ZYXEL
NETWORKS

User's Guide
NBG7510

Dual-Band WiFi 6 AX1800 Router

Default Login Details	
LAN IP Address Standard (Router) Mode	http://192.168.123.1
AP Mode	http://192.168.123.2 OR http://DHCP-assigned IP
Password	See the Zyxel Device label
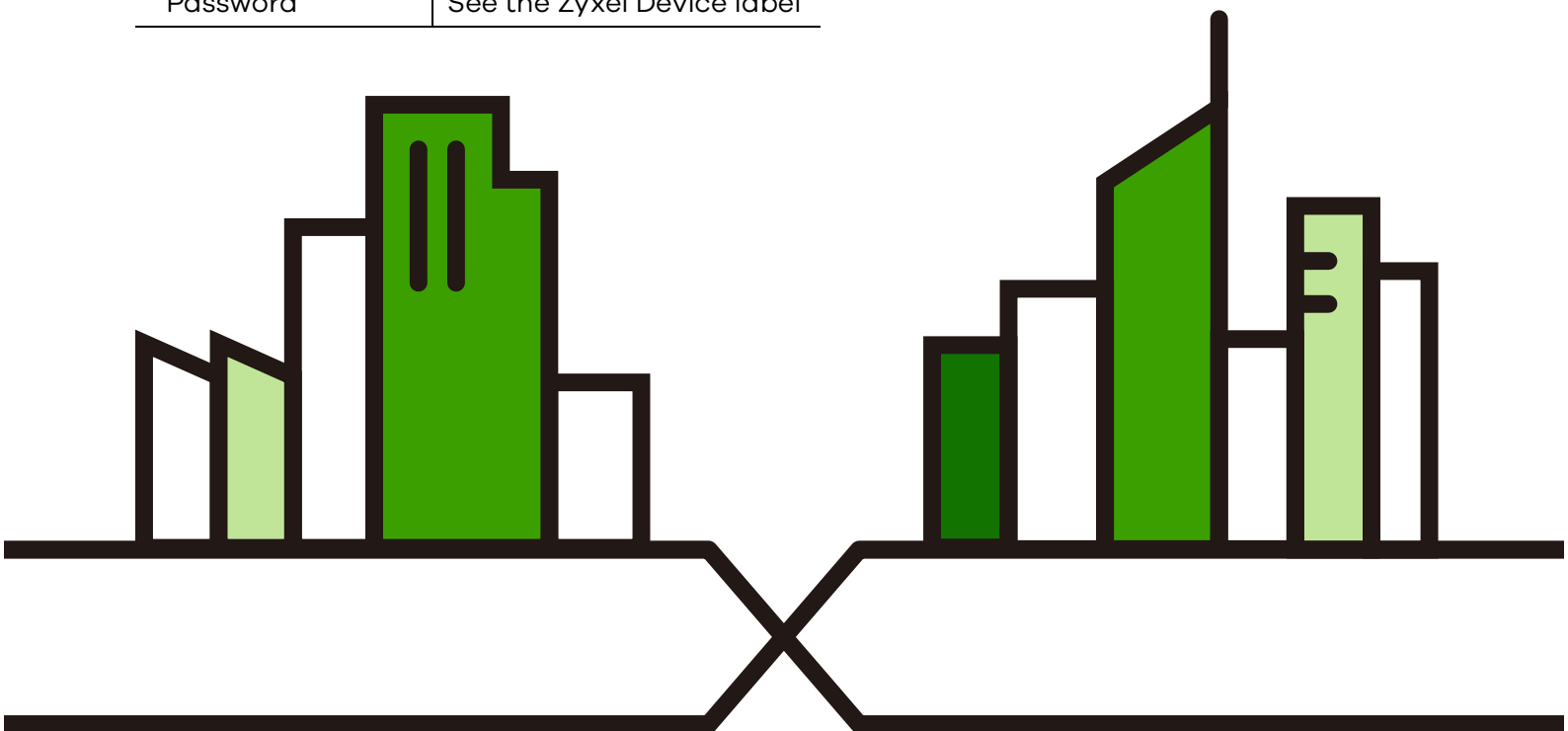
IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

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

- 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

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

Icons Used in Figures

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

Zyxel Device	Generic Router	Switch
Server	Firewall	USB Storage Device
Printer		

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introducing the Zyxel Device

1.1 Overview

This chapter introduces the main features and applications of the Zyxel Device. The Zyxel Device is an Ethernet router, which provides fast Internet access.

The Zyxel Device supports WiFi6 that is most suitable in areas with a high concentration of users. You can schedule WiFi usage using Parental Control.

This table summarizes some of the features that are available at the time of writing.

Table 1   Features Supported

FEATURE	NBG7510
WiFi6 Standard	YES
2.4 GHz WLAN	YES
5 GHz WLAN	YES
Parental Control Schedule	YES
Parental Control URL Filter	NO
Rubber feet for desktop placement	NO
Wall-mount	YES
Operating mode	YES
Mobile app	YES
VLAN (Virtual Local Area Network)	YES
OpenVPN	NO
Guest WiFi	YES
Firewall	YES
NAT and Port Forwarding	YES
ALG (Application Layer Gateway)	YES
VPN (Virtual Private Network) Pass-through	NO
Port Triggering	YES
Dynamic DNS (Domain Name System)	YES
IPv6 support	YES
UPnP (Universal Plug-and-Play)	YES
Save configuration	YES
Firmware Version	1.00

1.2 Applications for the Zyxel Device

The Zyxel Device supports the following features.

Internet Access

The Zyxel Device provides Internet access by connecting the WAN port to your ISP through an Ethernet cable.

Computers can connect to the Zyxel Device's LAN ports (or wirelessly) and access the Internet simultaneously.

Figure 1   The Zyxel Device's Internet Access Application
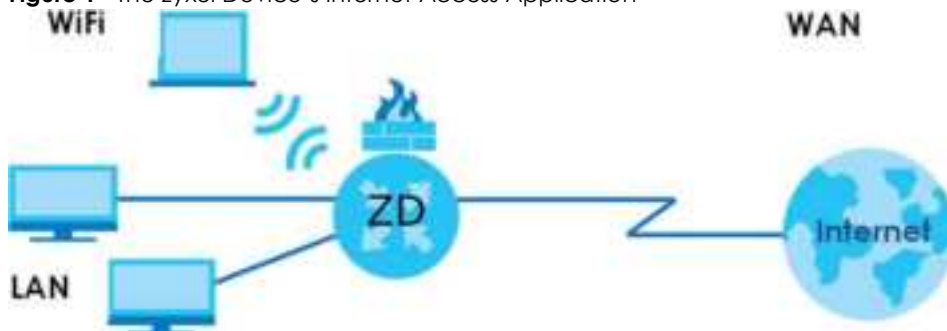
You can also configure the firewall on the Zyxel Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Connect the WAN port to the broadband modem or router. This way, you can access the Internet through an Ethernet connection and use the firewall and parental control functions on the Zyxel Device.

Figure 2   The Zyxel Device's Internet Access Application: Ethernet WAN
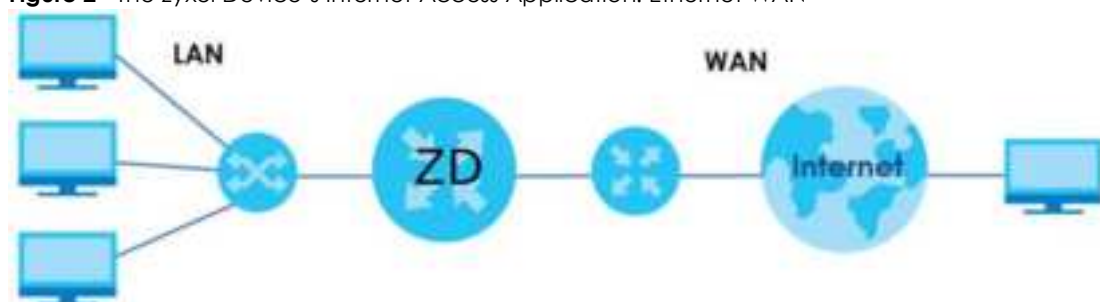
Dual-Band WiFi

IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the Zyxel Device to access network resources.

The Zyxel Device is a dual-band gateway that can use both 2.4 GHz and 5 GHz networks at the same time. You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz

band for time sensitive traffic like high-definition video, music, and gaming.

Figure 3   Dual-Band Application
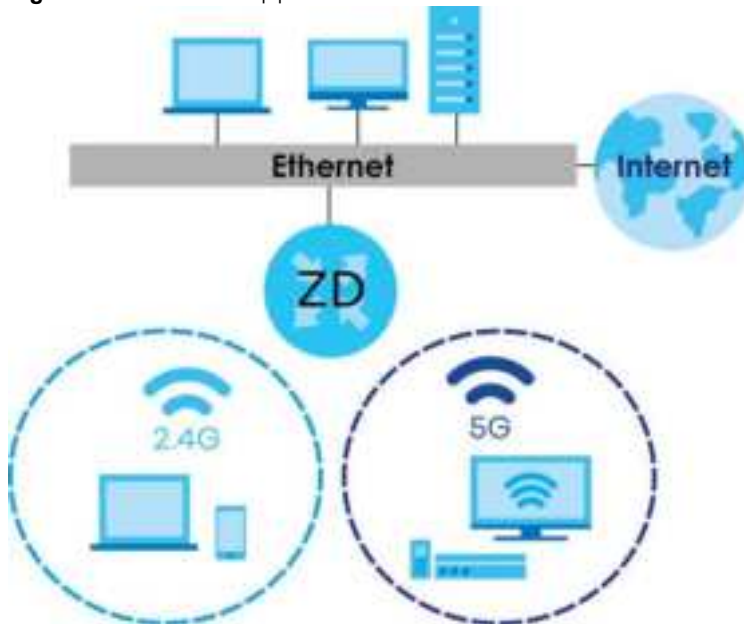
The Zyxel Device is a WiFi Access Point (AP) for IEEE 802.11b/g/n/a/ac/ax WiFi clients, such as notebook computers, iPads, smartphones, and so on. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

The Zyxel Device supports WiFi Protected Setup (WPS), which allows you to quickly set up a WiFi network with strong security. You can use WPS (WiFi Protected Setup) to create an instant WiFi network connection with another WPS-compatible device.

Figure 4   WiFi Access Example

Guest WiFi

The Zyxel Device allows you to set up a guest WiFi network where users can access the Internet through the Zyxel Device, but not to other networks connected to it.

IPv6 and IPv6 Firewall

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 support IPv6 rapid deployment (6RD).

Consequently, you can enable and create IPv6 firewall rules to filter IPv6 traffic.

Firewall protects your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

•allows traffic that originates from your LAN computers to go to all other networks.

•blocks traffic that originates on other networks from going to the LAN.

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

Figure 5   Firewall Default Action
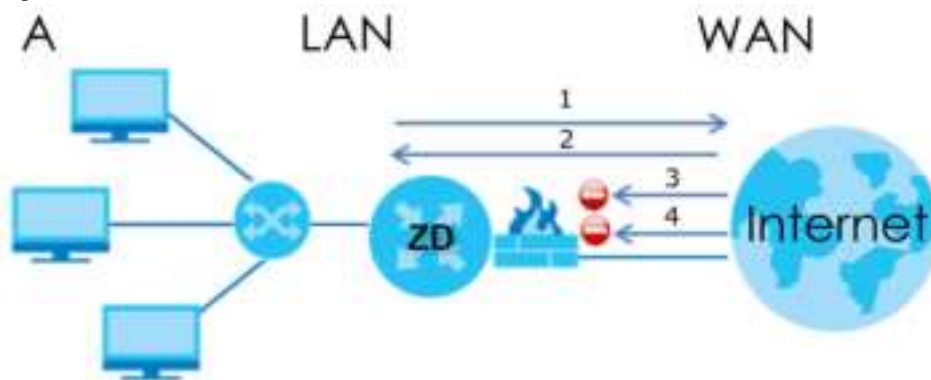
1.3 Operating Modes for the Zyxel Device

The Zyxel Device is available in both Standard (router) mode and AP mode.

1.3.1 Standard (Router) Mode

The Zyxel Device is set to standard (router) mode by default. The Zyxel Device is used to connect the local network to another network (for example, the Internet). In standard mode Zyxel Device has two IP addresses, a LAN IP address and a WAN IP address. It also has more routing features. In the example scenario below, Zyxel Device connects the local network to the Internet through a modem (**M**).

Figure 6   Standard Mode Example
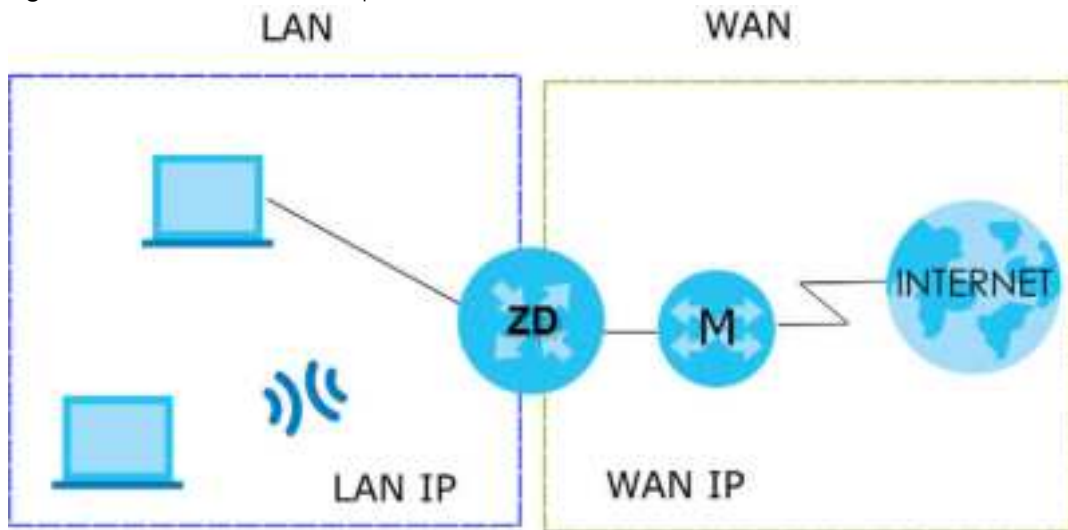
1.3.2 AP Mode

Use your Zyxel Device as a bridge if you already have a router or gateway on your network. In this mode your Zyxel Device bridges a wired network (LAN) and WiFi in the same subnet. In AP mode, Zyxel Device has one IP address and Zyxel Device interfaces are bridged together in the same network. In the example scenario below, Zyxel Device connects the local network to the Internet through a router (**R**).

Figure 7   AP Mode Example
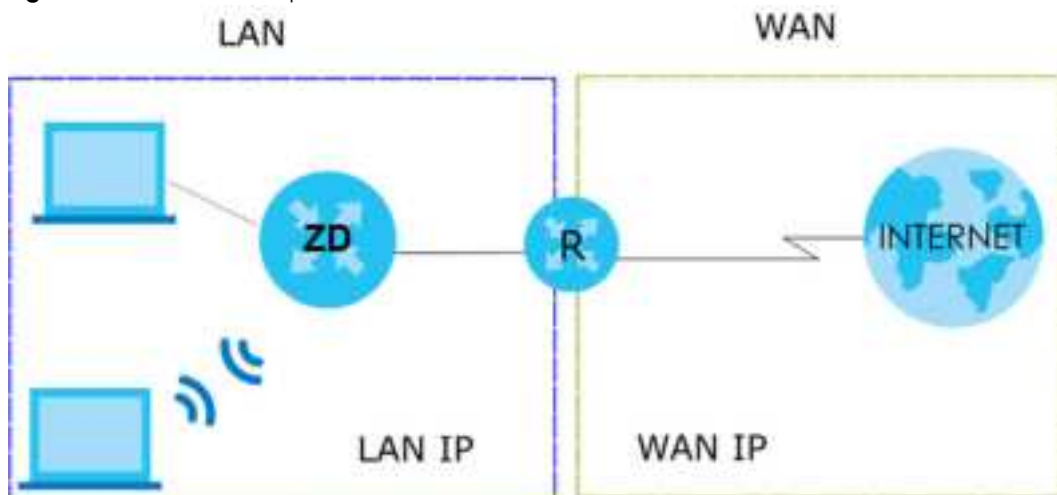
1.4 Ways to Manage the Zyxel Device

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

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

- Secure Shell (SSH), Telnet. Use for troubleshooting the Zyxel Device by qualified personnel.
- FTP. Use FTP for firmware upgrades and configuration backup or restore.

1.5 Good Habits for Managing the Zyxel Device

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

- Change the WiFi and Web Configurator passwords. Use a password that is not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the passwords and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Zyxel Device. You could simply restore your last configuration.

CHAPTER 2
Hardware

This chapter describes the top and side panels for the Zyxel Device.

2.1 Side Panel

The connection ports are located on the side panel.

Figure 8 Side Panel

The following table describes the items on the side panel of the Zyxel Device.

Table 2   Panel Ports and Buttons

LABEL	DESCRIPTION
WAN	For the Zyxel Device, connect an Ethernet cable to the WAN port for Internet access.
LAN1 – LAN3	Connect computers or other Ethernet devices to Ethernet LAN ports for Internet access.

Table 2   Panel Ports and Buttons (continued)

LABEL	DESCRIPTION
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
DC12V	Connect a power adapter to start the device.
WIFI/WPS	Press the **WIFI/WPS** button for 1.5 - 4 seconds to quickly setup a secure WiFi connection between the Zyxel Device and a WPS-compatible client device.

2.1.1 Top Panel LED

After you connect the power to the Zyxel Device, view the LEDs to ensure proper functioning of the Zyxel Device and as an aid to troubleshooting. The LED indicators are located on the top panel.

Figure 9   Top Panel

The following table describes the LED behavior on the top panel.

Table 3   LED Behavior

LED	COLOR	STATUS	DESCRIPTION
The LED Indicator	Red	Blinking	There is no Internet connection.
	Blue	On	The Internet is ready.
		Blinking	The Zyxel Device is booting up.
		Off	Power is off.
	Red/Blue	Blinking	The Zyxel Device is in the process of resetting to factory defaults.
	Purple	On	The Zyxel Device is updating firmware.
		Blinking	WPS is in progress.

2.2 Resetting the Zyxel Device

If you forget your password or cannot access the Web Configurator, insert a thin object into the RESET hole to reload the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to the factory default (see the device label), and the LAN IP address will be "192.168.123.1".

2.2.1 How to Use the RESET Button

1   Make sure the LED lights blue (not blinking).

2   Locate the Reset hole.

3   Insert a thin object into the Reset hole for more than 5 seconds or until the LED begins to blink red and blue and then release it. The LED will blink blue when the defaults have been restored and the Zyxel Device restarts.

2.3 WiFi/WPS Button

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

To activate WiFi/WPS:

1   Make sure the **POWER** LED lights blue and not blinking.

2   Press the **WiFi/WPS** button for 1.5-4 seconds and release it.

3   Press the WPS button on another WPS-enabled client device within range of the Zyxel Device within 120 seconds. The LED flashes purple while the Zyxel Device sets up a WPS connection with the client device.

4   Once the connection is successfully made, the LED will light up in blue.

2.4 Wall Mounting

Please refer to the installation guide below for the wall mounting procedures of the Zyxel Device. You may need screw anchors if mounting on a concrete or brick wall.

Figure 10 Wall Mounting Screw Specifications
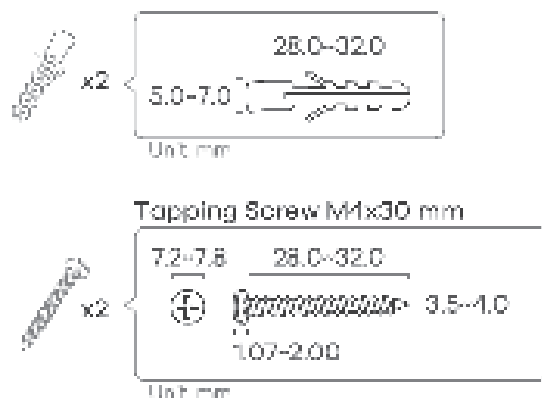
Table 4 Wall Mounting Information

Distances between holes	105 mm
M4 Screws	Two
Screw Anchors	Two

Do the following to attach your Zyxel Device to a wall.

1 Select a position free of obstructions on a wall strong enough to hold the weight of the Zyxel Device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

Figure 11 Wall Mounting Distance
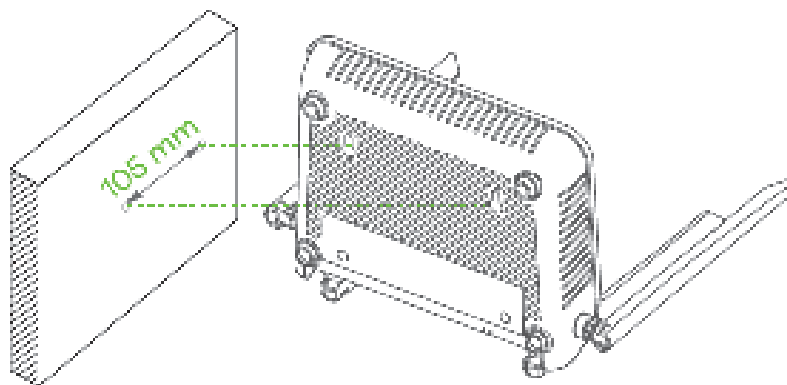
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

Do not wall mount the Zyxel Device over a height of 2 m.

3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in – leave a small gap of about 0.5 cm. If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

Figure 12   Wall Mounting Anchors
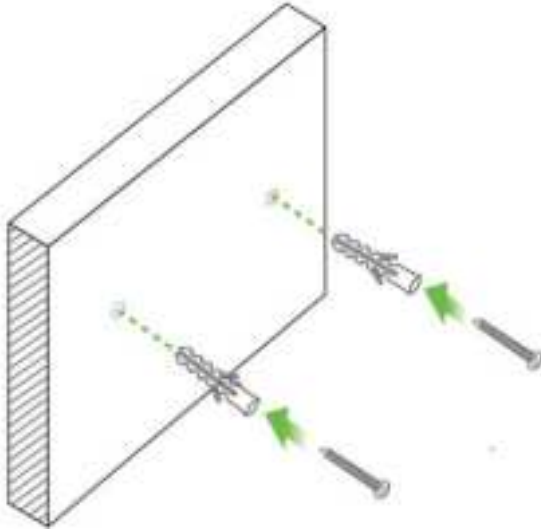
4 Make sure the screws are fastened well enough to hold the weight of the Zyxel Device with the connection cables.

5 Align the holes on the back of the Zyxel Device with the screws on the wall. Hang the Zyxel Device on the screws.

Figure 13   Wall Mounting Device
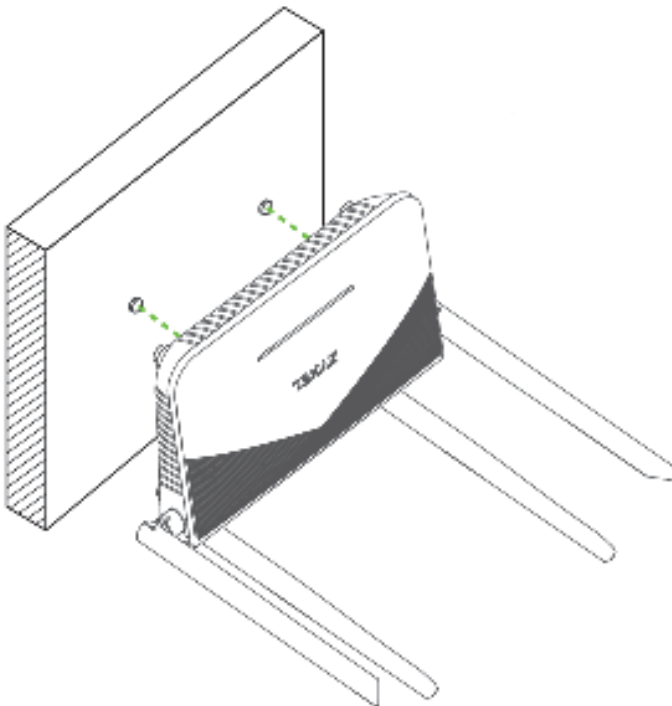
CHAPTER 3
Web Configurator

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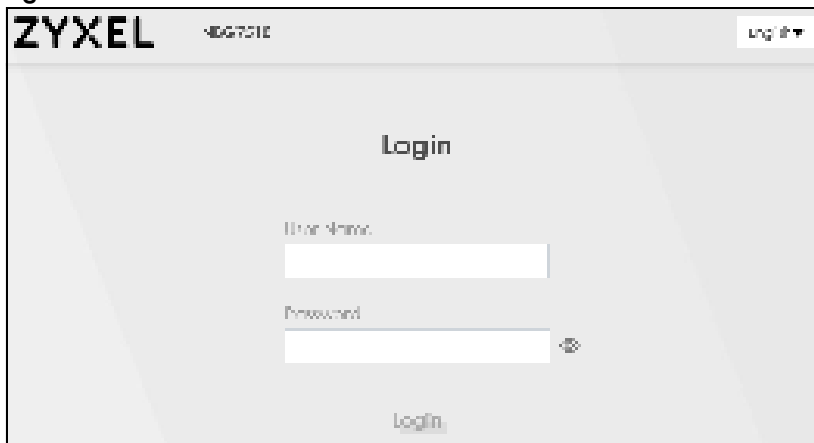
The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768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

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

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

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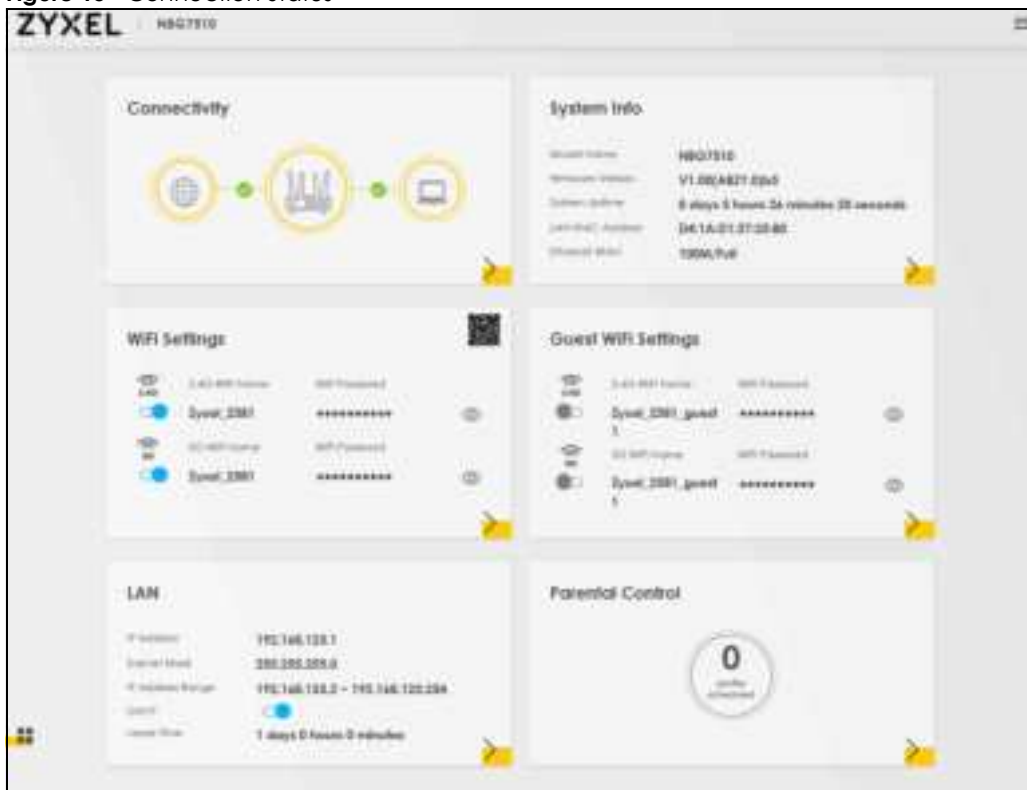
1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).

2 Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.123.3 to 192.168.123.254.

3 Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to http://192.168.123.1.

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

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

Figure 14   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.

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

Figure 15   Connection Status

3.2 Web Configurator Layout

Figure 16 Screen Layout

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

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

3.2.1 Settings Icon

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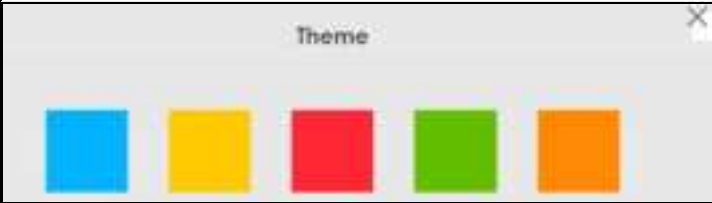
3.2.1.1 Side Bar

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

Figure 17 Side Bar

The icons provide the following functions.

Table 5   Web Configurator Icons in the Title Bar

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

3.2.1.2 Navigation Panel

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

Figure 18 Navigation Panel

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		Use this screen to configure basic Internet access, wireless settings, and parental control settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication or security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the Zyxel Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.
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.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	Wake on LAN	Use this screen to remotely turn on a device on the local network.
	TFTP Server Name	Use DHCP option 66 to identify a TFTP server name.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers.

Table 6   Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable the ALGs (Application Layer Gateways) in the Zyxel Device to allow applications to operate through NAT.
	Address Mapping	Use this screen to change your Zyxel Device's IP address mapping settings.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the Zyxel Device.
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		
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.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.
	Security Log	Use this screen to view all security related events. You can select the level and category of the security events in their proper drop-down list window.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
	NAT	Use this screen to view NAT statistics for connected hosts.
ARP table	ARP table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the Zyxel Device.
WLAN Station Status	WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the Zyxel Device's wireless LAN.
Maintenance		
Operating Mode	Operating Mode	Use this screen to change the operating mode of the Zyxel Device.
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.

Table 6   Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** > **MGMT Services** screen.
Time	Time	Use this screen to change your Zyxel Device's time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Settings	Log Settings	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 Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems.

3.2.1.3 Dashboard

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

Figure 19   Navigation Panel
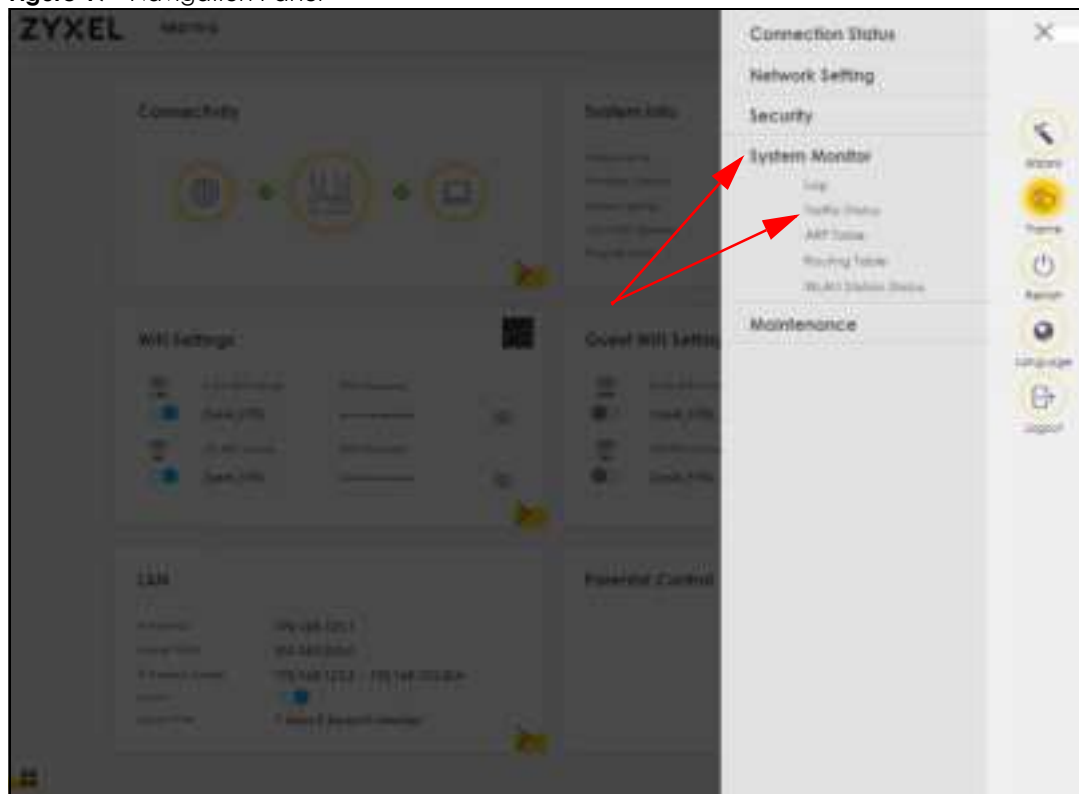
3.2.2 Layout Icon

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

Figure 20 Screen Order
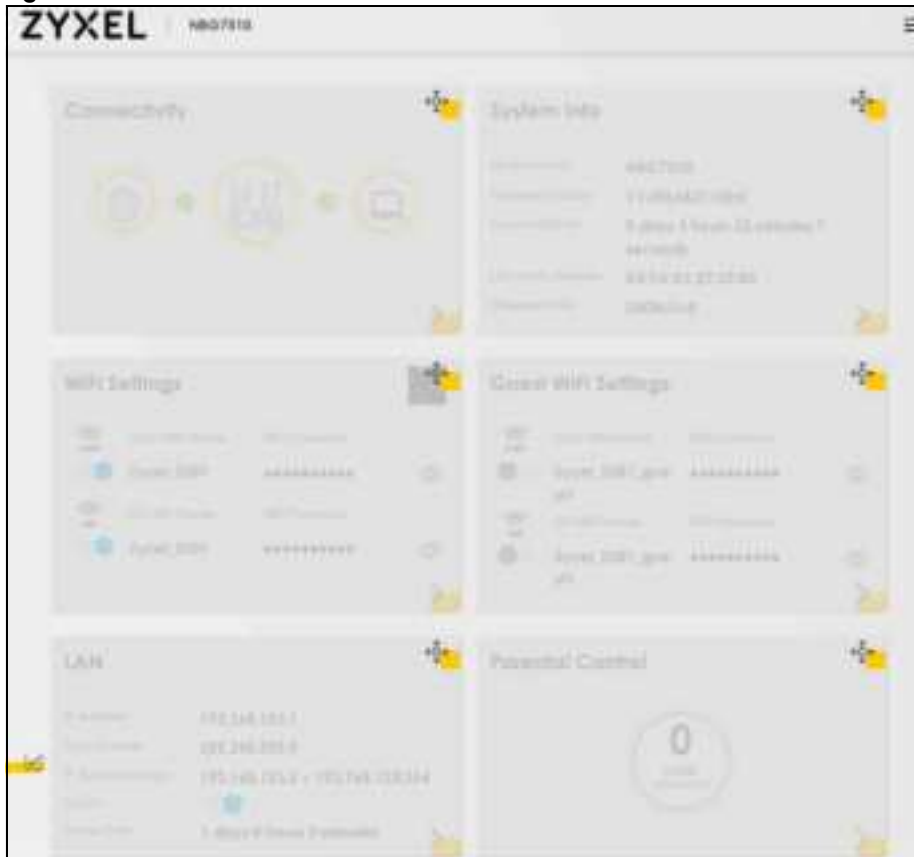
The following screen appears. Select a block and hold it to move around. Click the Check icon ( ) in the lower left corner to save the changes.

CHAPTER 4
Quick Start

4.1 Overview

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

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

4.2 Quick Start Setup

You can click the **Wizard** icon in the side bar to open the **Wizard** screens. After you click the **Wizard** icon, the following screen appears. Click **Let's go** to proceed with settings on time zone and 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 21   Wizard – Home

4.3 Quick Start Setup – Time Zone

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

Figure 22 Wizard – Time Zone
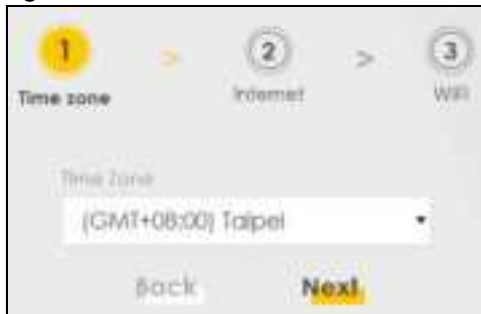
4.4 Quick Start Setup – Internet Connection

Select the Internet connection mode of the Zyxel Device. Click **Next** to continue.

Figure 23 Wizard – Internet
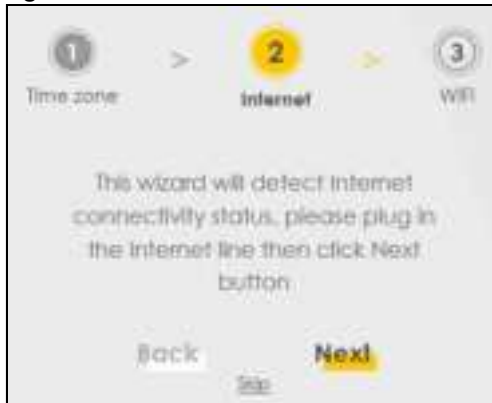
4.4.1 Successful Internet Connection

The Zyxel Device has Internet access.

Figure 24 Wizard – Successful Internet Connection
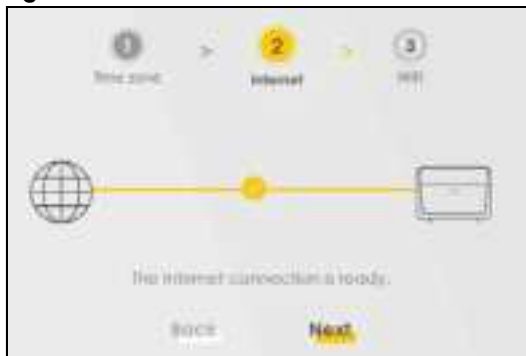
4.4.2 Unsuccessful Internet Connection

The Zyxel Device did not detect a WAN connection.

Figure 25 Wizard – Internet Connection is Down

4.5 Quick Start Setup – WiFi

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

Click the **Keep 2.4G and 5G the same** check box to use the same SSID for 2.4G and 5G wireless networks. Otherwise, deselect the check box to have two different SSIDs for 2.4G and 5G wireless networks. The screen and fields to enter may vary when you select or deselect the check box. Click **Done**.

Figure 26 Wizard – WiFi
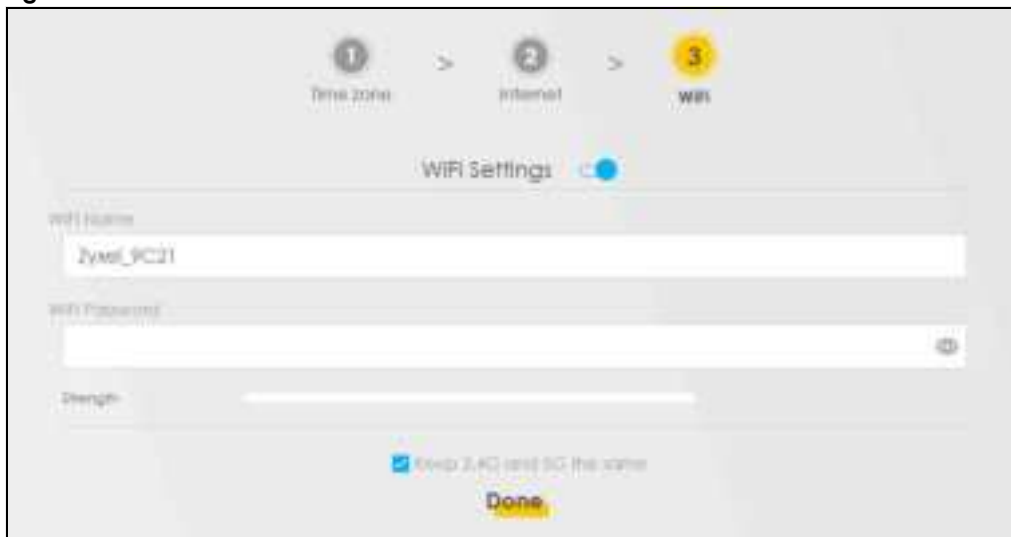
4.6 Quick Start Setup – Finish

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

CHAPTER 5
Tutorials

5.1 Overview

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

- Wired Network Setup
- WiFi Network Setup
- Network Security
- Device Maintenance

5.2 Wired Network Setup

This section shows you how to set up a wired connection.

5.2.1 Setting Up an Ethernet Connection

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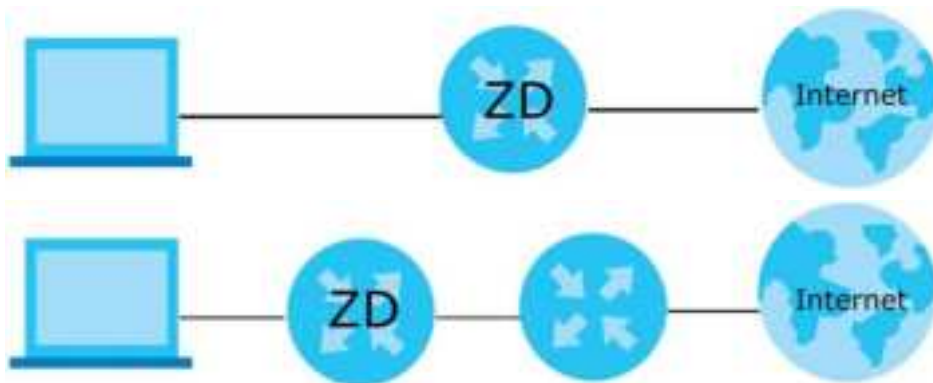
1   Make sure you have the Ethernet WAN port connect to a modem or router.

2   Go to **Network Setting** > **Broadband** and then the following screen appears. Click **Add New WAN Interface** to add a WAN connection.
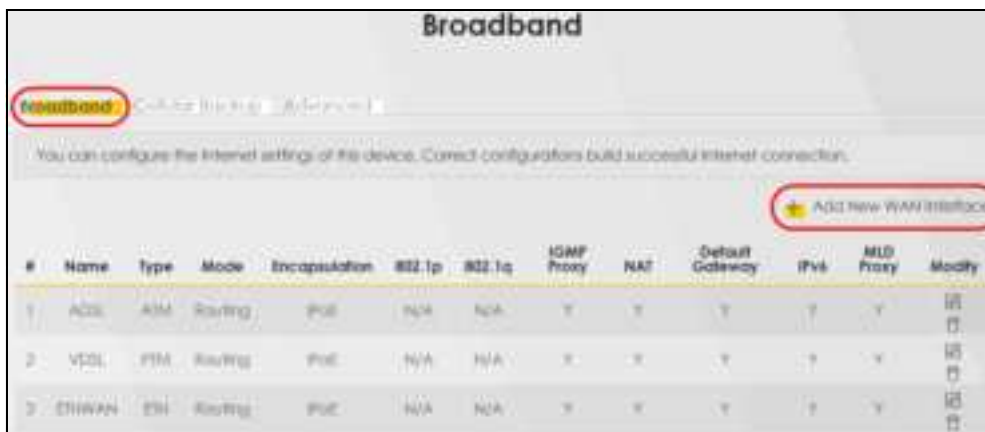
3 In this example, configure the following information for the Ethernet connection.

General	
Name	My ETH Connection
Type	Ethernet
Connection Mode	Routing
Encapsulation	IPoE
IPv6/IPv4 Mode	IPv4 Only

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

4a Enter a **Name** to identify your WAN connection.

4b Set the **Type** to **Ethernet**.

4c Set your Ethernet connection **Mode** to **Routing**.

4d Choose the **Encapsulation** specified by your Internet service provider. For this example, select **IPoE** or **PPPoE** as the WAN encapsulation type.

4e Set the **IPv4/IPv6 Mode** to **IPv4 Only**.

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

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

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

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

5.3 WiFi Network Setup

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

Figure 27 WiFi Network Setup
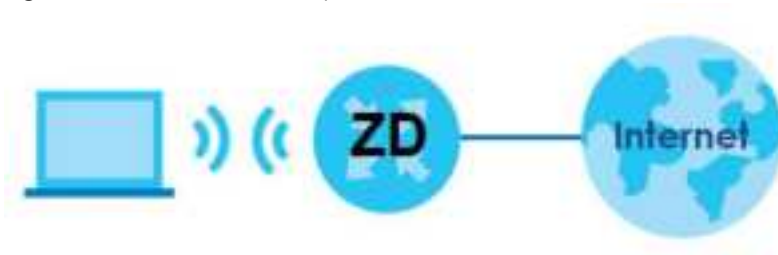
See the label on the Zyxel Device for the WiFi network settings and then connect manually to the Zyxel Device. See Section 5.3.2 on page 41. Alternatively, you can set up a WiFi network using WPS.

5.3.1 Changing Security on a WiFi Network

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

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

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

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

You can now use the WPS feature to establish a WiFi connection between your notebook and the Zyxel Device (see Section 5.3.2 on page 41). Now use the new security settings to connect to the Internet through the Zyxel Device using WiFi.

5.3.2 Connecting to the Zyxel Device's WiFi Network Using WPS

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

• **Push Button Configuration (PBC)** – Connect to the WiFi network by pressing a button. See Section 5.3.2.1 on page 41. This is the simplest method.

• **PIN Configuration** – Connect to the WiFi network by entering a PIN (Personal Identification Number) from a WiFi-enabled device in the Zyxel Device's Web Configurator. See Section 5.3.3 on page 44. This is the more secure method, because one device can authenticate the other.

5.3.2.1 WPS Push Button Configuration (PBC)

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

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

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

3 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.
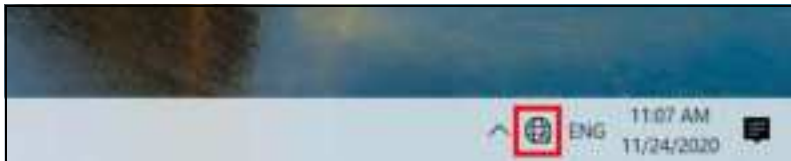
4 Locate the WiFi network of the Zyxel Device. The default WiFi network name is "Zyxel_XXXX" (2.4G) or "Zyxel_XXXX_5G" (5G). Then click **Connect**.
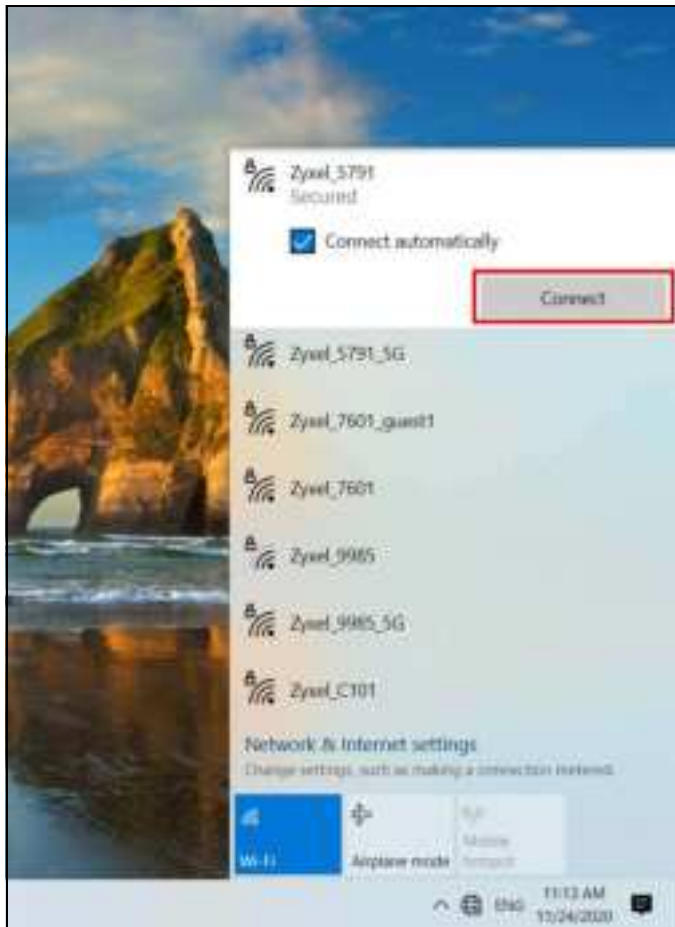
The Zyxel Device sends the WiFi network settings to Windows using WPS. Windows displays "Getting settings from the router".

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

5.3.3 Setting Up a Guest Network

A company wants to create two WiFi networks for different groups of users as shown in the following figure. Each WiFi network has its own SSID and security mode. Both networks are accessible on both 2.4G and 5G WiFi bands.

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

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

	GENERAL	GUEST
2.4/5G SSID	Employee	Guest
Security Level	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK
Pre-Shared Key	ForCompanyOnly	guest123

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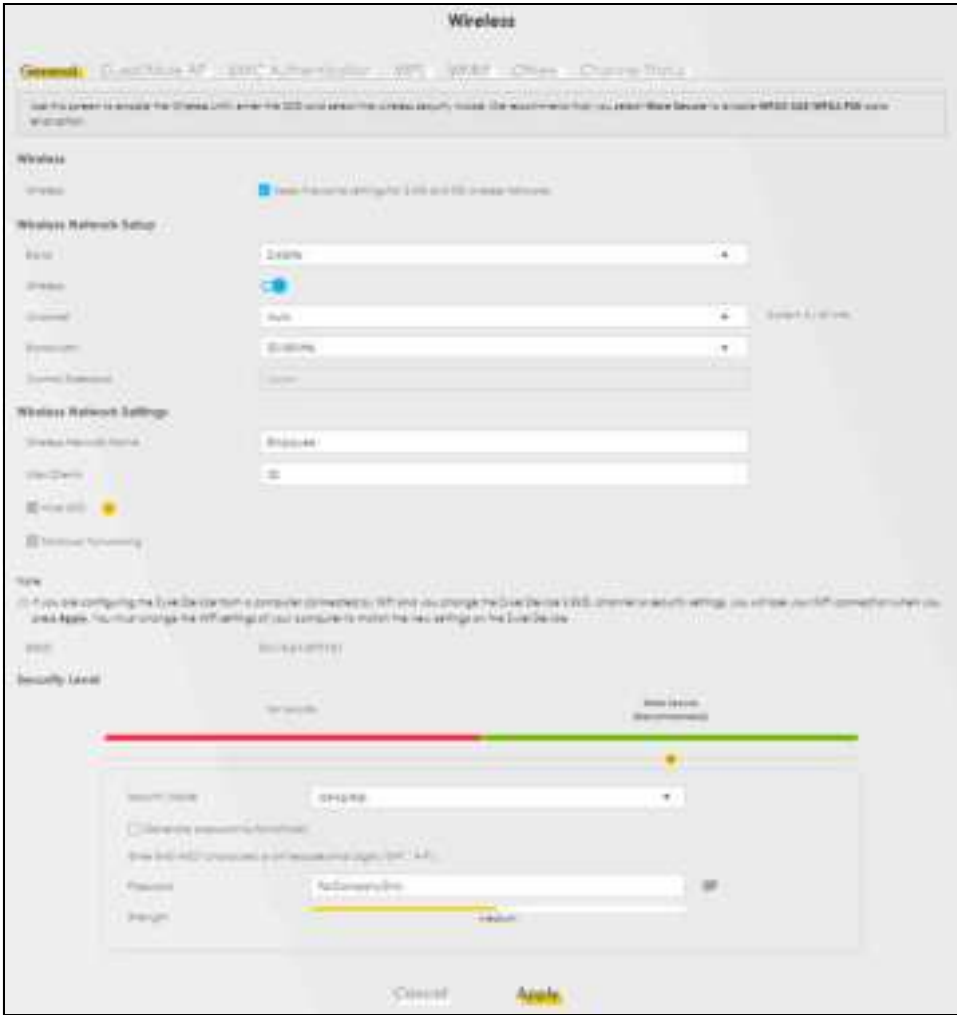
2 Go to the **Network Setting** > **Wireless** > **Guest/More AP** screen. Click the **Modify** icon to configure the second WiFi network group.

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

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

5.3.4 Setting Up Two Guest WiFi Networks on Different WiFi Bands

In this example, a company wants to create two Guest WiFi networks: one for the **Guest** group and the other for the **VIP** group as shown in the following figure. Each network will have its SSID and security mode to access the internet.
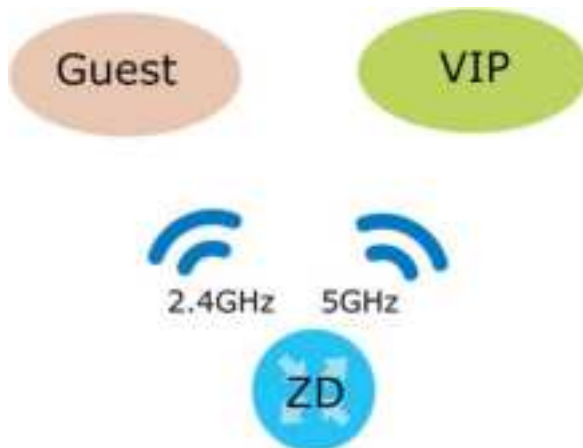
- The **Guest** group will use the 2.4G band.
- The **VIP** group will use the 5G band.

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

Table 7   WiFi Settings Parameters Example

BAND	2.4G	5G
SSID	Guest	VIP
Security Mode	WPA2-PSK	WPA2-PSK
Pre-Shared Key	guest123	123456789

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

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

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

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

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

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

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

5.4 Network Security

5.4.1 Configuring a Firewall Rule

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

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

2   Select **IPv4 Firewall/IPv6 Firewall** to enable the firewall, and then click **Apply**.
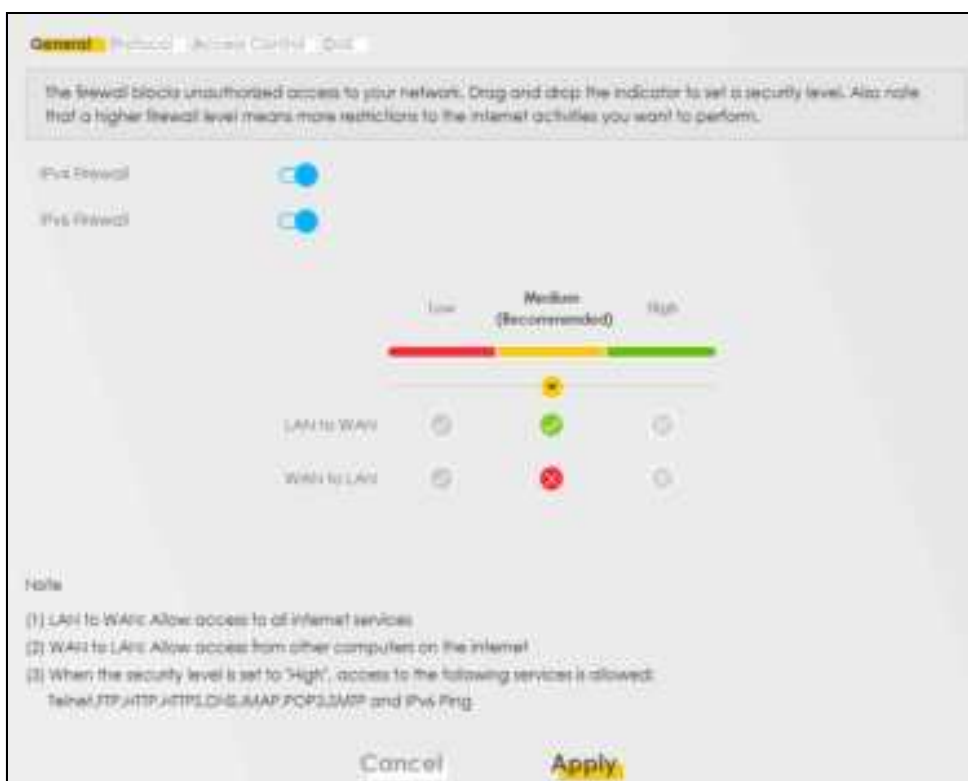
3   Open the **Access Control** screen to create a rule.

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

4a **Filter Name**: Enter a name to identify the firewall rule.

4b **Source IP Address**: Enter the IP address of the computer that initializes traffic for the application or service.

4c **Destination IP Address**: Enter the IP address of the computer to which traffic for the application or service is entering.

4d **Protocol**: Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP** or **ICMPv6**) used to transport the packets.

4e **Policy**: Select whether to (**ACCEPT**, **DROP**, or **REJECT**) the packets.

4f **Direction**: Select the direction (**WAN to LAN**, **LAN to WAN**, **WAN to ROUTER**, or **LAN to ROUTER**) of the traffic to which this rule applies.

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

5.4.2 Parental Control

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

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

5.4.2.1 Configuring Parental Control Schedule

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

• Internet usage scheduling.

Use this feature to:

• Limit the days and times a user can access the Internet.

This example shows you how to block a user from accessing the Internet during time for studying.

5.4.2.2 Configuring a Parental Control Schedule

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

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

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

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

2 Use this screen to add a Parental Control rule.

2a Enter the **Profile Name** given in the above parameter.

2b Click on the switch to enable **Profile Active**.

2c Select a device, and then click **Next** to proceed.
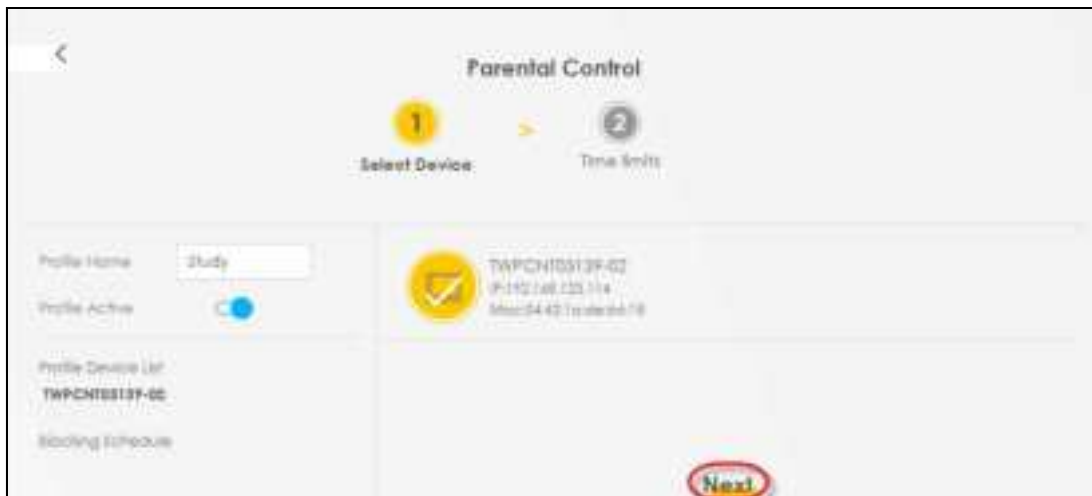
3 Use this screen to edit the Parental Control schedule.

3a Click **Add New Schedule** to add a second schedule.

3b Use the parameter given above to configure the time settings of your schedules.

3c Click **Save** to save the settings.
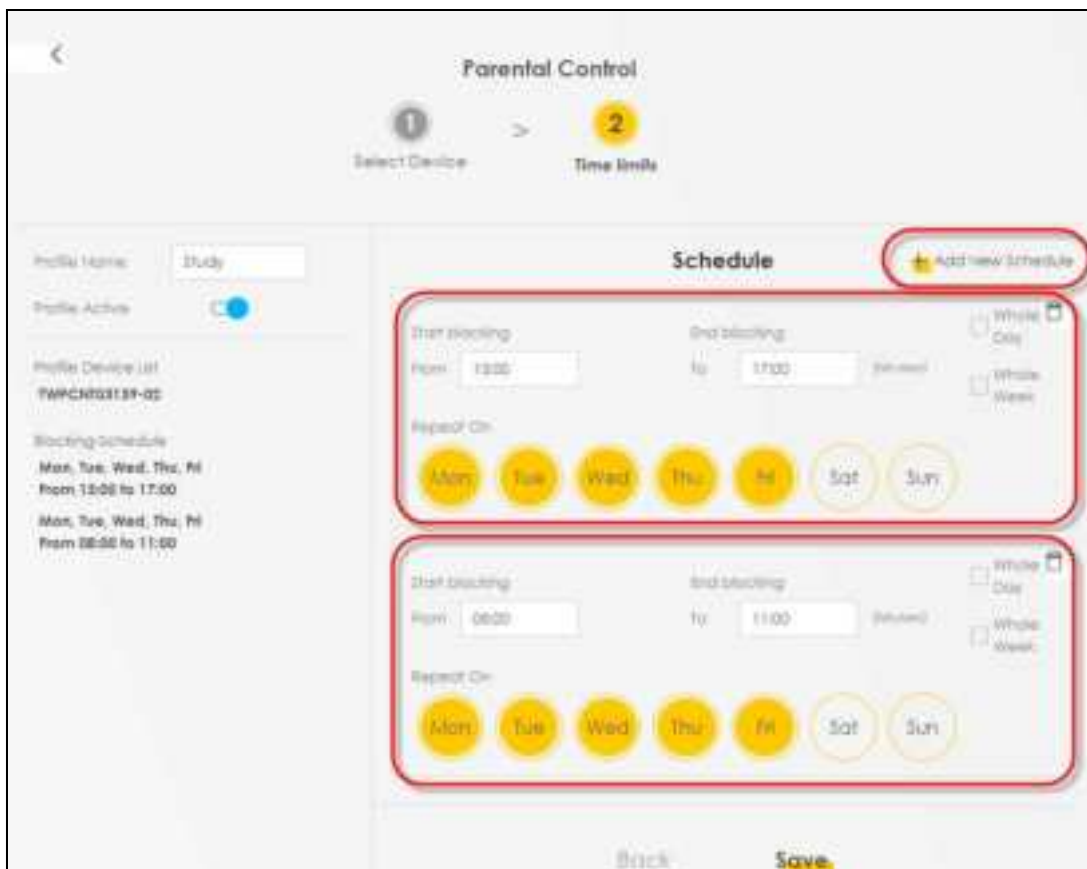
5.4.3 Configuring a MAC Address Filter

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

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

Figure 28 Configure a MAC Address Filter Example
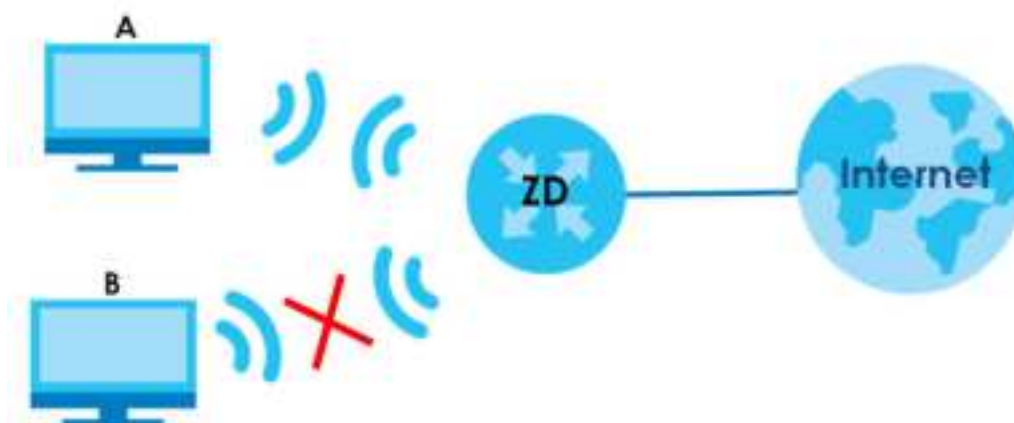
1   Go to the **Security** > **MAC Filter** > **MAC Filter** screen. Under **MAC Address Filter**, select **Enable**.

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

5.5 Device Maintenance

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

5.5.1 Backing up the Device Configuration

Back up a configuration file allows you to return to your previous settings.

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

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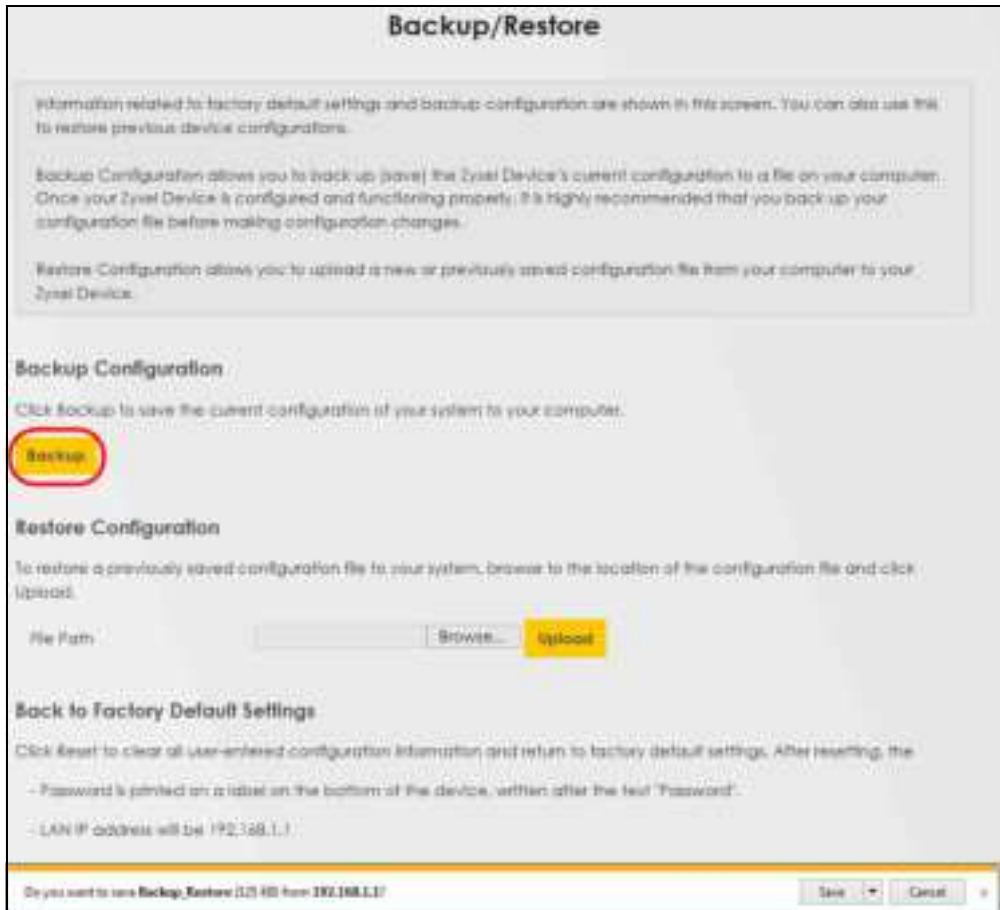
5.5.2 Restoring the Device Configuration

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

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

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

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

CHAPTER 6
Rover App Tutorials

6.1 Overview

This shows you how to use the Rover app to manage the Zyxel Device and its WiFi network.

This table below explains the terms used in this chapter:

Table 8   Tutorial Term Definition

TERM	DEVICE	ROLE
Rover Router	The Zyxel Device in Router Mode	Router
Rover AP	The Zyxel Device in AP Mode	Access Point
WRE6605 AP	The WRE6605 in AP Mode	Access Point
WRE6605 Repeater	The WRE6605 in Repeater Mode	Repeater

6.2 What You Can Do

- Set up your Rover Router with a repeater (the WRE6605 Repeater as an example) using a wireless connection; see Section 6.3.1 on page 61.
- Set up your Rover Router with an access point (the WRE6605AP as an example) using a wired connection; see Section 6.4.1 on page 62.
- Set up your Rover AP with arouter (Rover Router as an example) using a wired connection; see Section 6.4.2 on page 63.
- Use the **Home** screen to see how many devices are connected to your Zyxel Device; see Section 6.6 on page 65.
- Use the **WiFi Settings** screen to configure your general or guest WiFi network; see Section 6.7 on page 65.
- Use the **Devices** screen to view the information of WiFi clients connected to the Zyxel Device; see Section 6.8 on page 71.
- Use the **Parental Control** screen to configure parental control WiFi schedules to block or allow WiFi client device access to the Internet; see Section 6.9 on page 73.
- Use the **Others** screen to run a speed test, view your app version, or log out of the app; see Section 6.10 on page 76.

6.3 WiFi Network Setup

Connect your Rover Router to a repeater (the WRE6605 Repeater as an example).

6.3.1 Connect the Rover Router to the WRE6605 Repeater Using a WiFi Connection

Follow the steps below to set up a Rover Router with a WRE6605 Repeater to extend WiFi range. Connect the Rover Router to the Internet. The Rover Router must be connected to a modem/router using an Ethernet cable.

Table 9   Device Role

DEVICE	TERM	ROLE
Zyxel Device in Router mode	Rover Router	Router
WRE6605 in Repeater mode	WRE6605 Repeater	Repeater

Note: Make sure you reset the Rover Router and WRE6605 to factory defaults before switching to a different mode. Remember to back up your configuration settings before resetting your Zyxel Devices to factory defaults.

1   Turn on your modem/router for Internet access. Connect an Ethernet cable from a modem/router to the WAN port on the Rover Router.

2   Note the power LEDs on the Rover Router when you're done. The power LEDs should be steady blue. Place the Rover AP where you want WiFi coverage.

3   Download the Rover app to your smartphone and log into the WiFi network of the Rover Router. You may need to forget your current WiFi connection on your smartphone.

4   Change the default SSID and WiFi key on the Rover Router for better WiFi security; see Section 6.7.1 on page 66 for more information. After applying changes, you will need to reconnect to the Rover Router again using the new SSID and WiFi key.

5   Use WPS to copy the SSID and WiFi key from the Rover Router to the WRE6605 Repeater. Press the WPS button on the Rover Router for 1.5 to 4 seconds and then press the WPS button on the WRE6605Repeater for 2 seconds within 120 seconds.

6   Use the Rover app and the table below to see if the repeater is too far from the router; see Section 6.8 on page 71 for more information.

Table 10   Link Quality

ICON	CONNECTION TYPE	WIFI STATUS
	Wired	Wired Connection
	Wired	Blocked
	Wireless	Good to Go
	Wireless	Too Close to the Router
	Wireless	Weak WiFi
	Wireless	Blocked

6.4 Wired Network Setups

- Connect your Rover AP to a router (the Rover Router as an example).
- Connect your Rover Router to an access point (the WRE6605 AP as an example).

6.4.1 Connect your Rover AP to the Rover Router Using a Wired Connection

Follow the steps below to set up your Rover AP with arouter (the Rover Routeras an example). Connect the Rover Router to the Internet. The Rover Router must be connected to a modem/router using an Ethernet cable. Then, connect a LAN port on the Rover AP to a LAN port on the Rover Router using another Ethernet cable.

Table 11   Device Role

DEVICE	TERM	ROLE
Zyxel Device in Router mode	Rover Router	Router
Zyxel Device in AP mode	Rover AP	Access Point

Note: Make sure you reset the Rover Router and Rover AP to factory defaults before switching to a different mode. Remember to back up your configuration setting before resetting your devices to factory defaults. See Section 2.2 on page 22 for more information.

1 Turn on your modem/router for Internet access. Connect an Ethernet cable from a modem /router to the WAN port on the Rover Router.

2 Note the power LEDs when you're done. The power LEDs should be steady blue. Place the Rover AP where you want WiFi coverage and connect it to the Rover Router using an Ethernet cable.

3 Download the app to your smartphone and log into the Rover Router's WiFi network using the default label information on the back label. You may need to forget your current WiFi connection on your smartphone.

4   Change the default SSID and WiFi key on the Rover Router for better WiFi security; see Section 6.7.1 on page 66 for more information. After applying changes, you will need to reconnect to Rover Router again using the new SSID and WiFi key.

5   Use WPS to copy the SSID and WiFi key from the Rover Router to the Rover AP. Press the WPS button on the Rover Router for 1.5 to 4 seconds and then press the WPS button on the Rover AP until the LED blinks in purple within 120 seconds.

6   Use the Rover app and the table below to see if the access point is securely connected to the router; see Section 6.8 on page 71 for more information.

Table 12   Link Quality

ICON	CONNECTION TYPE	WIFI STATUS
	Wired	Wired Connection
	Wired	Blocked
	Wireless	Good to Go
	Wireless	Too Close to the Router
	Wireless	Weak WiFi
	Wireless	Blocked

6.4.2 Connect the Rover Router to the WRE6605 AP Using a Wired Connection

Follow the steps below to set up the Rover Router with an access point (the WRE6605AP as an example). Connect the Rover Router to the Internet. The Rover Router must be connected to a modem/router using an Ethernet cable. Then, connect the LAN port on the WRE6605AP to a LAN port on the Rover Router using another Ethernet cable.

Table 13   Device Role

DEVICE	TERM	ROLE
Zyxel Device in Router mode	Rover Router	Router
WRE6605 in AP mode	WRE6605 AP	Access Point

Note: Make sure you reset the Zyxel Device and WRE6605 to factory defaults before switching to a different mode. Remember to back up your configuration setting before resetting your devices to factory defaults. See Section 2.2 on page 22 for more information.

1 Turn on your modem/router for Internet access. Connect an Ethernet cable from a modem/router to the WAN port on the Rover Router.

2 Note the power LEDs when you're done. The power LEDs should be steady blue. Place the WRE6605 AP where you want WiFi coverage and connect it to the Rover Router using an Ethernet cable.

3 Download the Rover app to your smartphone and log into Rover Router's WiFi network using the default label information on the back label. You may need to forget your current WiFi connection on your smartphone.

4 Change the default SSID and WiFi key on the Rover Router for better WiFi security; see Section 6.7.1 on page 66 for more information. After applying changes, you will need to reconnect to the Rover Router again using the new SSID and WiFi key.

5 Use WPS to copy the SSID and WiFi key from the Rover Router to the WRE6605 AP. Press the WPS button on the Rover Router for 1.5 to 4 seconds and then press the WPS button for 2 seconds on the WRE6605 AP within 120 seconds.

6 Use the Rover app and the table below to see if the access point is securely connected to the router; see Section 6.8 on page 71 for more information.

Table 14   Link Quality

ICON	CONNECTION TYPE	WIFI STATUS
	Wired	Wired Connection
	Wired	Blocked
	Wireless	Good to Go
	Wireless	Too Close to the Router
	Wireless	Weak WiFi
	Wireless	Blocked

6.5 Network Management with the Rover App

You can use the Rover app to view WiFi connection status of your device, configure general and guest WiFi settings, add a parental control profile, and run a speed test.

6.6 Home Settings

Tap on the **Home** icon ( ) in the navigation panel. The **Home** screen displays and shows the number of the devices connected to the Zyxel Device.

You can tap **Connected Device** in the **Home** screen to go to the **Devices** screen. See Section 6.8 on page 71 for more device information.
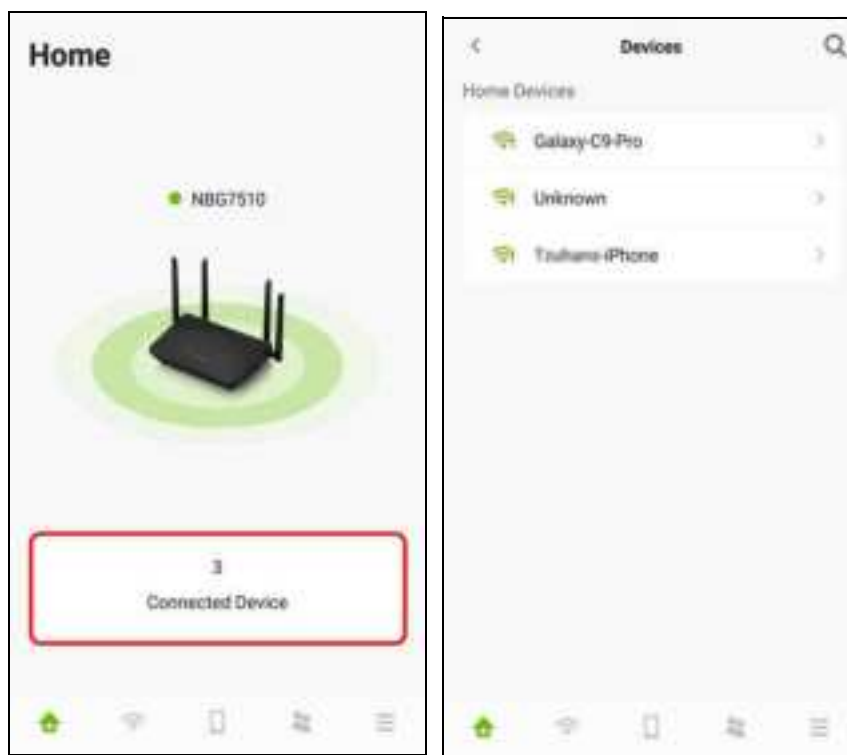
6.7 General WiFi and Guest Settings

Use this screen to configure settings for your main WiFi and guest network.

You can set up a guest WiFi network for your Zyxel Device. Company A wants to create a different WiFi network group for different types of users as shown in the following figure. This group has its own SSID and password.

• Employees in Company A will use a general Company WiFi network group.

• Visiting guests will use the Guest WiFi network group, which has a different SSID and password. Visiting guests cannot connect to the company network using guest WiFi.

Figure 29 General and Guest WiFi Network Example
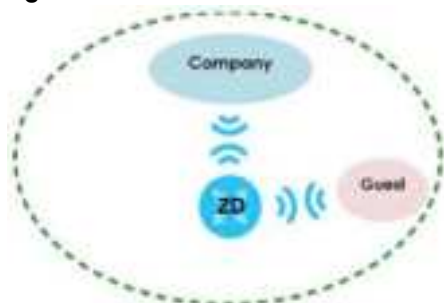
Figure 30 Visiting Guests Blocked from Company Network
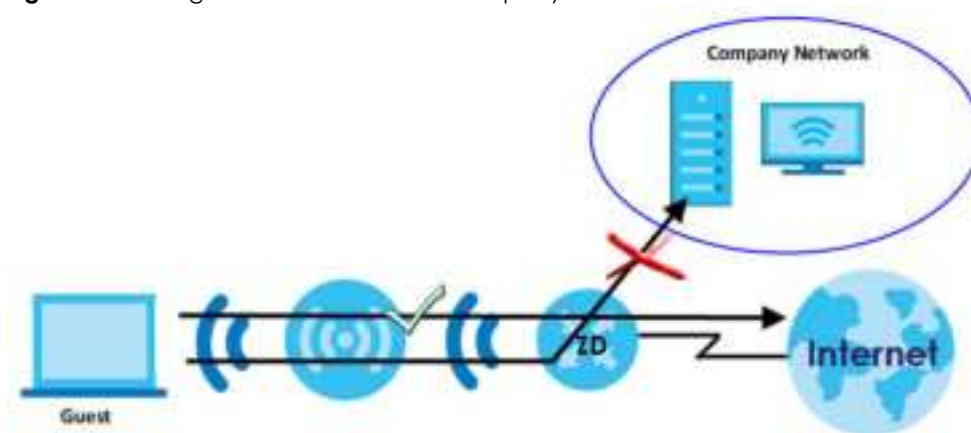
6.7.1 Setting Up General WiFi Settings

Follow the steps below to configure your general WiFi settings. Use the parameters in the table below to create a set of **WiFi Name** and **Password**.

The General WiFi Settings Parameters Example

GENERAL WIFI	
WiFi Name	Company
WiFi Password	company123

1 Tap on the **WiFi** icon ( ) in the navigation panel. The **WiFi > Home** screen displays. Tap on the () icon to edit your general **WiFi Name** and **WiFi Password**. In this example, enter Company as your general **WiFi Name** and company123 as your general **WiFi Password**. Click **Save** to save the changes.
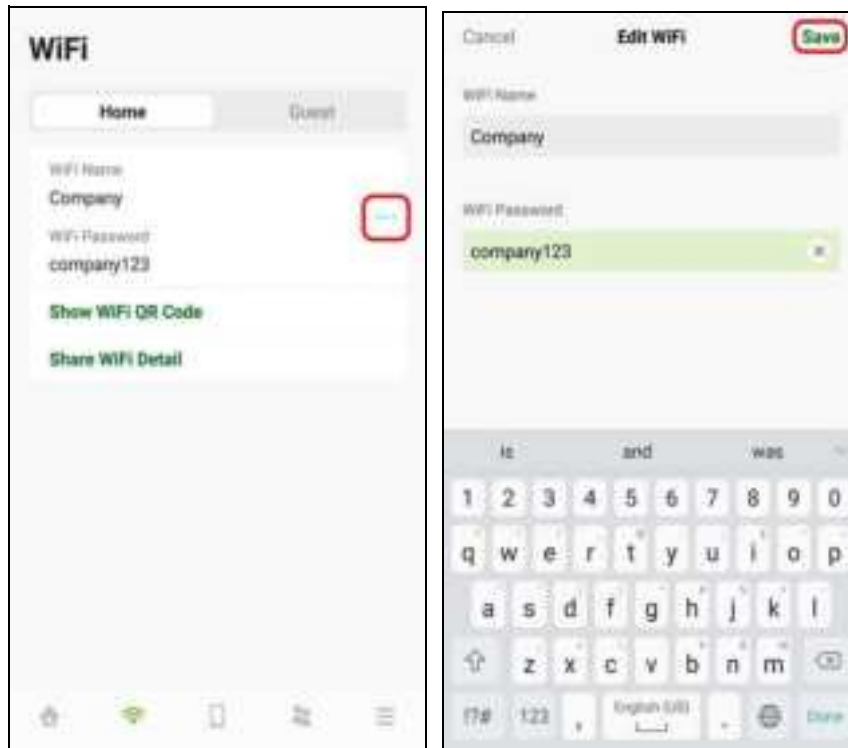
2 You can use the app to create a QR code with your WiFi network name and password. Tap **Show WiFi QR Code** in the **WiFi > Home** screen, the QR code will display as shown.
Use a smartphone to scan the QR code to join the general WiFi network. By printing and placing the QR code somewhere accessible, you can let your friends or guests scan the QR code and join the WiFi network directly without revealing your actual WiFi password.
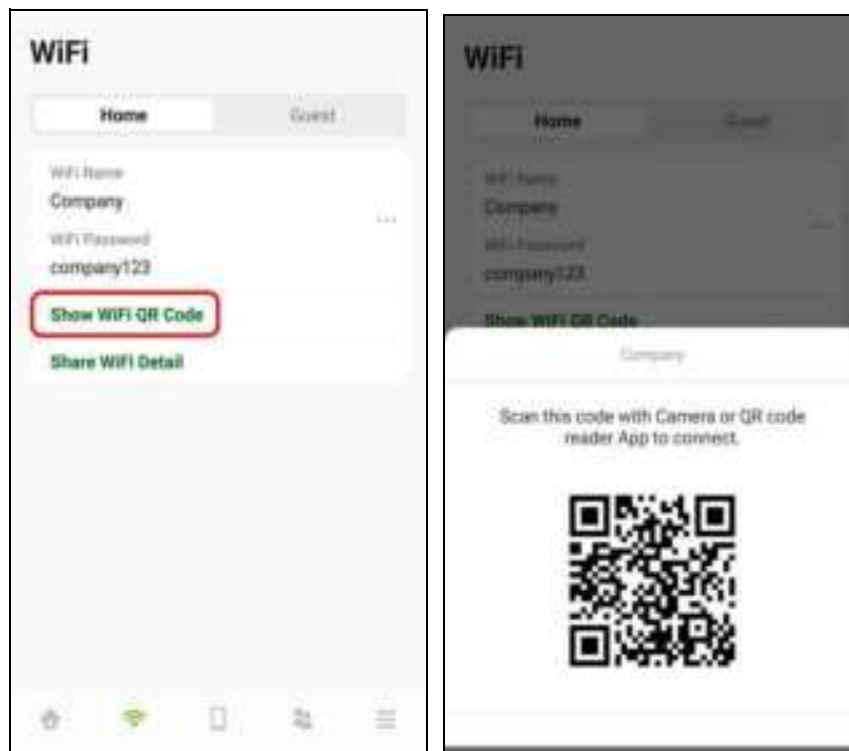
3 Tap **Share WiFi Detail** in the **WiFi > Home** screen. To share your general WiFi name and password with your friends, select a media, such as Gmail or Skype, to send connection info to your friends.
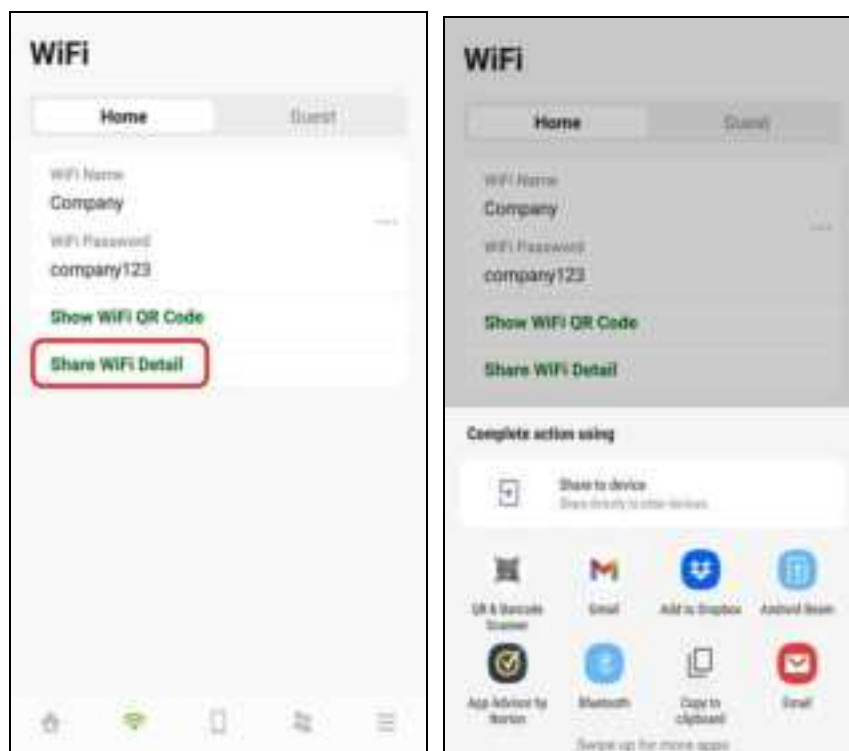
6.7.2 Setting Up Guest WiFi Settings

Follow the steps below to configure your guest WiFi settings. Use the parameters in the table below to create a different set of WiFi name and password.

Table 15   The Guest WiFi Settings Parameters Example

GUEST WIFI	
WiFi Name	Guest
WiFi Password	guest123

1 Tap on the **Guest** tab and then the **WiFi > Guest** screen appears. Click the switch to enable **Guest WiFi**. When the switch goes to the right, **Guest WiFi** is enabled. Tap on the(___) icon to edit the guest **WiFi Name** and **WiFi Password**. In this example, enter Guest as your guest **WiFi Name** and guest123 as your guest **WiFi Password**. Click **Save** to save the changes.
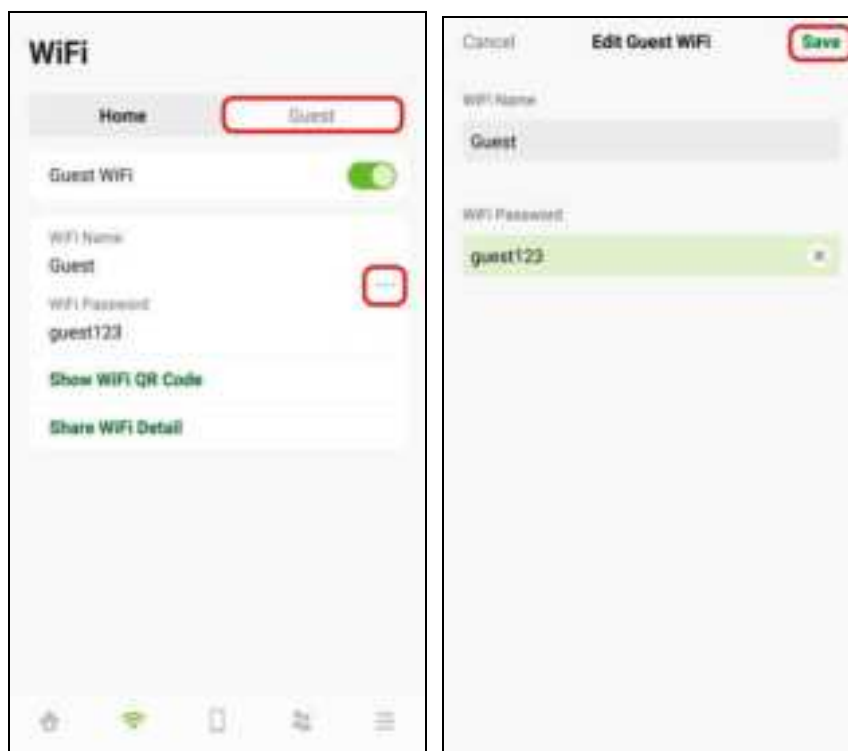
2 You can use the app to create a QR code with your WiFi network name and password. Click **Show WiFi QR Code** in the **WiFi > Guest** screen, the QR code will display as shown.
Use a smartphone to scan the QR code to join the guest WiFi network. By printing and placing the QR code somewhere accessible, you can let your friends or guests scan the QR code and join the WiFi network directly without revealing your actual WiFi password.

3 Tap **Share WiFi Detail** in the **WiFi > Guest** screen. To share your guest WiFi name and password with your friends, select a media, such as Gmail or Skype, to send connection info to your friends.
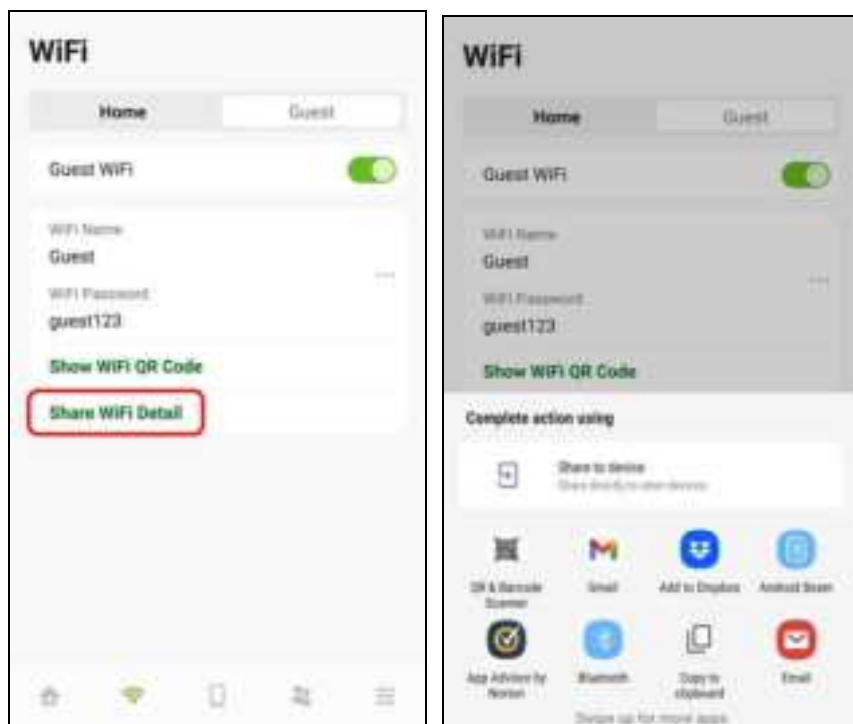
6.8 Device Settings

1 Tap on the **Device** icon ( ) in the navigation panel. Use the **Devices** screen to view the devices connected to the Zyxel Device. Tap on the Arrow icon ( )next the device name you want to see. In this example, tap on the Arrow icon ( )next to the **Galaxy-C9-Pro**. The **Galaxy-C9-Pro** screen displays.
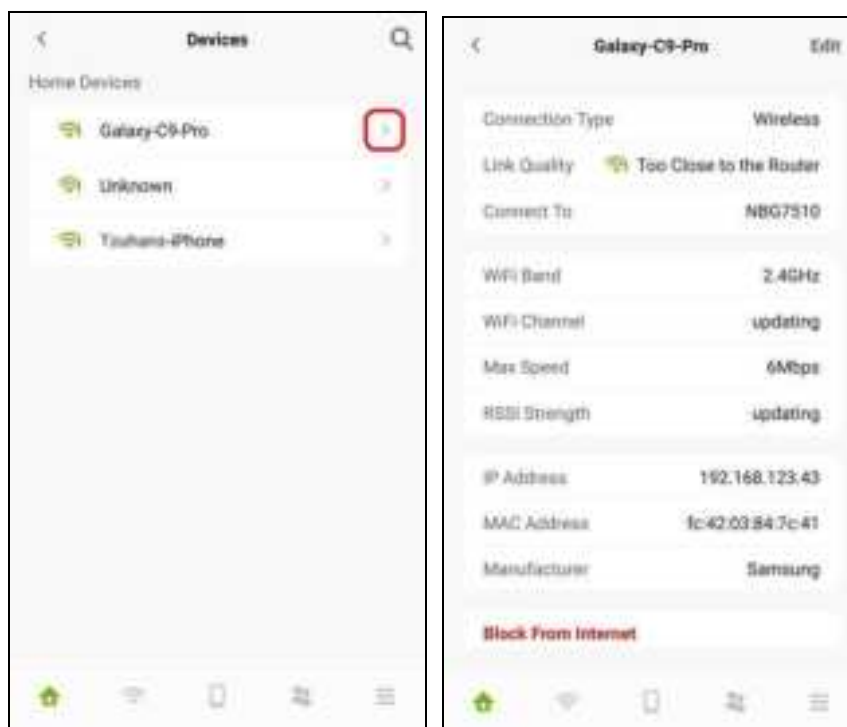
2 After you place your access point or repeater connected to the Zyxel Device, use the **Devices** screen and the table below to check WiFi connection status.

Table 16   Link Quality

ICON	CONNECTION TYPE	WIFI STATUS
	Wired	Wired Connection
	Wired	Blocked
	Wireless	Good to Go
	Wireless	Too Close to the Router
	Wireless	Weak WiFi
	Wireless	Blocked

Table 17   WiFi Connection Status

WIFI CONNECTION STATUS	ACTION
Too Close to the Router	Move the client device farther away from the Zyxel Device
Weak WiFi	Move the client device closer to the Zyxel Device

Move your Galaxy-C9-Pro farther away from your Zyxel Device as the WiFi status is **Too Close to the Router.**

3 To quickly block a client device from accessing your WiFi network, click **Block From Internet**. In this example, click **Block from Internet** in the **Galaxy-C9-Pro** screen. Click **Block** to save the changes.
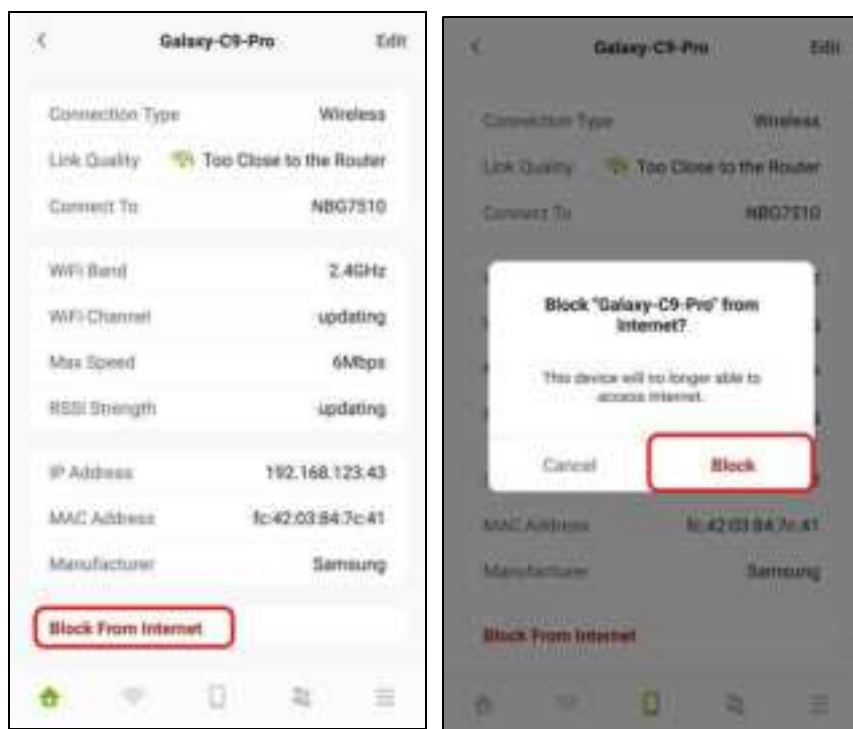
4 Click **Edit** if you want to modify your device name. Enter your device name and then click **Save** to save the changes.
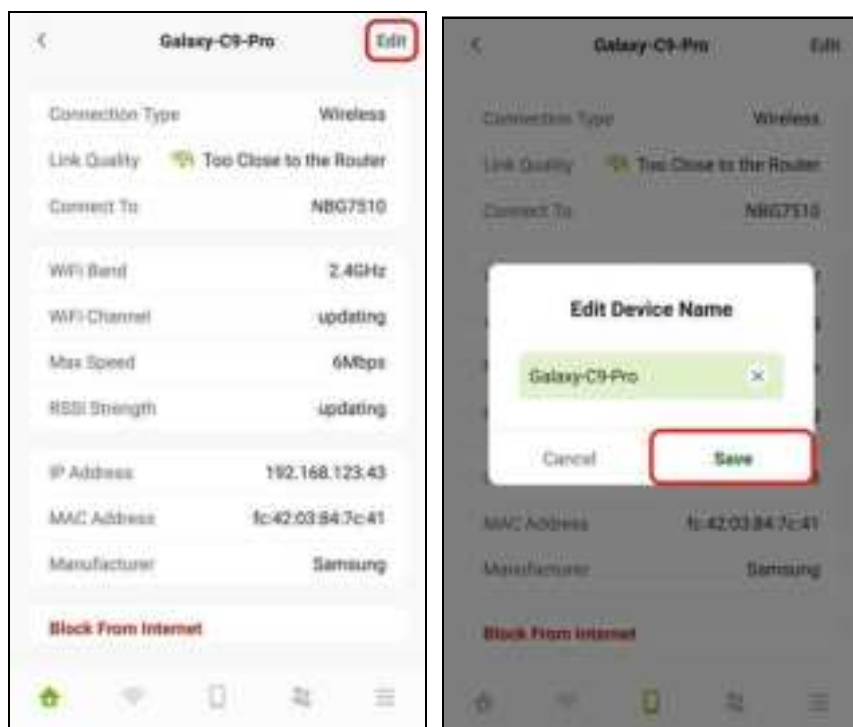
5 To look for a specific device, tap on the Search icon (🔍) in the **Devices** screen. Enter keywords to look for a device. Tap **Cancel** if you want to go back to the previous screen.
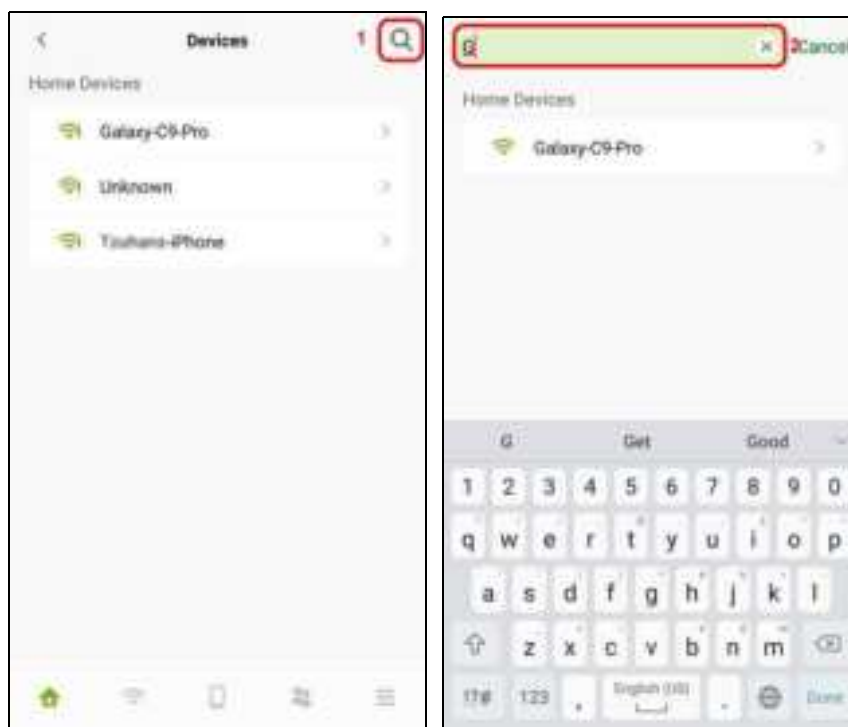
6.9 Parental Control Settings

1 Parental Control allows you to create and repeat a weekly schedule to restrict Internet usage for users. Tap on the **Parental Control** icon (🎮). The **Parental Control** screen displays. Tap **Create Profile** (only appears at the first time) or the Add icon (➕) to create a new parental control profile. The **New Profile** screen appears as shown.

The following example shows you how to create a studying schedule and block users from accessing the Internet for a certain period of time. Use the parameter below to create a profile. Tap **Create Profile** and then the **New Profile** screen appears. Enter Studying Schedule as the profile name.

PROFILE NAME	START TIME	END TIME	REPEAT ON
Studying Schedule	8:00 am	11:00 am	from Monday to Friday
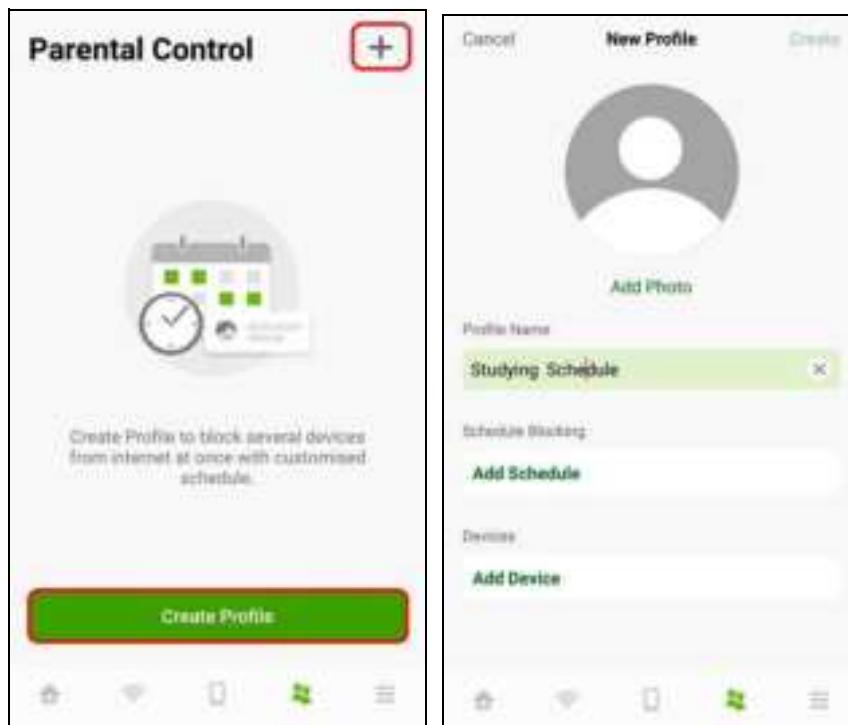
2 Click **Add Schedule** on the **Studying Schedule** screen to create a schedule. The **Add Schedule** screen displays. Select the day(s) of the week to repeat the rule and then enter the **Start Time** and **End Time** in the **Add Schedule** screen. In this example, select from Monday to Friday. Then, enter 8:00 as **Start Time**, and 11:00 as **End Time.**

Click **Add Device** to apply the **Studying Schedule** profile to a device. The **Add Device** screen appears as shown. Select the device you want to add and then click **Add** to save the changes.
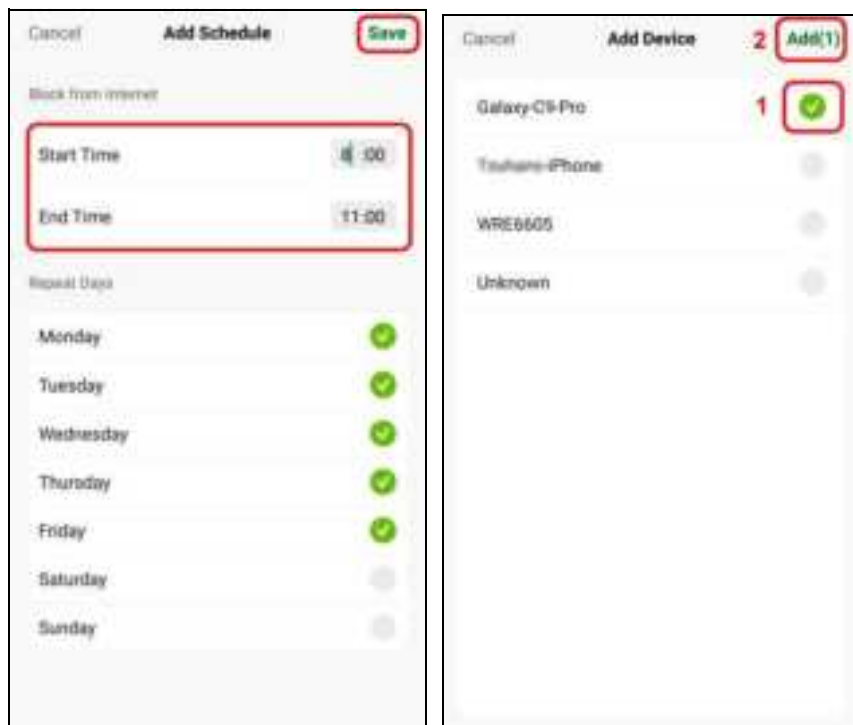
3 Tap on the Arrow icon ( ) next to the profile to go back and continue modifying your profile. In this example, click the Arrow icon ( ) next to Studying Schedule. The **Studying Schedule** screen will appear.
Click **Edit** if you want to modify the name of the profile. Click the switch to enable or disable this WiFi schedule profile. Click the ( ) icon if you want to edit the parental control schedule or apply this profile to another device. Click **Delete Profile** to remove this profile.
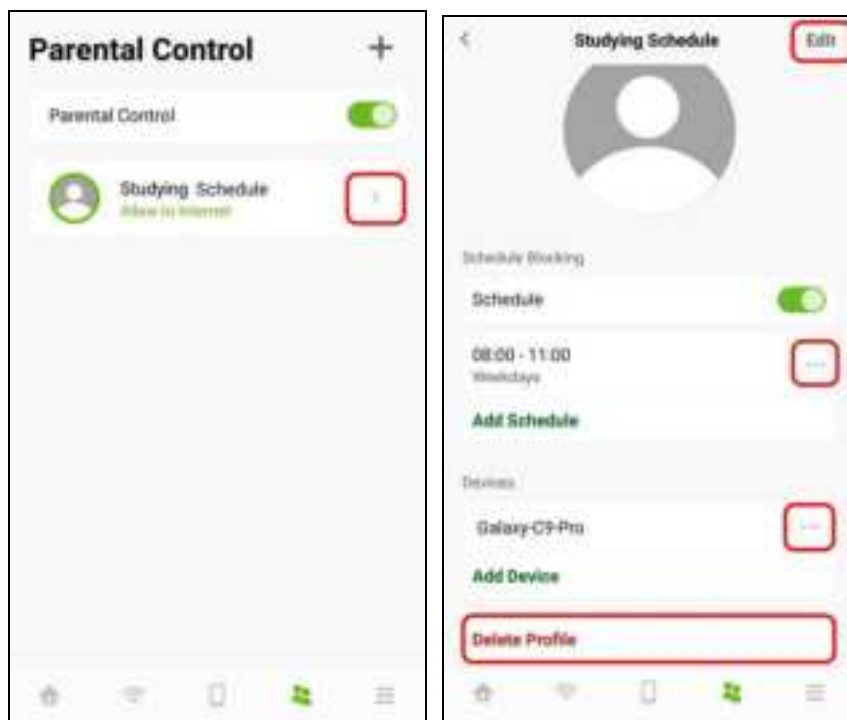
6.10 Others Settings

1 Tap on the **Others** icon ( ) in the navigation panel. The **Others** screen appears. Click Speed Test if you want to conduct a speed test for downstream and upstream data rates. The **Speed Test** screen appears. Click **Start** to the perform a test.
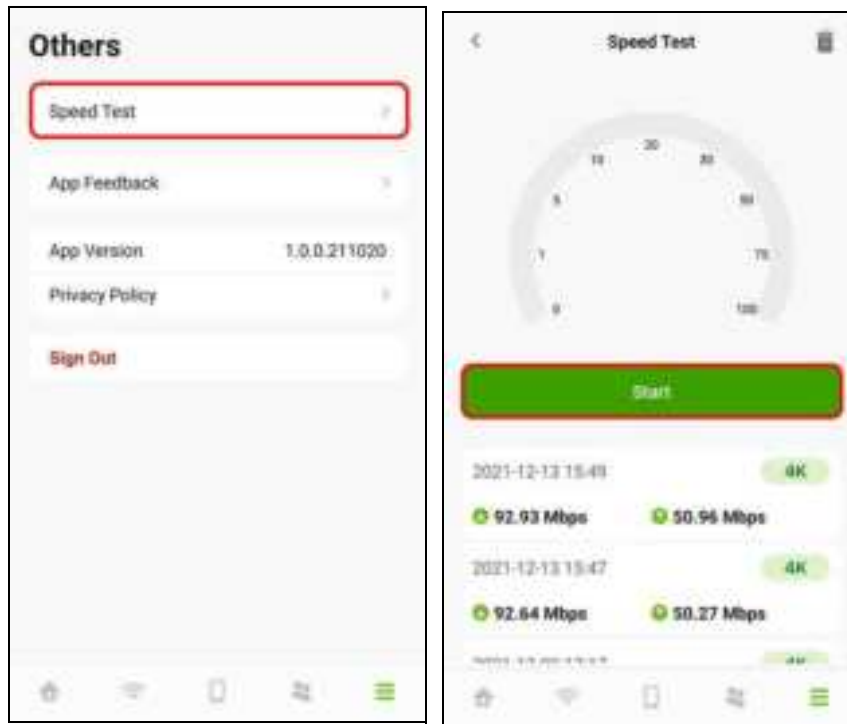
2 Click the Delete icon ( ) if you want to remove all previous test results. Click **Delete** to confirm the changes.
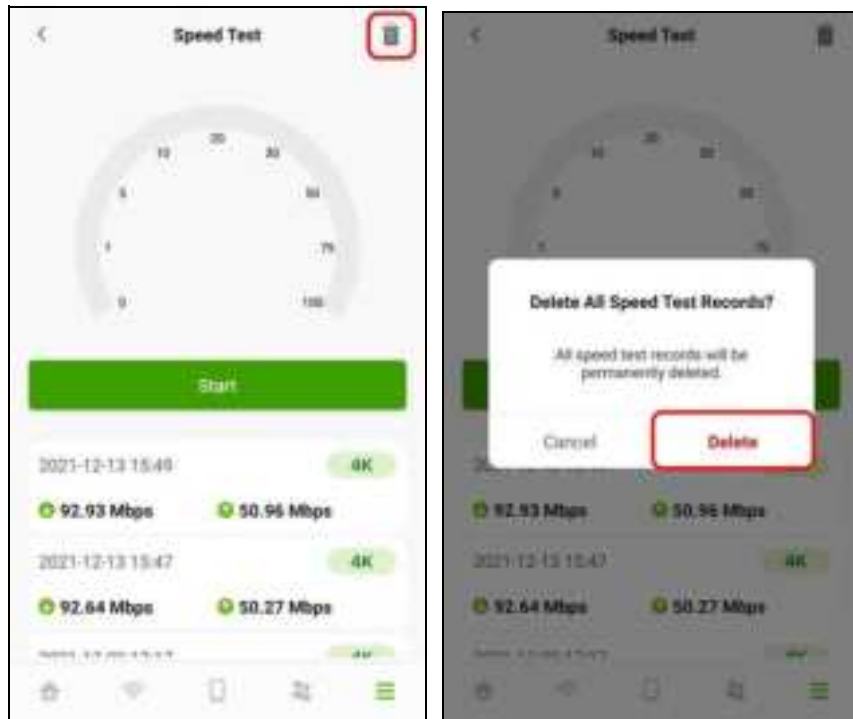
3 You can also use this screen to do the following:

- Give us feedback.
- View the app version.
- View the privacy policy.
- Log out of the app.
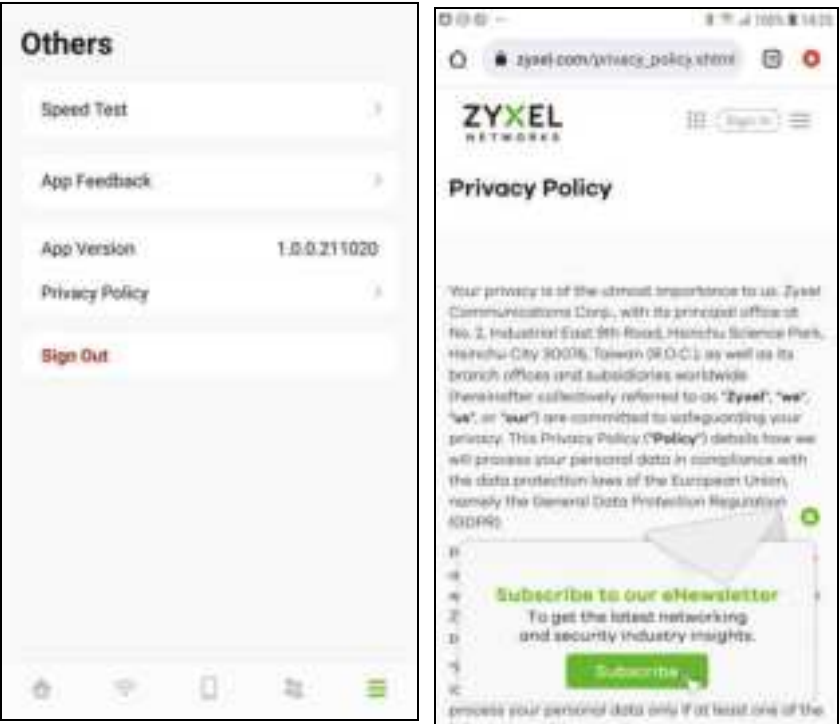
PART II
Technical Reference

CHAPTER 7
Connection Status

7.1 Connection Status Overview

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

7.1.1 Connectivity

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

Figure 31 Connectivity

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

Figure 32 Connectivity: Connected Devices

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.

7.1.2 Icon and Device Name

Select an icon and/or enter a name in the **Device Name** field for a connected device. Click **Save** to

save your changes.

Figure 33   Connectivity: Edit

7.1.3 System Info

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

Figure 34   System Info
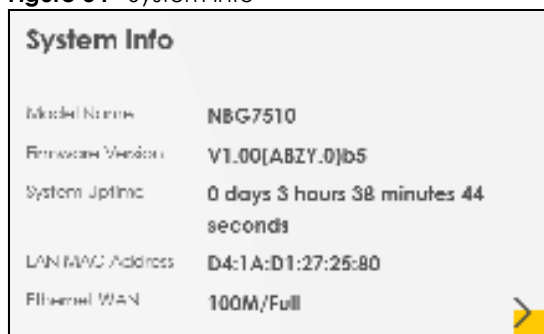
Click the Arrow icon ( ) to view more information on the status of your firewall and interfaces (WAN, LAN, and WLAN).

Figure 35 System Info: Detailed Information
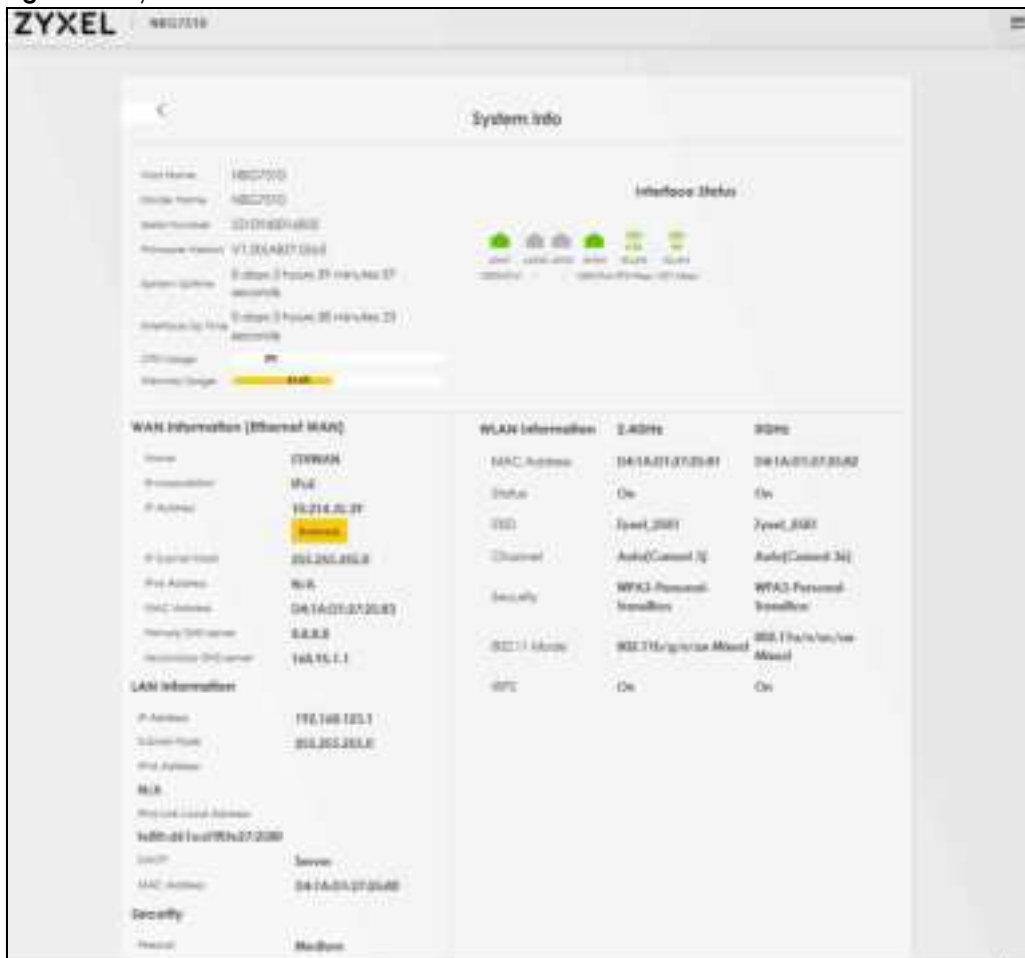
Each field is described in the following table.

Table 18 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the Zyxel Device system name. It is used for identification.
Model Name	This shows the model number of your Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This is the current version of the firmware inside the Zyxel Device.
System Uptime	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (**Maintenance** > **Reboot**), or when you reset it.
Interface Status	
Virtual ports are shown here. You can see the ports in use and their transmission rate.	
WAN Information (These fields display when you have an Ethernet WAN connection.)	
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.

Table 18   System Info: Detailed Information (continued)

LABEL	DESCRIPTION
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
Primary DNSv6 server	This field displays the first DNS server IPv6 address assigned by the ISP.
Secondary DNSv6 server	This field displays the second DNS server IPv6 address assigned by the ISP.
LAN Information	
IP Address	This is the current IP address of the Zyxel Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the Zyxel Device in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the Zyxel Device for the LAN interface. A link-local address is a special type of the IP address that is therefore only valid for communication within the local network segment or broadcast domain of the device. Typically, link-local addresses are used for automatic address configuration and neighbor discovery protocols.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: **Server** – The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** – The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** – The Zyxel Device is not providing any DHCP services to the LAN.
MAC Address	This shows the network adapter MAC (Media Access Control) Address of the LAN interface.
Security	
Firewall	This displays the firewall's current security level (**High**, **Medium**, **Low**, or **Disabled**).
WLAN Information	
MAC Address	This shows the WiFi adapter MAC (Media Access Control) Address of the WiFi interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a WLAN.
Channel	This is the channel number currently used by the WiFi interface.
Security	This displays the type of security mode the WiFi interface is using in the WLAN.
802.11 Mode	This displays the type of 802.11 mode the WiFi interface is using in the WLAN.
WPS	This displays whether WPS is activated on the WiFi interface.

7.1.4 WiFi Settings

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

Figure 36   WiFi Settings
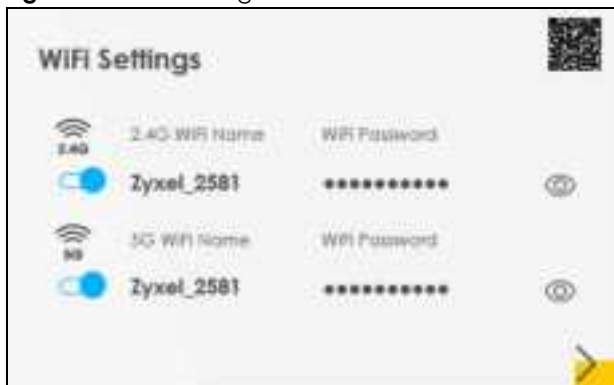
Click the Arrow icon (📝) to configure the SSIDs and/or passwords for your main wireless networks. Click the Eye icon (👁) to display the characters as you enter the WiFi Password.

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

Select **Keep 2.4G and 5G the same** to use the same SSID for 2.4 GHz and 5 GHz bands.

Figure 37   WiFi Settings: Configuration

Each field is described in the following table.

Table 19   WiFi Settings: Configuration

LABEL	DESCRIPTION
Keep 2.4G and 5G the same	Select this and the 2.4 GHz and 5 GHz wireless networks will use the same SSID. If you deselect this, the screen will change. You need to assign different SSIDs for the 2.4 GHz and 5 GHz wireless networks.
2.4 GHz/ 5 GHz WiFi	Click this switch to enable or disable the 2.4G/ 5G WiFi network. When the switch turns blue 🔵, the function is enabled.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed 👁, you will see the password in plain text. Otherwise, it is hidden.

Table 19   WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
Random Password	Select this to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

7.2 Guest WiFi Settings

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

Figure 38   Guest WiFi Settings

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

Figure 39   Guest WiFi Settings: Configuration

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

Figure 40   Guest WiFi Settings: Different SSIDs

Each field is described in the following table.

Table 20   WiFi Settings: Configuration

LABEL	DESCRIPTION
WiFi 2.4G/5G WiFi	Click this switch to enable or disable the 2.4 GHz and/or 5 GHz wireless networks. When the switch goes to the right , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this 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.

7.2.1 LAN

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

Figure 41   LAN
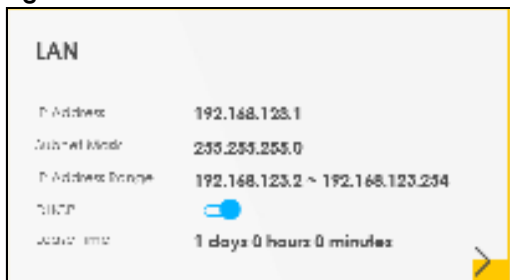
Click the Arrow icon () to configure the LAN IP settings and DHCP setting for your Zyxel Device.

Figure 42   LAN Setup

Each field is described in the following table.

Table 21   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, 192.168.123.1 (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 a DHCP-assigned address is valid, before it expires. When a client connects to the Zyxel Device, DHCP automatically assigns the client an IP addresses from the IP address pool. DHCP leases each addresses for a limited period of time, which means that past addresses are "recycled" and made available for future reassignment to other devices.

Table 21   Status Screen (continued)

LABEL	DESCRIPTION
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
Save	Click **Save** to save your changes.

7.3 The Parental Control Screen

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

Figure 43   Parental Control
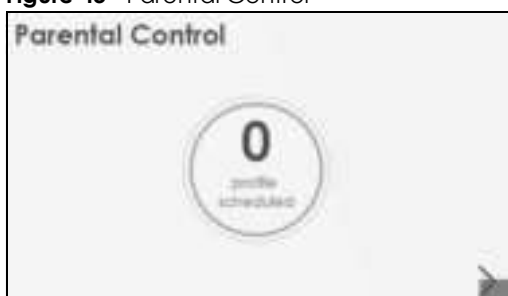
Click the yellow Arrow icon to open the following screen. Use this screen to enable parental control and add more profiles. Add a profile to create restricted access schedules.

Figure 44   Parental Control

Each field is described in the following table.

Table 22   Parental Control: Schedule

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not.
Scheduled Profile	This screen shows all the created profiles.
Add More Profile	Click this to create a new profile.

7.3.1 Create a Parental Control Profile

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

Figure 45 Parental Control: Add More Profile
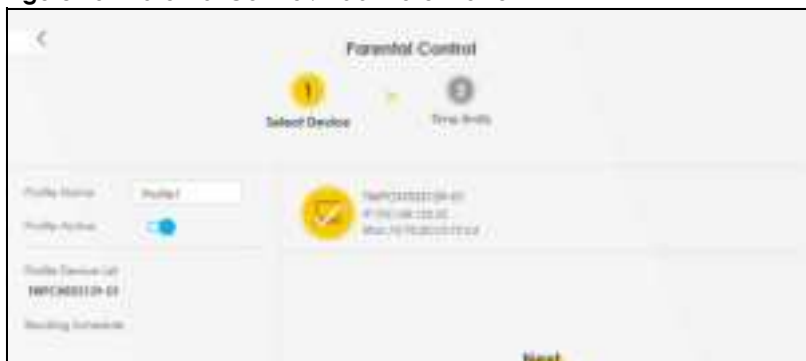
Each field is described in the following table.

Table 23   Parental Control: Add More Profile

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

7.3.2 Define a Schedule

Click **Next** to define time periods and days during which Internet access is blocked on the profile devices.

Figure 46 Parental Control: Schedule

Each field is described in the following table.

Table 24   Parental Control: Schedule

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable Internet access. When the switch goes to the right ![switch], the function is enabled. Otherwise, it is not.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile devices.
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Start/End blocking	Select the time period when Internet access is blocked on the profile devices. Select **All Day** and the scheduler rule will be activated for 24 hours.
Repeat On	Select the days when Internet access is blocked on the profile devices.
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save your changes.

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

Figure 47   Parental Control: Edit_Delete
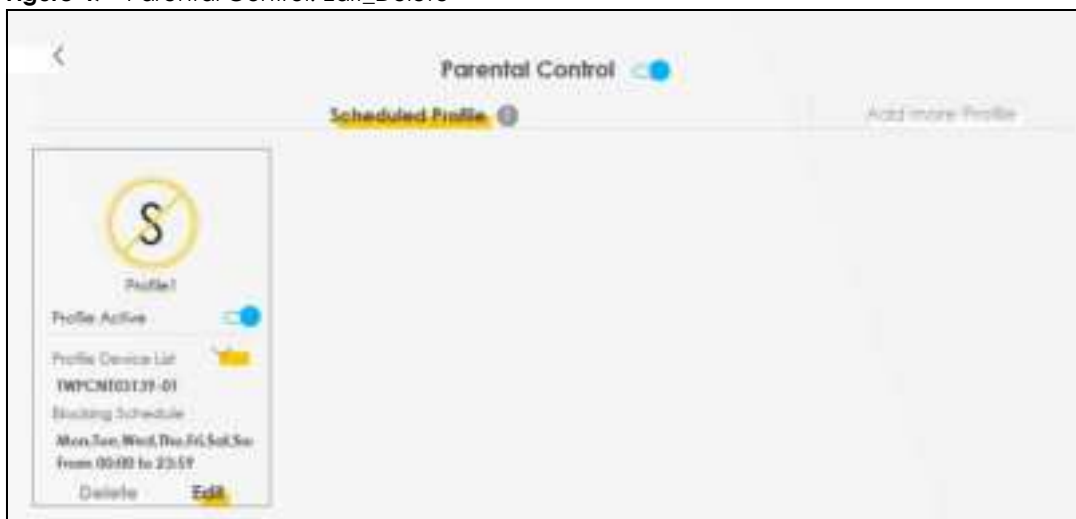
CHAPTER 8
Broadband

8.1 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 48 LAN and WAN
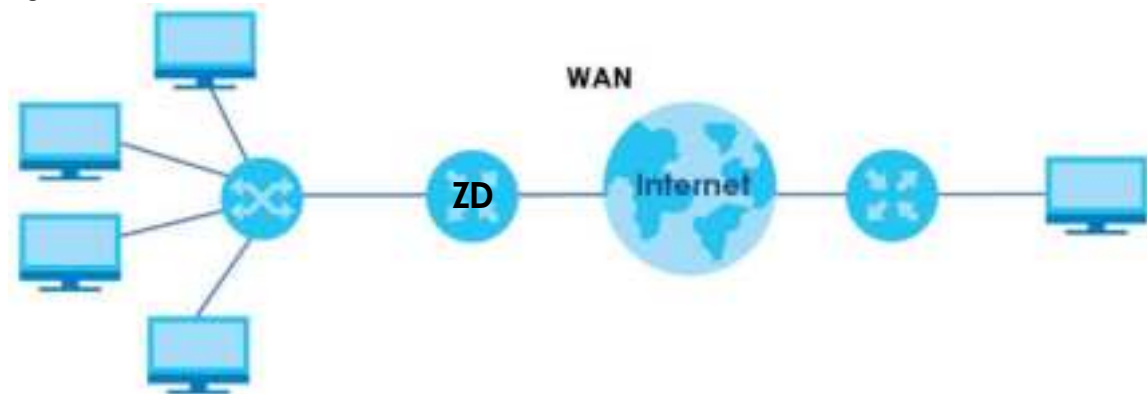
8.1.1 What You Can Do in this Chapter

- Use **Broadband** screens to view, remove or add a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 8.2 on page 94).

Table 25   WAN Setup Overview

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

8.1.2 What You Need to Know

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

WAN IP Address

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

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

IPv6 Introduction

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

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

        2001:db8:1a2b:15::1a2f:0/32

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

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

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the Zyxel Device has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The Zyxel Device generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The Zyxel Device uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 49   IPv6 Rapid Deployment
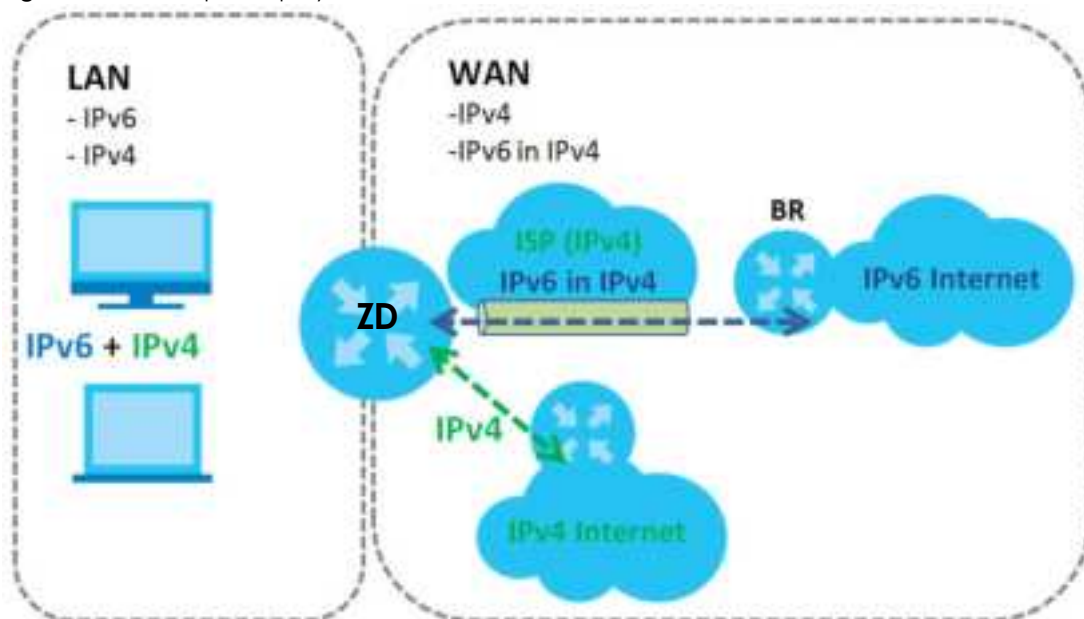
Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the Zyxel Device has an IPv6 WAN address and you set **IPv6/IPv4 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The Zyxel Device tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP's Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The Zyxel Device uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 50 Dual Stack Lite
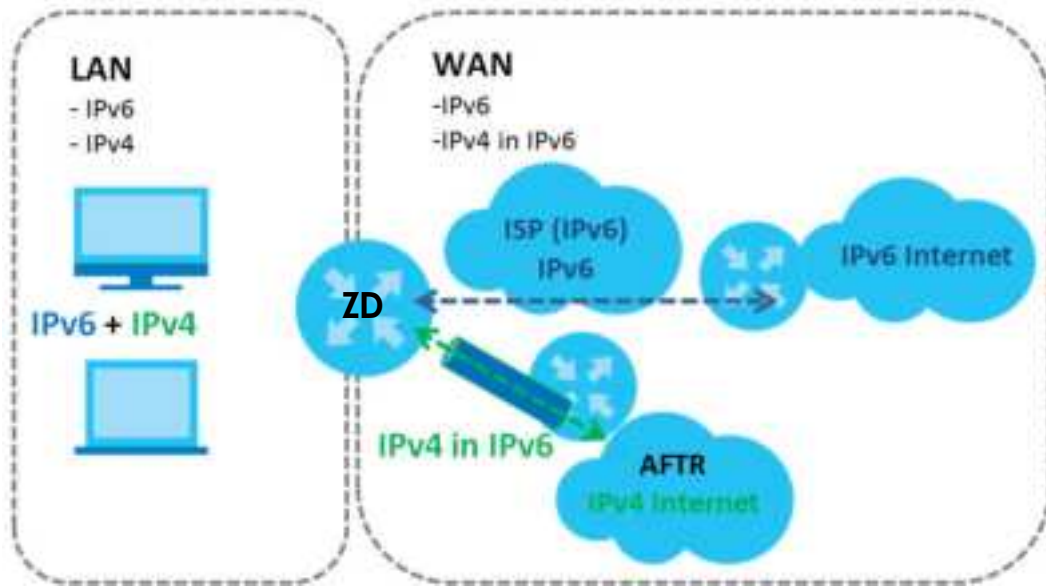
8.1.3 Before You Begin

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

8.2 Broadband Settings

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

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

Figure 51 Network Setting > Broadband

The following table describes the labels in this screen.

Table 26   Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows types of connections the Zyxel Device has.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the Zyxel Device act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the Zyxel Device use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

8.2.1 Add or Edit Internet Connection

Click **Add New WAN Interface** in the **Broadband** screen or the Edit icon next to an existing WAN interface to open the following screen. Use this screen to configure a WAN connection. The screen varies depending on the mode, encapsulation, and IPv6 or IPv4 mode you select.

Routing Mode

Use **Routing** mode if your ISP give you one IP address only and you want multiple computers to share an Internet account.

The following example screen displays when you select the **Routing** mode and **IPoE** encapsulation. The screen varies when you select other encapsulation and IPv6 or IPv4 mode.

Figure 52 Network Setting > Broadband > Add or Edit New WAN Interface (Ethernet)

The following table describes the labels in this screen.

Table 27   Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right 🔵, the function is enabled. Otherwise, it is not.
Name	Specify a descriptive name for this connection. This field is read-only if you are editing the WAN interface.
Type	This field shows the types of available connections. This field is read-only if you are editing the WAN interface.
Mode	Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. When you select **Ethernet**, the choices are **PPPoE** and **IPoE.**

Table 27   Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
IPv4/IPv6 Mode	Select **IPv4 Only** if you want the Zyxel Device to run IPv4 only.
	Select **IPv4 IPv6 DualStack** to allow the Zyxel Device to run IPv4 and IPv6 at the same time.
	Select **IPv6 Only** if you want the Zyxel Device to run IPv6 only.
VLAN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right , the function is enabled. Otherwise, it is not.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.
	Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.
IP Address (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
	This is available only when you set the **Encapsulation** to **IPoE**.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
	This is available only when you set the **Encapsulation** to **IPoE**.
DNS Server (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Obtain DNS Info Automatically	Select **Obtain DNS Info Automatically** if you want the Zyxel Device to use the DNS server addresses assigned by your ISP.
Use Following Static DNS Address	Select **Use Following Static DNS Address** if you want the Zyxel Device to use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Routing Feature (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
NAT	Click this switch to activate or deactivate NAT on this connection. When the switch goes to the right , the function is enabled. Otherwise, it is not.
IGMP Proxy	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group – it is not used to carry user data.
	Click this switch to have the Zyxel Device act as an IGMP proxy on this connection. When the switch goes to the right , the function is enabled. Otherwise, it is not.
	This allows the Zyxel Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Click this switch to have the Zyxel Device use the WAN interface of this connection as the system default gateway. When the switch goes to the right , the function is enabled. Otherwise, it is not.

Table 27   Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Fullcone NAT Enable	Click this switch to enable or disable full cone NAT on this connection. When the switch goes to the right ![switch], the function is enabled. Otherwise, it is not.
	This field is available only when you activate **NAT**.
	In full cone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.
6RD	The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 93 for more information.
	Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network. When the switch goes to the right ![switch], the function is enabled. Otherwise, it is not.
Automatically configured by DHCPC	The **Automatically configured by DHCPC** option is configurable only when you set the method of encapsulation to **IPoE**.
Manually Configured	Select **Manually Configured** if you have the IPv4 address of the relay server. Otherwise, select **Automatically configured by DHCPC** to have the Zyxel Device detect it automatically through DHCP.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1 – 32) for the IPv4 network.
IPv6 Address (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.)	
Obtain an IPv6 Address Automatically	Select **Obtain an IPv6 Address Automatically** if you want to have the Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select **Static IPv6 Address** if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interfaces. The gateway helps forward packets to their destinations.
IPv6 DNS Server (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. Configure the IPv6 DNS server in the following section.)	
Obtain IPv6 DNS Info Automatically	Select **Obtain IPv6 DNS Info Automatically** to have the Zyxel Device get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select **Use Following Static IPv6 DNS Address** to have the Zyxel Device use the IPv6 DNS server addresses you configure manually.
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
IPv6 Routing Feature (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. You can enable IPv6 routing features in the following section.)	
MLD Proxy Enable	Select this check box to have the Zyxel Device act as an MLD proxy on this connection. This allows the Zyxel Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.

Table 27   Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Apply as Default Gateway	Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway.
DS-Lite	This is available only when you select **IPv6 Only** in the **IPv4/IPv6 Mode** field. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 93 for more information. Click this switch to let local computers use IPv4 through an ISP's IPv6 network. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting** > **Broadband** screen or the **Edit** icon next to the connection you want to configure. The following example screen displays when you select **Bridge** mode.

Figure 53   Network Setting > Broadband > Add or Edit New WAN Interface (Ethernet-Bridge Mode)

The following table describes the fields in this screen.

Table 28   Network Setting > Broadband > Add/Edit New WAN Interface (VDSL over PTM or Ethernet-Bridge Mode)

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Name	Enter a service name of the connection.
Type (Ethernet)	Select **Ethernet** as the interface that you want to configure. This field is read-only is you are editing the WAN interface.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right ⬤, the function is enabled. Otherwise, it's not.

Table 28   Network Setting > Broadband > Add/Edit New WAN Interface (VDSL over PTM or Ethernet-Bridge Mode) (continued)

LABEL	DESCRIPTION
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.

Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

8.3 Technical Reference

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

Encapsulation

Be sure to use the encapsulation method required by your ISP. The Zyxel Device can work in bridge mode or routing mode. When the Zyxel Device is in routing mode, it supports the following methods.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However, the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

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

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges – they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and 2 bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

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

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

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

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Zyxel Device can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

    2001:db8:1a2b:15::1a2f:0/32

means that the first 32 bits (`2001:db8`) is the subnet prefix.

CHAPTER 9
Wireless

9.1 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.

9.1.1 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 9.2 on page 104)
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device (Section 9.3 on page 108).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device (Section 9.4 on page 112).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 9.5 on page 113).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 9.6 on page 114).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 9.7 on page 115).
- Use the **Channel Status** screen to scan the number of accessing points and view the results (Section 9.8 on page 118).

9.1.2 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.

WiFi6 / IEEE 802.11ax

WiFi6 is backwards compatible with IEEE 802.11a/b/g/n/ac and is most suitable in areas with a high concentration of users. WiFi6 devices support Target Wakeup Time (TWT) allowing them to automatically power down when they are inactive.

The following table displays the comparison of the different WiFi standards.

Table 29   WiFI Standards Comparison

WIFI STANDARD	MAXIMUM LINK RATE *	BAND	SIMULTANEOUS CONNECTIONS
802.11b	11 Mbps	2.4 GHz	1
802.11a/g	54 Mbps	2.4 GHz and 5 GHz	1
802.11n	600 Mbps	2.4 GHz and 5 GHz	1
802.11ac	6.93 Gbps	5 GHz	4
802.11ax	2.4 Gbps	2.4 GHz	128
	9.61 Gbps	5 GHz and 6 GHz	

    * The maximum link rate is for reference under ideal conditions only.

Finding Out More

See Section 9.9 on page 119 for advanced technical information on WiFi networks.

9.2 Wireless General Settings

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

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

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

Figure 54 Network Setting > Wireless > General
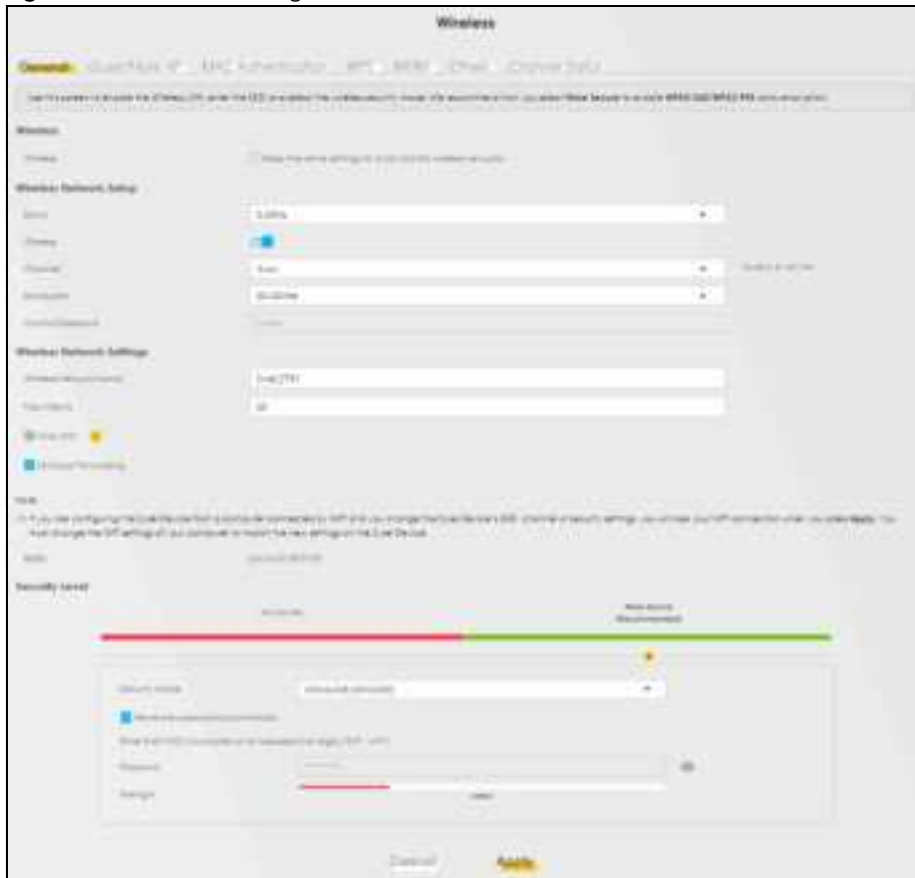
The following table describes the general WiFi labels in this screen.

Table 30 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	Select **Keep the same settings for 2.4G and 5G wireless networks** and the 2.4 GHz and 5 GHz wireless networks will use the same SSID and wireless security settings.
Wireless/WiFi Network Setup	
Band	This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax wireless clients while **5GHz** is used by IEEE 802.11a/n/ac/ax wireless clients.
Wireless/WiFi	Click this switch to enable or disable WiFi in this field. When the switch turns blue 〔🔵〕, the function is enabled. Otherwise, it is not.
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use **Auto** to have the Zyxel Device automatically determine a channel to use.

Table 30   Network Setting > Wireless > General (continued)

LABEL	DESCRIPTION
Bandwidth	Select whether the Zyxel Device uses a wireless channel width of **20MHz**, **40mHz**, **20/40MHz**, **20/40/80MHz** or **20/40/80/160MHz**.
	A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps.
	40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.
	An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher.
	Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
	Because not all devices support 40 MHz and/or 160 MHz channels, select **20/40MHz** or **20/40/80/160MHz** to allow the Zyxel Device to adjust the channel bandwidth automatically.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz** or **20/40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless/WiFi Network Settings	
Wireless/WiFi Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.
	Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
	This check box is grayed out if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen.
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen.
	Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.
	See the following sections for more details about this field.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

9.2.1 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 55   Wireless > General: No Security
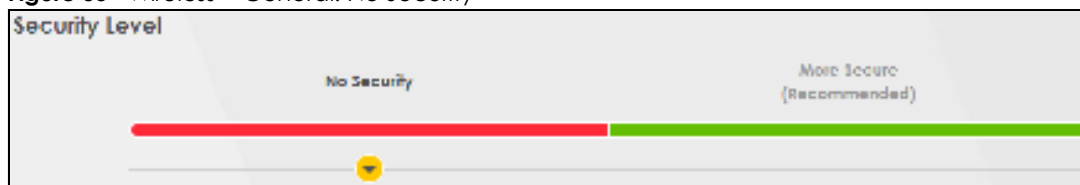
The following table describes the labels in this screen.

Table 31   Wireless > General: No Security

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

9.2.2 More Secure (Recommended)

The WPA-PSK (WiFi Protected Access-Pre-Shared Key) security mode provides both improved data encryption and user authentication over WEP. Using a pre-shared key, both the Zyxel Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be. The WPA3-SAE (Simultaneous Authentication of Equals handshake) security mode protects against dictionary attacks (password guessing attempts). It improves security by requiring a new encryption key every time a WPA3 connection is made. A handshake is the communication between the Zyxel Device and a connecting client at the beginning of a WiFi session.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA3-SAE** from the **Security Mode** list if your wireless client supports it. If you are not sure, select **WPA3-SAE/WPA2-PSK** or **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 56 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

The following table describes the labels in this screen.

Table 32   Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.
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. Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed 👁, you will see the password in plain text. Otherwise, it is hidden.

9.3 Guest/More AP Screen

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

Click **Network Setting > Wireless** > **Guest/More AP**. The following screen displays.

The following table introduces the supported wireless networks.

Table 33   Supported Wireless Networks

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

Figure 57   Network Setting > Wireless > Guest/More AP

The following table describes the labels in this screen.

Table 34   Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active, while a gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the Zyxel Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	This displays if the guest WLAN function has been enabled for this WLAN. If **Home Guest** displays, clients can connect to each other directly. If **External Guest** displays, clients are blocked from connecting to each other directly. **N/A** displays if guest WLAN is disabled.
Modify	Click the **Edit** icon to configure the SSID profile.

9.3.1 The Edit Guest/More AP Screen

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

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

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

Figure 58 Network Setting > Wireless > Guest/More AP > Edit

The following table describes the fields in this screen.

Table 35   Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Click this switch to enable or disable the wireless LAN in this field. When the switch turns blue, the function is enabled; otherwise, it is not.
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
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.

Table 35   Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the **Access Scenario** field.
Access Scenario	If you select **Home Guest**, clients can connect to each other directly.
	If you select **External Guest**, clients are blocked from connecting to each other directly.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled.
SSID Subnet	Click on this switch to **Enable** this function if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients.
	This option cannot be used if the WPS function is enabled in the **Network** > **Wireless** > **WPS** screen or if the **Keep 2.4G and 5G wireless network name the same** check box is selected in **Network** > **Wireless > General**.
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool.
	The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	
Security Mode	Select **More Secure (WPA2-PSK)** to add security on this wireless network. The wireless clients which want to associate to this network must have the same wireless security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen.
	Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.
	See Section 9.2.1 on page 106 for more details about this field.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials.
	If you did not select **Generate password automatically**, 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 of your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it's hidden.
	Click this to show more fields in this section. Click again to hide them.
Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption.
	Select **AES** if your wireless clients can all use AES.
	Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

Table 35   Network Setting > Wireless > Guest/More AP > Edit (continued)

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

9.4 MAC Authentication

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

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

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

Figure 59   Network Setting> Wireless > MAC Authentication
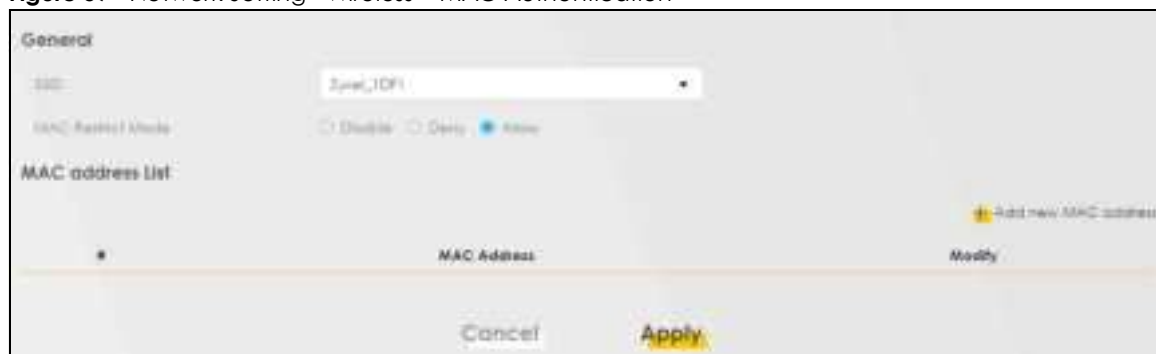
The following table describes the labels in this screen.

Table 36   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	

Table 36   Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
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.

9.5 WPS

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

WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection.Your devices must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your device supports it. See Section 9.9.5.1 on page 122 for more information about WPS.

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection (see Section 9.2.2 on page 107).

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

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

Figure 60 Network Setting > Wireless > WPS

The following table describes the labels in this screen.

Table 37   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 2 minutes of pressing this button.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

9.6 WMM

Use this screen to enable WiFi MultiMedia (**WMM**) and **WMM Automatic Power Save** (**APSD**) in wireless networks for multimedia applications. **WMM** enhances data transmission quality, while **APSD** improves

power management of wireless clients. This allows delay-sensitive applications, such as voice and videos, to run more smoothly.

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

Figure 61 Network Setting > Wireless > WMM
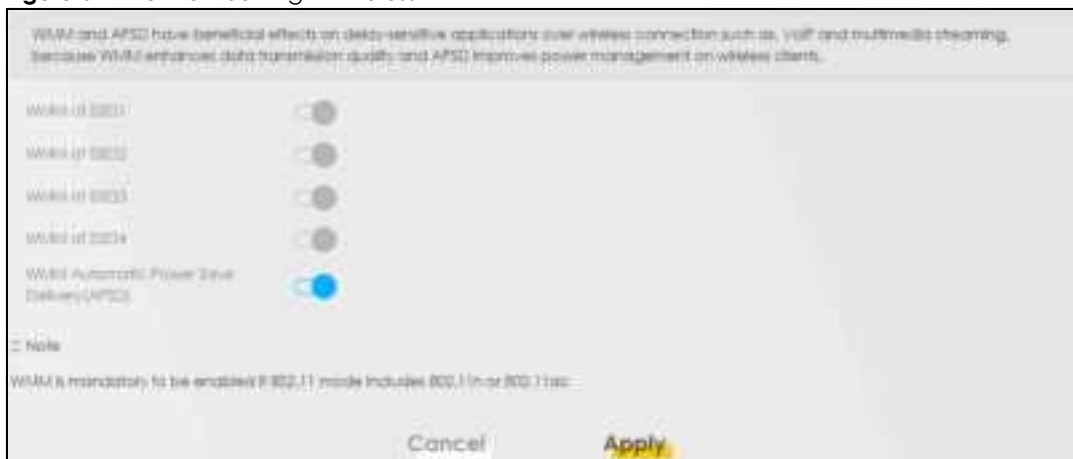
Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

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

The following table describes the labels in this screen.

Table 38   Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM of SSID	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.

9.7 Others Screen

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

See Section 9.9.2 on page 120 for detailed definitions of the terms listed here.

Figure 62 Network Setting > Wireless > Others

The following table describes the labels in this screen.

Table 39   Network Setting > Wireless > Others

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

Table 39   Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Mode	For 2.4 GHz frequency WiFi devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n/ax Mixed** to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. For 5 GHz frequency WiFi devices: • Select **802.11a Only** to allow only IEEE 802.11a compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11ac Only** to allow only IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. • Select **802.11a/n Mixed** to allow either IEEE 802.11a or IEEE 802.11n compliant WiFi 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 WiFi 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 IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac/ax Mixed** to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 9.9.5 on page 122 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Protected Management Frames	WiFi with Protected Management Frames (PMF) provides protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging. Select **Capable** if the WiFi client supports PMF, then the management frames will be encrypted. Select **Required** to force the WiFi client to support PMF; otherwise the authentication cannot be performed by the Zyxel Device. Otherwise, select **Disabled**.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

9.8 Channel Status

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

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

Note: The blue value is the AP count. It's the number of access points (AP) in the wireless LAN channel.

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

Figure 63   Network Setting > Wireless > Channel Status

9.9 Technical Reference

This section discusses wireless LANs in depth.

9.9.1 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 64   Example of a WiFi Network
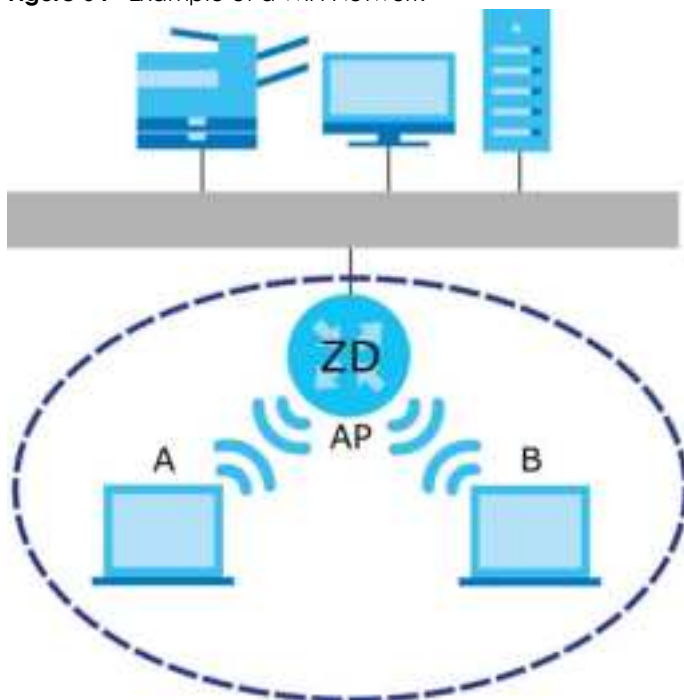
The WiFi network is the part in the blue circle. In this WiFi network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

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.

9.9.2 Additional Wireless Terms

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

Table 40   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.

9.9.3 WiFi Security Overview

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

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

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

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

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

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

9.9.3.1 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.

9.9.3.2 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.

9.9.3.3 Encryption

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

---

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.

The types of encryption you can choose depend on the type of authentication. (See Section 9.9.3.3 on page 121 for information about this.)

Table 41   Types of Encryption for Each Type of Authentication

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

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

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

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

9.9.4 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.

9.9.5 WiFi Protected Setup (WPS)

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

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

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

9.9.5.1 Push Button Configuration

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

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

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

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

2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the Zyxel Device, see Section 9.5 on page 113).

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 5 seconds.

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

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

9.9.5.2 How WPS Works

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

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

Figure 65   How WPS Works
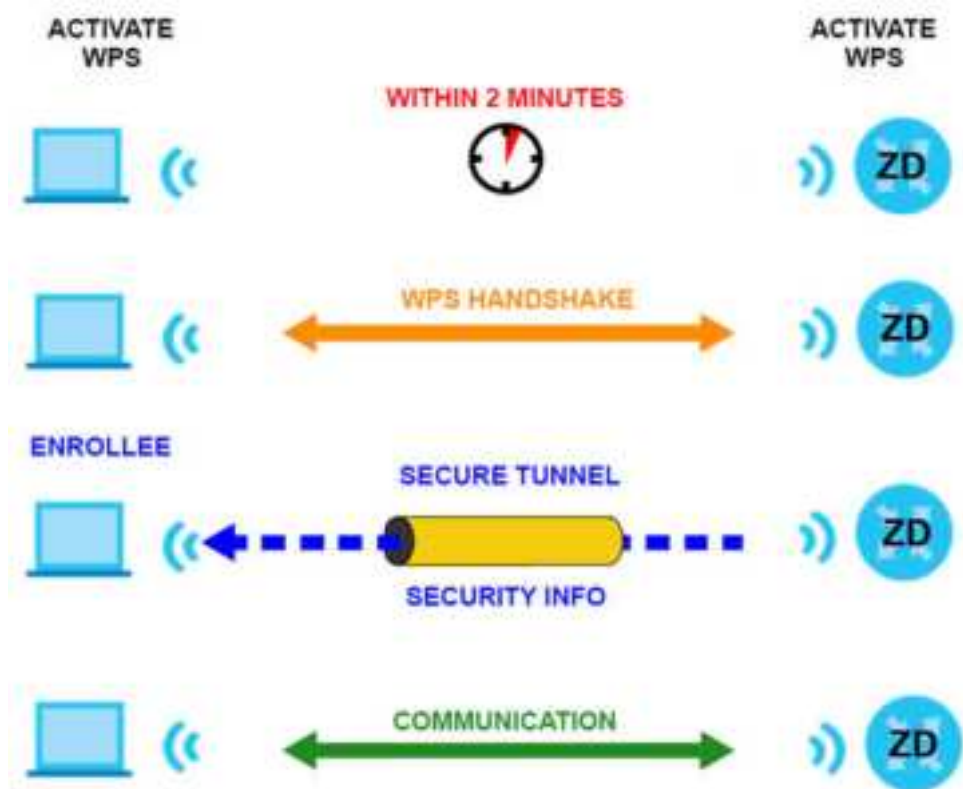
The roles of registrar and enrollee last only as long as the WPS setup process is active (2 minutes). The next time you use WPS, a different device can be the registrar if necessary.

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

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

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

9.9.5.3 Example WPS Network Setup

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

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

Figure 66 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 67 WPS: Example Network Step 2
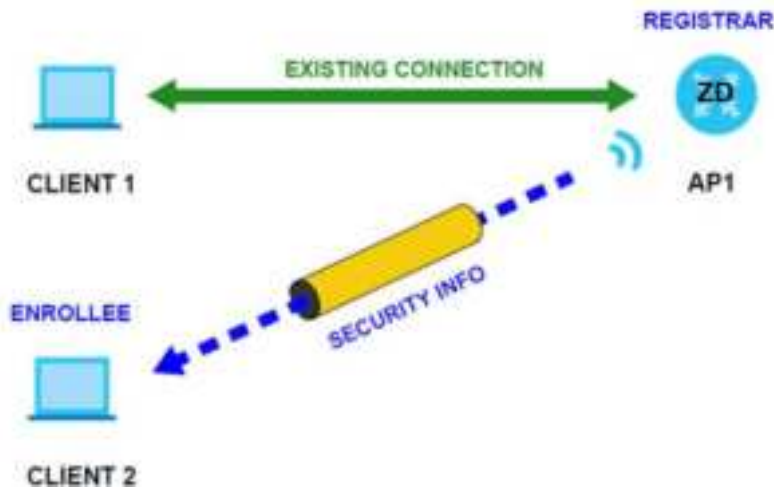
In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 68 WPS: Example Network Step 3
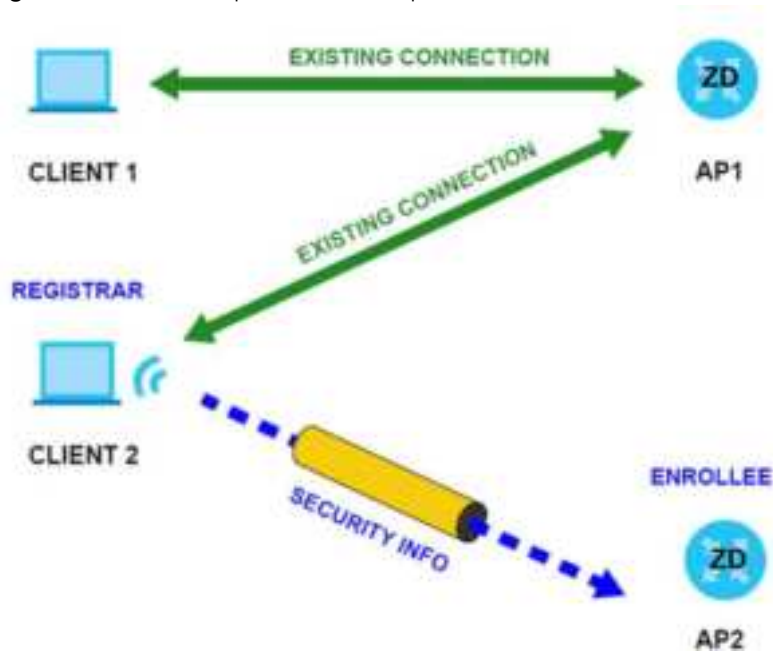
9.9.5.4 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

CHAPTER 10
Home Networking

10.1 Overview

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

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

Figure 69   Home Networking Example

10.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 10.2 on page 129).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 10.3 on page 133).
- Use the **UPnP** screen to enable UPnP (Section 10.4 on page 135).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 10.5 on page 136).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. (Section 10.6 on page 138).
- Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. (Section 10.7 on page 139).

10.1.2 What You Need To Know

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

10.1.2.1 About LAN

IP Address

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

Subnet Mask

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

DHCP

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

DNS

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

RADVD (Router Advertisement Daemon)

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

10.1.2.2 About UPnP

How do I know if I am using UPnP?

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

NAT Traversal

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

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

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

Cautions with UPnP

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

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

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

UPnP and Zyxel

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

See Section on page 142 for examples on installing and using UPnP.

10.1.3 Before You Begin

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

10.2 LAN Setup

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

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices. Click **Network Setting** > **Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

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

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

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

Figure 70 Network Setting > Home Networking > LAN Setup

The following table describes the fields in this screen.

Table 42   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, 192.168.123.1 (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	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.
Days/Hours/ Minutes	DHCP server leases an address to a new 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	

Table 42   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
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.
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>
EUI64	Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format.
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.
LAN Global Identifier Type	Select **EUI64** to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select **Manual** to manually enter an interface ID for the LAN interface's global IPv6 address.
EUI64	Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address.
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Prefix Setup	Select **Delegate prefix from WAN** to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select **Static** to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: **Stateless**: The Zyxel Device uses IPv6 stateless auto-configuration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. **Stateful**: The Zyxel Device uses IPv6 stateful auto-configuration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: **From 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	This shows the status of the DHCPv6. **DHCP Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.

Table 42   Network Setting > Home Networking > LAN Setup (continued)

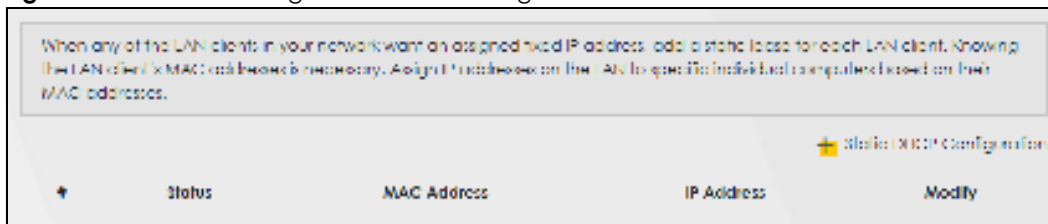| LABEL	DESCRIPTION
IPv6 DNS Values	
IPv6 DNS Server 1 – 3	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **User Defined** – Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6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

10.3 Static DHCP

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

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

10.3.1 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 71   Network Setting > Home Networking > Static DHCP

The following table describes the labels in this screen.

Table 43   Network Setting > Home Networking > Static DHCP

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

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

Figure 72   Static DHCP: Static DHCP Configuration

The following table describes the labels in this screen.

Table 44   Static DHCP: Static DHCP Configuration

LABEL	DESCRIPTION
Active	Select **Enable** to activate static DHCP in your Zyxel Device.
Group Name	The **Group Name** is normally **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.

10.4 UPnP

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

See Section on page 142 for more information on UPnP.

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

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

Figure 73 Network Setting > Home Networking > UPnP

The following table describes the labels in this screen.

Table 45   Network Settings > Home Networking > UPnP

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

10.5 LAN Additional Subnet

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

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Zyxel Device supports multiple logical LAN interfaces through its physical Ethernet

interface with the Zyxel Device itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

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

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

Figure 74   Network Setting > Home Networking > Additional Subnet

The following table describes the labels in this screen.

Table 46   Network Setting > Home Networking > Additional Subnet

| LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings.
Active	Click this switch to configure a LAN network for the Zyxel Device. When the switch goes to the right ⬤, the following fields will be configurable. Otherwise, they are not.
IPv4 Address	Enter the IP address of your Zyxel Device in dotted decimal notation.

Table 46   Network Setting > Home Networking > Additional Subnet (continued)

LABEL	DESCRIPTION
Subnet Mask	Your Zyxel Device will automatically calculate the subnet mask based on the IPv4 address that you assign. Unless you are implementing subnetting, use this value computed by the Zyxel Device.
Public LAN	
Active	Click this switch to enable or disable the Public LAN feature. When the switch goes to the right, the function is enabled. Otherwise, it is not. Your ISP must support Public LAN and static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.
Offer Public IP by DHCP	Click this switch to enable or disable the Zyxel Device to provide public IP addresses by DHCP server. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Enable ARP Proxy	Click this switch to enable or disable the ARP (Address Resolution Protocol) proxy. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

10.6 Wake on LAN

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

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

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

Figure 75 Network Setting > Home Networking > Wake on LAN

The following table describes the labels in this screen.

Table 47   Network Setting > Home Networking > Wake on LAN

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

10.7 TFTP Server Name

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

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

Figure 76   Network Setting > Home Networking > TFTP Server Name

The following table describes the labels in this screen.

Table 48   Network Setting > Home Networking > TFTP Server Name

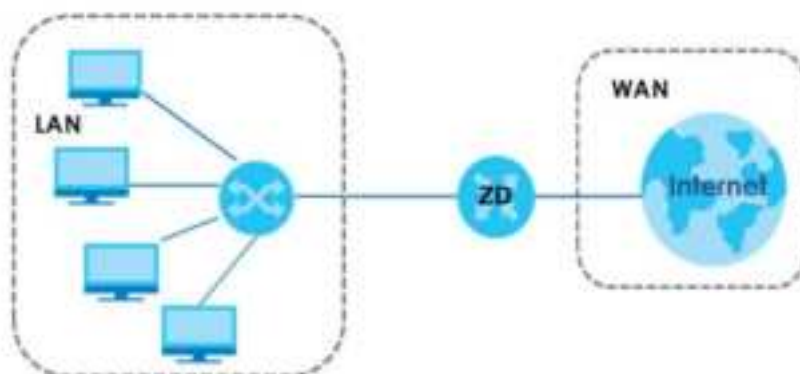| LABEL	DESCRIPTION
TFTP Server Name	Enter the IP address or the host name of a single TFTP server.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

10.8 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 77   LAN and WAN IP Addresses

10.8.1 DHCP Setup

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

IP Pool Setup

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

10.8.2 DNS Server Addresses

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

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

• The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.

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

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

10.8.3 LAN TCP/IP

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

IP Address and Subnet Mask

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

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

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

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

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

Private IP Addresses

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

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

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

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

# 10.9 Turn on UPnP in Windows 10 Example

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

Make sure the computer is connected to the LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.
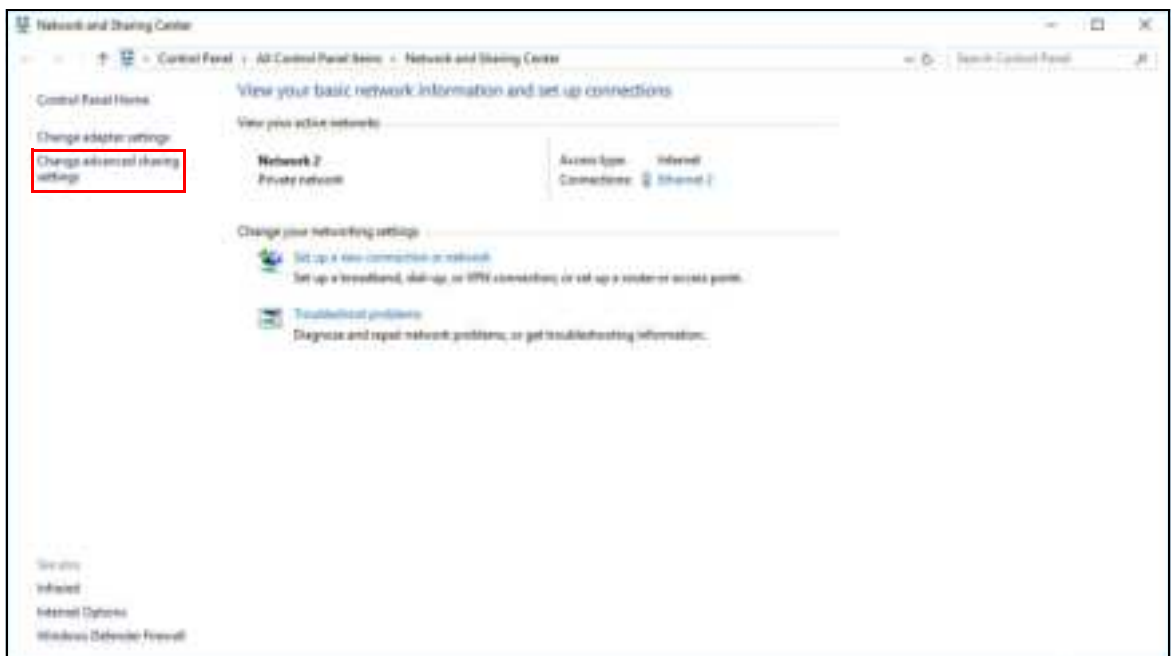
**1**   Click the start icon, **Settings** and then **Network & Internet**.
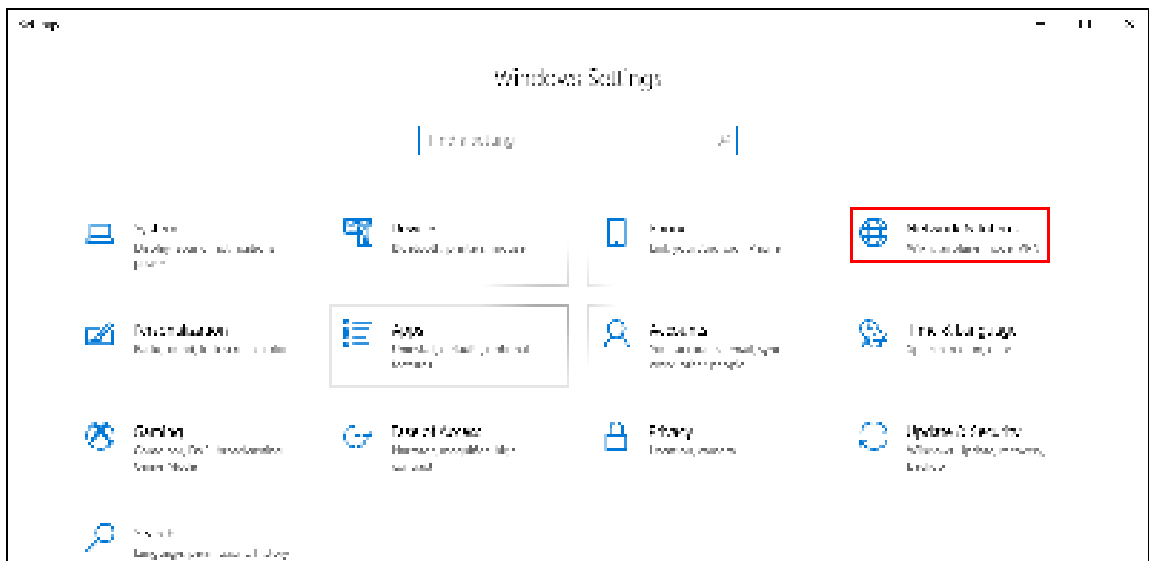
2   Click **Network and Sharing Center**.
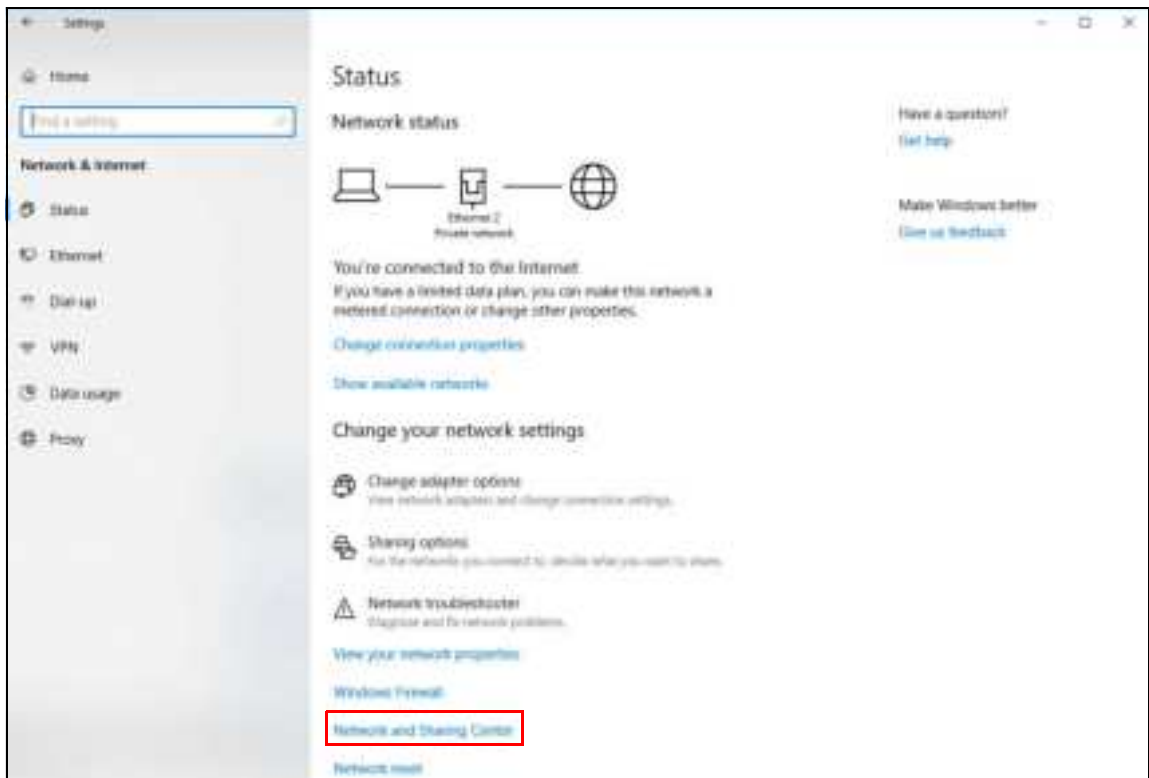
3 Click **Change advanced sharing settings**.

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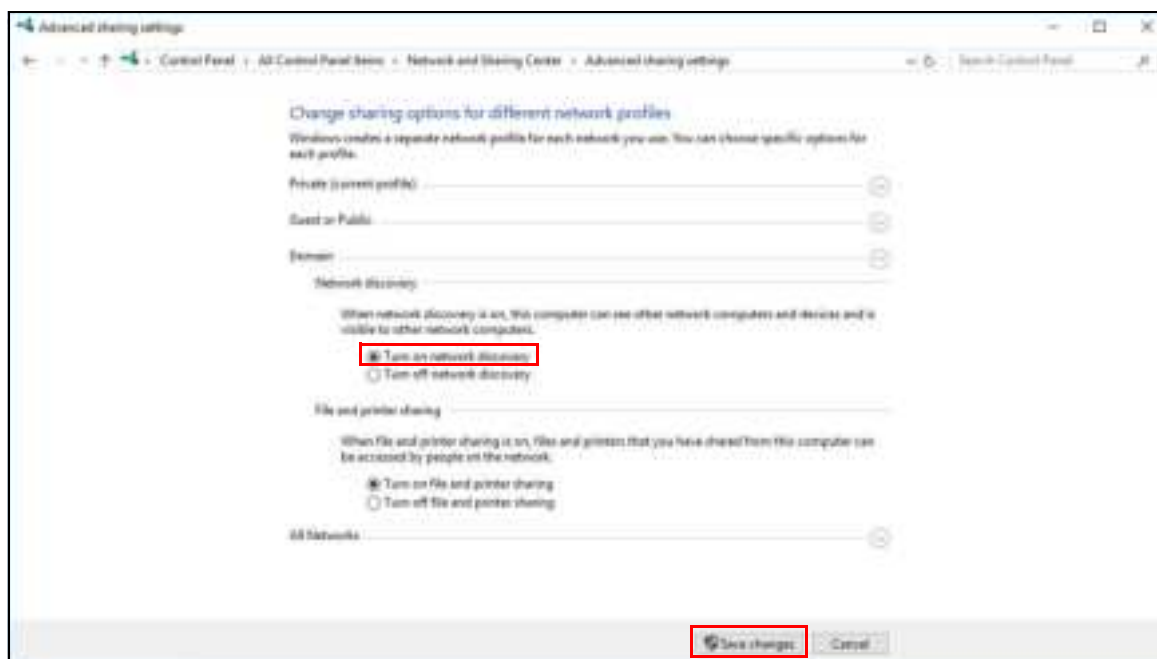
10.9.1 Auto-discover Your UPnP-enabled Network Device

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

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

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

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

Figure 78   Network Connections
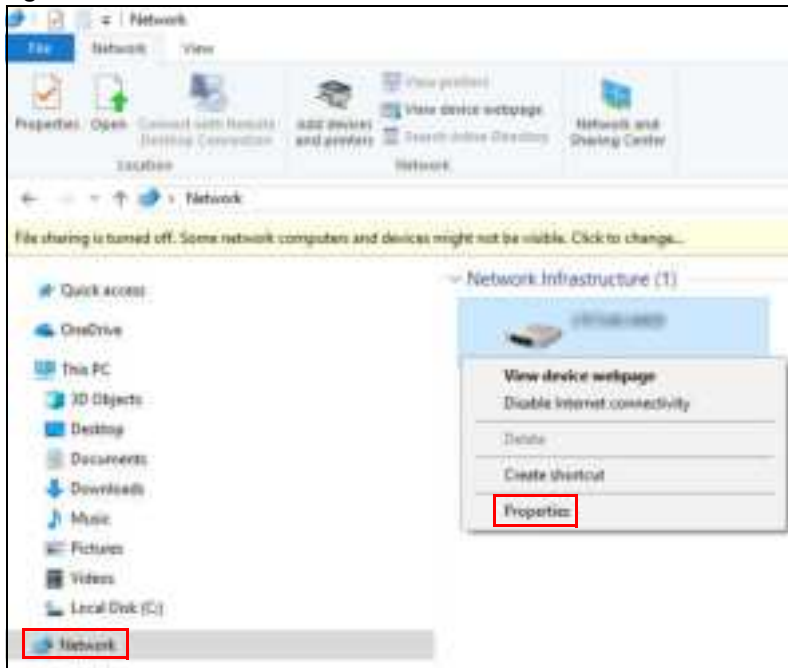
**3**   In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 79   Internet Connection Properties

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

Figure 80 Internet Connection Properties: Advanced Settings
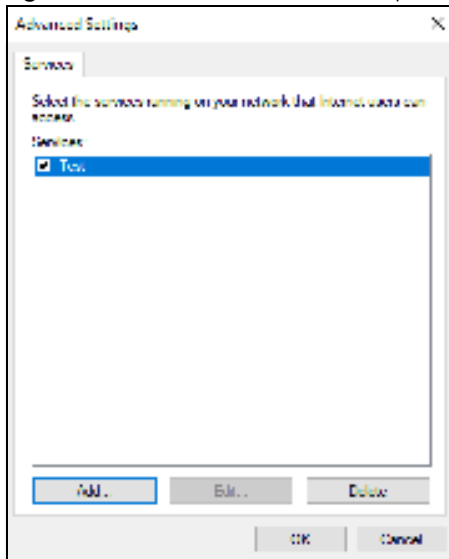
Figure 81 Internet Connection Properties: Advanced Settings: Add
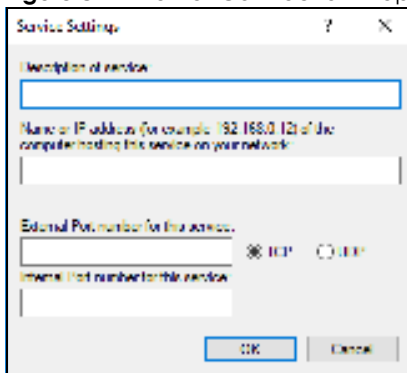
Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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

Figure 82 System Tray Icon
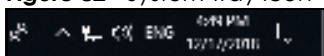
6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 83 Internet Connection Status
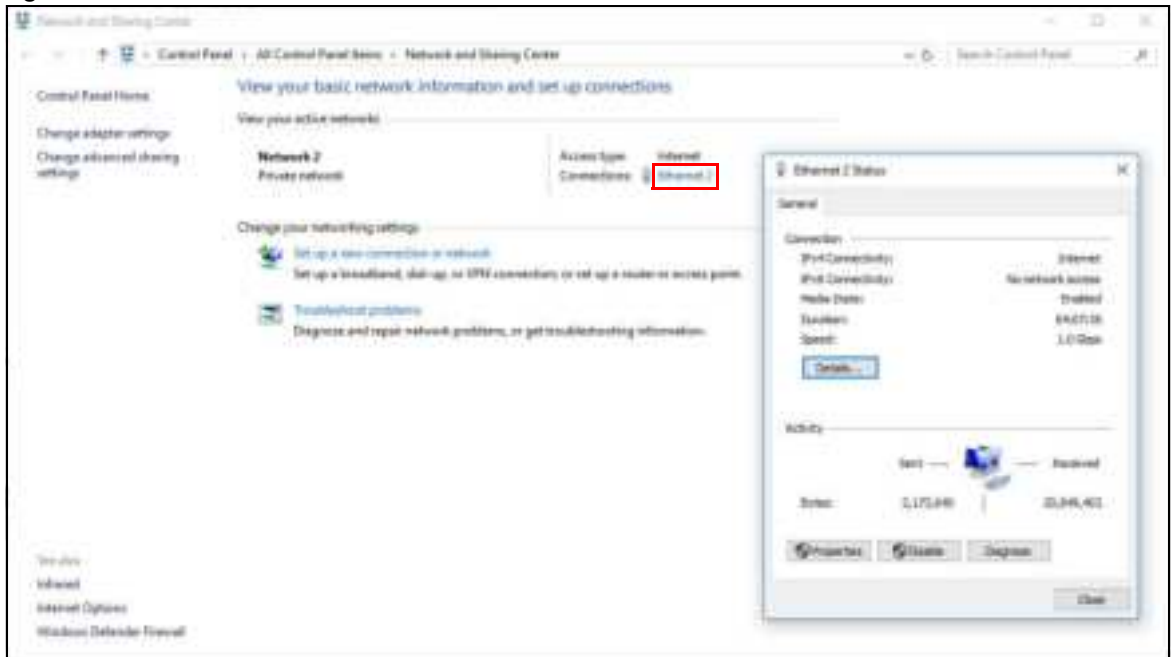
10.10 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

Figure 84   Network Connections
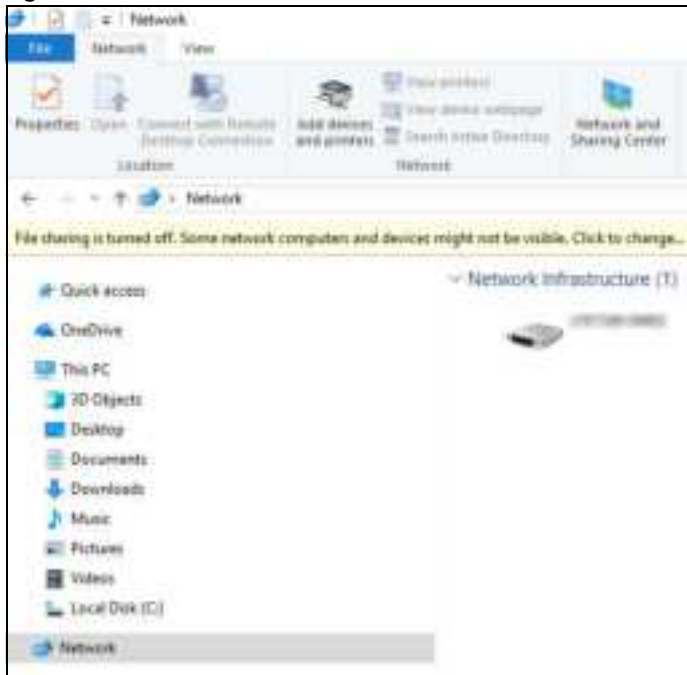
3   An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.

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

Figure 85   Network Connections: Network Infrastructure
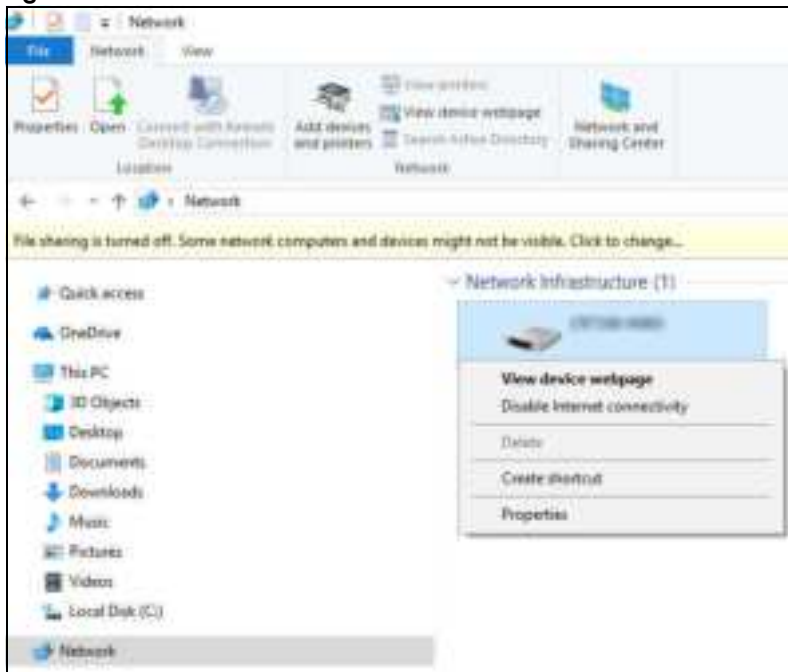
5   Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays information about the Zyxel Device.

Figure 86   Network Connections: Network Infrastructure: Properties: Example

10.10.1 DHCP Setup

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

IP Pool Setup

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

10.10.2 DNS Server Addresses

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

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

• The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.