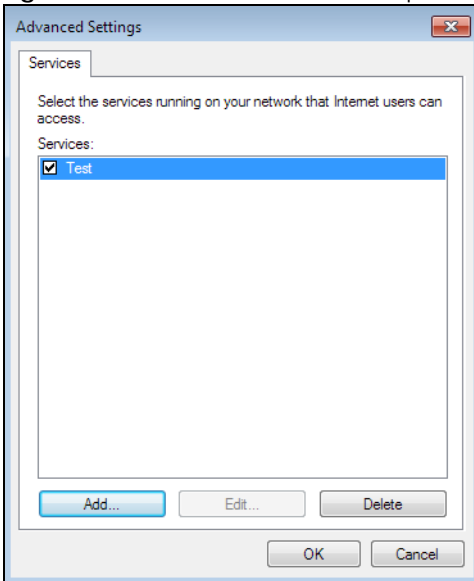
Figure 48   Internet Connection Properties: Advanced Settings: Add
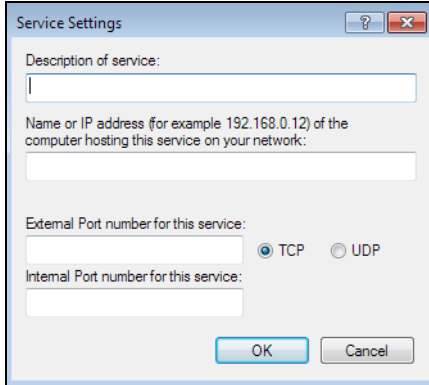
Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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

Figure 49   System Tray Icon

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

Figure 50   Internet Connection Status
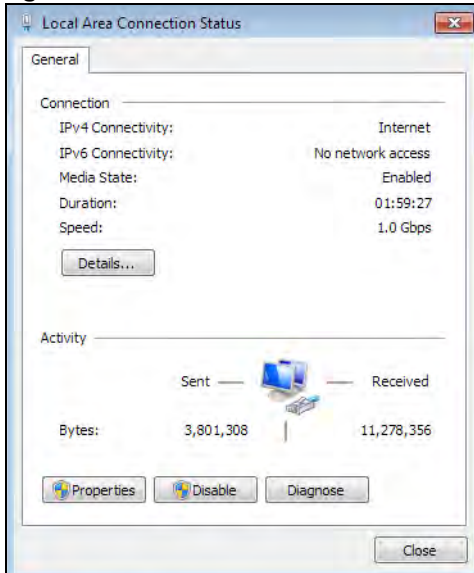
7.7 Turning on UPnP in Windows 10 Example

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

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

1 Click the start icon, **Settings** and then **Network & Internet**.
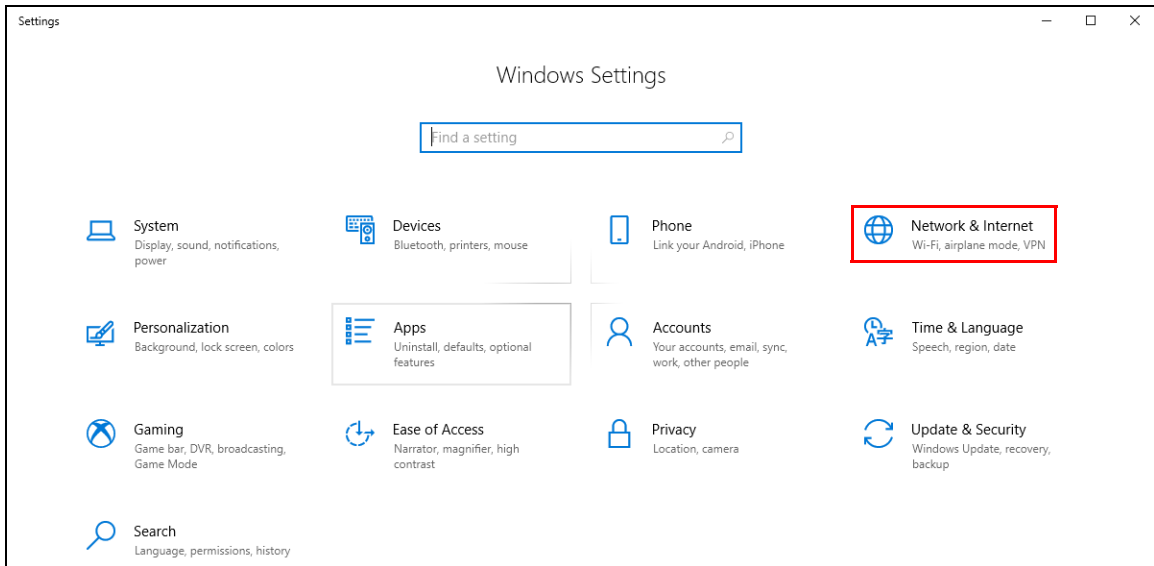
2 Click **Network and Sharing Center**.
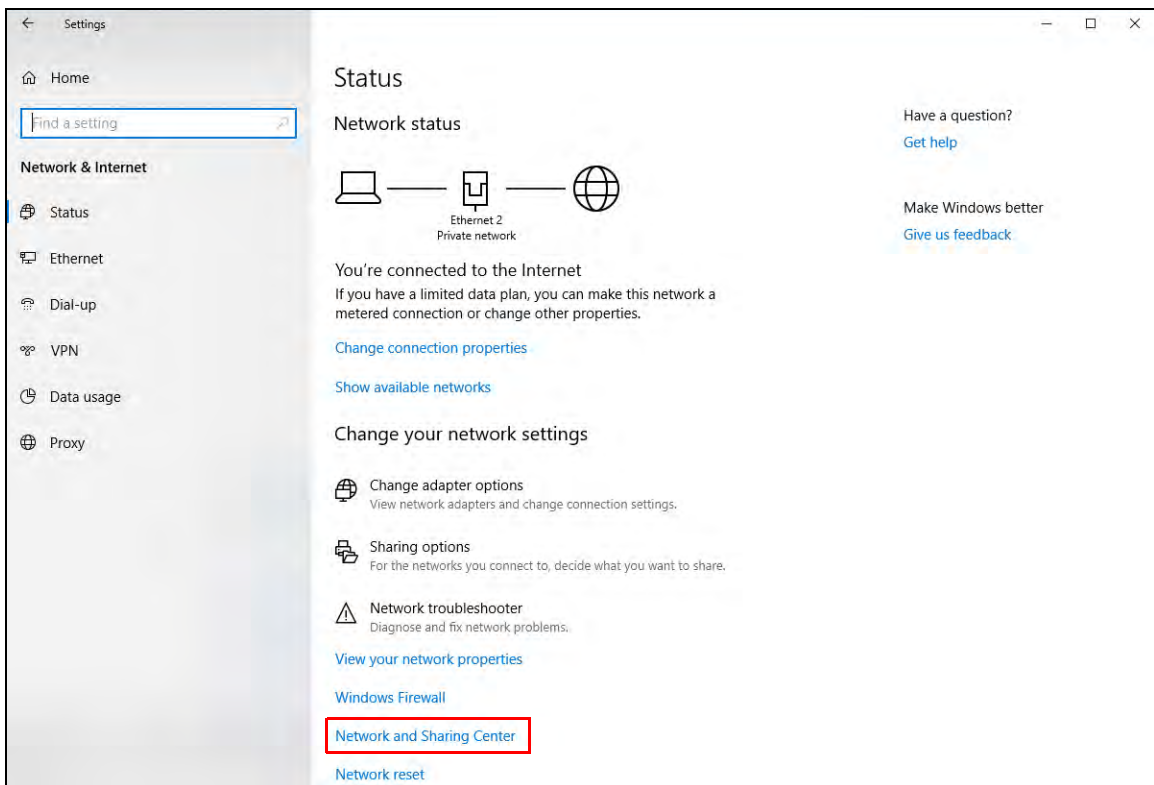
3 Click **Change advanced sharing settings**.
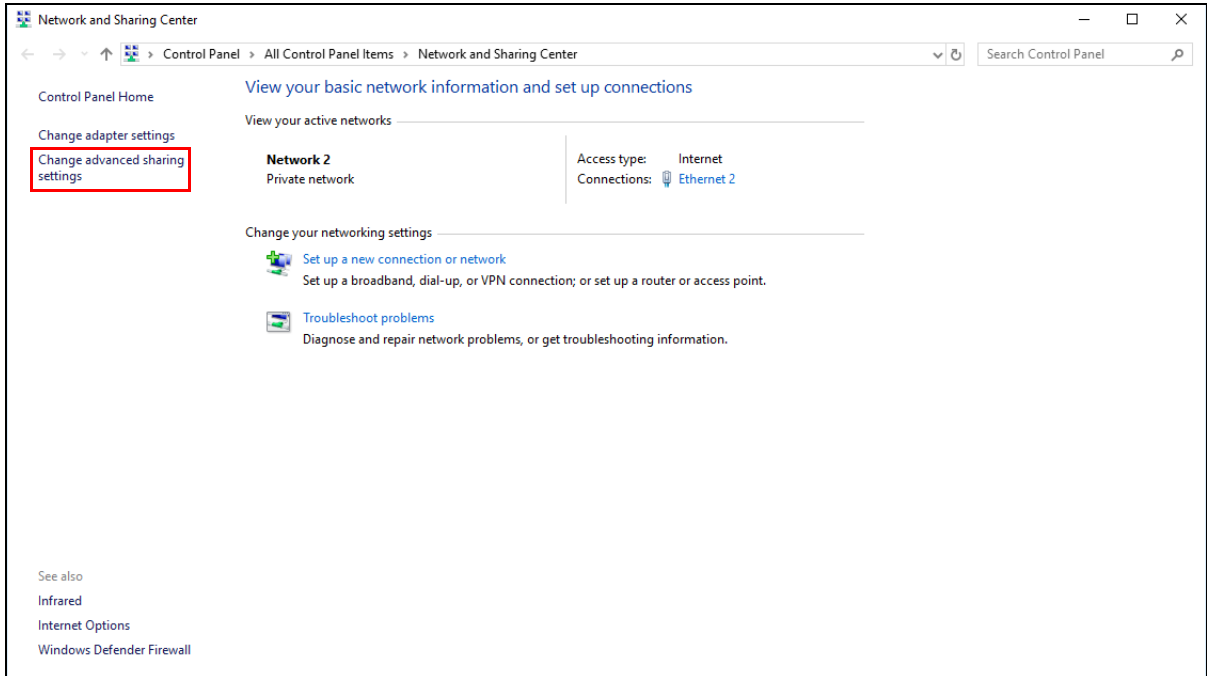
4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.
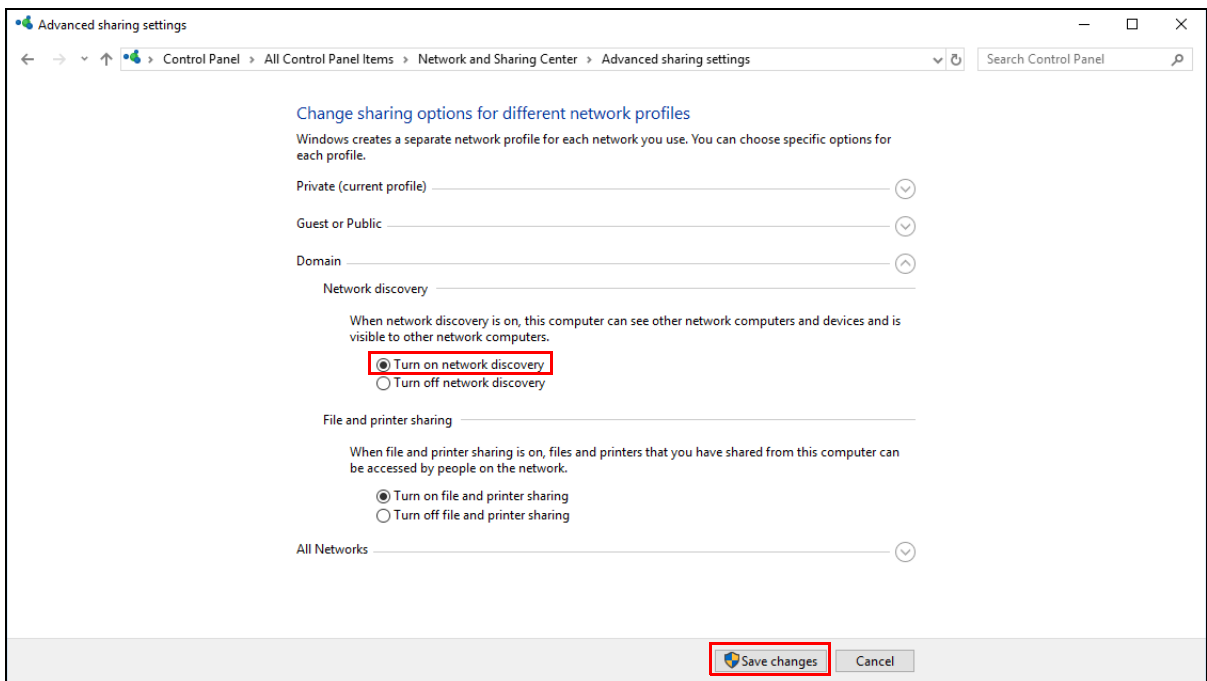
7.7.1 Auto-discover Your UPnP-enabled Network Device

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

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

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

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

Figure 51 Network Connections
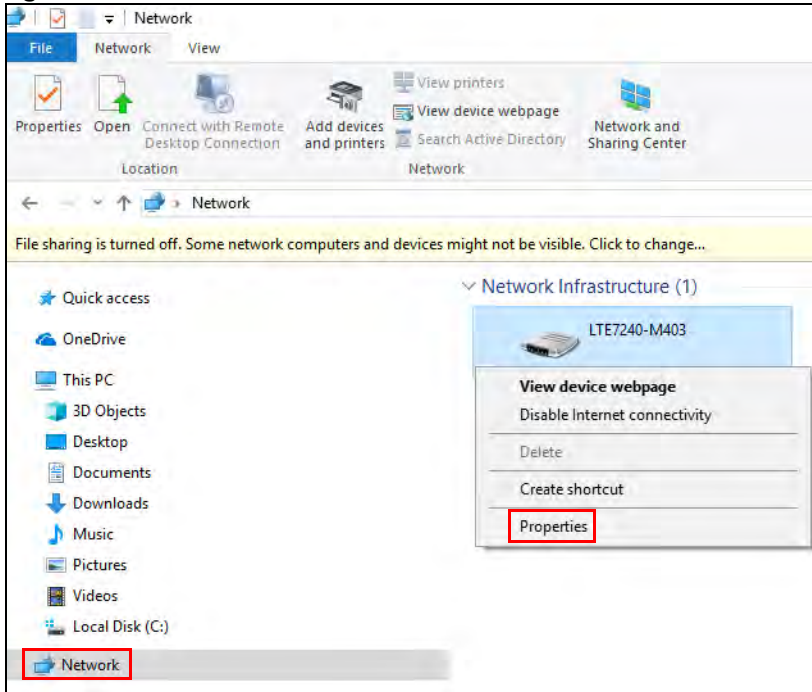
3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 52 Internet Connection Properties
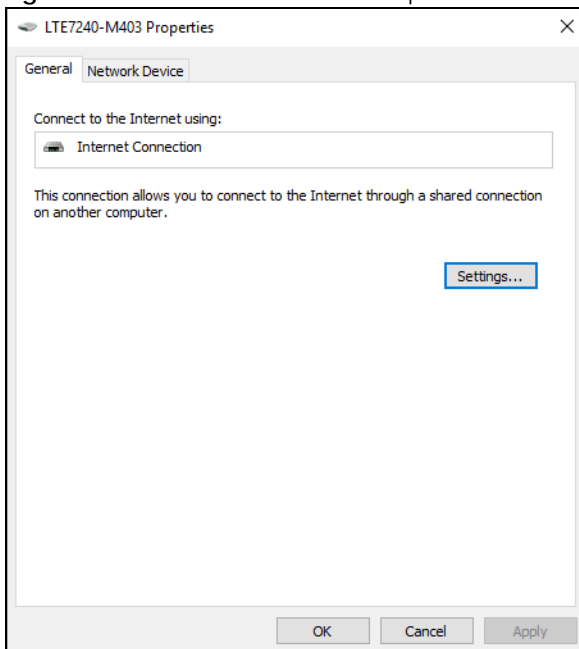
4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 53   Internet Connection Properties: Advanced Settings
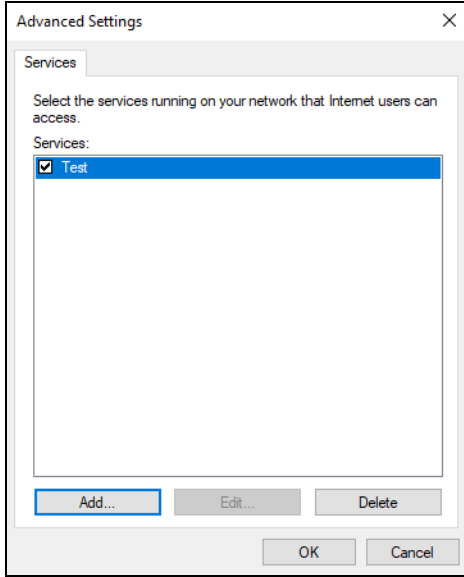
Figure 54   Internet Connection Properties: Advanced Settings: Add
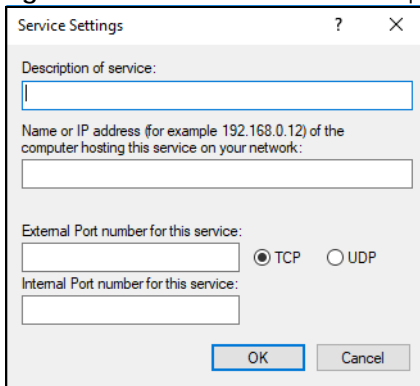
Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.
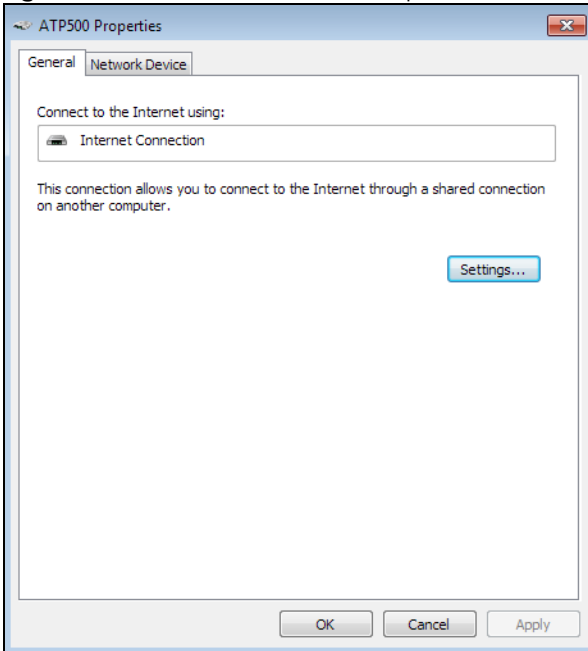
5   Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 55   System Tray Icon
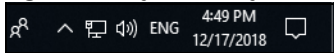
6   To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 56   Internet Connection Status
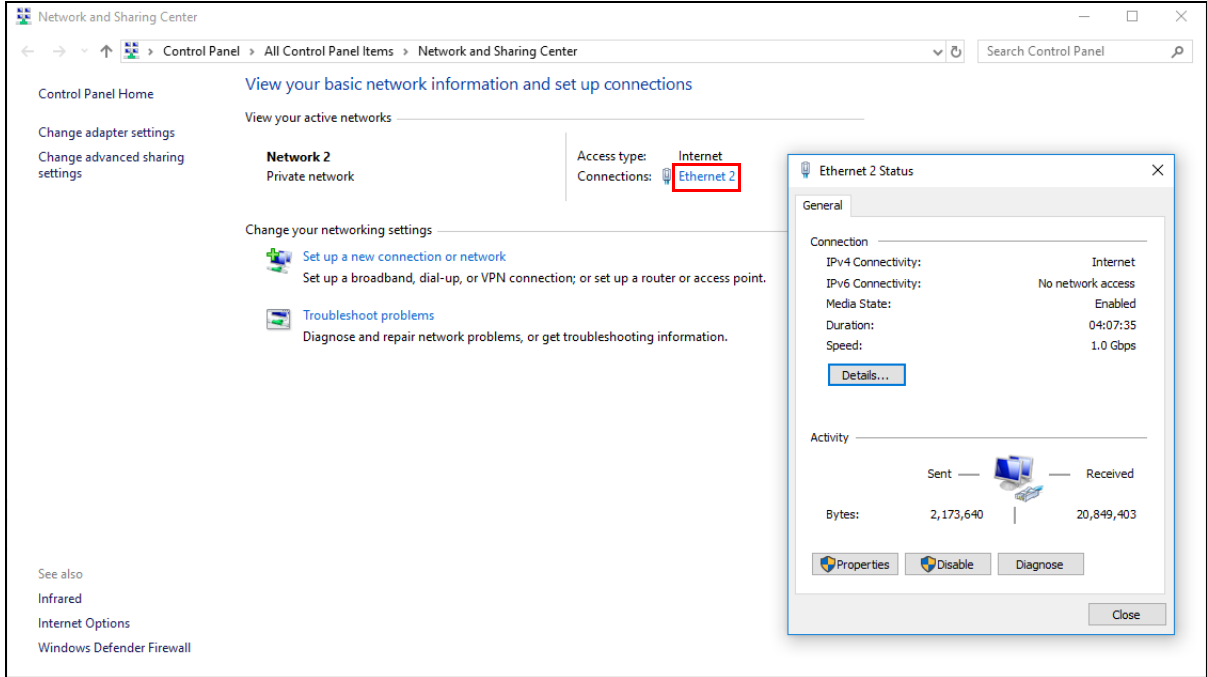
7.8 Web Configurator Easy Access in Windows 7

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

Follow the steps below to access the Web Configurator.

1   Open **Windows Explorer**.

2   Click **Network**.

Figure 57   Network Connections
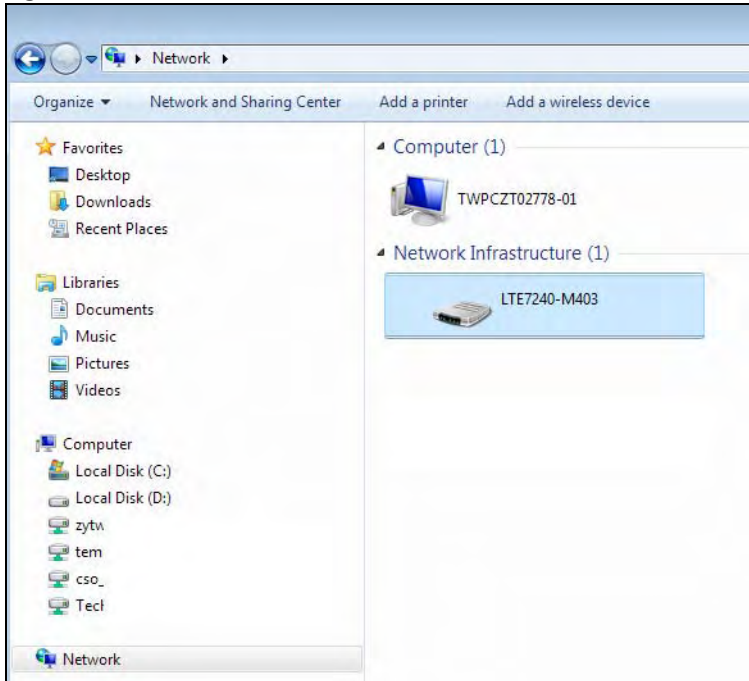
3   An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.

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

Figure 58   Network Connections: My Network Places
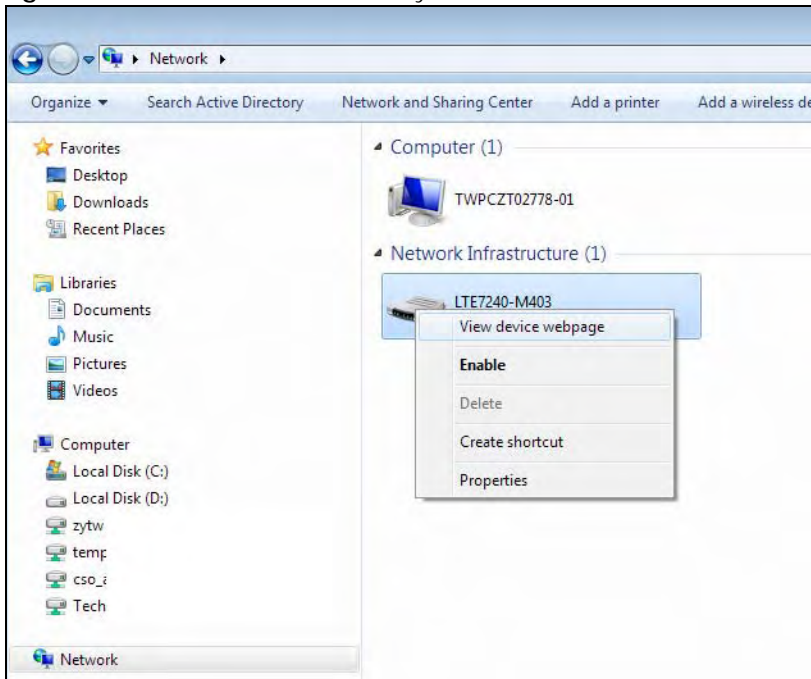
5   Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays with information about the Zyxel Device.

Figure 59 Network Connections: My Network Places: Properties: Example
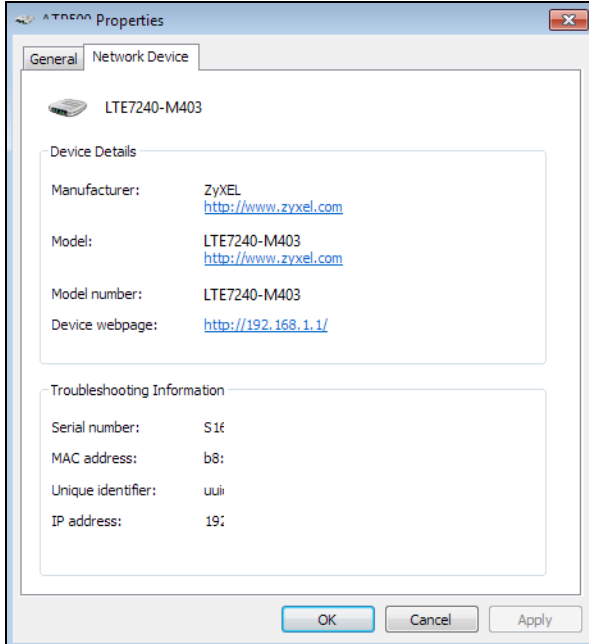
7.9 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

Figure 60   Network Connections
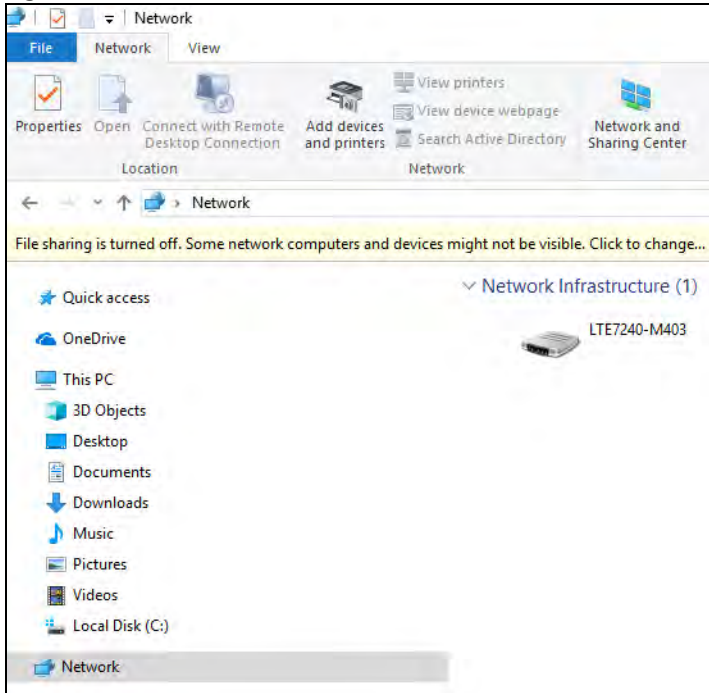
3   An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.

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

Figure 61   Network Connections: Network Infrastructure
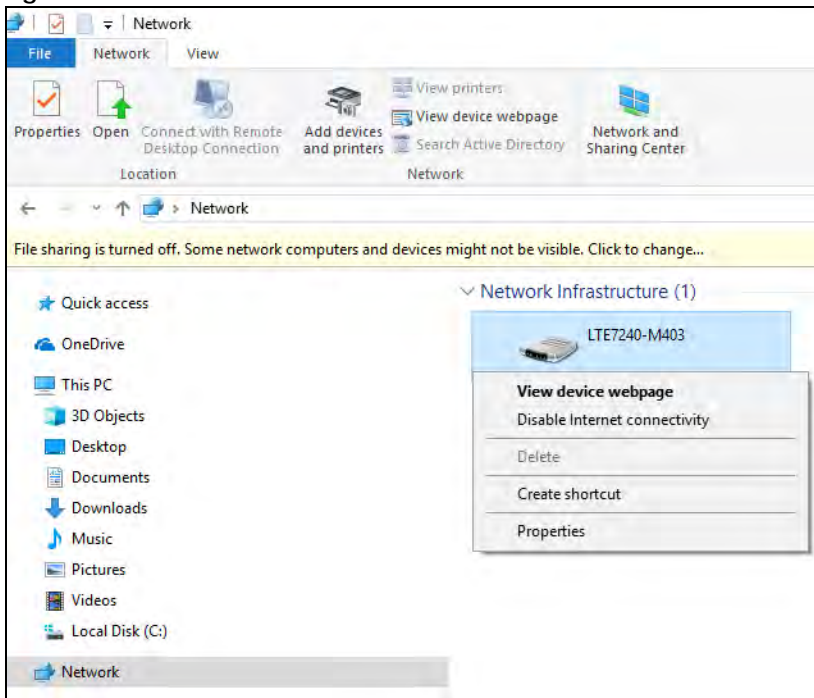
5   Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays information about the Zyxel Device.

Figure 62 Network Connections: Network Infrastructure: Properties: Example
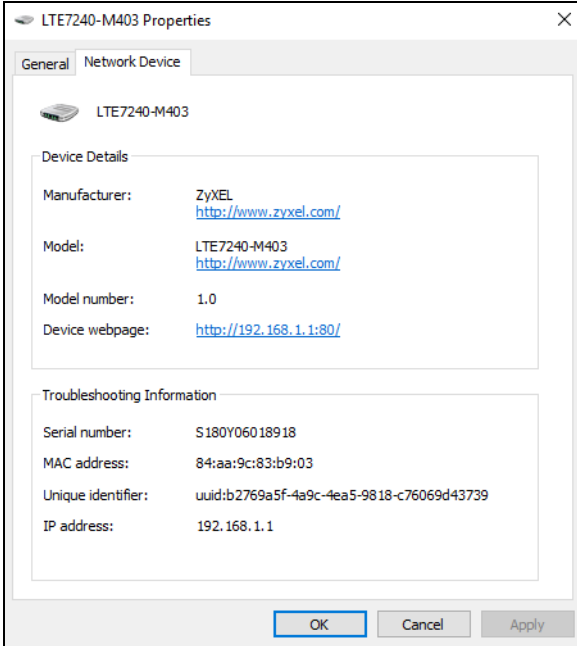
CHAPTER 8
Routing

8.1 Overview

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

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

Figure 63   Example of Static Routing Topology
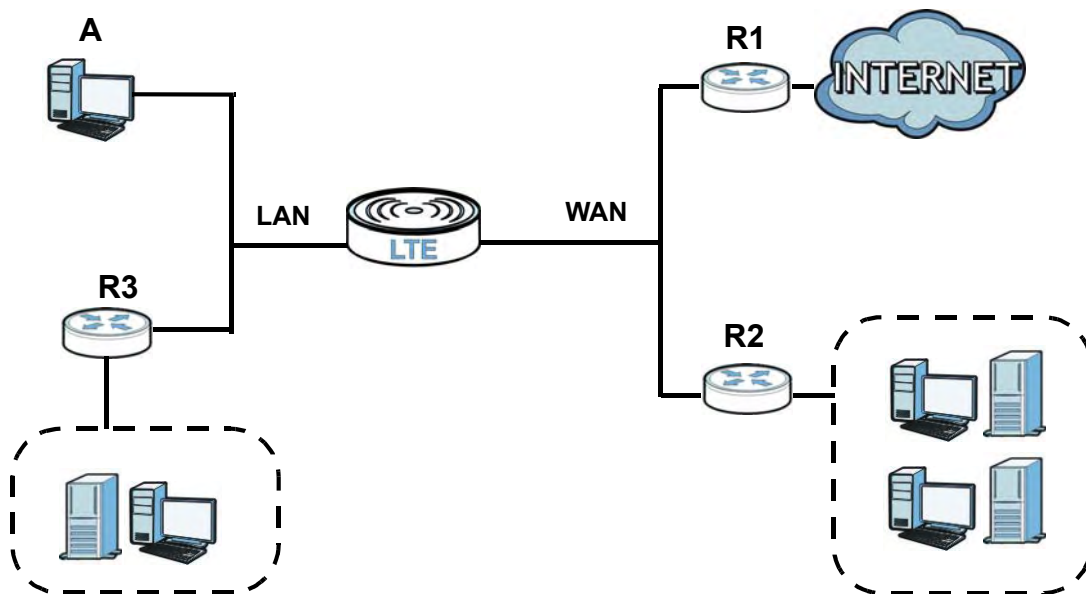
8.2 Configuring Static Route

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

Figure 64   Network Setting > Routing > Static Route

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.

Add New Static Route

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

The following table describes the labels in this screen.

Table 26   Network Setting > Routing > Static Route

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

8.2.1 Add/Edit Static Route

Click **Add New Static Route** in the **Static Route** screen, the following screen appears. Configure the required information for a static route.

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

Figure 65 Routing: Add New Static Route

The following table describes the labels in this screen.

Table 27   Routing: Add/Edit

LABEL	DESCRIPTION
Active	Activates static route.
Route Name	Assign a name for your static route (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign ($) vertical bar (|) ampersand (&) semicolon (;)
IP Type	Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4/IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD).
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. 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.
IP Subnet Mask	Enter the IP subnet mask here.
Use Gateway IP Address	Enables forwarding packets to a gateway IP address or a bound interface.
Gateway IP Address	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Gateway IP Address**, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the Zyxel Device's LAN or WAN port. The gateway helps forward packets to their destinations.
Use Interface	You can decide if you want to forward packets to a gateway IP address (**Default**) or a bound interface (**Cellular WAN**). If you want to configure bound interface, choose an interface through which the traffic is sent. You must have the WAN interfaces already configured in the **Broadband** screen.

Table 27   Routing: Add/Edit (continued)

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

8.3 The DNS Route Screen

Configure how domain name - IP address mapping queries are forwarded from the Zyxel Device to a DNS (Domain Name System) server if your Zyxel Device has multiple WAN interfaces. Click **Network Setting > Routing > DNS Route** to open the **DNS Route** screen.

Figure 66   Network Setting > Routing > DNS Route
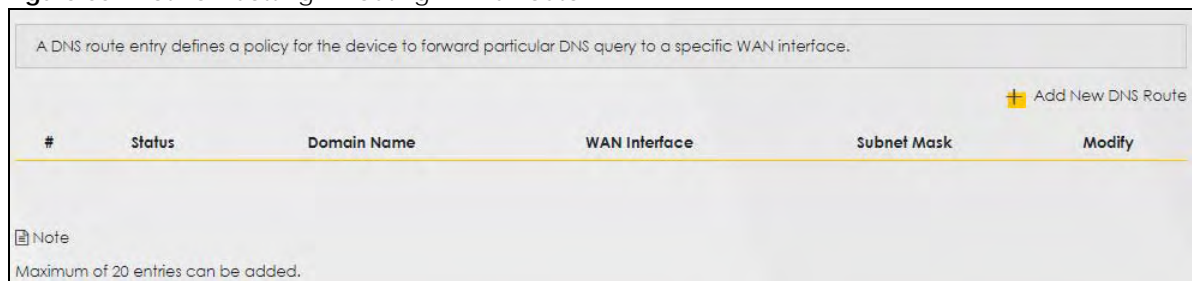
The following table describes the labels in this screen.

Table 28   Network Setting > Routing > DNS Route

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

8.3.1 Add/Edit DNS Route

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

Figure 67   Add New DNS Route

The following table describes the labels in this screen.

Table 29   DNS Route: Add/Edit

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

8.4 The Policy Route Screen

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. Policy routes allow you to override the default routing behavior. Policy-based routing is applied to outgoing packets, and is especially useful when there are more than two Internet connections available in your home or office network.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

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 68   Network Setting > Routing > Policy Route

The following table describes the labels in this screen.

Table 30   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.

8.4.1 Add/Edit Policy Route

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

Figure 69   Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 31   Policy Route: Add/Edit

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

8.5 RIP

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

8.5.1 The RIP Screen

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

Figure 70   Network Setting > Routing > RIP

The following table describes the labels in this screen.

Table 32   Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select **Passive** to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the check box to activate the settings.
Disable Default Gateway	Select the check box to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 9
Network Address Translation (NAT)

9.1 Overview

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

9.1.1 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 9.2 on page 96).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings (Section 9.3 on page 99).
- Use the **DMZ** screen to configure a default server (Section 9.4 on page 102).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 9.5 on page 103).

9.1.2 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.

Finding Out More

See for advanced technical information on NAT.

9.2 The Port Forwarding Screen

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

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring 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 71   Multiple Servers Behind NAT Example
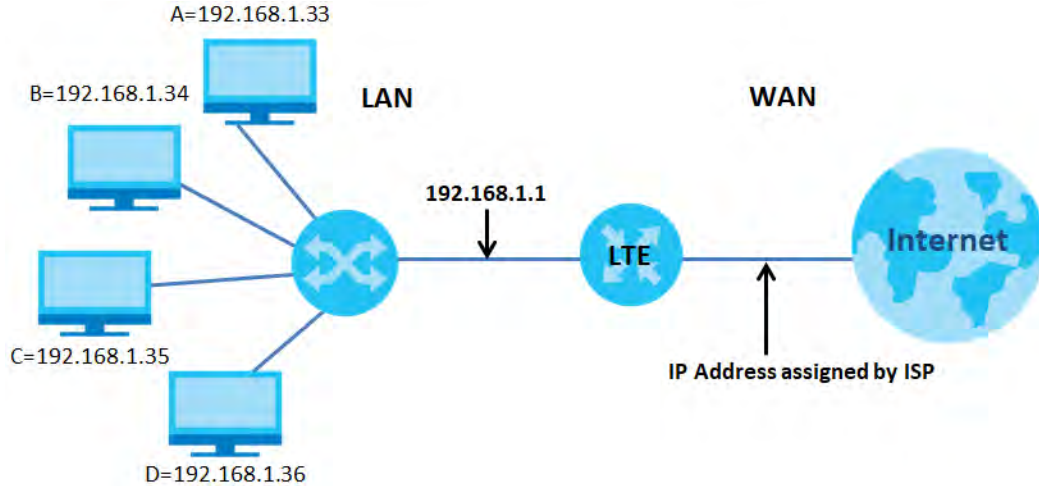
9.2.1 The Port Forwarding Screen

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

Note: TCP port 7547 is reserved for TR-069 requests.

Figure 72   Network Setting > NAT > Port Forwarding

The following table describes the fields in this screen.

Table 33   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.

Table 33   Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
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.

9.2.2 Add/Edit Port Forwarding

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

Figure 73   Port Forwarding: Add/Edit

Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 34   Port Forwarding: Add/Edit

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

9.3 The Port Triggering Screen

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.

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

The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol ("open" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After the computer's connection for that service closes, another computer on the LAN can use the service in the same manner.

For example:

Figure 74 Trigger Port Forwarding Process: Example
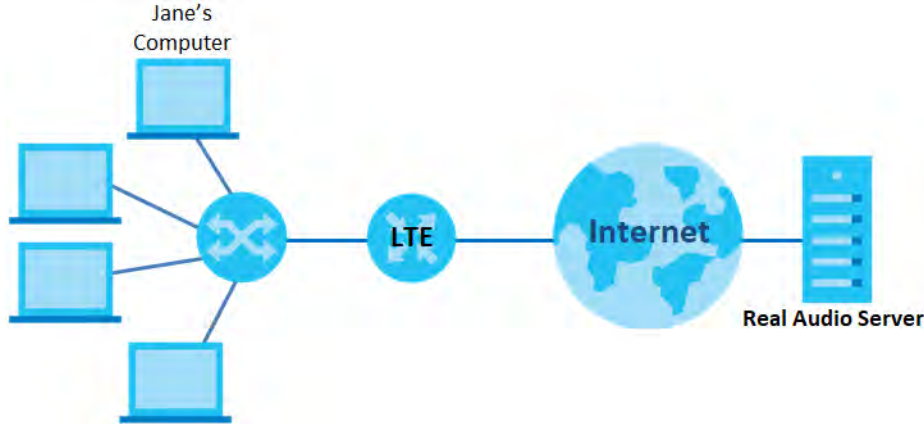
1   Jane requests a file from the Real Audio server (port 7070).

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

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

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

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

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

Note: TCP port 7547 is reserved for system use.

Note: The maximum number of trigger ports for a single rule or all rules is 999.

Note: The maximum number of open ports for a single rule or all rules is 999.
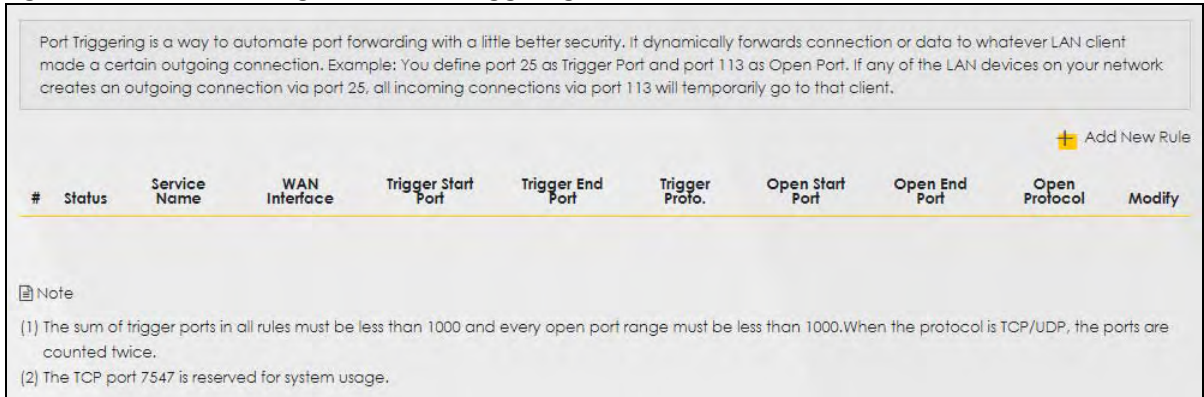
The following table describes the labels in this screen.

Table 35   Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Protocol	This is the open transport layer protocol.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

9.3.1 Add/Edit Port Triggering Rule

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

Figure 76   Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 36   Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (blue switch) or disable (gray switch) to activate or deactivate the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

9.4 The DMZ Screen

A client in the Demilitarized Zone (DMZ) is no longer behind the Zyxel Device and can therefore run any Internet application such as video conferencing and Internet gaming without restrictions. This, however, may pose a security threat to the Zyxel Device. Use this screen to specify the IP address of a default

server to receive packets from ports not specified in the **Port Triggering** screen. Click **Network Setting > NAT > DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address and click **Apply** to activate the DMZ host.
Otherwise, clear the IP address field and click **Apply** to de-activate the DMZ host.

Figure 77   Network Setting > NAT > DMZ

The following table describes the fields in this screen.

Table 37   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.

9.5 The ALG Screen

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 78   Network Setting > NAT > ALG

The following table describes the fields in this screen.

Table 38   Network Setting > NAT > ALG

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

Dynamic DNS Setup

10.1 DNS Overview

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

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

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, 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 don't 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.

10.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 10.2 on page 106).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device (Section 10.3 on page 107).

10.1.2 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.

10.2 The DNS Entry Screen

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure DNS routes on the Zyxel Device. Click **Network Setting > DNS** to open the **DNS Entry** screen.

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

Figure 79 Network Setting > DNS > DNS Entry
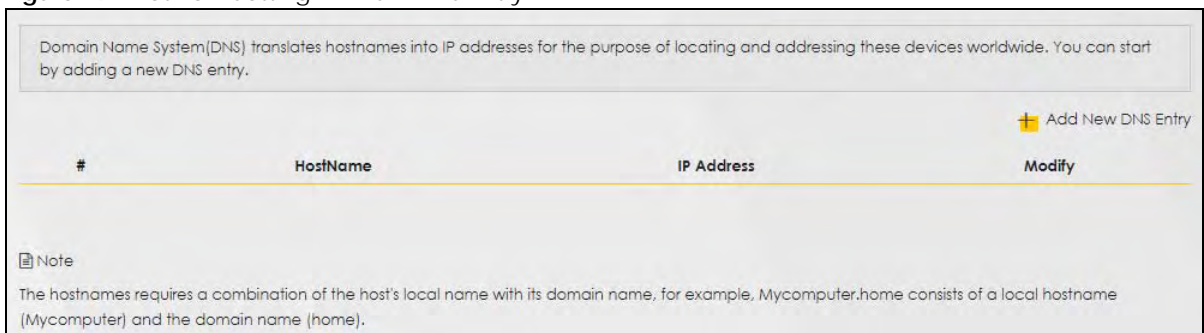
The following table describes the fields in this screen.

Table 39   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.

10.2.1 Add/Edit DNS Entry

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

Figure 80 DNS Entry: Add/Edit

The following table describes the labels in this screen.

Table 40 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IPv4 Address	Enter the IPv4 address of the DNS entry.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

10.3 The Dynamic DNS Screen

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 81 Network Setting > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 41   Network Setting > DNS > > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Type the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	
User Authentication Result	This shows **Success** if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.