User's Guide
Nebula Mobile Router

Default Login Details

LAN IP Address	http://192.168.1.1
User Name	admin
Password	See the Zyxel Device label

Version 1.18 Ed 3, 04/2025
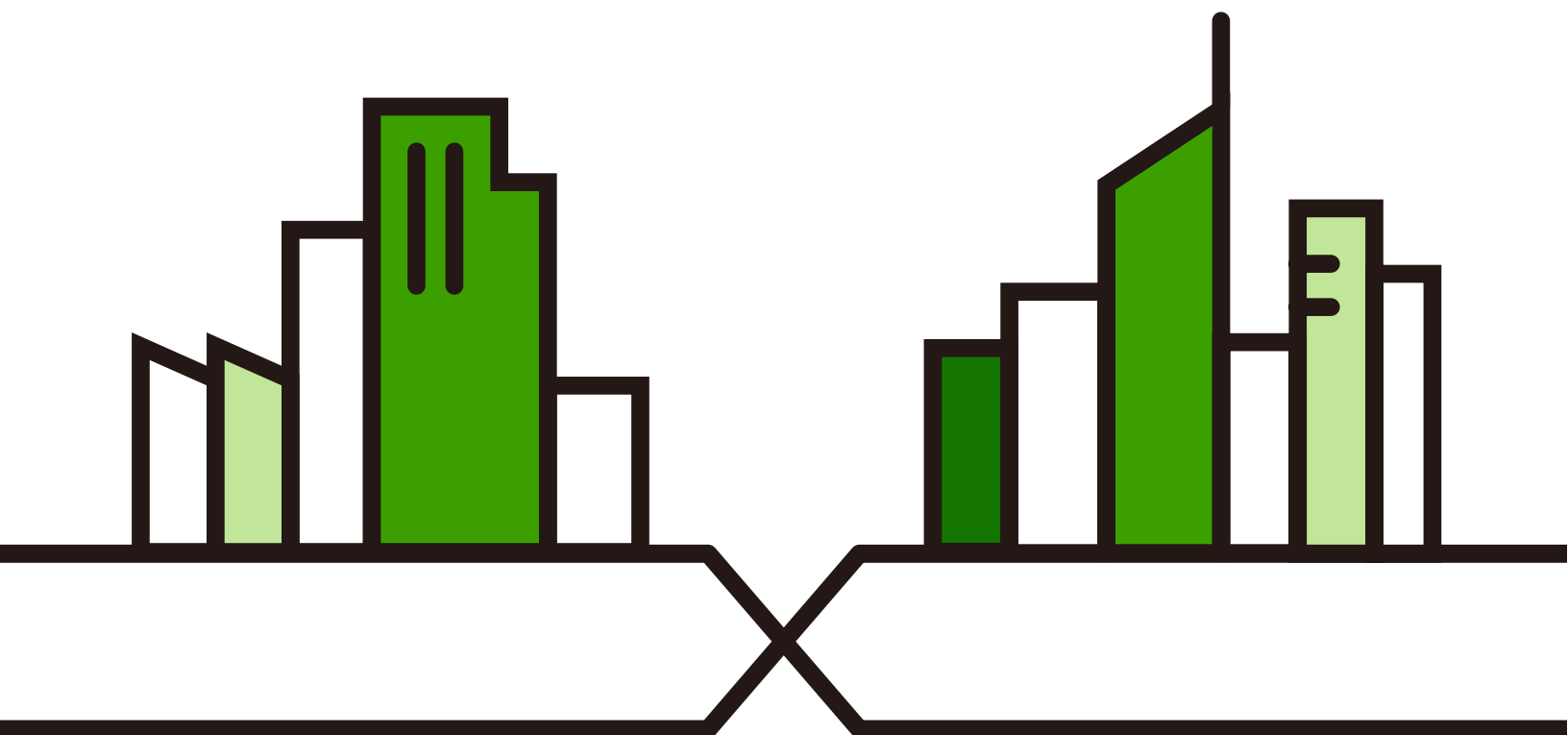
This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in product features or web configurator brand style. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

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

- The Nebula Control Center help portal

  Go to *https://nebula.zyxel.com/cc/ui/index.html#/help* to register the Zyxel Device to the NCC.

- The Zyxel Air app help

  Go to *https://service-provider.zyxel.com/app-help/ZyxelAir/index.html* to find the best location to place 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.
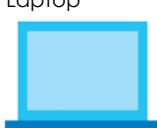
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

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	4G LTE/5G NR Base Station	Desktop
Laptop	Smart TV	Wireless Device

Accessibility and Compatibility

Introduction

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

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

Accessibility Feature – Screen Reader Support

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

To use the screen reader, do the following:

1 Open your screen reader software.

2 Navigate to this User's Guide; the screen reader should automatically start reading the contents.

3 Use the keyboard shortcuts to navigate through this User's Guide (refer to the screen reader documentation).

Accessibility Feature – Keyboard Navigation

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

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

How to Access Support Services

We offer the following ways to contact our Zyxel support team.

Email Support: support.zyxel.com

Send a detailed description of your issue, including any error messages, screenshots, or steps you have already taken to resolve the problem. The response time is typically within 24 hours.

User Forums and Community Support: *https://community.zyxel.com/en*

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

1.1 Overview

The Zyxel Device refers to the following models:

Indoor Mobile Routers

• Nebula LTE3301-PLUS (4G LTE-A Indoor Router)
• Nebula NR5101(5G NR Indoor IAD)
• Nebula FWA505 (5G NR Indoor IAD)
• Nebula FWA510 (5G NR Indoor IAD)

Outdoor Mobile Routers

• Nebula LTE7461-M602 (4G LTE-A Outdoor Router)
• Nebula NR7101(5G New Radio Outdoor Router)
• Nebula FWA710 (5G New Radio Outdoor Router)

1.1.1 Feature Differences

The Zyxel Device is a router that supports (but is not limited to) the following features. Note the following differences between the Zyxel Device models:

Table 1   Feature Differences 1

FEATURE/MODEL	NEBULA LTE3301-PLUS	NEBULA LTE7461-M602	NEBULA NR5101	NEBULA NR7101
2.4G WiFi	Y	Y (for config only)	Y	Y (for config only)
5G WiFi	Y	N	Y	N
1G LAN Port	Y	Y	Y	Y
2.5G LAN Port	N	N	N	N
External Antenna Support	Y	N	Y	N
Ethernet WAN	Y	N	Y	N
Dual SIM Slots	N	N	N	Y
Cellular Backup	Y	N	Y	Y
Cellular IP Passthrough	Y	Y	Y	Y
Cellular Lock	Y	Y	N	Y
Cellular SMS	Y	N	Y	N
Guest/More AP	Y	N	Y	N
More AP Edit	Y	N	Y	N

Table 1   Feature Differences 1 (continued)

FEATURE/MODEL	NEBULA LTE3301-PLUS	NEBULA LTE7461-M602	NEBULA NR5101	NEBULA NR7101
WLAN Scheduler	Y	N	Y	N
Channel Status	N	N	N	N
USB File Sharing	Y	N	Y	N
Parental Control	Y	N	Y	N
Network Monitoring	N	Y	Y	Y
Proxy ARP	N	N	N	Y
FQ_Codel (Fair Queuing with Controlled Delay)	N	N	N	Y
PIN Modification	Y	Y	Y	Y
IGMP Proxy	Y	Y	Y	Y
MLD Proxy	Y	Y	Y	Y
Fullcone NAT	N	Y	Y	Y
464XLAT	N	N	N	N
DHCP	Y	Y	Y	Y
DHCP Options	Y	Y	Y	Y
Policy Route	Y	Y	Y	Y
RIP	Y	Y	Y	N
ALG	Y	Y	Y	Y
Port Triggering	Y	Y	Y	Y
Dynamic DNS	Y	Y	Y	Y
VLAN Group	N	N	N	Y
Interface Grouping	Y	Y	Y	Y
Speed Test	N	Y	N	Y
XMPP	N	N	N	Y
TR-069 Client	Y	Y	Y	Y
Email Notification	Y	Y	Y	Y
Module Upgrade	N	N	N	Y
Schedule Reboot	Y (NCC Web Portal)	Y	Y	Y
Firmware Version	1.15	1.15	1.15	1.15

Table 2   Feature Differences 2

FEATURE/MODEL	NEBULA FWA505	NEBULA FWA510	NEBULA FWA710
2.4G WiFi	Y	Y	Y (for config only)
5G WiFi	Y	Y	N
1G LAN Port	Y	N	N
2.5G LAN Port	N	Y	Y
External Antenna Support	Y	Y	N
Ethernet WAN	Y	Y	N

Table 2   Feature Differences 2 (continued)

FEATURE/MODEL	NEBULA FWA505	NEBULA FWA510	NEBULA FWA710
Dual SIM Slots	N	N	N
Cellular Backup	Y	Y	N
Cellular IP Passthrough	Y	Y	Y
Cellular Lock	N	N	Y
Cellular SMS	Y	Y	N
Guest/More AP	Y	Y	N
More AP Edit	Y	Y	N
WLAN Scheduler	Y	Y	N
Channel Status	Y	Y	N
USB File Sharing	Y	Y	N
Parental Control	Y	N	N
Network Monitoring	N	Y	Y
Proxy ARP	N	N	Y
FQ_Codel (Fair Queuing with Controlled Delay)	N	N	N
PIN Modification	Y	Y	Y
IGMP Proxy	Y	Y	Y
MLD Proxy	Y	Y	N
Fullcone NAT	Y	Y	N
464XLAT	Y	Y	N
DHCP	Y	Y	Y
DHCP Options	Y	Y	Y *Supports **Custom DHCP Options** screen
Policy Route	N	N	Y
RIP	N	Y	N
ALG	N	N	N
Port Triggering	N	N	N
Dynamic DNS	N	N	Y
VLAN Group	N	N	Y
Interface Grouping	N	N	Y
Speed Test	N	N	Y
XMPP	N	N	N
TR-069 Client	Y	Y	Y
Email Notification	N	N	N
Module Upgrade	N	N	N
Schedule Reboot	Y (NCC Web Portal)	Y (NCC Web Portal)	Y (NCC Web Portal)
Firmware Version	1.18	1.15	1.15

See the Quick Start Guide for how to do the hardware installation, mounting, and Internet setup.

1.2 Nebula Management

You can manage the Zyxel Device with the Zyxel Nebula Control Center. The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula routers. You need to create a Zyxel Account to log into the NCC for management first. You can access the NCC through the NCC web portal through a web browser on your computer or the Nebula Mobile app on your smartphone, see for more information.

For more information on configuring the Zyxel Device on the NCC, go to *https://nebula.zyxel.com/cc/ ui/index.html#/help*. You will be prompted to log into the NCC using your NCC account.

For advanced configurations, such as configuring WAN settings, wireless LAN settings and firewall settings, use the Zyxel Device Web Configurator. To find the best place for your Zyxel Device to receive the optimal cellular signal or perform a signal strength test, use the Zyxel Air app.

Table 3   Management Methods

MANAGEMENT METHOD	WHEN TO USE IT
Nebula Mobile APP	Registration and Monitoring
NCC Web Portal	Registration, Monitoring and Basic Management
Zyxel Device Web Configurator	Advanced Management
ZyxelAir App	Zyxel Device Installation

Note: The configurations you make in the NCC have priority over the configurations in the Web Configurator and the Zyxel Air app.

The Nebula Control Center (NCC) is an alternative cloud-based network management system that allows you to remotely manage and monitor the Zyxel Nebula Security Appliances (**SA**), Ethernet Switches (**S**), and Access Points (**AP**). You may also access the Web Configurator in cloud mode.

Figure 1   NCC Example Network Topology
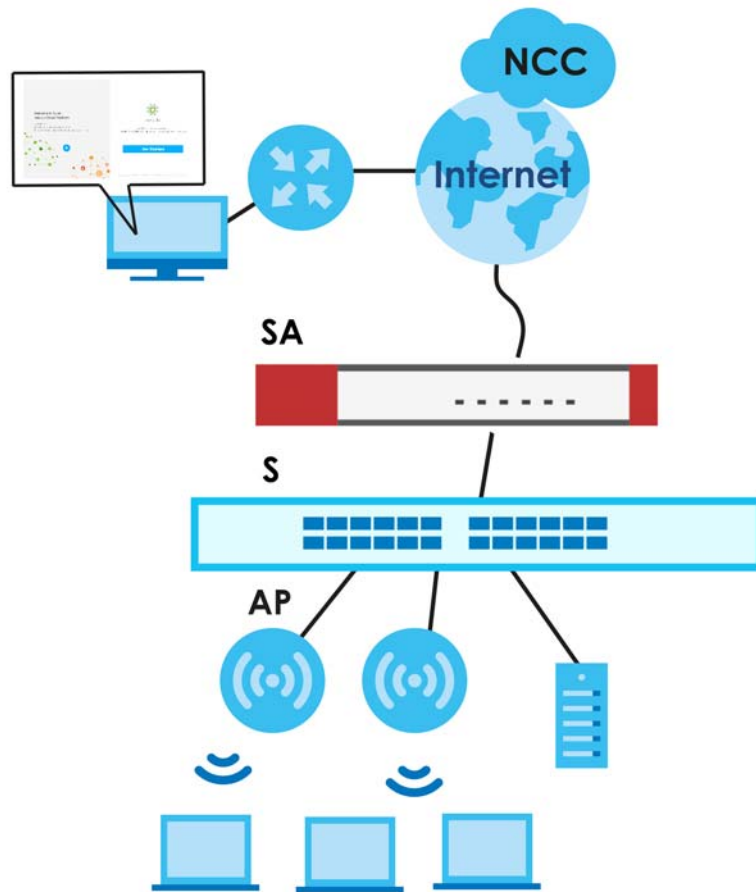
1.2.1 Register Your Zyxel Device Using the Nebula Web Portal

1   Go to *https://nebula.zyxel.com*. Click **Get Started**.
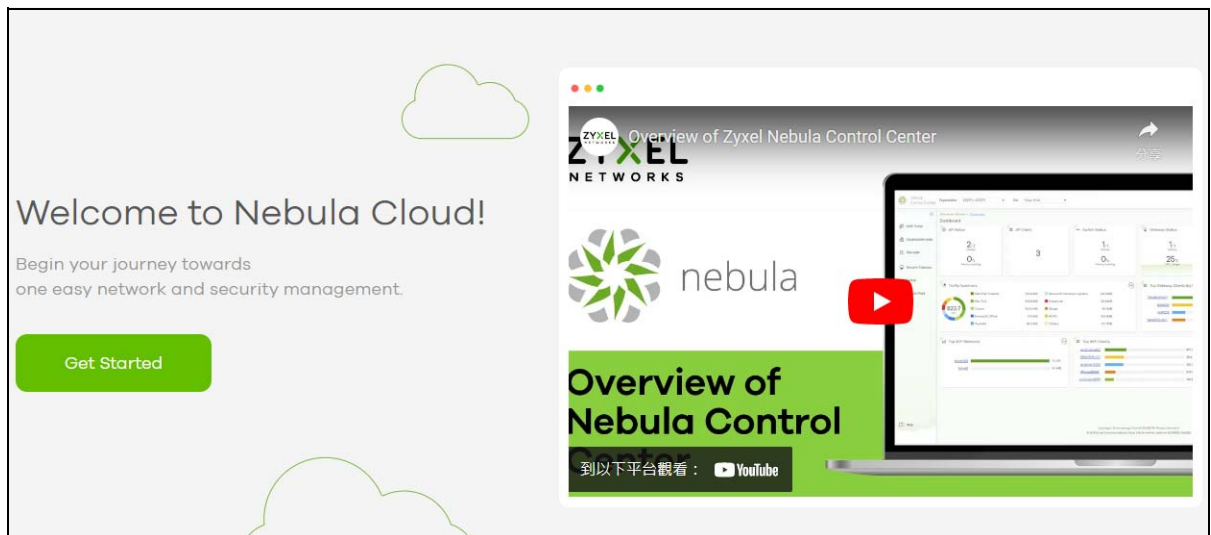
2 The login screen displays. Enter your Zyxel Account information to log in. If you do not have one, click **Create account**. You will be redirected to another screen where you can sign up for a Zyxel Account.

3 Click **Create organization** to create an organization and a site (using the Nebula setup wizard), or select an existing site.

4 If you are creating the first organization under your account, click **Let's Start** to begin.
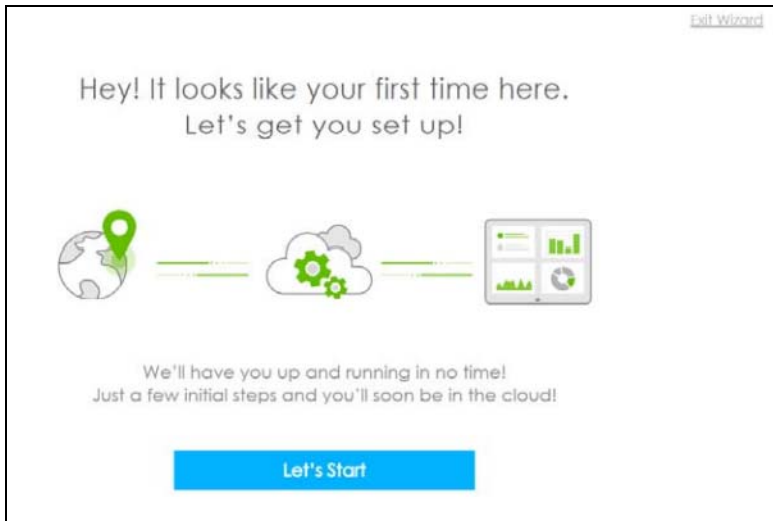
5 Enter a descriptive name for your organization and site. Both names must consist of 1 to 64 characters.

6 Select the time zone of your location. This will set the time difference between your time zone and Coordinated Universal Time (UTC).

7 Click **Next** to continue.

8 Enter your Zyxel Device MAC address and serial number. Enter a descriptive name for your Zyxel Device.

9 Click the **+Add** button to register and add the Zyxel Device to the site. You can register multiple Zyxel Device at a time.

10 Click **Next** to proceed to setting up your WiFi network and guest WiFi network.

Note: Your default web configurator login password will be changed when you register your Zyxel Device at NCC. Make sure to check the changed password and change it to your preferred one before logging in the web configurator. The password must be at least 8 characters long, including one letter and one number. ~!@#$%^&*()_+'-={};:<> are allowed.

1.3 Applications for the Zyxel Device

See the above table for which applications are supported by your Zyxel Device.

Wireless WAN

The Zyxel Device can connect to the Internet through a 4G/5G SIM card to access a wireless WAN connection. Just insert a SIM card into the SIM card slot of the Zyxel Device.

You can also install external antennas to improve your wireless WAN signal strength, see Table 1 on page 18 for more information.

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

Internet Access

Your Zyxel Device provides shared Internet access by connecting to a cellular network. A computer can connect to the Zyxel Device's **LAN** port for configuration through the Web Configurator.

Figure 2 Zyxel Device's Internet Access Application
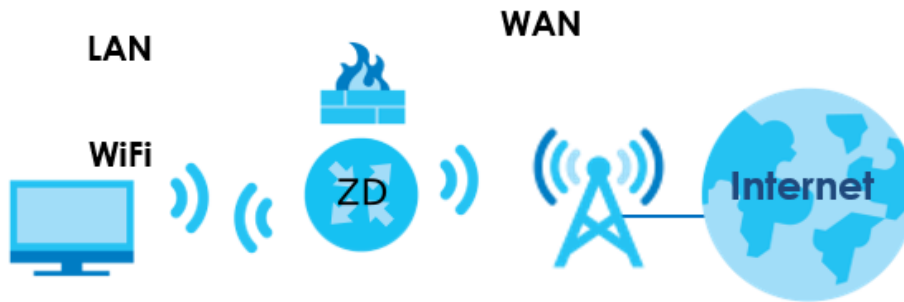
Wireless LAN (WiFi)

WiFi clients can connect to the Zyxel Device to access network resources and the Internet. The Zyxel Device supports WiFi Protected Setup (WPS), which allows you to quickly set up a WiFi network with strong security.

Your Zyxel Device WiFi may only be for configuration, see Table 1 on page 18 for more information.

Figure 3 Zyxel Device's Wireless LAN
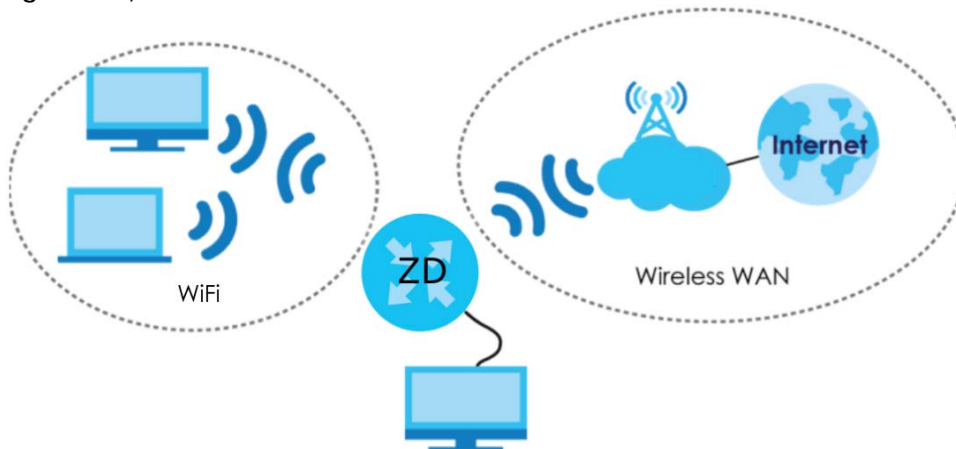
Carrier Aggregation

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

Figure 4 Zyxel Device's CA Application
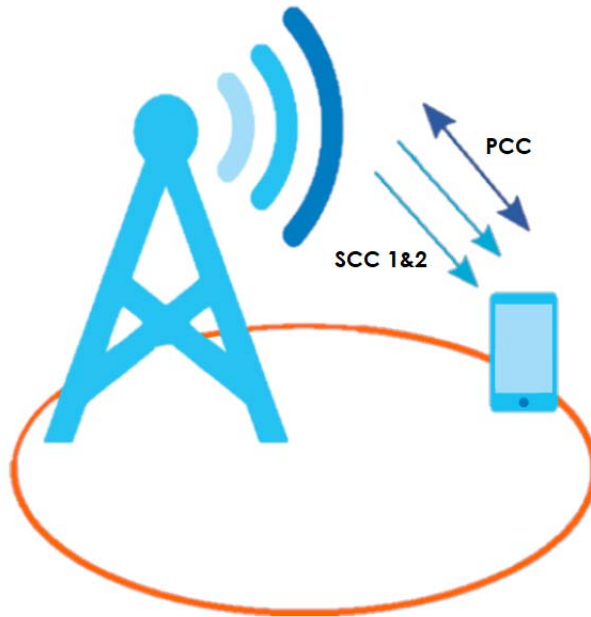
Ethernet WAN

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

If you have another broadband modem or router available, you can use the Ethernet WAN port and then connect it to the broadband modem or router. This way, you can access the Internet through an Ethernet connection and still use the Firewall function on the Zyxel Device.

See Section 1.1.1 on page 18 to see if your Zyxel Device supports an Ethernet WAN port.

Figure 5 Zyxel Device's Internet Access Application: Ethernet WAN
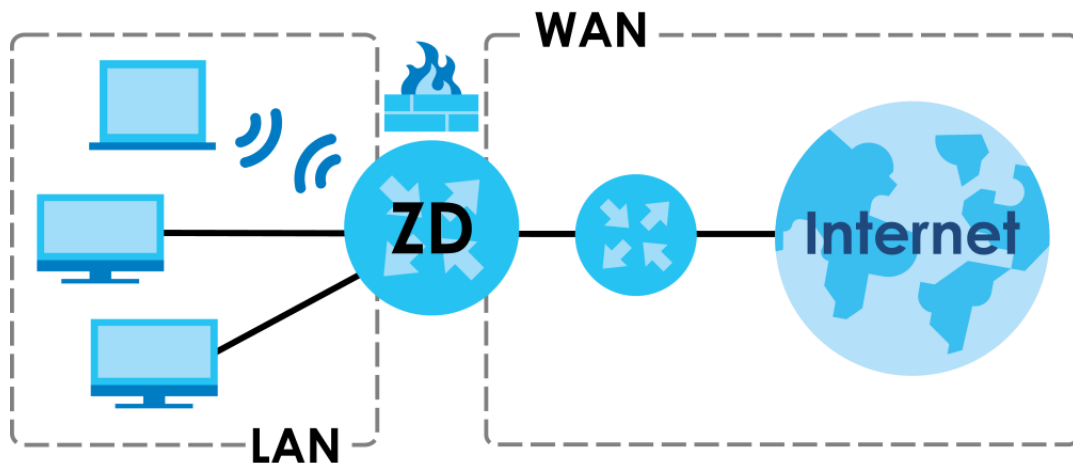
In the figure above, you can also configure Firewall on the Zyxel Device for secure Internet access. When the Firewall is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Cellular Backup

Some Zyxel Devices support a WAN backup connection to ensure always-on Internet connectivity.

For Zyxel Devices that support Ethernet WAN, when the Ethernet WAN goes down, the Zyxel Devices automatically switch to use the cellular WAN connection.

The WAN connection priority is as follows:

1 Ethernet WAN

2 Cellular WAN

For Zyxel Devices that support dual SIM slots, when the primary cellular WAN goes down, the Zyxel Devices automatically switch to use the backup connection on the second SIM card.

See to see if your Zyxel Device supports Cellular Backup.

1.4 How to Manage your Zyxel Device

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

- Web Configurator. This is recommended for everyday management of Zyxel Device using a (supported) web browser.
- Nebula Control Center Web Portal. Use the NCC web portal to monitor your Zyxel Device. You can register your Zyxel Device to a site and organization using the NCC web portal.
- Nebula Mobile App. Use the Nebula mobile app to monitor your Zyxel Device. You can register your Zyxel Device to a site and organization using the Nebula Mobile app. Download the Nebula Mobile app at Apple Store or Google Play.
- Zyxel Air. Use the Zyxel Air app (available on the App Store for Apple devices and Google Pay for Android devices) for setup and management of the Zyxel Device on your smartphone. You can also use the app for finding the optimal 5G NR signal strength. This User's Guide provides information about using the Zyxel Air app. To install the app, scan the QR code on the QSG.

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

CHAPTER 2
Hardware Panels

2.1 Overview

This chapter describes the LEDs and port panels of the Zyxel Device.

2.2 LEDs

The following figures show the Zyxel Device LED indicators. None of the LEDs are on if the Zyxel Device is not receiving power.

Note: Blinking (slow) means the LED blinks once per second. Blinking (fast) means the LED blinks once per 0.5 second.

Indoor Mobile Routers

- Nebula LTE3301-PLUS
- Nebula NR5101
- Nebula FWA505
- Nebula FWA510

Outdoor Mobile Routers

- Nebula LTE7641-M602
- Nebula NR7101
- Nebula FWA710

Nebula LTE3301-PLUS

Figure 6 LED Indicators (Nebula LTE3301-PLUS)

The following are the LED descriptions for your Zyxel Device.

Table 4   LED Descriptions (Nebula LTE3301-PLUS)

LED	COLOR	STATUS	DESCRIPTION
POWER	White	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting or self-testing.
		Off	The Zyxel Device is not receiving power.
Internet	White	On	There is Internet connection.
		Blinking	The Zyxel Device is sending or receiving IP traffic.
		Off	There is no Internet connection.
LTE/3G	White	On	The Zyxel Device is registered and successfully connected to a 4G network.
		Blinking (slow)	The Zyxel Device is connected to a 3G network.
		Blinking (fast)	The Zyxel Device is trying to connect to a 3G/4G network.
		Off	There is no service.
	Green	On	The Zyxel Device has an Ethernet connection on the WAN.
		Off	There is no Ethernet connection on the WAN.
Signal Strength	Green	On	The signal strength is excellent.
	Amber	On	The signal strength is fair.
	Red	On	The signal strength is poor.
		Blinking	There is no SIM card inserted, no signal, or the signal strength is below the poor level.
		Off	The SIM card is invalid, or the PIN code is not correct.
WLAN	Green	On	The 2.4G wireless network is activated.
		Blinking (slow)	The Zyxel Device is setting up a WPS connection with a 2.4G wireless client.
		Blinking (fast)	The Zyxel Device is communicating with 2.4G wireless clients.
	White	On	The 5G wireless network is activated.
		Blinking (slow)	The Zyxel Device is setting up a WPS connection with a 5G wireless client.
		Blinking (fast)	The Zyxel Device is communicating with 2.4G and 5G wireless clients.
		Off	The wireless network is not activated.
USB	White	On	The Zyxel Device recognizes a USB connection through the USB port.
		Blinking	The Zyxel Device is sending/receiving data to/from the USB device connected to it.
		Off	The Zyxel Device does not detect a USB connection through the USB port.

Nebula NR5101

Figure 7   LED Indicators (Nebula NR5101 LED)
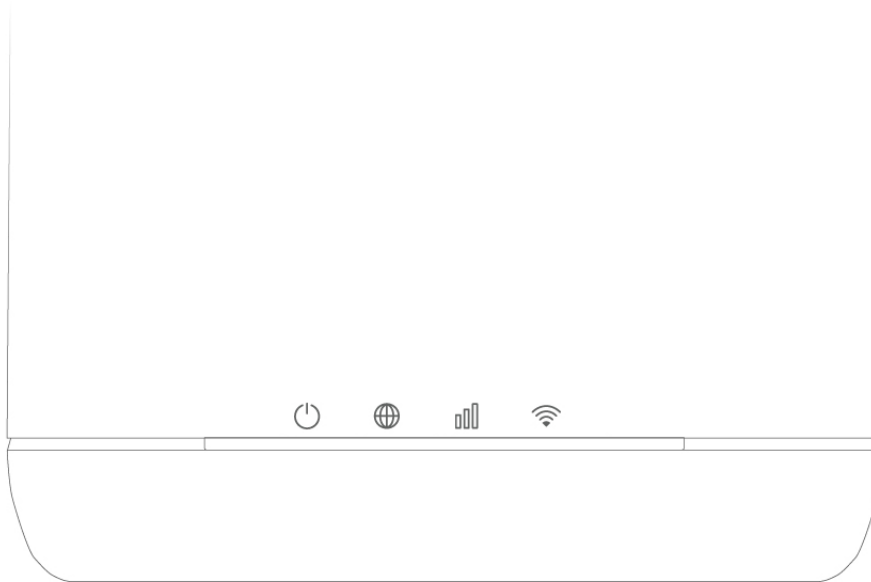
The following are the LED descriptions for your Zyxel Device.

Table 5   LED Descriptions (Nebula NR5101 LED Behavior)

LED	COLOR	STATUS	DESCRIPTION
Power/USB	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting.
		Off	The Zyxel Device is not receiving power.
	Blue	On	A USB device is connected to the USB port on the Zyxel Device.
Internet/SMS	Green	On	The Zyxel Device is connected to the Internet using 3G/4G.
		Blinking	There is a new SMS message.
		Off	The Zyxel Device is not connected to the Internet.
	Blue	On	The Zyxel Device is connected to the Internet using 5G.
Cellular Signal Strength	Green	On	The signal strength is excellent.
	Orange	On	The signal strength is fair.
	Red	On	The signal strength is poor.
		Blinking	There is no cellular signal, or signal strength is below the poor level.
WiFi/WPS	Green	On	WiFi is enabled.
		Blinking (fast)	Data is being transmitted and received.
		Blinking (slow)	WPS is activated, and the Zyxel Device is establishing a WPS connection.

Nebula FWA505

Figure 8   LED Indicators (Nebula FWA505 LED)
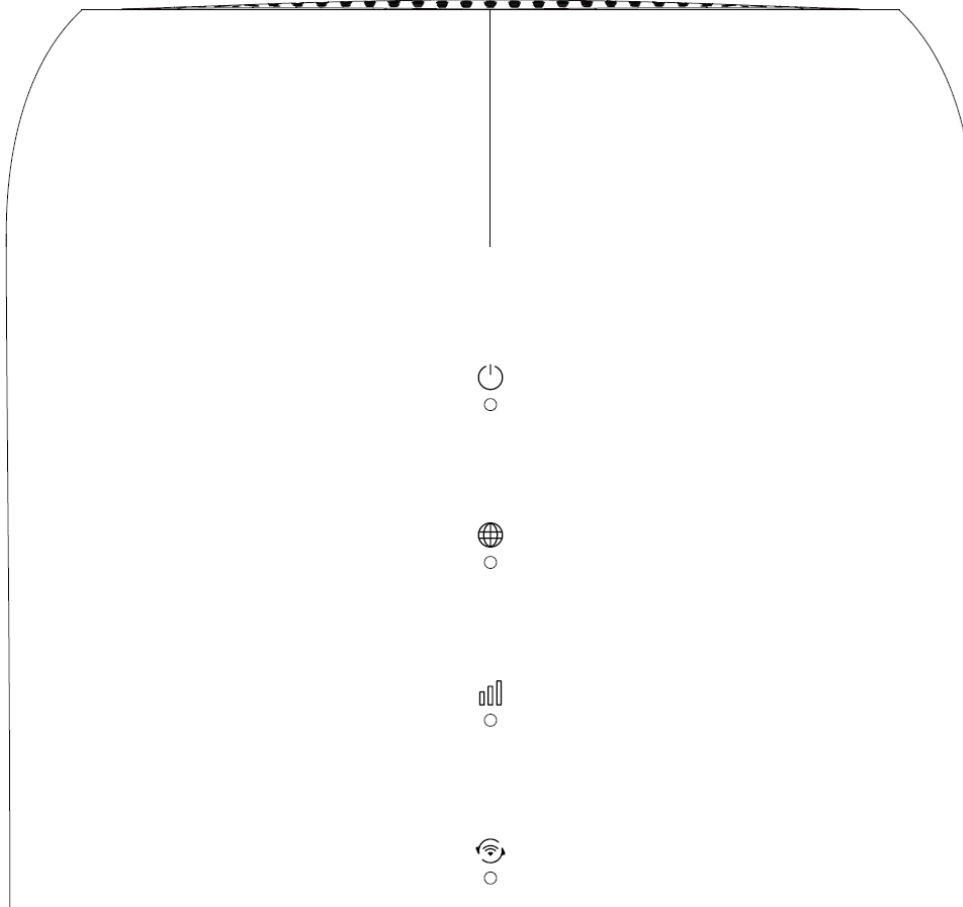
The following are the LED descriptions for your Zyxel Device.

Table 6   LED Descriptions (Nebula FWA505)

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting.
		Off	The Zyxel Device is not receiving power.
	Red	On	Zyxel Device error, need to take action.
	Blue	On	There is a new SMS message.
		Blinking	The Inbox is full.
Internet	Blue	On	The Zyxel Device is connected to the Internet using 5G.
	Green	On	The Zyxel Device is connected to the Internet using 4G, or is connected in Ethernet WAN mode.
	Red	On	Internet connection is unavailable.

Table 6   LED Descriptions (Nebula FWA505) (continued)

LED	COLOR	STATUS	DESCRIPTION
Cellular Signal Strength	Blue	On	The signal strength is good.
		Blinking	No SIM card or invalid SIM card.
	Green	On	The signal strength is medium.
	Red	On	The signal strength is poor.
		Blinking	There is no cellular signal, or signal strength is below the poor level.
WiFi/WPS	Green	On	WiFi is enabled.
		Blinking	WPS is activated, and the Zyxel Device is establishing a WPS connection.
		Off	WiFi is disabled.

Nebula FWA510

Figure 9   LED Indicators (Nebula FWA510)

The following are the LED descriptions for your Zyxel Device.

Table 7   LED Descriptions (Nebula FWA510)

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is booting.
		Off	The Zyxel Device is not receiving power.
	Red	On	Zyxel Device error, need to take action.
SMS	Green	On	There is a new SMS message.
		Blinking	The Inbox is full.
		Off	There is no unread SMS message.
Cellular Signal Strength	Blue	On	The signal strength is good.
	Green	On	The signal strength is medium.
	Red	On	The signal strength is poor.
		Blinking	There is no cellular signal, or signal strength is below the poor level.
		Off	The Zyxel Device is booting.

Table 7   LED Descriptions (Nebula FWA510) (continued)

LED	COLOR	STATUS	DESCRIPTION
Internet ⊕	Blue	On	The Zyxel Device is connected to the Internet using 5G.
	Green	On	The Zyxel Device is connected to the Internet using 4G, or is connected in Ethernet WAN mode.
	Red	On	Internet connection is unavailable.
WiFi/WPS	Green	On	WiFi is enabled.
		Blinking	WPS is activated, and the Zyxel Device is establishing a WPS connection.
		Off	WiFi is disabled.

Nebula LTE7641-M602

Figure 10   LED Indicators (Nebula LTE7641-M602)

The following are the LED descriptions for your Zyxel Device.

Table 8   LED Descriptions (Nebula LTE7461-M602)

COLOR	STATUS	DESCRIPTION
Red	Blinking	The Zyxel Device is booting or self-testing.
	On	The Zyxel Device encountered an error.
Green	Blinking	The Zyxel Device is trying to connect to the Internet.
	On	The Zyxel Device is connected to the Internet.
Amber	Blinking	The Zyxel Device WiFi is on.

Nebula NR7101

Figure 11   LED Indicators (Nebula NR7101)
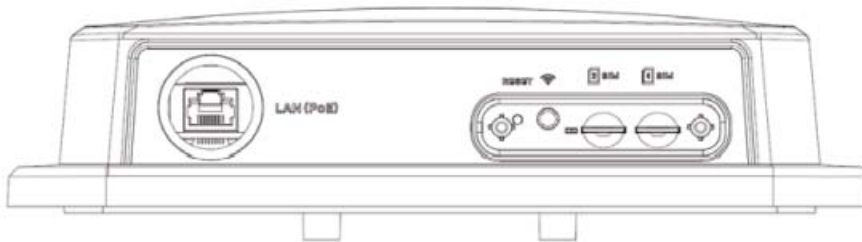
The following are the LED descriptions for your Zyxel Device.

Table 9   LED Descriptions (Nebula NR7101)

COLOR	STATUS	DESCRIPTION
Green	On	The Zyxel Device is connected to the Internet.
	Blinking	The Zyxel Device is trying to connect to the Internet.

Table 9   LED Descriptions (Nebula NR7101) (continued)

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

Nebula FWA710

Figure 12   LED Indicators (Nebula FWA710)
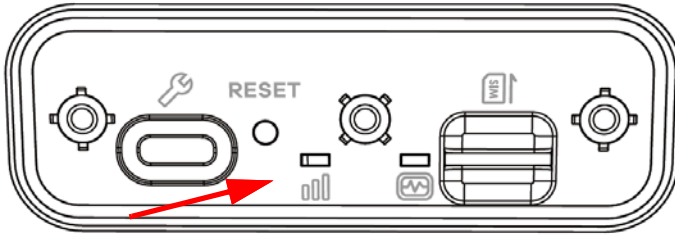
The following are the LED descriptions for your Zyxel Device.

Table 10   LED Descriptions (Nebula FWA710)

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

2.3 Panel Ports

The following figures show the panel ports and buttons of the Zyxel Device.

Indoor Mobile Routers

• Nebula LTE3301-PLUS

• Nebula NR5101

- Nebula FWA505
- Nebula FWA510

Outdoor Mobile Routers

- Nebula LTE7461-M602
- Nebula NR7101
- Nebula FWA710

Nebula LTE3301-PLUS

Place the Zyxel Device with the feet at the bottom and the ports facing you. The two antenna ports are located on the rear panel, closer to the top of the Zyxel Device.

Figure 13   Rear Panel (Nebula LTE3301-PLUS)
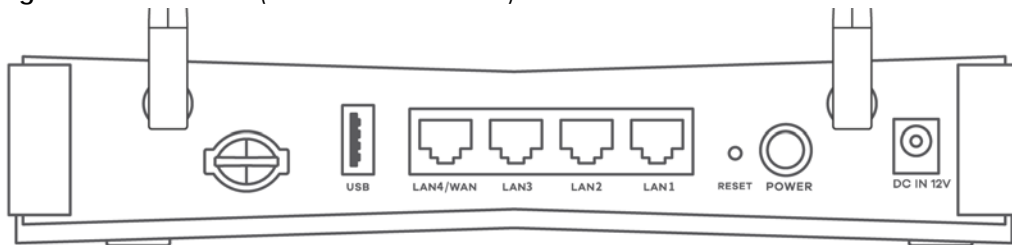
The WiFi / WPS button is on the front panel of the Zyxel Device, closer to the right, with the ports positioned farther from you.

Figure 14   WPS and WiFi On/Off Button on the Front Panel (Nebula LTE3301-PLUS)

The following table describes the ports and buttons on your Zyxel Device.

Table 11   Panel Ports and Buttons (Nebula LTE3301-PLUS)

LABELS	DESCRIPTION
ANT1-ANT2	Install the external antennas to strengthen the cellular signal.
Micro SIM	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.
USB	The USB port of the Zyxel Device is used for file sharing.
LAN4/WAN	LAN mode: LAN4 is a 1G LAN port that supports speeds of 100/1000 Mbps. Connect computers or other Ethernet devices to Ethernet ports for Internet access. WAN mode: The 1G WAN port supports speeds of 100/1000 Mbps. Use an Ethernet cable to connect the WAN port to a gateway/modem for Internet connection.
LAN3- LAN1	LAN3 – LAN1 are 1G LAN ports that support speeds of 100/1000 Mbps. Connect computers or other Ethernet devices to Ethernet ports for Internet access.

Table 11   Panel Ports and Buttons (Nebula LTE3301-PLUS) (continued)

LABELS	DESCRIPTION
RESET	Press the **RESET** button for more than 5 seconds to return the Zyxel Device to the factory defaults. Press the **RESET** button for more than 2 seconds but less than 5 seconds, it will cause the system to reboot.
POWER	Press the **POWER** button after the power adapter is connected to start the Zyxel Device.
POWER / DC IN	Connect the power adapter and press the **POWER** button to start the Zyxel Device.
WiFi	Press the WLAN (WiFi) button for more than 5 seconds to enable WiFi.
WPS	After WiFi is enabled, press the WLAN button for more than one second but less than 5 seconds to quickly set up a secure wireless connection between the Zyxel Device and a WPS-compatible client.

Nebula NR5101

Place the Zyxel Device with the ports facing you and closer to the bottom.

Figure 15   Rear Panel (Nebula NR5101)
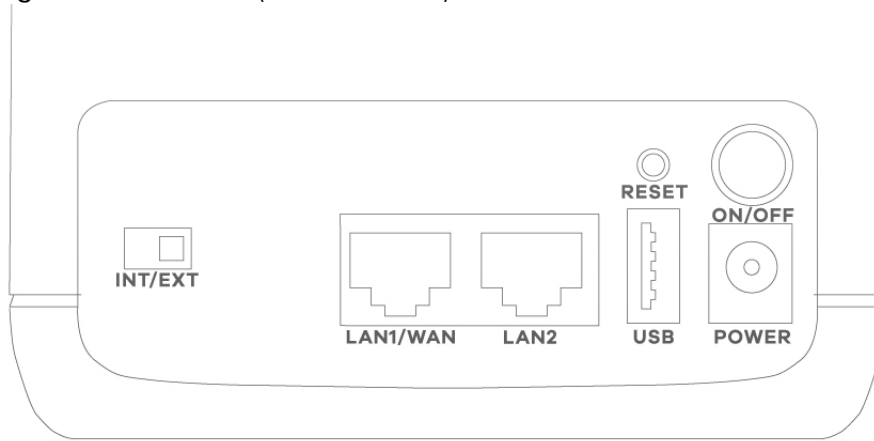
The WPS and WiFi On/Off button is on the top of the Zyxel Device.

Figure 16   WPS and WiFi On/Off Button on the Top Panel (NR5101)

The two antenna ports are in the middle of the rear panel of the Zyxel Device.

Figure 17   Antenna Ports on the Rear Panel (NR5101)

The Micro SIM card slot is on the bottom of the Zyxel Device.

Figure 18   Micro SIM card slot on the bottom panel (NR5101)
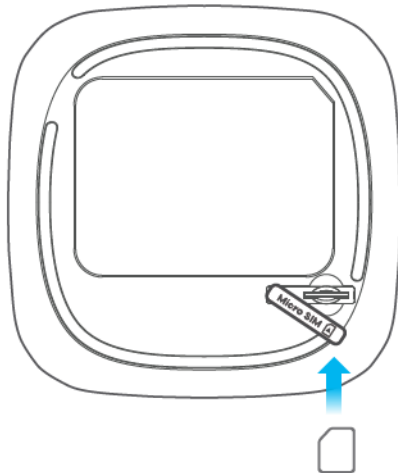
The following table describes the ports and buttons on your Zyxel Device.

Table 12   Panel Ports and Buttons (Nebula NR5101)

LABELS	DESCRIPTION
WPS/WiFi On and Off	Press for 1 second: Enable or disable WiFi. Press for more than 5 seconds: Activate WPS connection process.
ANT1-ANT2 / Antenna	Install the external antennas to strengthen the cellular signal. Note: To use the external antennas, you must set the **INT/EXT** switch to **EXT**.
INT/EXT	Select between the internal or external cellular antennas.
LAN1/WAN	LAN mode: LAN1 is a 1G LAN port that supports speeds of 100/1000 Mbps. Connect computers or other Ethernet devices to Ethernet ports for Internet access. WAN mode: The 1G WAN port supports speeds of 100/1000 Mbps. Use an Ethernet cable to connect the WAN port to a gateway/modem for Internet connection.
LAN2	Connect a computer to the LAN using an RJ45 cable.
RESET	Press for 2 seconds: Reboot the Zyxel Device. Press for 5 seconds: Restore the Zyxel Device to its factory default settings.
USB	The USB port of the Zyxel Device is used for file sharing.
POWER Button	Press the **POWER** button after the power adapter is connected to start the Zyxel Device.
POWER	Connect the power adapter and press the **POWER** button to start the Zyxel Device.
Micro SIM	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.
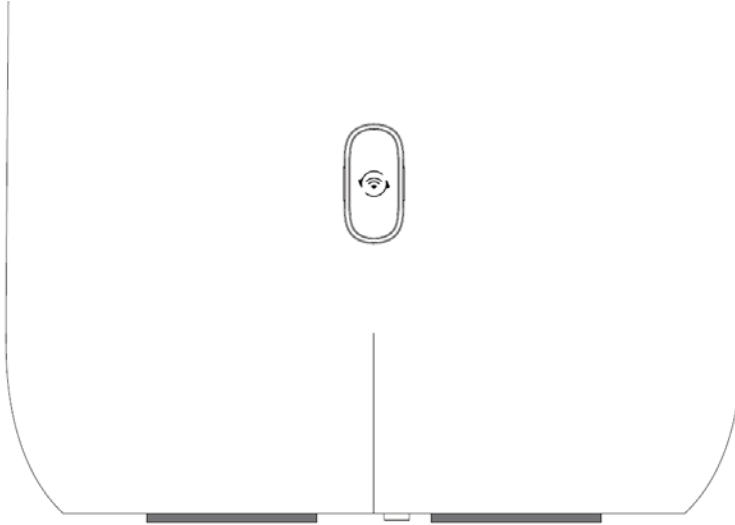
Nebula FWA505

Place the Zyxel Device with the ports facing you and closer to the bottom. The two antenna ports are located on the rear panel, closer to the top of the Zyxel Device.

Figure 19   Rear Panel (Nebula FWA505)
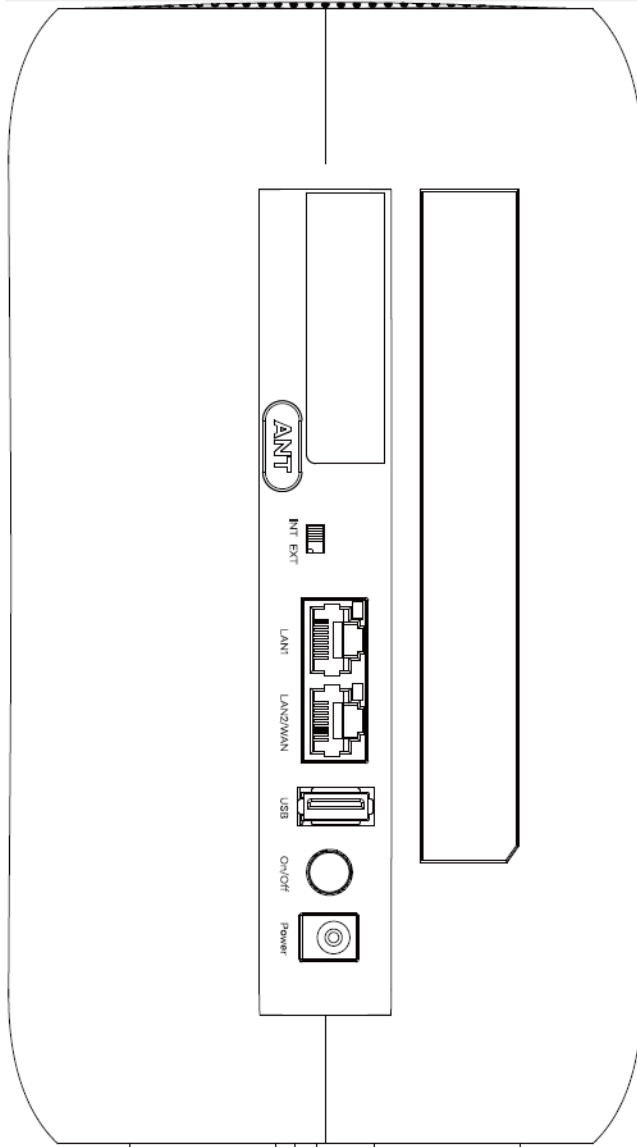
The WPS and WiFi On/Off button is on the front panel of the Zyxel Device, further from you, near the bottom.

Figure 20 WPS and WiFi On/Off Button on the Front Panel (FWA505)

The Micro SIM card slot is at the bottom of the Zyxel Device.

Figure 21 Micro SIM card slot on the Bottom Panel (FWA505)
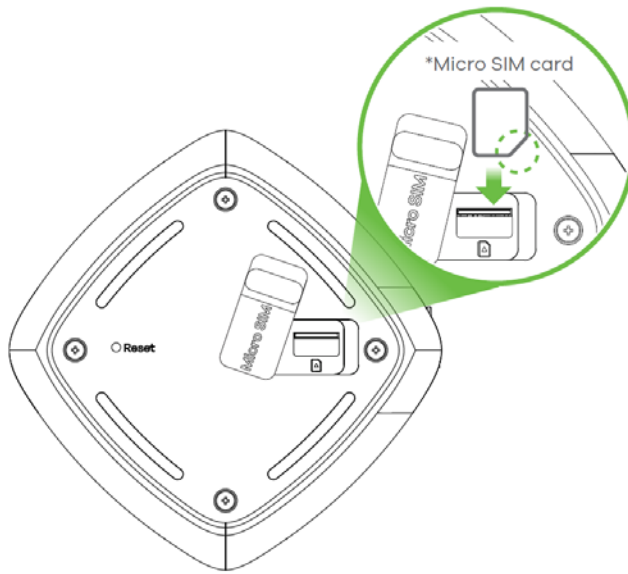
The following table describes the ports and buttons on your Zyxel Device.

Table 13   Panel Ports and Buttons (Nebula FWA505)

LABELS	DESCRIPTION
ANT1-ANT2/Antenna	Install the external antennas to strengthen the cellular signal. Note: To use the external antennas, you must set the **INT/EXT** switch to **EXT**.
INT/EXT	Select between the internal or external cellular antennas.
LAN1	Connect a computer to the LAN using an RJ45 cable.
LAN2/WAN	LAN mode: Connect a computer to the LAN using an RJ45 cable. WAN mode: Connect the Zyxel Device to the Internet through the WAN.

Table 13   Panel Ports and Buttons (Nebula FWA505) (continued)

LABELS	DESCRIPTION
USB	The USB port of the Zyxel Device is used for file sharing.
ON/OFF	Press the **ON/OFF** button after the power adapter is connected to start the Zyxel Device.
POWER	Connect the power adapter and press the **ON/OFF** button to start the Zyxel Device.
WiFi/WPS	Press the WiFi/WPS button to activate WPS connection process. See Section 2.4 on page 46 for more information.
RESET	Press the **RESET** button to reboot or reset the Zyxel Device. See Section 2.5 on page 49 for more information.
Micro SIM	Insert a Micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.

Nebula FWA510

Place the Zyxel Device with the ports facing you and closer to the bottom. The two antenna ports are located on the rear panel, closer to the top of the Zyxel Device.

Figure 22   Rear Panel (Nebula FWA510)

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

Figure 23 WiFi / WPS on the Front Panel (Nebula FWA510)

The Micro SIM card slot and RESET button are on the bottom of the Zyxel Device.

Figure 24 Micro SIM card slot and RESET button on the bottom panel (Nebula FWA510)
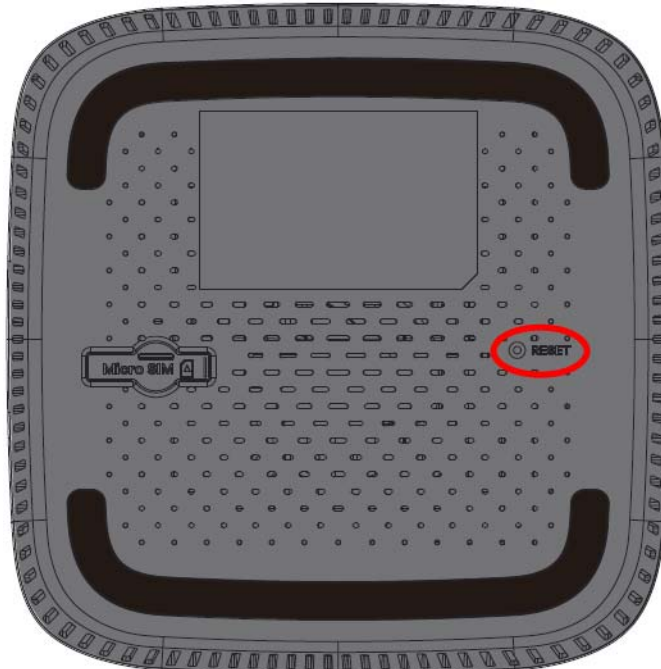
The following table describes the ports and buttons on your Zyxel Device.

Table 14   Panel Ports and Buttons (Nebula FWA510)

LABELS	DESCRIPTION
ANT1-ANT2/Antenna	Install the external antennas to strengthen the cellular signal. Note: To use the external antennas, you must set the **INT/EXT** switch to **EXT**.
USB	The USB port of the Zyxel Device is used for file sharing.

Table 14   Panel Ports and Buttons (Nebula FWA510) (continued)

LABELS	DESCRIPTION
LAN2/WAN	LAN mode: Connect a computer to the LAN using an RJ45 cable. WAN mode: Connect the Zyxel Device to the Internet through the WAN.
LAN1	Connect a computer to the LAN using an RJ45 cable.
WiFi/WPS	Press the WiFi/WPS button to activate WPS connection process. See Section 2.4 on page 46 for more information.
RESET	Press the **RESET** button to reboot or reset the Zyxel Device. See Section 2.5 on page 49 for more information.
ON/OFF	Press the **ON/OFF** button after the power adapter is connected to start the Zyxel Device.
POWER	Connect the power adapter and press the **ON/OFF** button to start the Zyxel Device.
Micro SIM	Insert a Micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.
INT/EXT	Select between the internal or external cellular antennas.

Nebula LTE7461-M602

Place the Zyxel Device with the ports facing you.

Figure 25   Bottom Panel (Nebula LTE7461-M602)

The following table describes the ports and buttons on your Zyxel Device.

Table 15   Panel Ports and Buttons (Nebula LTE7461-M602)

LABELS	DESCRIPTION
LAN (PoE)	Connect a computer through the PoE injector for configuration. Connect the PoE injector to a power outlet to start the device.
WiFi	Press the WLAN (WiFi) button for more than 5 seconds to enable WiFi.
WPS	After WiFi is enabled, press the WLAN button for more than one second but less than 5 seconds to quickly set up a secure WiFi connection between the Zyxel Device and a WPS-compatible client.
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
Micro SIM	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.

Nebula NR7101

Place the Zyxel Device with the ports facing you.

Figure 26 Bottom Panel (Nebula NR7101)
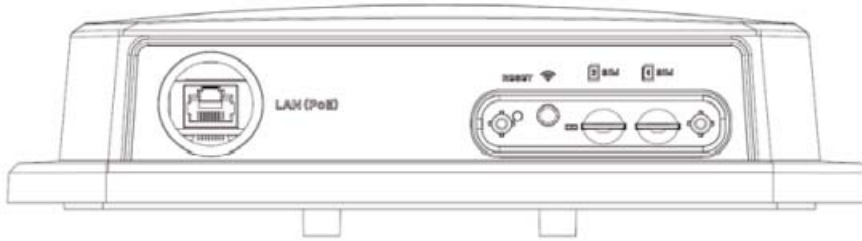
The following table describes the ports and buttons on your Zyxel Device.

Table 16   Panel Ports and Buttons (Nebula NR7101)

LABELS	DESCRIPTION
LAN (PoE)	Connect the PoE port on the PoE injector to the Zyxel Device's LAN port through an Ethernet cable. Connect the LAN port on the PoE injector to your computer's RJ45 port through another Ethernet cable.
RESET	Press the **RESET** button to reboot or reset the Zyxel Device. See Section 2.5 on page 49 for more information.
WiFi/WPS	Press the WiFi/WPS button to activate WPS connection process. See Section 2.4 on page 46 for more information.
SIM 1/2	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.

Nebula FWA710

Place the Zyxel Device with the ports facing you.

Figure 27 Bottom Panel (Nebula FWA710)
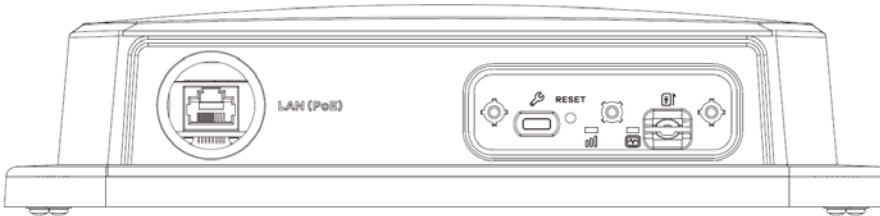
The following table describes the ports and buttons on your Zyxel Device.

Table 17   Panel Ports and Buttons (Nebula FWA710)

LABELS	DESCRIPTION
LAN (PoE)	Connect the PoE port on the PoE injector to the Zyxel Device's LAN port through an Ethernet cable. Connect the LAN port on the PoE injector to your computer's RJ45 port through another Ethernet cable.
RESET	Press the **RESET** button to reboot or reset the Zyxel Device. See Section 2.5 on page 49 for more information.
Micro SIM	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.

2.4 WiFi/WPS Button

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

Follow the steps below to activate WiFi or WPS on the Zyxel Device.

Activating WiFi

1 Make sure the power is on.

2 Press the WiFi/WPS button (see the following table) then release it.

Table 18   How to Enable WiFi

MODELS	WIFI BUTTON PRESS HOLD TIME
Nebula LTE3301-PLUS	More than 5 seconds.
Nebula LTE7461-M602	
Nebula NR7101	
Nebula NR5101	Press for 1 second.
Nebula FWA505	More than 10 seconds.
Nebula FWA510	WiFi can only be enabled/ disabled through the Web Configurator.

3 Check the WiFi LED to see if the WiFi is successfully turned on. See Section 2.2 on page 28 for your Zyxel Device LED behavior.

Activating WPS

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

1 Ensure WiFi is turned on.

2 Press the WiFi/WPS button (see the following table) then release it.

Table 19   How to Enable WPS

MODELS	WIFI BUTTON PRESS HOLD TIME
Nebula LTE3301-PLUS	More than 1 second but less than 5 seconds
Nebula LTE7461-M602	
Nebula NR7101	
Nebula NR5101	More than 5 seconds.
Nebula FWA505	More than 3 seconds.
Nebula FWA510	

3 Press the WPS button on another WPS-enabled device within range of the Zyxel Device (within 120 seconds).

4 Once the connection is successfully made, check the LED for connection status. See Section 2.2 on page 28 for the Zyxel Device LED behavior.

For Nebula LTE3301-PLUS, the WiFi / WPS button is on the front panel of the Zyxel Device, closer to the right, with the ports positioned farther from you.

Figure 28   Nebula LTE3301-PLUS WiFI/WPS Button

For Nebula LTE7461-M602, the WiFi / WPS button is on the rear panel of the Zyxel Device, closer to the right, with the ports facing you.

Figure 29   Nebula LTE7461-M602

For Nebula NR5101, the WPS and WiFi On/Off button is on the top of the Zyxel Device.

Figure 30   Nebula NR5101 WiFi/WPS Button
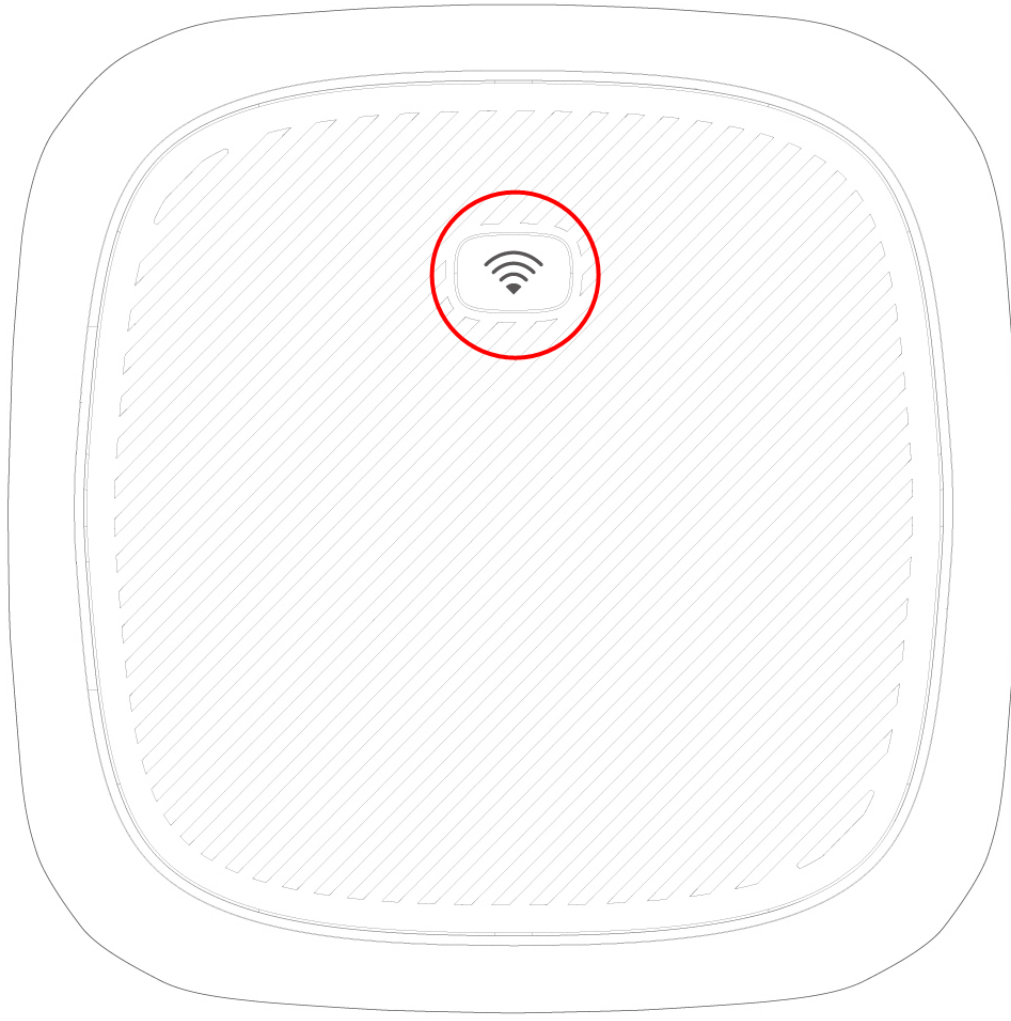
For Nebula NR7101, the WPS and WiFi On/Off button is on the bottom of the Zyxel Device.

Figure 31   Nebula NR7101 WiFi/WPS Button
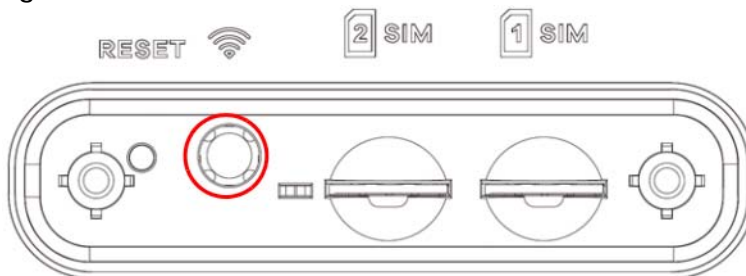
For Nebula FWA505, the WPS and WiFi On/Off button is on the front panel of the Zyxel Device.

Figure 32   Nebula FWA505 WiFi/WPS Button

For Nebula FWA510, the WPS and WiFi On/Off button is on the front panel of the Zyxel Device.

Figure 33   Nebula FWA510 WiFi/WPS Button

2.5 RESET Button

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

Figure 34 Nebula LTE3301-PLUS
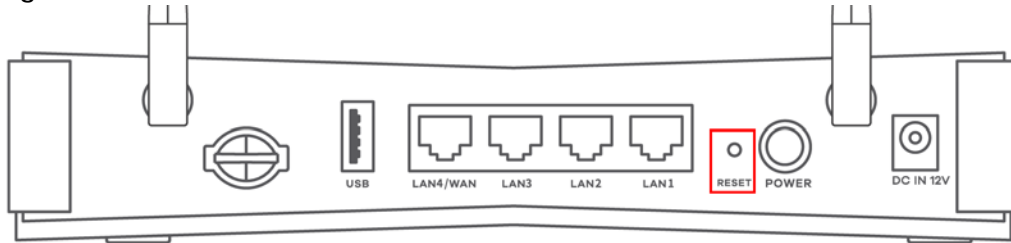
Figure 35 Nebula LTE7461-M602

Figure 36 Nebula NR5101
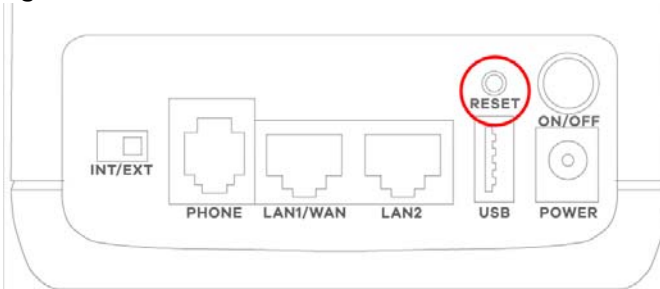
Figure 37 Nebula NR7101
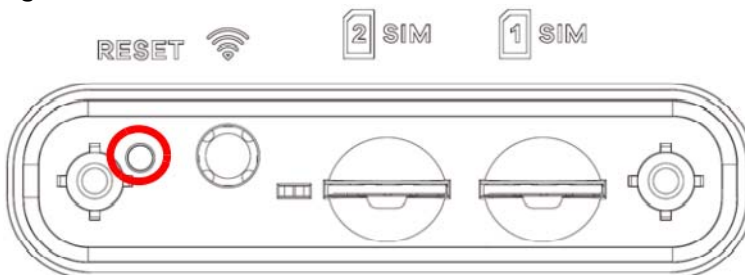
Figure 38 Nebula FWA505
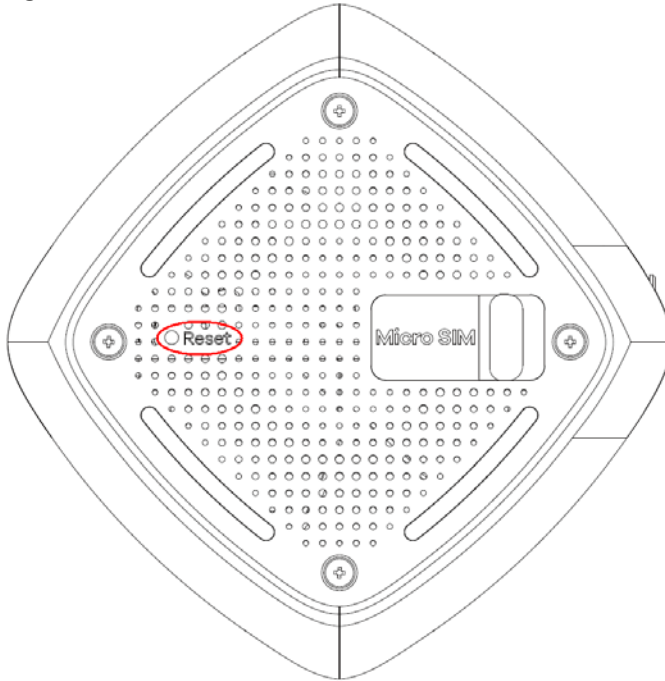
Figure 39 Nebula FWA510
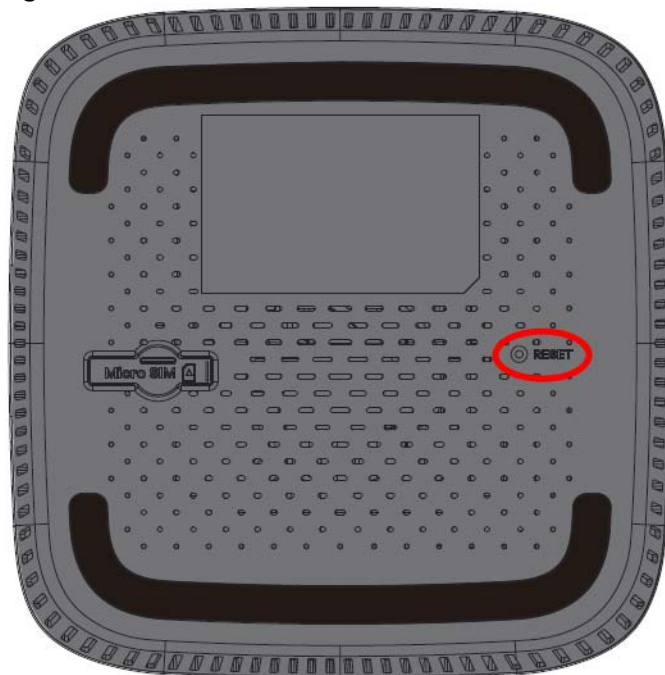
Figure 40 Nebula FWA710
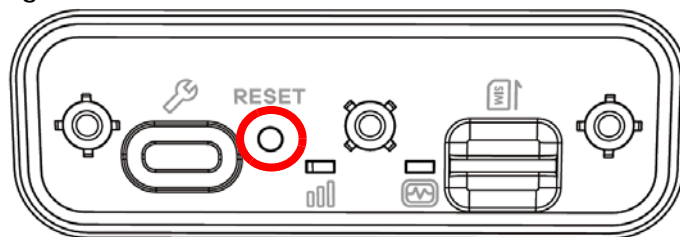
1 Make sure the Zyxel Device is connected to power and the **POWER** LED is on.

2 Using a thin object, press the **RESET** button for more than 5 seconds.

Note: If you press the **RESET** button for less than 5 seconds, the Zyxel Device will reboot.

CHAPTER 3
Web Configurator

3.1 Overview

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

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

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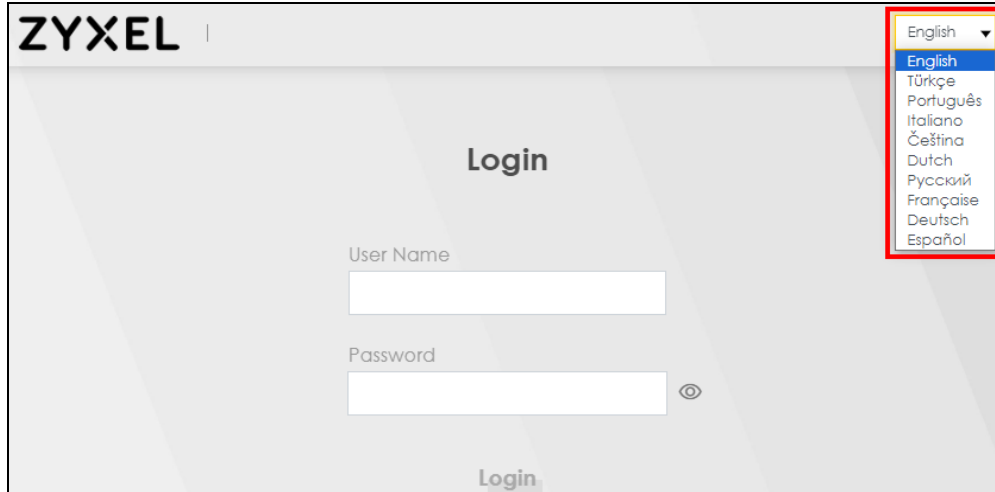
3.1.1 Access the Web Configurator

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

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

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

4 If a "Your connection is not private" message appears, click **Advanced**, then click **Proceed to 192.168.1.1(unsafe)** to go to the login screen.
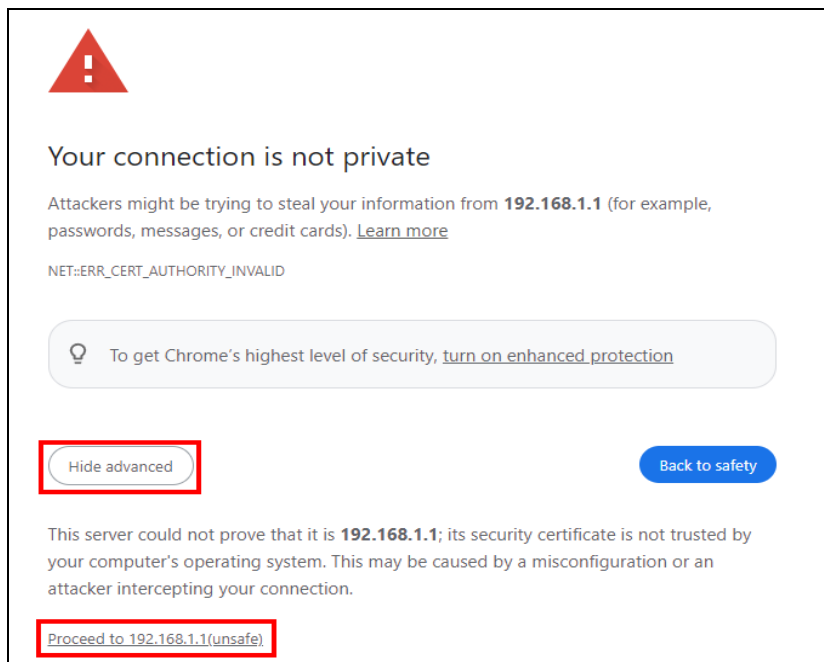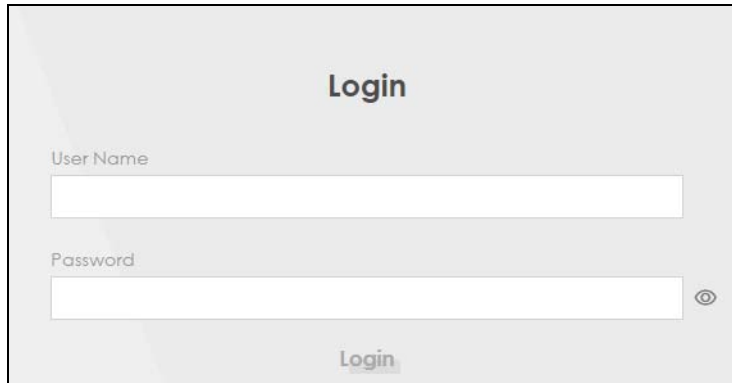
Note: If you see this warning page, it indicates that your browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to 192.168.1.1.
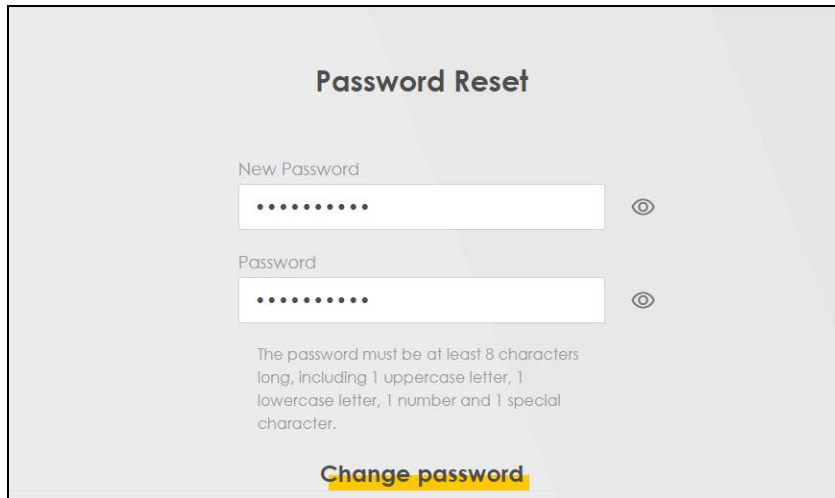
5 A login screen displays. Select the language you prefer (upper right).

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

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

Password Reset

New Password

⬤⬤⬤⬤⬤⬤⬤⬤⬤   👁
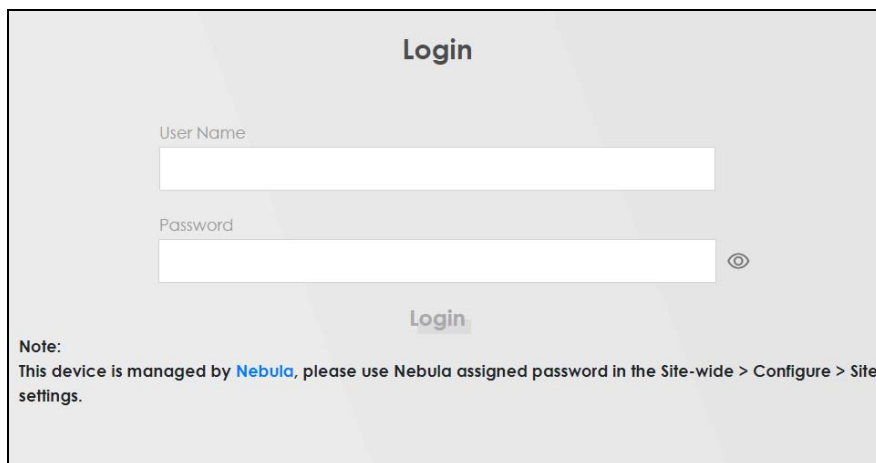
Password

⬤⬤⬤⬤⬤⬤⬤⬤⬤   👁

The password must be at least 8 characters long, including 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character.

Change password

When the Zyxel Device is managed by NCC, you will be prompted to use the Nebula-assigned password to log in. The Nebula-assigned password can be found in Nebula Web Portal: **Site-wide** > **Configure** > **Site settings**: **Device configuration**.

Login

User Name

Password   👁

Login

Note:
This device is managed by Nebula, please use Nebula assigned password in the Site-wide > Configure > Site settings.

7   The **Connection Status** screen appears. Use this screen to configure basic Internet access and WiFi settings.
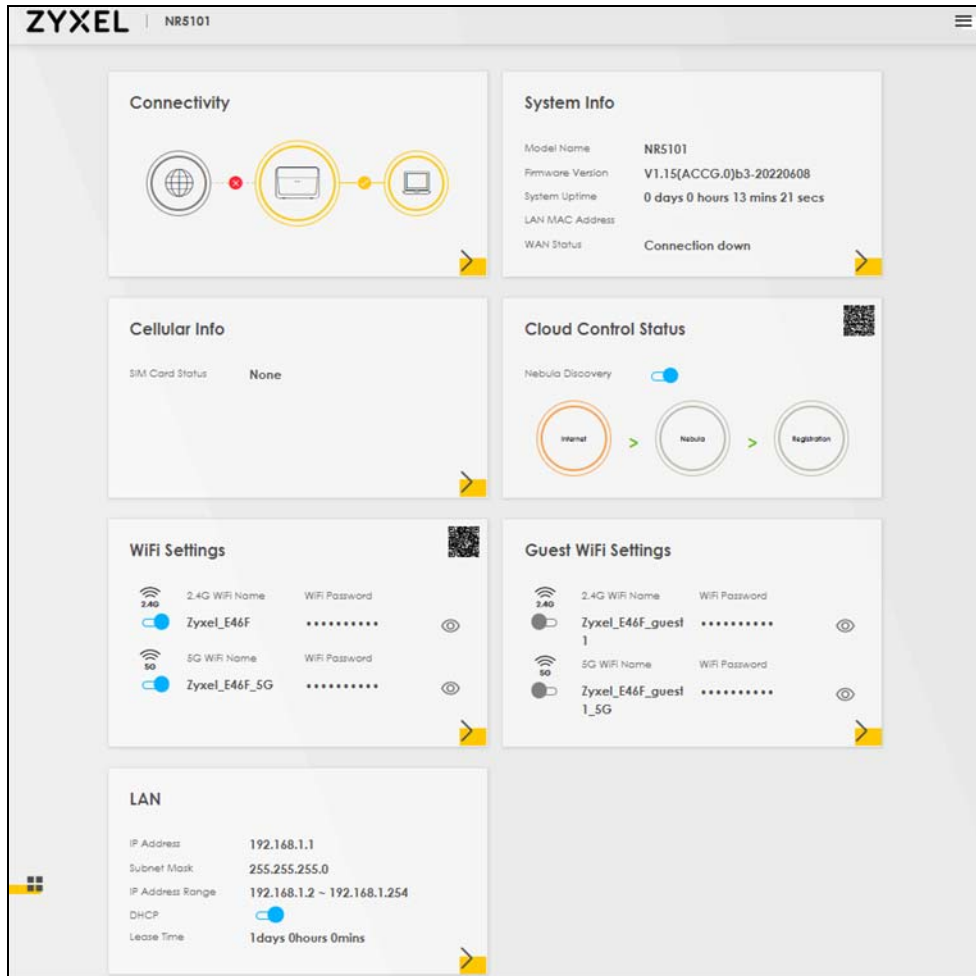
3.2 Web Configurator Layout

Figure 41   Screen Layout
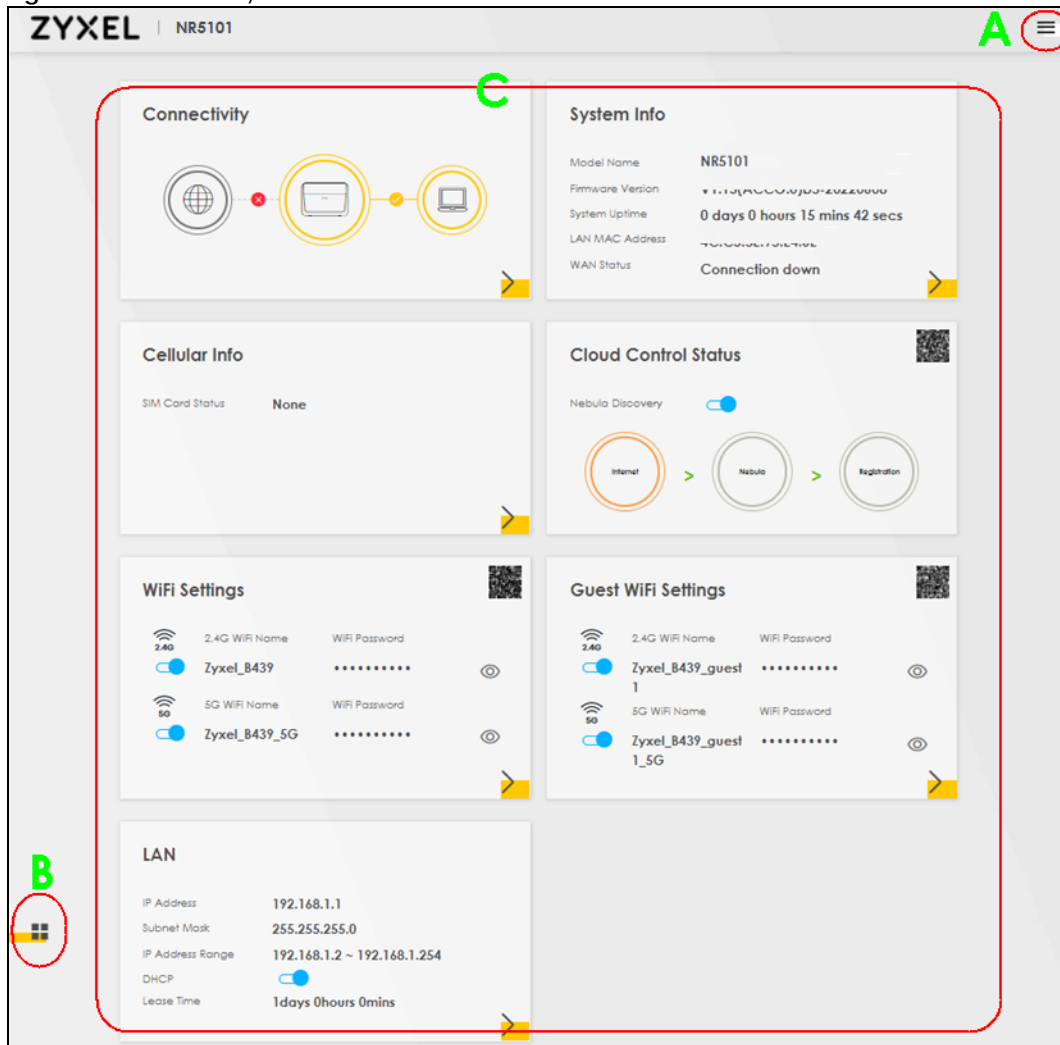
As illustrated above, the main screen is divided into these parts:

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

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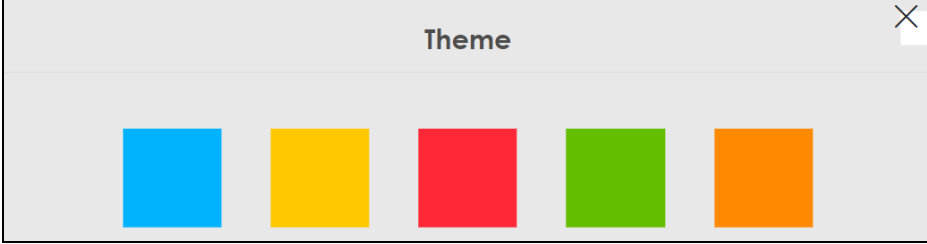
Click this icon (☰) to see the side bar and navigation panel.

3.2.1.1 Side Bar

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

The icons provide the following functions.

Table 20   Web Configurator Icons in the Title Bar

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

3.2.1.2 Navigation Panel

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

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

Figure 42 Navigation Panel
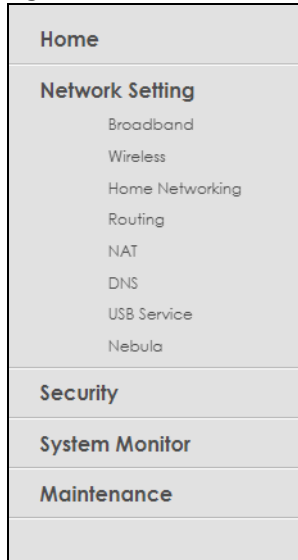
Table 21   Navigation Panel Summary

LINK	TAB	FUNCTION
Home		Use this screen to configure basic Internet access and wireless settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
	Ethernet WAN	Use this screen to convert the LAN port as WAN port, or restore the WAN port to LAN port.
	Cellular WAN	Use this screen to configure a cellular WAN connection.
	Cellular APN	Use this screen to configure the Access Point Name (APN) provided by your service provider.
	Cellular SIM	Use this screen to enter a PIN for your SIM card to prevent others from using it.
	Cellular Band	Use this screen to configure the cellular frequency bands that can be used for Internet access as provided by your service provider.
	Cellular PLMN	Use this screen to view available PLMNs and select your preferred network.
	Cellular IP Passthrough	Use this screen to enable IP Passthrough on the Zyxel Device.
	Cellular Lock (LTE)	Use this screen to enable or disable PCI Lock for 4G LTE connections.
	Cellular Lock (5G)	Use this screen to enable or disable PCI Lock for 5G NR connections.
	Cellular SMS	Use this screen to enable SMS Inbox and receive SMS messages.
Wireless	General	Use this screen to configure the WiFi settings and WiFi authentication or security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the Zyxel Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.

Table 21   Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced WiFi settings.
	WLAN Scheduler	Use this screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces.
	Channel Status	Use this screen to scan WiFi 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.
	Custom DHCP	Use this screen to configure additional DHCP options.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers.
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable the ALGs (Application Layer Gateways) in the Zyxel Device to allow applications to operate through NAT.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
USB Service	USB Service	Use this screen to enable file sharing through the Zyxel Device.
VLAN Group	VLAN Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to map a port to create multiple networks on the Zyxel Device.
Nebula	Nebula	Use this screen to enable **Nebula Discovery** and configure proxy server settings.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Parental Control	Parental Control	Use this screen to define time periods and days during which the Zyxel Device performs parental control and/or block web sites with the specific URL.

Table 21   Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.
	Security Log	Use this screen to view all security related events. You can select the level and category of the security events in their proper drop-down list window. Levels include: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: • Account • Attack • Firewall • MAC Filter
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the Zyxel Device.
WLAN Station Status	WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the Zyxel Device's WiFi.
Cellular WAN Status	Cellular WAN Status	Use this screen to look at the cellular Internet connection status.
Maintenance		
System	System	Use this screen to set the Zyxel Device name and Domain name.
User Account	User Account	Use this screen to change the user password on the Zyxel Device.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** screen.
	MGMT Services for IP Passthrough	Use this screen to enable various approaches to access this Zyxel Device remotely from a WAN and/or LAN connection.
	Trust Domain for IP Passthrough	Use this screen to enable public IP addresses to access this Zyxel Device remotely from a WAN and/or LAN connection.
TR-069 Client	TR-069 Client	Use this screen to configure your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.

Table 21   Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Time	Time	Use this screen to change your Zyxel Device's time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Setting	Log 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.
	Module Upgrade	Use this screen to upload the module firmware to your Zyxel Device.
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 43   Navigation Panel
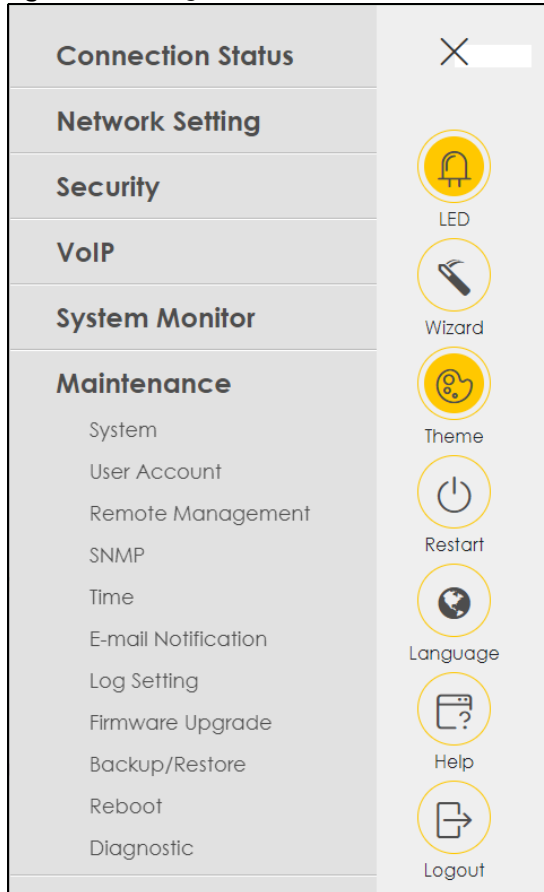
3.2.2 Widget Icon

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

Figure 44   Check Icon
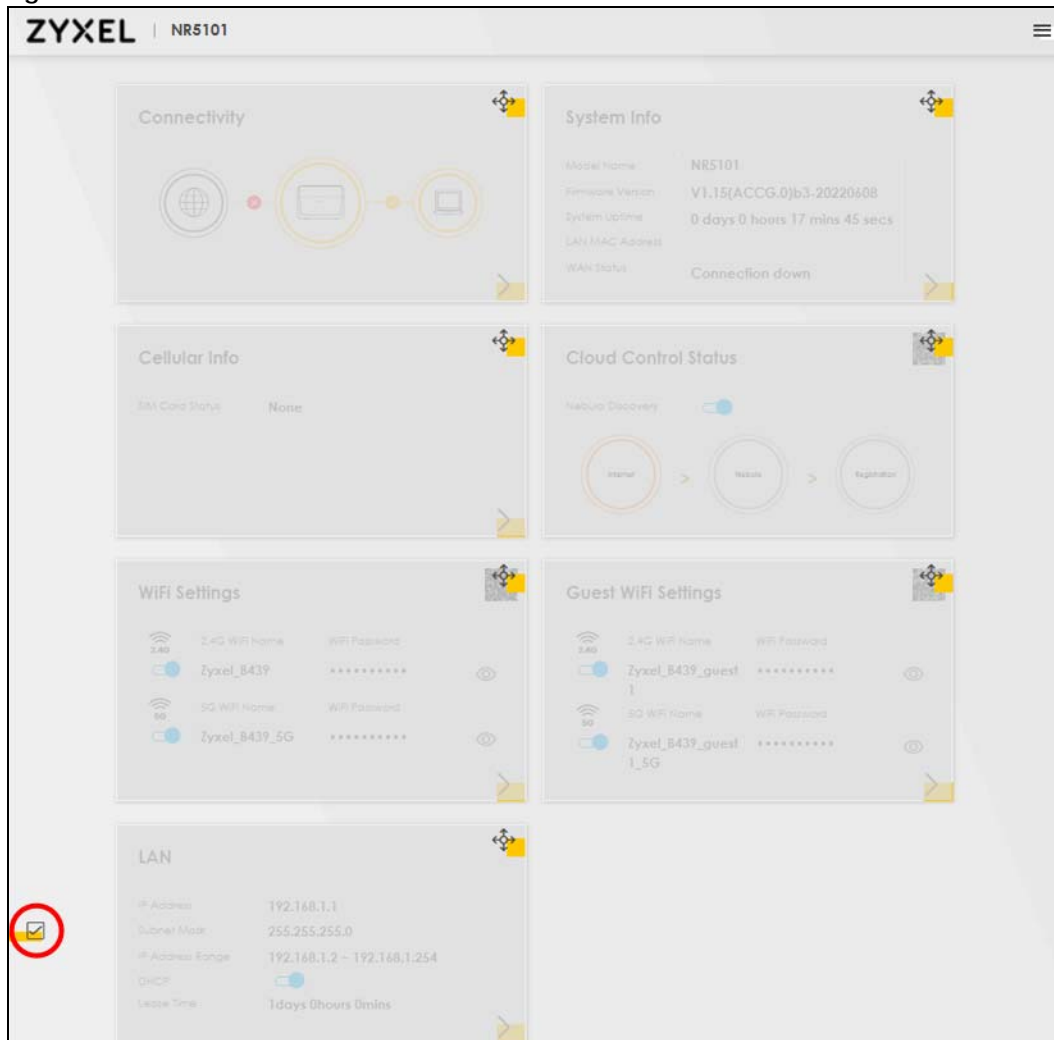
CHAPTER 4
Quick Start

4.1 Quick Start Overview

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

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

4.2 Quick Start Setup

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

Figure 45   Wizard – Home
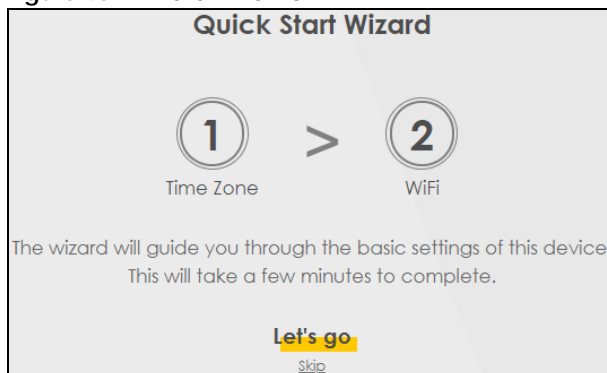
4.3 Quick Start Setup – Time Zone

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

Figure 46 Wizard – Time Zone

4.4 Quick Start Setup – WiFi

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

Select **Keep 2.4G and 5G the same** to use the same SSID for 2.4G and 5G WiFi networks. Otherwise, clear the checkbox to have two different SSIDs for 2.4G and 5G WiFi networks. The screen and fields to enter may vary when you select or clear the checkbox.

Figure 47 Wizard – WiFi

Note: Only the Nebula LTE3301-PLUS supports the **Country** feature.

Note: You can also enable the wireless service using any of the following methods:
Click **Network Setting** > **Wireless** to open the **General** screen. Then select **Enable** in the **WiFi** field. Or, press the **WiFi ON/OFF** button for more than 5 seconds.

4.5 Quick Start Setup – Finish

Your Zyxel Device saves and applies your settings.

CHAPTER 5
Web Interface Tutorials

5.1 Web Interface Overview

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

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

5.1.1 Unlock the SIM Card

This section shows you how to unlock the SIM card if the SIM card you insert into the Zyxel Device has PIN code protection.

1 When you access the Web Configurator **Home** screen, a warning message will appear. Click **OK**. If you accidentally close the message, go to **Network Setting** > **Broadband** > **Cellular SIM**.
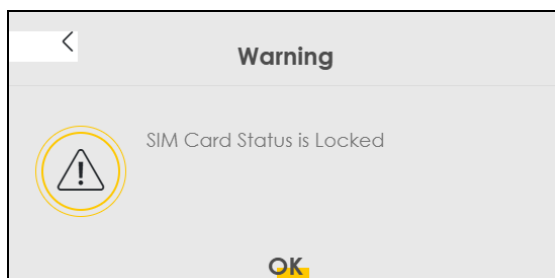
2 Enter the 4-digit PIN code (0000 for example) provided by your ISP in the **PIN** field.

Note: If you enter the PIN code incorrectly too many times, the SIM card will be blocked. You can check the remaining times from **Attempts remaining**. See Section 5.1.2 on page 68 to unlock the SIM card.

3 To avoid unlocking the SIM card after each restart, slide the **Auto Unlock PIN** switch to the right to have the Zyxel Device automatically unlock the SIM card. Otherwise, slide the switch to the left, you will need to manually enter the PIN every time you restart the Zyxel Device or reinsert the SIM card.

4 Click **Apply**.

5.1.2 Unblock the SIM Card

This SIM card will be blocked if you enter the PIN code incorrectly too many times. Follow the steps below to unblock the SIM card.

1 Contact your ISP for the Personal Unblocking Key (PUK) code.

2 When you access the Web Configurator **Home** screen, a warning message will appear. Click **OK**. If you accidentally close the message, go to **Network Setting** > **Broadband** > **Cellular SIM**.
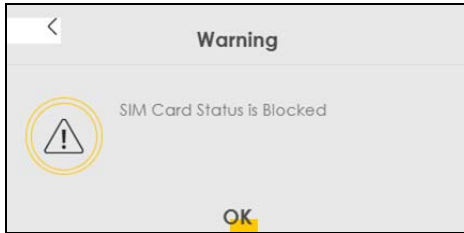
3 Enter the PUK code provided by your ISP in the **PUK** field.

Note: If you enter the PUK code incorrectly too many times, your SIM card will be permanently locked, and you will need a new SIM card. You can check the remaining times from **Attempts remaining**.

4 Set up a new PIN code by entering a 4-digit PIN code (0000 for example) in the **New PIN** field.

5 Click **Apply**.

5.2 Device Settings

This section shows you how to:

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

You can rename your device, and change the admin password.
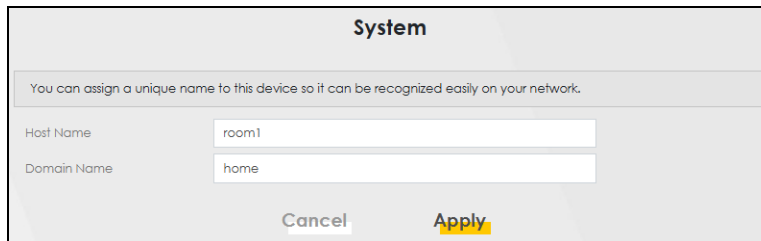
5.2.1 Rename Your Zyxel Device

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

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

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

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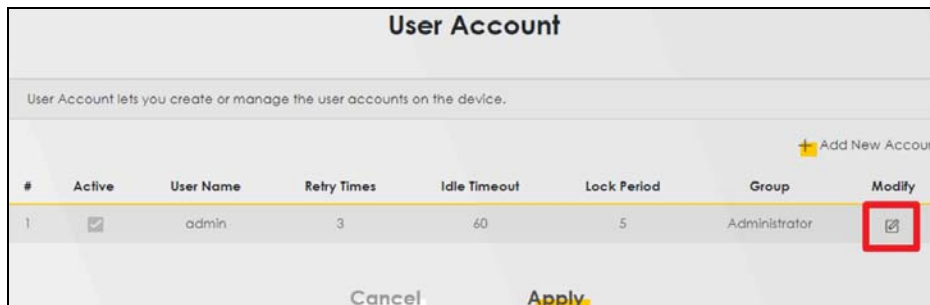
System

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

Host Name	room1
Domain Name	home

Cancel   **Apply**

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

5.2.2 Change the Admin Password

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

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

User Account

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

+ Add New Account

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

Cancel   **Apply**

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

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

5.2.3 Change the Management IP Address

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

1 Change your computer's IP address to the same subnet as the Zyxel Device. For example, if the default static IP address of the Zyxel Device is 192.168.1.1, set your computer IP address between 192.168.1.2 and 192.168.1.254.
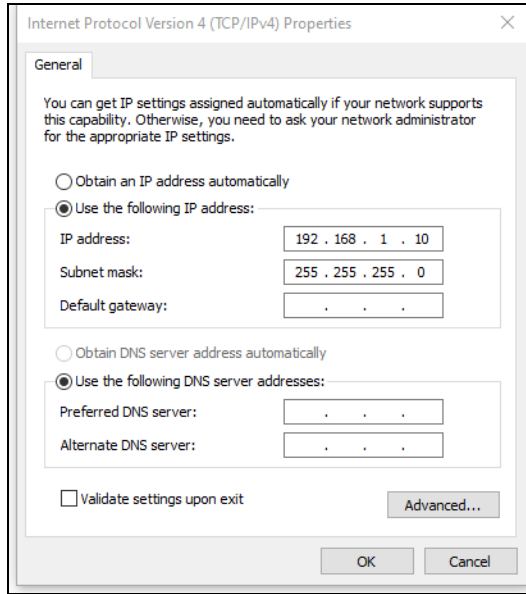
2 Log into the Zyxel Device using the default IP address "192.168.1.1". Go to **Network Setting** > **Home Networking**. Enter your preferred IPv4 address in the **IP Address** field. For example, "192.168.1.15". Click **Apply** and the Zyxel Device will disconnect from your computer due to the IP address change.

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

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

5.3 Wired Network Setup

This section shows you how to:

- *Set Up an Ethernet Connection*

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

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

5.3.1 Set Up an Ethernet Connection

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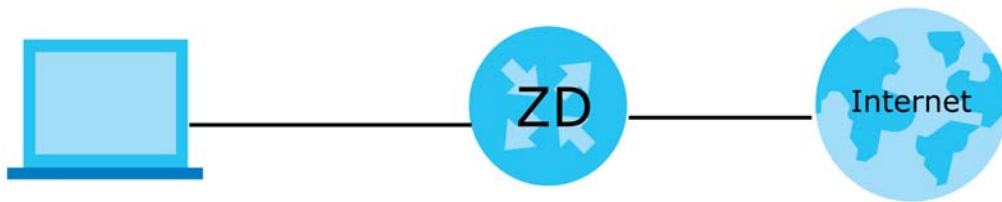
This example shows you how to configure an Ethernet WAN connection.

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

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

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	Y	Y	
2	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	Y	Y	
3	ETHWAN	ETH	Routing	IPoE	N/A	N/A	Y	Y	Y	Y	Y	

3   To set the Zyxel Device to **Routing** mode, see *Routing Mode on page 74*.
To set the Zyxel Device to **Bridge** mode, see *Bridge Mode on page 76*.

Routing Mode

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

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

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

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

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

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

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

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

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	My ETH Connecti	ETH	Routing	IPoE	N/A	N/A	Y	Y	Y	Y	N	✎ 🗑

Bridge Mode

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

General	
Name	My ETH Connection
Type	Ethernet
Connection Mode	Bridge

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

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

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

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

5.4 WiFi Network Setup

This section shows you how to:

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

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.

For NR Outdoor devices, the WiFi network if only for configuring the Zyxel Device. Remember to turn it off after all configurations are done.

Figure 48   WiFi Network Setup
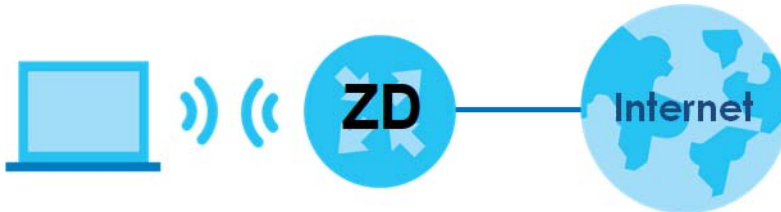
Figure 49   Zyxel Device Configuration through WiFi Connection

See the label on the Zyxel Device for the WiFi network settings and then connect manually to the Zyxel Device. Alternatively, you can connect to the Zyxel Device WiFi network using WPS. See Section 2.4 on page 31.

5.4.1 Change Security Settings on a WiFi Network

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

SSID	Example
Security Mode	WPA3-SAE/WPA2-PSK
Pre-Shared Key	Admin1234!!
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**.

Wireless

General   Guest/More AP   MAC Authentication   WPS   WMM   **Others**   Channel Status   MESH

The configurations below are the advanced wireless settings.

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

Cancel   Apply

You can now use the WPS feature to establish a WiFi connection between your notebook and the Zyxel Device (see Section 8.7 on page 176). Now use the new security settings to connect to the Internet through the Zyxel Device using WiFi.

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

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

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

5.4.2.1 WPS Push Button Configuration (PBC)

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

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

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

3 Log into the Zyxel Device's Web Configurator, and then go to the **Network Setting** > **Wireless** > **WPS** screen. Enable **WPS** and **Method 1 PBC**, click **Apply**, and then click the **WPS button**.
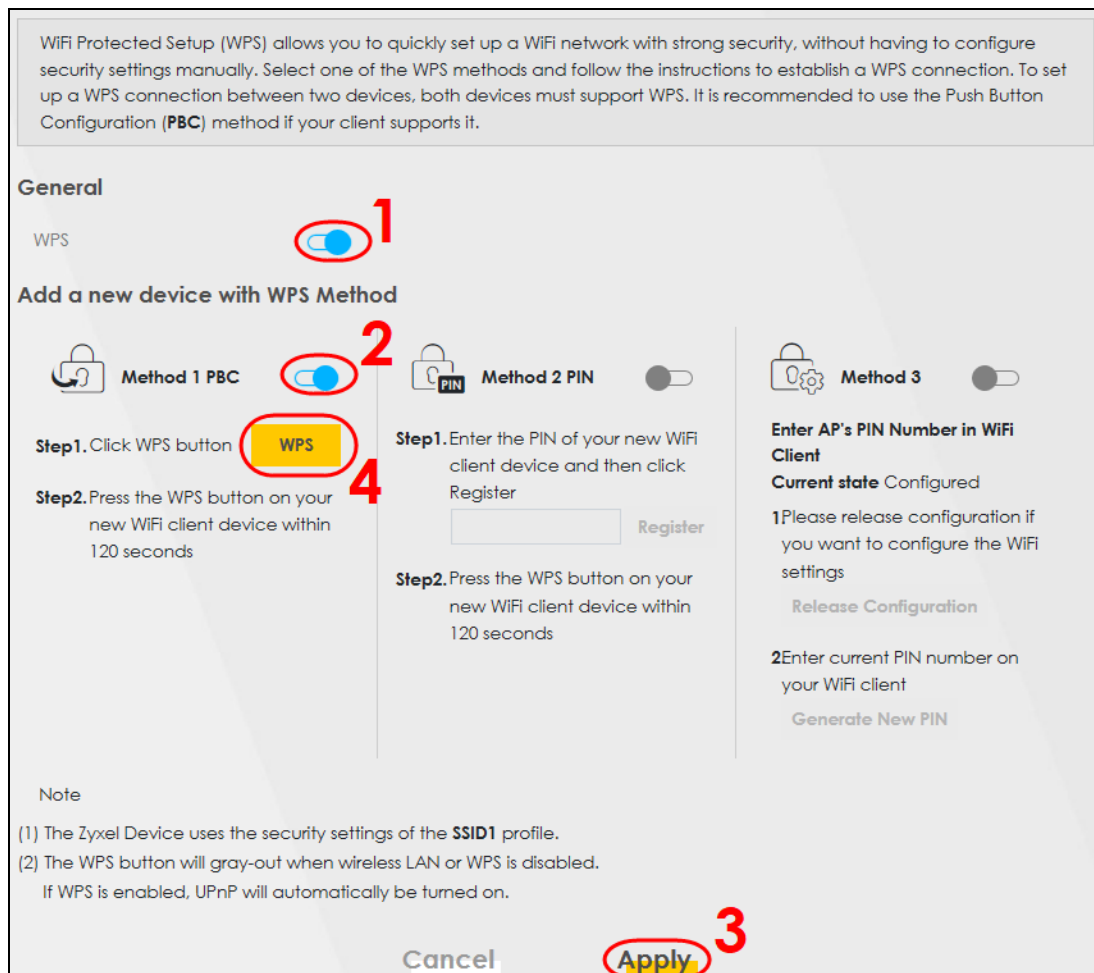
4 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.
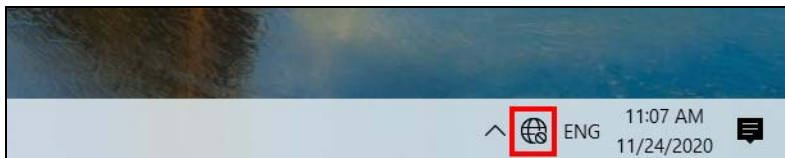
5 Locate the WiFi network of the Zyxel Device. The default WiFi network name is "Zyxel_XXXX" (2.4G) or "Zyxel_XXXX_5G" (5G). Then click **Connect**.
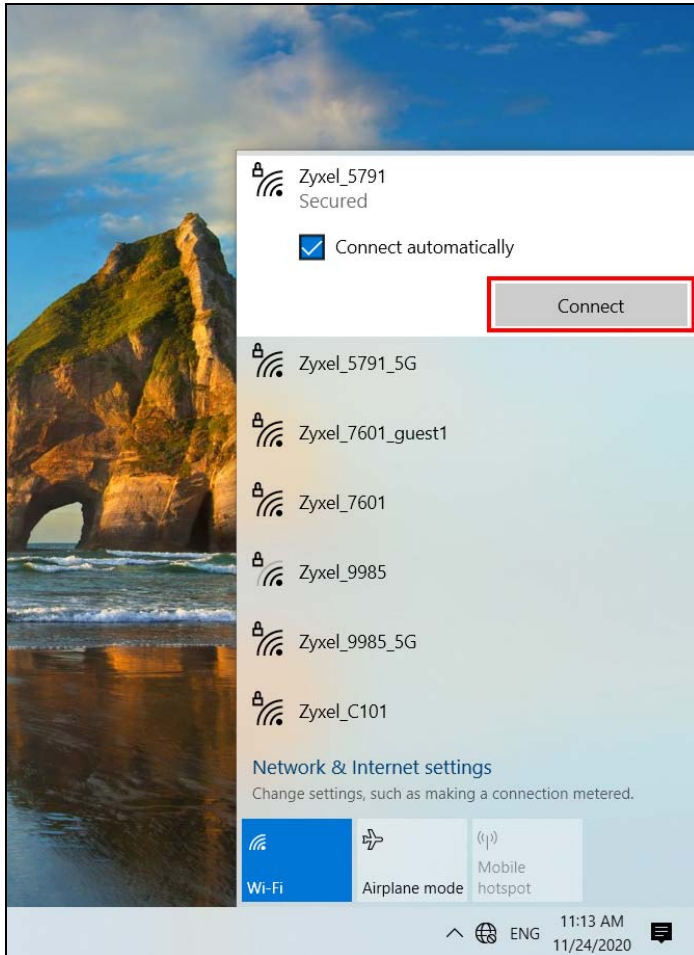
The Zyxel Device sends the WiFi network settings to Windows using WPS. Windows displays "Getting settings from the router".
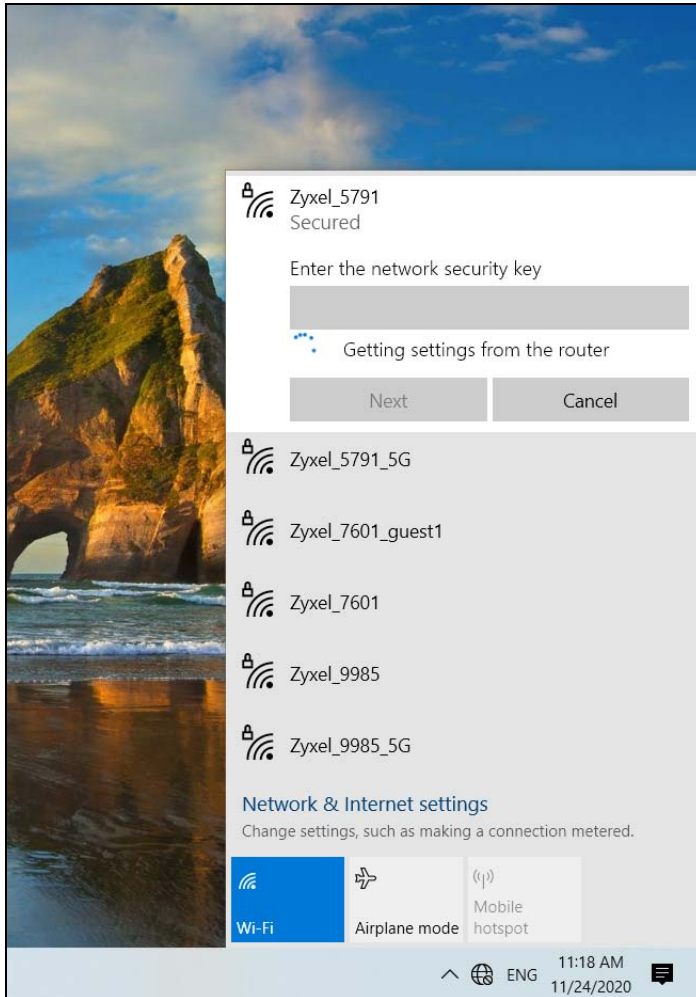
The WiFi device is then able to connect to the WiFi network securely.

5.4.2.2 WPS PIN Configuration

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

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

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

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

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

5.4.3 Set Up a Guest Network

The Zyxel Device authenticates the WiFi device using the PIN, and then sends the WiFi network settings to the device using WPS. This process may take up to 2 minutes. The WiFi device is then able to connect to the WiFi network securely. A company wants to create two WiFi networks for different groups of users as shown in the following figure. Each WiFi network has its own SSID and security mode. Both networks are accessible on both 2.4G and 5G WiFi bands.
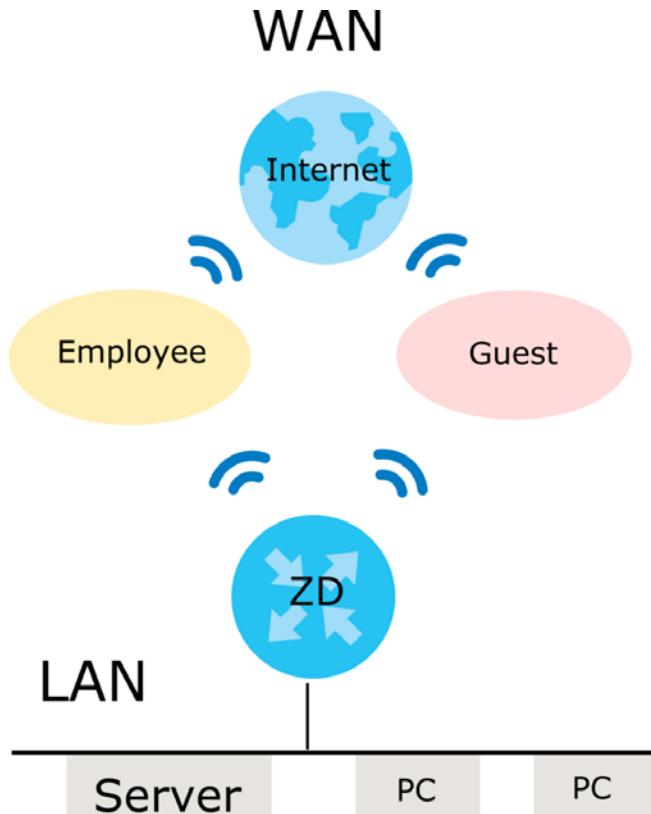
- Employees using the **General** WiFi network group will have access to the local network and the Internet.
- Visitors using the **Guest** WiFi network group with a different SSID and password will have access to the Internet only.

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

	GENERAL	GUEST
2.4/5G SSID	Example	Guest
Security Level	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK
Pre-Shared Key	ForCompanyOnly123!	Guest123456!

Go to the **Network Setting** > **Wireless** > **General** screen. Use this screen to set up the company's general WiFi network group. Configure the screen using the provided parameters and click **Apply**. Note that if you have employees using 2.4G 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.

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

WiFi

WiFi   ☑ Keep the same settings for 2.4G and 5G WiFi networks

WiFi Network Setup

Band   2.4GHz   ▼

WiFi   ⬤━

Channel   Auto   ▼   Current : 11 / 20 MHz

Bandwidth   20/40MHz   ▼

Control Sideband   Lower

WiFi Network Settings

WiFi Network Name   Zyxel_2830

Max Clients   32

☐ Hide SSID   ⓘ

☑ Multicast Forwarding

BSSID   D8:EC:E5:34:28:20

Security Level

            No Security   More Secure
                                                (Recommended)

Security Mode   WPA2-PSK   ▼

☑ Generate password automatically

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

Password   ••••••••••   👁

Strength   ─────────────────   strong

Cancel   **Apply**

---

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

General **Guest/More AP** MAC Authentication WPS WMM Others Channel Status MESH

This screen allows you to configure a guest wireless network that allows access to the Internet only through the Zyxel Device.

#	Status	SSID	Security	Guest WLAN	Modify
1	💡	Guest	WPA2-Personal	External Guest	✏

6 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**.

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

5.4.4 Set Up Two Guest WiFi Networks on Different WiFi Bands

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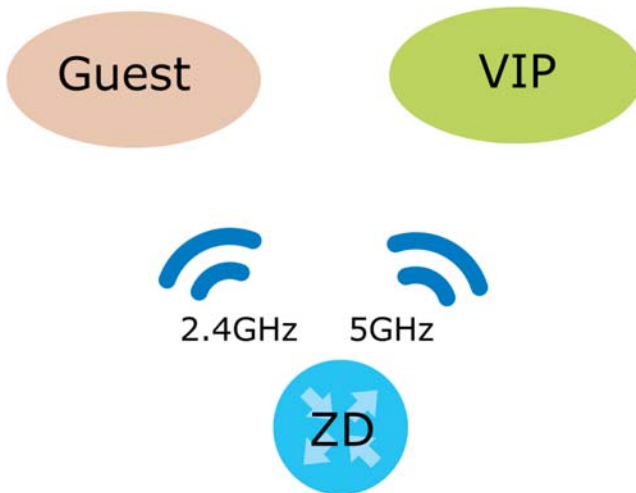
- The **Guest** group will use the 2.4G band.
- The **VIP** group will use the 5G band.

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

Table 22   WiFi Settings Parameters Example

BAND	2.4G	5G
SSID	Guest	VIP
Security Mode	WPA2-PSK	WPA2-PSK
Pre-Shared Key	Guest123456!	Zyxel1234@@!

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**.

More AP Edit

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

Wireless Network Setup

Wireless

Wireless Network Settings

Wireless Network Name   Guest

☐ Hide SSID

☑ Guest WLAN

Access Scenario   External Guest

Max. Upstream
Bandwidth   Kbps

Max. Downstream
Bandwidth   Kbps

Note

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

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

SSID Subnet

Security Level

No Security   More Secure
                                    (Recommended)

Security Mode   WPA2-PSK

Protected
Management Frames   Capable

☐ Generate password automatically

The password must be at least 8 characters long, including 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character, or 64 hexadecimal digits ("0-9", "A-F")

Password   Guest123456!

Strength   strong

Cancel   **OK**

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

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

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

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

5.4.5 Configure the Channel and Bandwidth for Each WiFi Band

For optimal WiFi network performance, you can change the bandwidth and channel for a specific band to improve the throughput and minimize the interference. You can refer to Table 23 on page 92 for the recommended setup.

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

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

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

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

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

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

Table 23   Recommended Application for Each Band

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

Table 23   Recommended Application for Each Band (continued)

BAND	BANDWIDTH	CHANNEL	APPLICATION
5 GHz	40 MHz	36, 40, 44, 48	HD streaming, online meetings
	80 MHz	36, 40, 44, 48 or 52-128	4K/8K streaming, multiplayer gaming

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

5.5 Cellular Network Setup

This section shows you how to:

- Set Up a Cellular Network Connection
- Set Up a Cellular APN Setting

5.5.1 Set Up a Cellular Network Connection

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

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

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

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

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

5.5.2 Set Up a Cellular APN Setting

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

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

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

- **APN Manual Mode**: Enable this to configure your APN cellular information manually.
- **APN**: Enter the Access Point Name (APN) provided by your ISP. You can enter a name up to 30 printable ASCII characters, including spaces.
- **Username**: Type the username provided by your ISP for authentication. The allowed username is up to 31 printable ASCII characters.

- **Password**: Type the password provided by your ISP for authentication. The allowed password is up to 31 printable ASCII characters.

- **Authentication Type**: Select the authentication type (**PAP**, **CHAP**, **PAP/CHAP**) used by the Zyxel Device.

- **PDP Type**: Select the IP address type (**IPv4**, **IPv6**, **IPv4/IPv6**) the Zyxel Device uses for connection.

- **IP Passthrough**: Enable this to turn off the routing functionality on the Zyxel Device.

- **Passthrough Mode**: Select **Fixed** to specify the MAC address of the computer using the public IP address provided by the ISP. Otherwise, select **Dynamic**.

- **Static Gateway Enable**: Select Enable to use a static IP address for your gateway.

- **Static Gateway Address**: Enter the IP address of your gateway.

- **Subnet mask Prefix**: Enter the subnet address of your gateway.

- **DHCP Lease Time**: Enter the lease time provided by your DHCP server.

5.6 USB Applications

This section shows you how to:

- Set Up File Sharing on Your Zyxel Device
- Access Your Shared Files From a Computer

5.6.1 File Sharing

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

5.6.1.1 Set Up File Sharing on Your Zyxel Device

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

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

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

USB Service

FileSharing MediaServer

The device can share Files from your USB flash drive or disk when you attach it to the USB port. You may Start from deciding which folders in the USB disks to share and which users can access the shared folders.

Information

Volume	Capacity	Used Space
usb1_sda1	0 MB	0 MB

Server Configuration

File Sharing Services

Share Directory List

➕ Add New Share

Active	Status	Share Name	Share Path	Share Description	Modify

Account Management

➕ Add New User

Status	User Name
⏳	admin

Cancel   Apply

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

USB Service

FileSharing MediaServer

The device can share Files from your USB flash drive or disk when you attach it to the USB port. You may Start from deciding which folders in the USB disks to share and which users can access the shared folders.

Information

Volume	Capacity	Used Space
usb1_sda1	0 MB	0 MB

Server Configuration

File Sharing Services ⬤

Share Directory List

＋ Add New Share

Active	Status	Share Name	Share Path	Share Description	Modify

Account Management

＋ Add New User

Status	User Name
⧗	admin

Cancel   **Apply**

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

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

Add New Share

Volume	usb1_sda1 ▼	
Share Path	BobShare	**Browse**
Description	Bob	
Access Level	Public ▼	

Cancel   **OK**

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

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

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

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

Account Management

➕ Add New User

Status	User Name
⧗	admin
⧗	Zyxel

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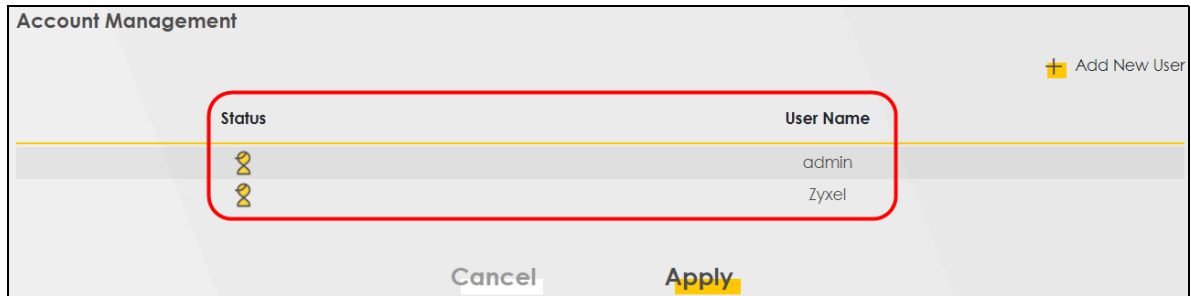
8 File sharing is now configured. You can see the USB storage device listed in the table below.

Share Directory List

➕ Add New Share

Active	Status	Share Name	Share Path	Share Description	Modify
☑	💡	BobShare	/mnt/usb1_sda1/BobShare	Bob	📝 🗑
☑	💡	JoshShare	/mnt/usb1_sda1/JoshShare	Josh	📝 🗑

5.6.1.2 Access Your Shared Files From a Computer

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

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

1 Open Windows Explorer.

2 In the Windows Explorer's address bar, enter a double backslash "\\" followed by the IP address of the Zyxel Device (the default IP address of the Zyxel Device is 192.168.1.1
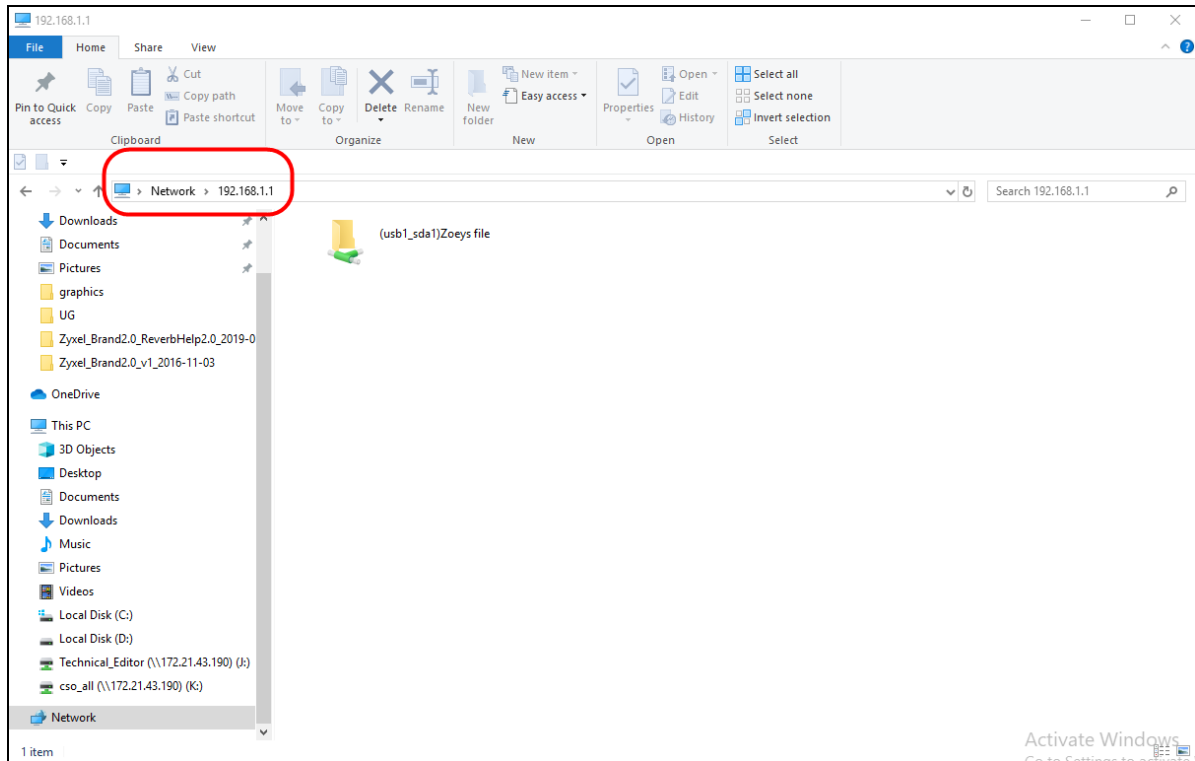
3 Double-click on **(usb1_sda)Zoeys file**, and then enter the share's username and password if prompted.

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

5.7 Network Security

This section shows you how to:

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

5.7.1 Configure a Firewall Rule

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

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

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

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

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

- **Filter Name**: Enter a name to identify the firewall rule.**Source IP Address**: Enter the IP address of the computer that initializes traffic for the application or service.

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

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

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

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

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

5.7.2 Set Up Parental Control

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

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

5.7.2.1 Configure Parental Control Schedule and Filter

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

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

Use this feature to:

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

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

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

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

Parental Control Screen

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

Add New PCP Screen

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

- Select **Enable** to enable the rule you are configuring.

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

- Select an user this rule applies to in **Home Network User**, then click **Add**. You will see the MAC address of the user you just select in **Rule List**.

2 Under **Internet Access Schedule**:

- Click **+ Add New Time** to add a second schedule.

- Use the parameter given above to configure the time settings of your schedule.

3 Under **Network Service**:

- In **Network Service Setting**, select **Block**.

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

4 Under **Site / URL Keyword**:

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

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

- Select **Redirect blocked site to Zyxel Family Safety page** to redirect the web browser to the Zyxel Family Safety page if he or she tries to access a website with the blocked URL keyword.

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

5.7.2.2 Configuring a Parental Control Schedule

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

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

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

1   Click **Add more Profile** to open the **Parental Control** screen.
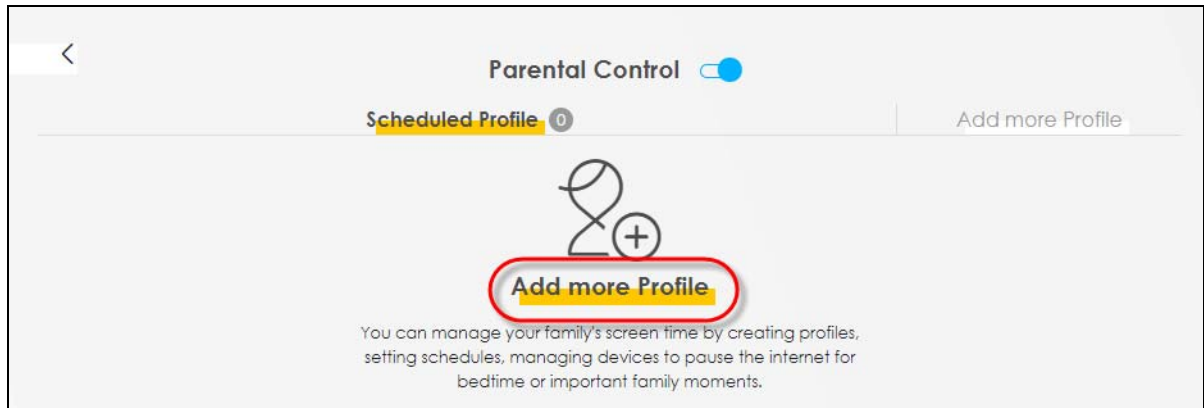
2   Use this screen to add a Parental Control rule.

- Enter the **Profile Name** given in the above parameter.

- Click on the switch to enable **Profile Active**.

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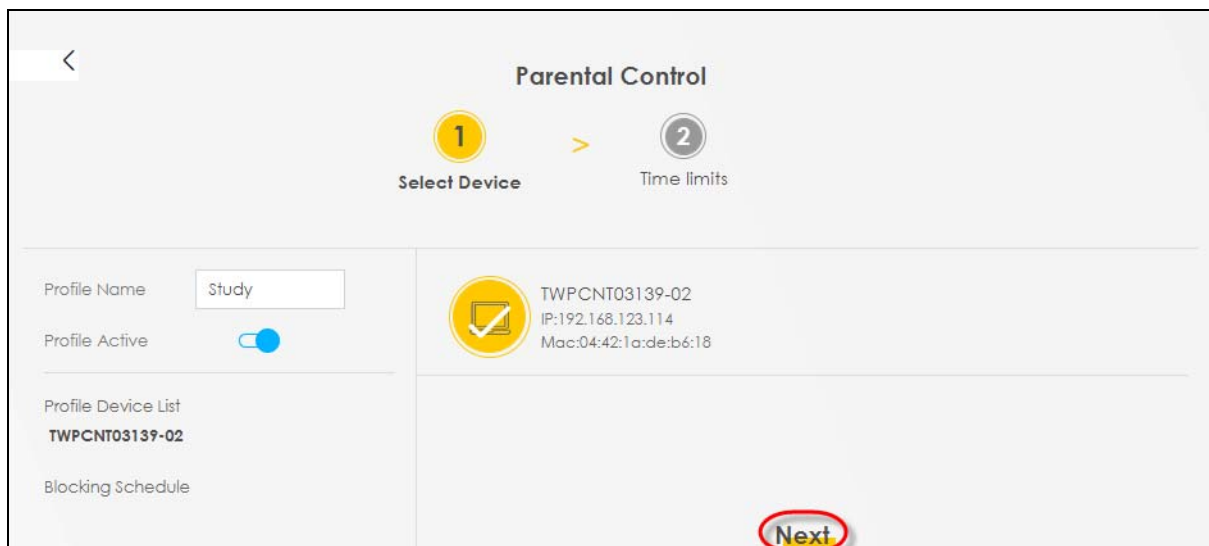
3   Use this screen to edit the Parental Control schedule.

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

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

- Click **Save** to save the settings.

5.7.3 Configure a MAC Address Filter for Wired LAN Connections

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

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

Figure 50   Configure a MAC Address Filter Example
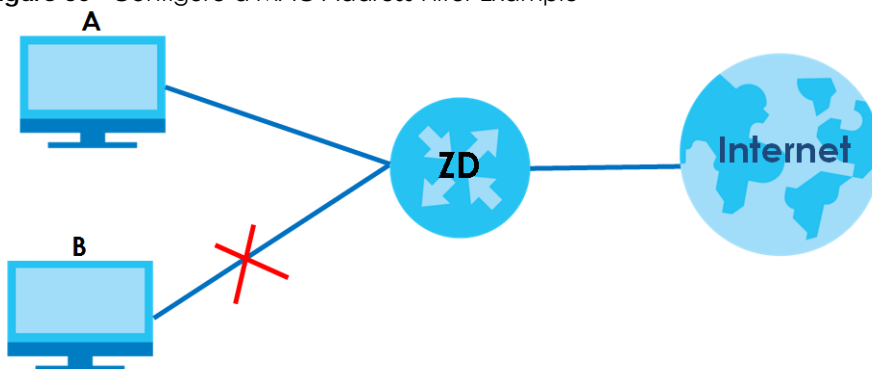
1   Go to the **Security** > **MAC Filter** > **MAC Filter** screen. Under **MAC Address Filter**, select **Enable**.

MAC Filter

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the LAN client to configure this screen.

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

| MAC Restrict Mode | ● Allow ○ Deny |

➕ Add New Rule

Set	Active	Host Name	MAC Address	Delete

📄 Note

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

Cancel   Apply

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

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

| MAC Restrict Mode | ○ Allow ● Deny |

➕ Add New Rule

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

Cancel   Apply

5.8 Device Maintenance

This section shows you how to:

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

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

5.8.1 Upgrade the Firmware

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

1 To download the latest firmware of your Zyxel Device, go to *https://www.zyxel.com/service-provider* and search for your model. The latest firmware will be available under the **Downloads & resources** tab. The model code for the Zyxel Device in this example is v5.13(ABLZ.1). Note the model code for your Zyxel Device.

2 Unzip the file.

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

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

Firmware Upgrade

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

Download the latest firmware file from the Zyxel website and upload it to your Zyxel Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the Zyxel Device will reboot.

Restore Partial Default Settings After Firmware Upgrade
Reset All Settings Except Mesh After Firmware Upgrade resets all your configurations, except for Mesh WiFi settings, to the factory defaults after firmware upgrade.

Upgrade Firmware

Reset All Settings After Firmware Upgrade	☐
Reset All Settings Except Mesh After Firmware Upgrade	☐
Current Firmware Version: V5.18(ACHN.0)b2	
File Path	Choose File No file chosen **Upload**

Upgrade WWAN Package

Current WWAN Package Version: 1.24	
File Path	Choose File No file chosen **Upload**

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

5.8.2 Back up the Device Configuration

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

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

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

Backup/Restore

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

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

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

Backup Configuration

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

Backup

Restore Configuration

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

File Path   Browse...   Upload

Back to Factory Default Settings

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

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

- LAN IP address will be 192.168.1.1

Do you want to save **Backup_Restore** (125 KB) from **192.168.1.1**?   Save ▼   Cancel   ✕

5.8.3 Restore the Device Configuration

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

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

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

Backup/Restore

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

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

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

Backup Configuration

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

Backup

Restore Configuration

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

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

Back to Factory Default Settings

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

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

- LAN IP address will be 192.168.1.1

- DHCP will be reset to default setting

Reset

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

5.8.4 How to Reset the Zyxel Device to the Factory Defaults

To reset the Zyxel Device, you can press the **RESET** button on the rear panel for more than 5 seconds. Alternatively, you can use the web configurator to reset the Zyxel Device.

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

Perform Mesh Full Factory Reset

Mesh Full Factory Reset allows you to clear the controller and agents' all user-entered configuration information and return to factory default settings. After resetting, the

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

- LAN IP address will be 192.168.1.1

- DHCP will be reset to default setting

Reset All Settings

Perform Mesh Partial Factory Reset

Mesh Partial Factory Reset allows you to keep certain user configurables while bringing the reset of the controller and agents to factory default setting.

- System will keep Wi-fi settings, include these user settings (Mesh Enable/Disable, Mesh Controller Mode, Mesh Backhaul information, Single SSID Enable/Disable, SSIDs, WPA keys, Encryption modes, 2.4GHz Enable/Disable, 5GHz Enable/Disable, Guest Wi-Fi Enable/Disable, Guest Wi-Fi isolation setting, 802.11 Mode, PMF setting)

Reset All Settings Except Mesh

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

5.9 Remote Access from WAN

This section shows you how to:

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

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

5.9.1 Configure Access to Your Zyxel Device

Perform the following to configure access to your Zyxel Device:

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

Remote Management

MGMT Services Trust Domain

Use this screen to configure the interfaces through which services can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device.

Service Control

WAN Interface used for services   ● Any_WAN ○ Multi_WAN

               ■ ETHWAN

Service	LAN	WLAN	WAN	Trust Domain	Port
HTTPS	☐ Enable	☐ Enable	☐ Enable	☐ Enable	443
FTP	☐ Enable	☐ Enable	☐ Enable	☐ Enable	21
TELNET	☐ Enable	☐ Enable	☐ Enable	☐ Enable	23
SSH	☐ Enable	☐ Enable	☐ Enable	☐ Enable	22
SNMP	☐ Enable	☐ Enable	☐ Enable	☐ Enable	161
PING	☐ Enable	☐ Enable	☐ Enable	☐ Enable	

Cancel   Apply

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

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

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

3   You may change the server **Port** number for a service if needed, however you must use the same port number in order to use that service for remote management.

5.9.2 Configure the Trust Domain

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

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

Remote Management

MGMT Services   **Trust Domain**

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the
Maintenance > Remote Management > MGMT Services screen.

➕ Add Trust Domain

IP Address   Delete

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

Add Trust Domain

Enter the IP address of the management station permitted to access the local management services. If specific
services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can
access the Zyxel Device from the WAN using the specified services.

IP Address   [/prefix length]

Cancel   OK

PART II
Technical Reference

CHAPTER 6
Connection Status

6.1 Connection Status Overview

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

6.1.1 Connectivity

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

Figure 51   Connectivity
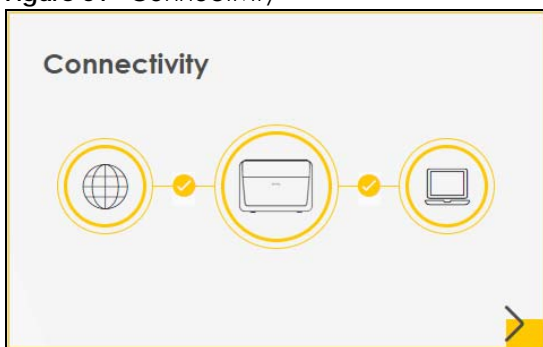
Click the Arrow icon ( ) to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

Figure 52   Connectivity: Connected Devices
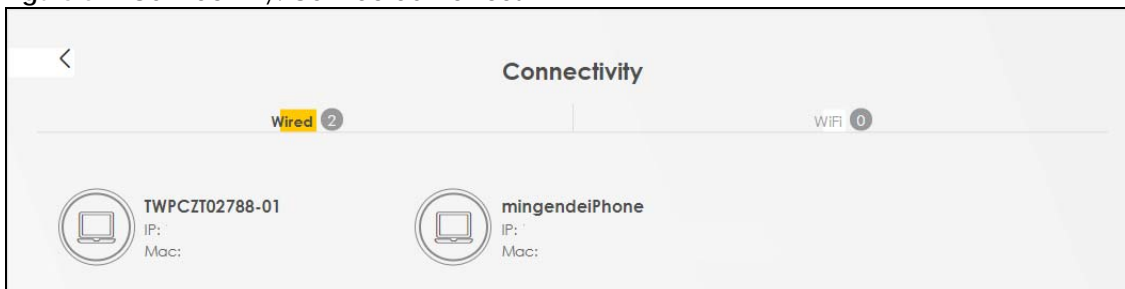
You can change the icon and name of a connected device. Place your mouse within the device block, and an Edit icon ( ) will appear. Click the Edit icon, and you will see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Click to enable ( ) **Internet Blocking** for a connected WiFi client.

6.1.2 Icon and Device Name

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

Figure 53   Connectivity: Edit
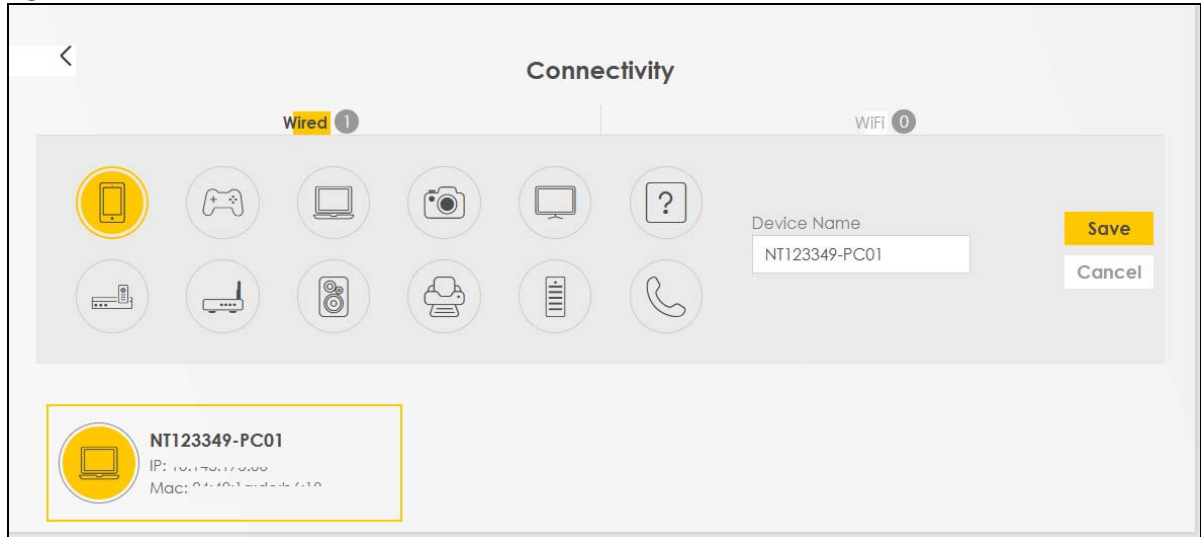
6.1.3 System Info

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

Figure 54   System Info
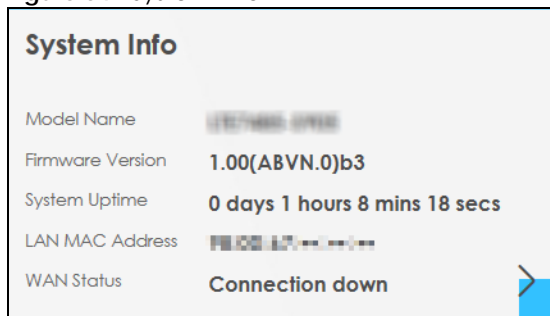
Click the Arrow icon ( ) to view more information on the status of your firewall and interfaces (WAN,
LAN, and WLAN).

Figure 55 System Info: Detailed Information
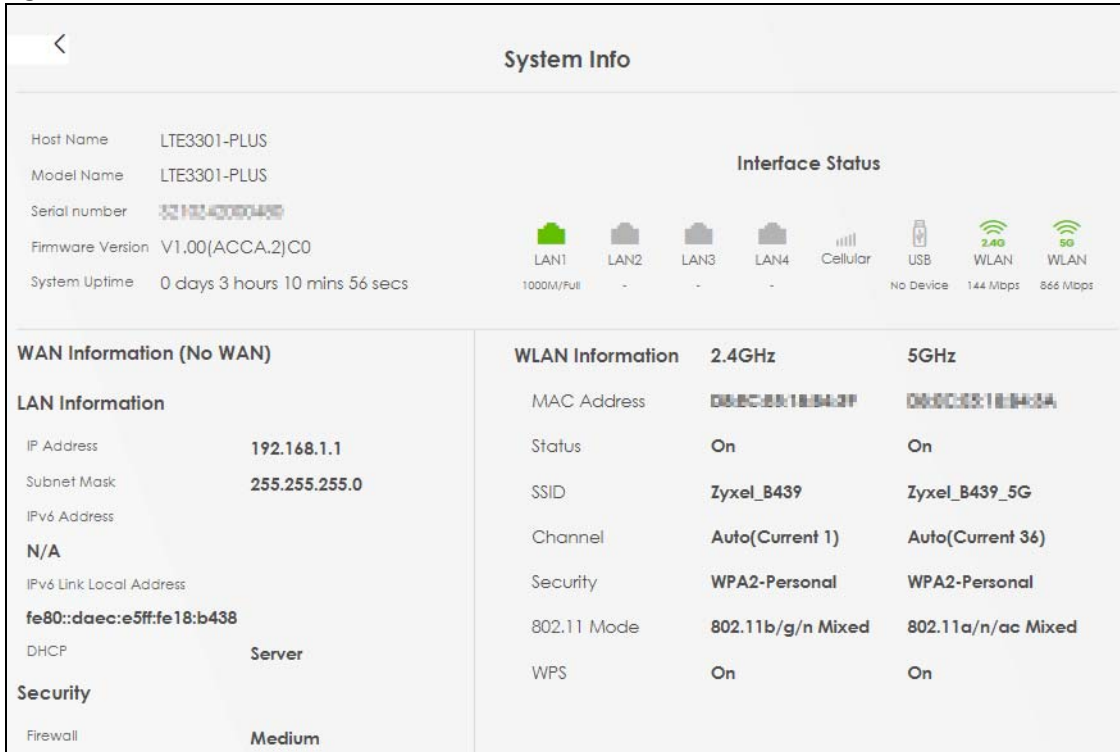
Each field is described in the following table.

Table 24   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 a WAN connection.)	
Link Type	This field displays the type of WAN connection that the Zyxel Device is currently using, such as **Cellular WAN** or **Ethernet**.
APN	This field displays the Access Point Name (APN).
Mode	This field displays the current mode of your Zyxel Device.
IP Address	This field displays the current IPv4 address of the Zyxel Device in the WAN.
IP Subnet Mask	This field displays the current IPv4 subnet mask of the Zyxel Device in the WAN.
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device in the WAN.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.

Table 24   System Info: Detailed Information (continued)

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

6.1.4 Cellular Info

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

Figure 56   Cellular Info

Cellular Info

Mode	**IP Passthrough Mode**
Status	**Up**
IP Address	**10.204.58.202**
Primary DNS server	**210.241.208.1,139.175.1.1**
Access Technology	**LTE**
Signal Strength	**-71**

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

Figure 57   Cellular Info: Detailed Information

Cellular Info

Module Information

IMEI	351964110000165
Module SW Version	EG12EAPAR01A05M4G

SIM Status

SIM Card Status	**Available**
IMSI	466011801891892
ICCID	89886018157708842319
PIN Protection	**Disable**
PIN Remaining Attempts	3

IP Passthrough Status

IP Passthrough Enable	**Disable**

Cellular Status

Cellular Status	**Up**
Data Roaming	**Disable**
Operator	**Far EasTone**
PLMN	46601

Service Information

Access Technology	LTE
Band	LTE_BC7
RSSI	-53
Cell ID	56410647
Physical Cell ID	23
UL Bandwidth (MHz)	20
DL Bandwidth (MHz)	20
RFCN	3250
RSRP	-80
RSRQ	-9
RSCP	N/A
EcNo	N/A
TAC	59242
LAC	N/A
RAC	N/A
BSIC	N/A
SINR	19

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

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

The following table describes the labels in this screen.

Table 25   Cellular Info: Detailed Information

LABEL	DESCRIPTION
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Module SW Version	This shows the software version of the cellular network module.

Table 25   Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
SIM Status	
SIM Card Status	This displays the SIM card status:
	None – the Zyxel Device does not detect that there is a SIM card inserted.
	Waiting SIM Available – the SIM card is detected but not available yet.
	Available – the SIM card could either have or do not have PIN code security.
	Locked – the SIM card has PIN code security, but you did not enter the PIN code yet.
	Blocked – you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card.
	Error – the Zyxel Device detected that the SIM card has errors.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (**ICCID**). This is the serial number of the SIM card.
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.
	Shows **Enable** if the service provider requires you to enter a PIN to use the SIM card.
	Shows **Disable** if the service provider lets you use the SIM without inputting a PIN, or you disable **PIN Protection** in **Network Setting** > **Broadband** > **Cellular SIM**.
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
IP Passthrough Mode	This displays the IP Passthrough mode.
	This displays **Dynamic** and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device.
	This displays **Fixed** and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.
Data Roaming	This displays if data roaming is enabled on the Zyxel Device.
	Data roaming is to use your Zyxel Device in an area which is not covered by your service provider. Enable roaming to ensure that your Zyxel Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Operator	This displays the name of the service provider.
PLMN	This displays the PLMN (Public Land Mobile Network) number.
GNSS Information	
Global Navigation Satellite System (GNSS) sends position and timing data from high orbit artificial satellites. It works with GPS navigational satellites to provide better receiver accuracy and reliability than just using GPS alone. This is necessary for 5G networks that require very accurate timing for time and frequency synchronization. With GNSS, your can easily locate the Zyxel Device with accurate information.	
Note: Not all models support the GNSS feature.	
Enable	This shows if GNSS is enabled.
	Note: This can only be configured by a qualified service technician.

Table 25   Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
Scan OnBoot	This shows Enable if Scan OnBoot is enabled, so that GNSS runs automatically after the Zyxel Device is turned on. Note: This can only be configured by a qualified service technician.
Scan Status	This shows GNSS error codes for debugging by a qualified service technician.
HDOP	Horizontal Dilution of Precision (HDOP) shows how accurate data collected by the Zyxel Device is according to the current satellite configuration. A smaller value of HDOP means a higher precision.
Display Format	This shows the latitude and longitude display modes. There are three modes: 0, 1, and 2. Below are examples for these modes shown in latitude/longitude. 0 – ddmm.mmmmN/S, dddmm.mmmmE/W 1 – ddmm.mmmmmm, N/S, dddmm.mmmmmm, E/W 2 – (–)dd.ddddd, (–)ddd.ddddd N/S/E/W: North/South/East/West "–" : Negative values refer to South latitude/West longitude respectively. Positive values refer to North latitude/East longitude.
Latitude	This shows the latitude coordinate of the Zyxel Device. These positioning values (latitude, longitude, and altitude) help you locate the Zyxel Device accurately.
Longitude	This shows the longitude coordinate of the Zyxel Device.
Elevation	This shows the altitude of the Zyxel Device above sea level in meters.
Positioning Mode	This shows the GNSS positioning mode. 2D ("2") GNSS positioning mode displays latitude and longitude co-ordinates; 3D ("2") GNSS positioning mode displays latitude and longitude co-ordinates, and elevation.
Course over ground	This shows the course of the Zyxel Device based on true North. Course Over Ground (COG) is different from the direction an object is headed, but the path derived from its actual motion (considered as Track), since the motion of an object is often with respect to other factors like wind and tides.
Speed Over Ground	This shows the Speed Over Ground (SOG) of the Zyxel Device. SOG is the true object speed over the surface of the Earth.
Last Fix Time	This shows the last time in UTC format that the position of the Zyxel Device was updated.
Number Of Satellites	This shows the number of current active satellites. GNSS requires at least 4 satellites to determine the position of the Zyxel Device.
NR-NSA Information	
MCC	This shows the Mobile Country Code (MCC). MCC is a unique code that identifies the country where a Public Land Mobile Network (PLMN) is at.
MNC	This shows the Mobile Network Code (MNC). MNC is a unique code that identifies a Public Land Mobile Network (PLMN) in a country. MCC and MNC combined together are used to identify a globally unique PLMN.
Service Information Note: If the cellular service provider supports carrier aggregation (CA), then this section displays statistics for the connection's primary component carrier (PCC).	
Access Technology	This displays the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.
Band	This displays the current cellular band of your Zyxel Device (WCDMA2100).
RSSI (dBm)	This displays the strength of the cellular signal between an associated cellular station and the Zyxel Device.

Table 25   Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting. The value depends on the type of the mobile network (such LTE, UMTS, GSM) to which the Zyxel Device is connecting: • For UMTS, it is the Cell Identity as defined in SIB3 3GPP-TS.25.331, 3GPP-TS.24.008. • For LTE, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331. The value is '0' (zero) or 'N/A' if there is no network connection.
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Zyxel Device and the mobile network it is connecting to. The normal range is 1 to 504.
UL Bandwidth (MHz)	This shows the uplink cellular channel bandwidth from the Zyxel Device to the base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
DL Bandwidth (MHz)	This shows the downlink cellular channel bandwidth from the base station to the Zyxel Device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting. The value depends on the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting: • For UMTS (3G), it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. • For LTE, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. The value is '0' (zero) or 'N/A' if there is no network connection.
RSRP (dBm)	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133. An undetectable signal is indicated by the lower limit, example –140 dBm. This parameter is for LTE only. The normal range is –44 to –140. The signal is better when the value is closer to -44. The value is –140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSRQ (dB)	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example –240. This parameter is for LTE only. The normal range is –30 to –240. The value is –240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device. The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example –120 dBm. This parameter is for UMTS only. The normal range is –30 to –120. The value is –120 if the Current Access Technology is not UMTS. The value is 'N/A' if there is no network connection.

Table 25   Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level. The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example –240 dB. This parameter is for UMTS only. The normal range is –30 to –240. The value is –240 if the Current Access Technology is not UMTS or there is no network connection.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN. The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
RAC	This displays the RAC (Routing Area Code), which is used in mobile network "packet domain service" (PS) to identify a routing area within a location area. In a mobile network, the Zyxel Device uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and uses RAC to identify the location of data service like HSDPA or LTE. The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station. This parameter is for GPRS only. The value is '0' (zero) if the Current Access Technology is not GPRS. The value is 'N/A' if there is no network connection.
SINR (dB)	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good or bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI). PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer). PMI determines how cellular data are encoded for the antennas to improve downlink rate.
SCC Information	If the cellular service provider supports carrier aggregation (CA), then this section displays statistics for the connection's secondary component carriers (SCCs).
#	This displays the ID of the SCC. Some cellular providers support two or more SCCs.
NR Physical Cell ID	This displays the Physical Cell ID (PCI) of the SCC.
UL Bandwidth (MHz)	This shows the uplink cellular channel bandwidth from the Zyxel Device to the base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.

Table 25   Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
DL Bandwidth (MHz)	This shows the downlink cellular channel bandwidth from the base station to the Zyxel Device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the SCC.
Band	This displays the current cellular band used by the SCC.
RSSI	This displays the cellular signal strength between an associated cellular station and the Zyxel Device for this SCC.
NR RSRP	This displays the Received Signal Code Power of the SCC.
NR RSRQ	This displays the Reference Signal Receive Quality of the SCC.
NR SINR (dBm)	This displays the Signal to Interference plus Noise Ratio (SINR) of the SCC.
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber.
	The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.
	This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.

6.1.5 Cloud Control Status

Use this screen to enable or disable Nebula Discovery. You can also view the Internet connection status, Nebula connection status and the Zyxel Device registration status in this screen.

Figure 58   Cloud Control Status
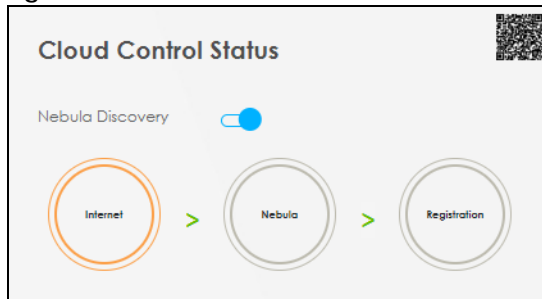
When the Zyxel Device is being managed by NCC, the Cloud Control Status will appear as the following.

Figure 59   Cloud Control Status – NCC Managed
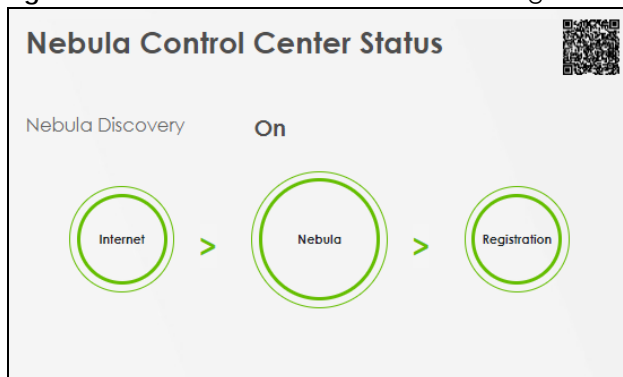
Each field is described in the following table.

Table 26   Cloud Control Status

LABEL	DESCRIPTION
Nebula Discovery	Enable this to have the Zyxel Device connect to the NCC and change to the NCC management mode if the Zyxel Device is connected to the Internet and has been registered on the NCC. This is not configurable and will only display **ON** when your Zyxel Device is being managed by NCC.
Cloud Control Status	This field displays: • The Zyxel Device Internet connection status. • The connection status between the Zyxel Device and the NCC. • The Zyxel Device registration status on the NCC. Mouse over the circles to display detailed information. To pass your Zyxel Device management to the NCC, make sure your Zyxel Device is connected to the Internet. Then go to the NCC and register your Zyxel Device. **Internet** • Green: The Zyxel Device is connected to the Internet. • Orange: The Zyxel Device is not connected to the Internet. **Nebula** • Green: The Zyxel Device is connected to the NCC. • Gray: The Zyxel Device is not connected to the NCC. **Registration** • Green: The Zyxel Device is registered on the NCC. • Gray: The Zyxel Device is not registered on the NCC. Please note that all circles will gray out if you disable **Nebula Discovery**. When a circle is gray or orange, hover the mouse over the circle to check the diagnostic message.
QR Code	Click on the QR code icon at the top right corner to show the QR code you can use to register the Zyxel Device on the NCC using the Nebula Mobile app.

6.1.6 WiFi Settings

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

Figure 60   WiFi Settings (for 2.4G and 5G models)
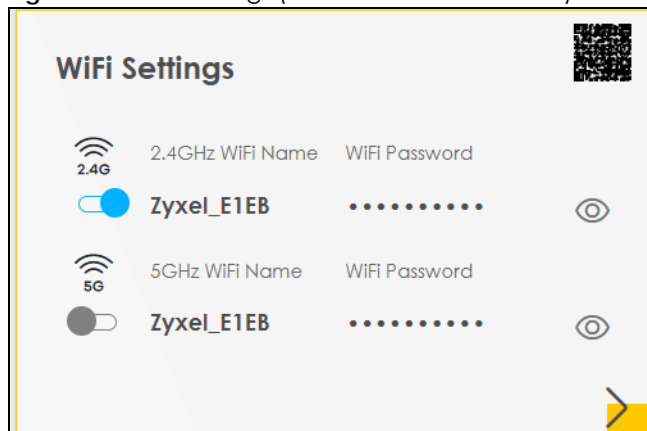
Click the Arrow icon (>) to configure the SSIDs and/or passwords for your main WiFi networks. Click the Eye icon (👁) to display the characters as you enter the WiFi Password.

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

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

Figure 61 WiFi Settings: Configuration (for 2.4G and 5G models)

Each field is described in the following table.

Table 27   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.
2.4G / 5G WiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz network. When the switch turns blue ⬤, the function is enabled.
WiFi Name	The SSID (Service Set Identifier) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for the WiFi. You can use up to 32 printable characters, including spaces.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually enter a pre-shared key from 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces. Click the Eye icon to show or hide the password for your WiFi network. When the Eye icon is slashed ⌀, you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

6.2 Guest WiFi Settings

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

Figure 62   Guest WiFi Settings (for 2.4 GHz and 5 GHz models)
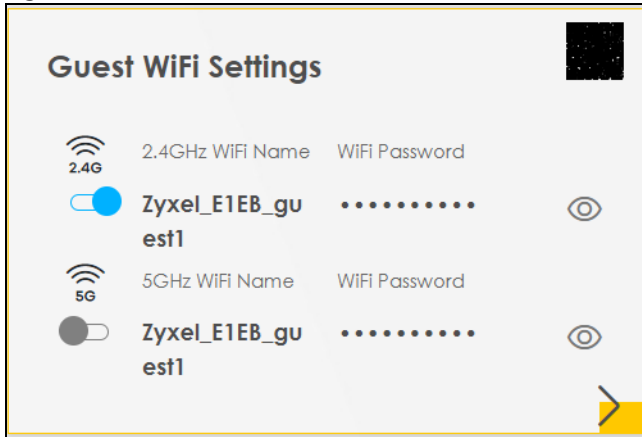
Click the Arrow icon (⟩) to open the following screen. Use this screen configure the SSIDs and/or passwords for your guest WiFi networks.

Figure 63   Guest WiFi Settings: Configuration (for 2.4G and 5G models)
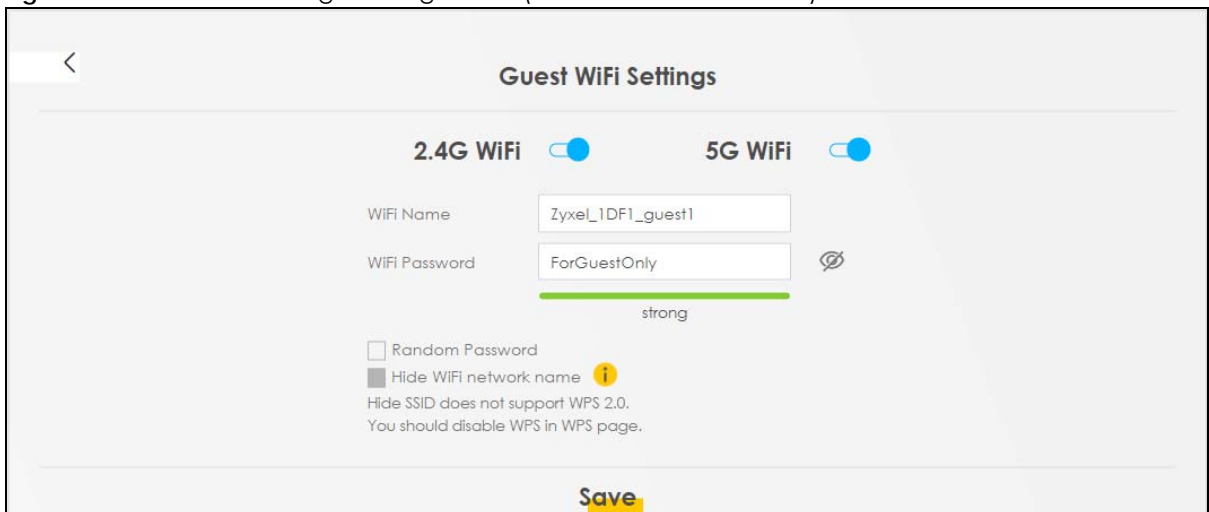
To assign different SSIDs to the 2.4 GHz and 5 GHz guest wireless networks, clear the **Keep 2.4G and 5G the same** checkbox in the **WiFi Settings** screen, and the **Guest WiFi Settings** screen will change.

Figure 64   Guest WiFi Settings: Different SSIDs (for 2.4G and 5G models)

Each field is described in the following table.

Table 28   WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4G/5GWiFi	Click this switch to enable or disable the 2.4 GHz / 5 GHz WiFi 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 printable characters, including spaces) for the WiFi.
WiFi Password	If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device. If you did not select **Random Password**, you can manually enter a pre-shared key from 8 to 64 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
	Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed 🚫, you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option.
Hide WiFi network name	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID.
Save	Click **Save** to save your changes.

6.2.1 LAN

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

Figure 65   LAN

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

Figure 66   LAN Setup

Each field is described in the following table.

Table 29   LAN Setup

LABEL	DESCRIPTION
Group Name	Select the interface group you want to use. Usually **Default**.
LAN IP Setup	
IP Address	Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.

Table 29   LAN Setup (continued)

LABEL	DESCRIPTION
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.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
Save	Click **Save** to save your changes.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 7
Broadband

7.1 Broadband Overview

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

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

Figure 67   LAN and WAN
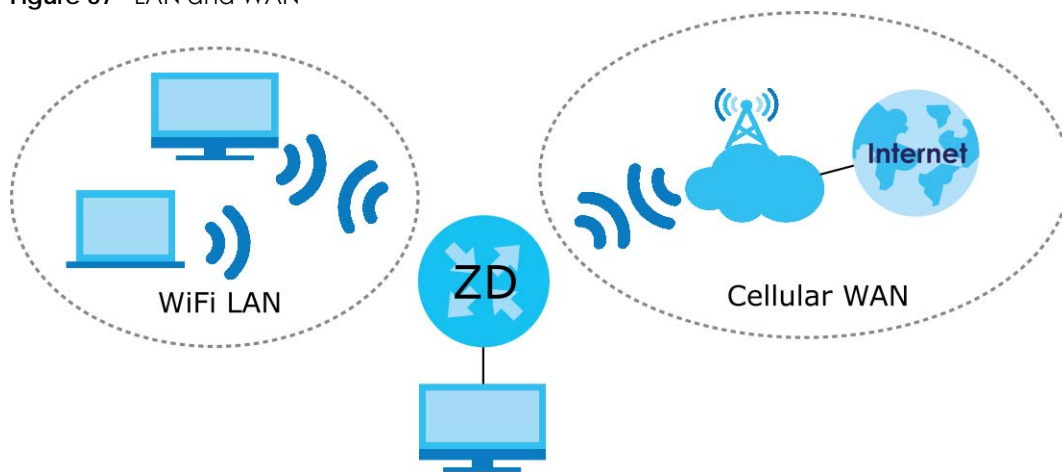
7.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 7.2 on page 134).
- Use the **Ethernet WAN** screen to convert LAN port number four as a WAN port or restore the Ethernet WAN port to a LAN port (Section 7.3 on page 140).
- Use the **Cellular WAN** screen to configure a cellular WAN connection (Section 7.5 on page 141).
- Use the **Cellular APN** screen to configure the APN setting (Section 7.6 on page 143).
- Use the **Cellular SIM** screen to enter the PIN of your SIM card (Section 7.7 on page 148).
- Use the **Cellular Dual SIM** screen to configure your dual SIM cards settings and cellular backup (Section 7.8 on page 150).
- Use the **Cellular Band** screen to view or edit a cellular WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 7.9 on page 151).
- Use the **Cellular PLMN** screen to display available Public Land Mobile Networks (Section 7.10 on page 152).
- Use the **Cellular IP Passthrough** screen to configure a cellular WAN connection (Section 7.11 on page 155).

- Use the **Cellular Lock** screens to configure the base station you choose to connect to (Section 7.12 on page 156).
- Use the **Cellular SMS** screen to send and receive SMS messages from the Zyxel Device (Section 7.13 on page 158).

Table 30   WAN Setup Overview

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

7.1.2 What You Need to Know

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

WAN IP Address

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

APN

An Access Point Name (APN) is the name of a gateway between a cellular network and another network, such as the Internet. The Zyxel Device requires an APN to connect to a cellular network. Different APNs may provide different services, such as Internet access or MMS (Multi-Media Messaging Service), and different charging methods.

464XLAT

Enable 464XLAT to send IPv4 traffic through the Zyxel Device when the Zyxel Device has an IPv6 WAN address.

464XLAT sends traffic from an IPv4 private network to another IPv4 network across an IPv6-only network. The Zyxel Device acts as a Customer-side Translator (CLAT). The CLAT adds an IPv6 prefix to the outgoing IPv4 packets, encapsulating IPv4 addresses as IPv6 addresses. When the packets go through the IPv6-only network, a Provider-side Translator (PLAT) removes the IPv6 prefixes so as the IPv4 addresses can reach the target IPv4 network.

Figure 68   464XLAT
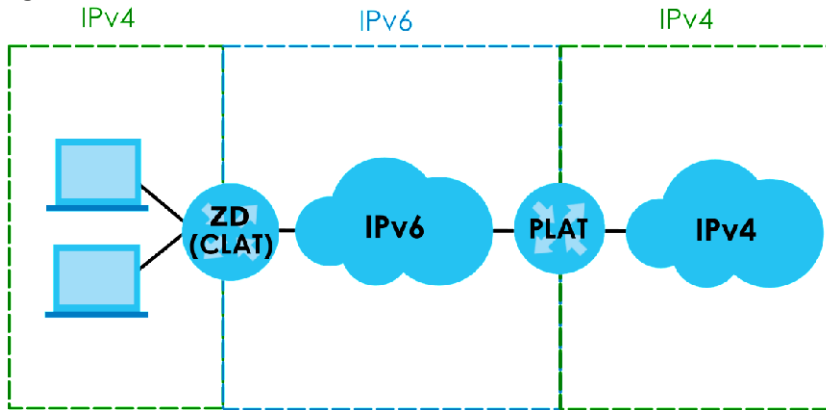
7.1.3 Before You Begin

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

7.2 Broadband

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

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

Figure 69 Network Setting > Broadband

The following table describes the labels in this screen.

Table 31   Network Setting > Broadband

LABEL	DESCRIPTION
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is a cellular or Ethernet connection.
Mode	This shows the connection is in routing mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the Zyxel Device act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the Zyxel Device use the WAN interface of this connection as the 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 **Modify** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

7.2.1 Add or Edit Internet Connection

Click the **Edit** or **Modify** icon next to a WAN interface to open the following screen. Use this screen to configure a WAN connection.

Figure 70 Network Setting > Broadband > Add or Edit New WAN Interface (Ethernet WAN)

Figure 71 Network Setting > Broadband > Add or Edit New WAN Interface (Cellular WAN)

The following table describes the labels in this screen.

Table 32   Network Setting > Broadband > Add or Edit New WAN Interface

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Name	**This is the service name of the connection.**
Type	This shows the type of the connection the Zyxel Device is currently associated with.
Mode	This shows the connection is in **Routing** or **Bridge** mode.
	If the Zyxel Device is in routing mode, your ISP gives you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	This is the method of encapsulation used by this connection.
IPv4/IPv6 Mode	This shows **IPv4 IPv6 DualStack**.
	IPv4 IPv6 DualStack allows the Zyxel Device to run IPv4 and IPv6 at the same time.
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	
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
IP Address	
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.

Table 32   Network Setting > Broadband > Add or Edit New WAN Interface (continued)

LABEL	DESCRIPTION
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.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
DNS Server	
	Select **Obtain DNS Info Automatically** if you want the Zyxel Device to use the DNS server addresses assigned by your ISP. Select **Use Following Static DNS Address** if you want the Zyxel Device to use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Routing Feature	
NAT	Click this switch to activate or deactivate NAT on this connection. When the switch goes to the right , the function is enabled.
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. 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.
Fullcone NAT	Click this switch to enable or disable fullcone NAT on this connection. When the switch goes to the right , the function is enabled. This field is available only when you activate **NAT**. In fullcone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.
DHCPC Options	
Request Options	Select **Option 43** to have the Zyxel Device get vendor specific information from DHCP packets sent from the DHCP server. Select **Option 120** to have the Zyxel Device get an IP address or a fully-qualified domain name of a SIP server from DHCP packets sent from the DHCP server. Select **Option 121** to have the Zyxel Device get static route information from DHCP packets sent from the DHCP server.
Sent Options	
option 60	Select this and enter the device identity you want the Zyxel Device to add in the DHCP discovery packets that go to the DHCP server.
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.
option 61	Select this and enter any string that identifies the device.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID	Enter the hardware type, a time value and the MAC address of the device.

Table 32   Network Setting > Broadband > Add or Edit New WAN Interface (continued)

LABEL	DESCRIPTION
option 125	Select this to have the Zyxel Device automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
IPv6 Address	
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	
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	
MLD Proxy	Select this check box or option 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.
Apply as Default Gateway	Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway.
464XLAT	Enable this to have the Zyxel Device translate outgoing IPv4 packets to IPv6 packets. Use this function if you want to use IPv4 devices and services when your ISP provides an IPv6-only mobile network. See Section 7.1.2 on page 133 for more information about 464XLAT.
Auto Prefix64	Enable this to have the Zyxel Device automatically add the IPv6 prefix assigned by your ISP to the outgoing IPv4 packets. Disable this and configure the **Static IPv6 Prefix** field if you want to manually assign an IPv6 prefix.
Static IPv6 Prefix	Enter an IPv6 prefix that the Zyxel Device adds to the outgoing IPv4 packets.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

7.3 WAN Backup

Use this screen to configure your Zyxel Device's Internet settings if the wired connection is down. You can use an alternative network, and assign an IP address to verify the accessibility of the Internet and the time interval allowed between each connection check.

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

Note: This feature is only available if **Ethernet WAN** > **State** is enabled.

Figure 72   Network Setting > Broadband > Ethernet WAN

The following table describes the fields in this screen.

Table 33   Network Setting > Broadband> WAN Backup

LABEL	DESCRIPTION
WAN Backup Enable	Select Enable to have the Zyxel Device use the cellular connection as your WAN or a backup when the wired WAN connection fails.
Primary WAN	This field displays the connection the Zyxel Device would use first when the wired WAN connection fails. You can choose **Ethernet** or **Cellular** as the primary WAN connection for your Zyxel Device.
The Destination for Connection Check	Configure this field to test your Zyxel Device's WAN accessibility. Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the Zyxel Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Connection Check Interval	When the Zyxel Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Enter the number of seconds (30 recommended) for the Zyxel Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.

Table 33   Network Setting > Broadband> WAN Backup (continued)

LABEL	DESCRIPTION
Check Fail Limit	Enter the number of times that your Zyxel Device will ping the IP addresses configured in the **Destination for Connection Check** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

7.4 Ethernet WAN

Use this screen to have a LAN port act as an Ethernet WAN port. When the switch goes to the right, the LAN port acts as an Ethernet WAN port. Otherwise, the LAN port remains as a LAN port. Click **Apply** to save your changes back to the Zyxel Device. See Section 1.1.1 on page 18 to see if your Zyxel Device supports Ethernet WAN.

Note: The Ethernet WAN has priority over the cellular WAN. When both WAN interfaces are available, the Zyxel Device uses the Ethernet WAN connection. If the Ethernet WAN interface is down, the Zyxel Device will automatically switch to use the cellular WAN.

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

Figure 73   Network Setting > Broadband > Ethernet WAN

7.5 Cellular WAN

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

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

Figure 74   Network Setting > Broadband > Cellular WAN

The following table describes the fields in this screen.

Table 34   Network Setting > Broadband > Cellular WAN

LABEL	DESCRIPTION
Data Roaming	Click this to enable ( ) data roaming on the Zyxel Device. With cellular roaming, a SIM card works in areas which are not covered by the SIM's service provider. Enable roaming to keep the Zyxel Device connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered, such as a different country. Note: Roaming charges may apply when Data Roaming is enabled.
Network Monitoring Feature	
Network Monitoring	Use this field to allow Zyxel Device to try reconnecting to the base station if the cellular connection is lost. After the third try, the Zyxel Device will reboot to try to reconnect with the base station. The LED will blink red to indicate that it is rebooting. Note: This feature only works if there is a previous cellular connection between the Zyxel Device and the base station.
Proxy ARP Feature	
Proxy ARP	Enable this to set your Zyxel Device as a server to handle ARP queries from different subnets. The Zyxel Device will offer Zyxel Device's own MAC address as an reply.

Table 34   Network Setting > Broadband > Cellular WAN (continued)

LABEL	DESCRIPTION
FQ_Codel Setting	
FQ_Codel	Select this field to enable **FQ_Codel** on the Zyxel Device. Clear this field if your network does not have much real-time traffic.
	Use Fair Queuing with Controlled Delay (FQ_Codel) to reduce delays in traffic that could affect real-time communications, such as video conferencing, live streaming, and voice over Internet phone calls
	FQ_Codel limits traffic throughput, by dropping traffic so as to reduce buffer queuing that causes delays. It does not prioritize traffic by type.
APN Manual Mode	Disable this to have the Zyxel Device configure the APN (Access Point Name) of a cellular network automatically. Otherwise, Click this to enable (⬤) and enter the APN manually in the field below.
APN	This field allows you to display the Access Point Name (APN) in the profile.
	Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method.
	You can enter up to 64 printable ASCII characters. Spaces are allowed.
Username	Enter the user name. You can enter up to 64 printable ASCII characters. Spaces are allowed.
Password	Enter the password associated with the user name above. You can enter up to 64 printable ASCII characters. Spaces are allowed.
Authentication Type	Select the type of authentication method peers use to connect to the Zyxel Device in cellular connections.
	In Password Authentication Protocol (**PAP**) peers identify themselves with a user name and password. In Challenge Handshake Authentication Protocol (**CHAP**) additionally to user name and password the Zyxel Device sends regular challenges to make sure an intruder has not replaced a peer. Otherwise select **PAP/CHAP** or **None**.
PDP Type	Select **IPv4** if you want the Zyxel Device to run IPv4 (Internet Protocol version 4 addressing system) only.
	Select **IPv4/IPv6** if you want the Zyxel Device to run both IPv4 and IPv6 (Internet Protocol version 4 and 6 addressing system) at the same time.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

7.6 Cellular APN

Click **Network Setting** > **Broadband** > **Cellular APN** to display the following screen. Use this screen to manage the APNs that Zyxel Device is connected to.

Note: This feature is only available on certain models.

Figure 75 Network Setting > Broadband > Cellular APN

The following table describes the labels in this screen.

Table 35   Network Setting > Broadband > Cellular APN

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

7.6.1 Edit Cellular APN1/APN2

On the **Cellular APN** screen, click the **Edit** icon next to an APN to configure its settings.

Note: The **IP Passthrough** fields are not available for models that support the **Network Setting** > **Broadband** > **Cellular IP Passthrough** screen.

Note: APN information can be obtained from your cellular service provider.

Note: Automatic mode is not supported in all cellular modes.

Figure 76 Network Setting > Broadband > Cellular APN > Edit APN

The following table describes the fields in this screen.

Table 36   Network Setting > Broadband > Cellular APN > Edit APN

LABEL	DESCRIPTION
Enable	Click this to enable (⬤) the APN on the Zyxel Device
APN Manual Mode	Disable this to have the Zyxel Device configure the APN (Access Point Name) of a cellular network automatically. Otherwise, Click this to enable (⬤) and enter the APN manually in the field below.
APN	This field allows you to display the Access Point Name (APN) in the profile. Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method. You can enter up to 64 printable ASCII characters. Spaces are allowed.
Username	Enter the user name. You can enter up to 64 printable ASCII characters. Spaces are allowed.
Password	Enter the password associated with the user name above. You can enter up to 64 printable ASCII characters. Spaces are allowed.

Table 36   Network Setting > Broadband > Cellular APN > Edit APN

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

7.6.2 Using Separate APNs for Data and Management Traffic

Multiple APN Access allows a cellular device to open data sessions with two or more APNs, and then send data through the APNs simultaneously. If your cellular service provider supports Multiple APN Access, the Zyxel Device can use this feature to segregate cellular traffic.

Follow the steps below to configure the Zyxel Device to use separate APNs for data and management traffic.

1   At **Network Setting** > **Broadband** > **Cellular WAN**, ensure that the Zyxel Device is connected to two data-enabled APNs. If your cellular service provider supports this feature, the Zyxel Device will connect to two APNs automatically.

Broadband

Broadband   Ethernet WAN   **Cellular WAN**   Cellular SIM   Cellular Band   Cellular PLMN   Cellular IP Passthrough
Cellular SMS

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

Roaming

Data Roaming

Note

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

APN Settings

APN Manual Mode

APN

Username   (Optional)

Password   👁   (Optional)

Authentication Type   None   ▼

PDP Type   IPv4   ▼

Note

(1) APN information can be obtained from the service provider.
(2) **Automatic APN Mode** is not supported when operating in 3G only mode.

Cancel   Apply

2   Go to **Maintenance** > **Remote Management** > **MGMT Services**. Set **WAN Interface used for services** to **Multi_WAN**, and then select **Cellular WAN 2**.

3 Go to **Maintenance** > **TR-069 Client**. Set **WAN Interface used by TR-069 Client** to **Multi_WAN**, and then select **Cellular WAN 2**.

7.7 Cellular SIM Configuration

Use this screen to enter a PIN for your SIM card, in order to prevent others from using it.

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

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

Figure 77 Network Setting > Broadband > Cellular SIM

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

The following table describes the fields in this screen.

Table 37   Network Setting > Broadband > Cellular SIM

LABEL	DESCRIPTION
PIN Management	
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. Click to enable ( ) if the service provider requires you to enter a PIN to use the SIM card. Click to disable if the service provider lets you use the SIM without inputting a PIN.
Auto Unlock PIN	If **PIN Protection** is enabled, the SIM card requires a PIN code to unlock the PIN lock. Slide the switch to the right to have the Zyxel Device automatically unlock the PIN lock. Otherwise, slide the switch to the left. You will need to manually enter the PIN every time you reboot the Zyxel Device or reinsert the SIM card to use the SIM card.
PIN Modification	
more...	Click the icon( ) to show fore fields in this section. Click the icon ( ) to hide them. Note: PIN Modification and its following fields will show upon enabling PIN Protection in the previous field.
New PIN	Enter a four-digital code to set as the new PIN code. Note: This field will show upon clicking the icon ( ).

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

LABEL	DESCRIPTION
PIN	If you enabled PIN verification, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly too many times, the ISP may block your SIM card and not let you use the account to access the Internet.
Attempts Remaining	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card. If your ISP locks your SIM card, you will need to request a PUK code from them to unlock it.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previous screen without saving.

7.8 Cellular Dual SIM

Some Zyxel Devices support dual SIM card slots for cellular backup (failover) to ensure Internet connectivity. To see if your Zyxel Device supports Cellular Dual SIM, see Section 1.1.1 on page 18. Use this screen to set the main SIM card slot and configure cellular backup with dual SIM cards.

To enable cellular backup on the Zyxel Device, select **Auto** in the **Preferred SIM Slot** field and enable **Switch when Detach**.

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

Figure 78   Network Setting > Broadband > Cellular Dual SIM

The following table describes the fields in this screen.

Table 38   Network Setting > Broadband > Cellular Dual SIM

LABEL	DESCRIPTION
Dual SIM	
Preferred SIM Slot	To have the Zyxel Device automatically detect and choose the SIM card slot that has a SIM card inserted, select **Auto**. If both cards are inserted, the primary Internet connection uses SIM 1, and the cellular backup connection is SIM 2.
	To have the Zyxel Device only use the SIM card in slot 1, select **SIM 1**. There is no cellular backup. If the SIM card is in slot 2, then the Zyxel Device won't have Internet access.
	To have the Zyxel Device only use the SIM card in slot 2, select **SIM 2**. There is no cellular backup. If the SIM card is in slot 1, then the Zyxel Device won't have Internet access.
	If you change from **SIM 1**, **SIM 2** to **Auto**, the Zyxel Device will choose the SIM card slot you previously selected if it has an inserted SIM card.
Switch and Detach	To enable cellular backup on the Zyxel Device, enable the switch (to the right).
Cancel	Click **Cancel** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes.

7.9 Cellular Band Configuration

Either select **Auto** to have the Zyxel Device connect to an available network using the default settings on the SIM card or select the type of the network (**NR5G**, **4G**, **3G**) to which you want the Zyxel Device to connect.

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

Figure 79   Network Setting > Broadband > Cellular Band

The following table describes the fields in this screen.

Table 39   Network Setting > Broadband > Cellular Band

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

7.10 Cellular PLMN Configuration

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

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

Figure 80   Network Setting > Broadband > Cellular PLMN
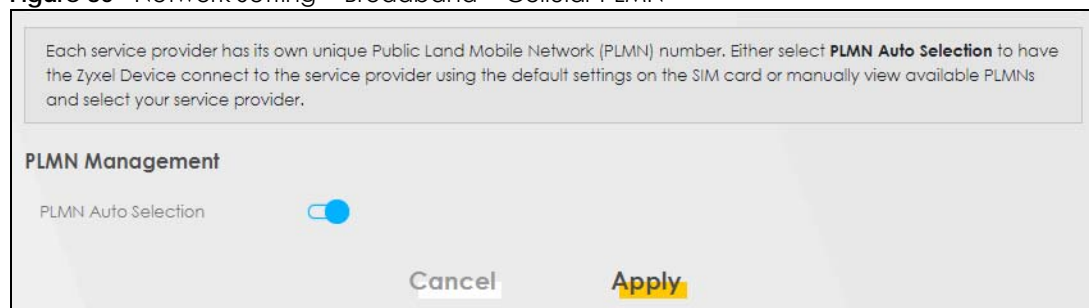
The following table describes the labels in this screen.

Table 40   Network Setting > Broadband > Cellular PLMN

LABEL	DESCRIPTION
PLMN Management	
PLMN Auto Selection	Click to enable ( ) and have the Zyxel Device automatically connect to the first available mobile network. Select disabled to display the network list and manually select a preferred network.

Table 40   Network Setting > Broadband > Cellular PLMN

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

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

Figure 81   Network Setting > Broadband > Cellular PLMN > Manual Scan Warning
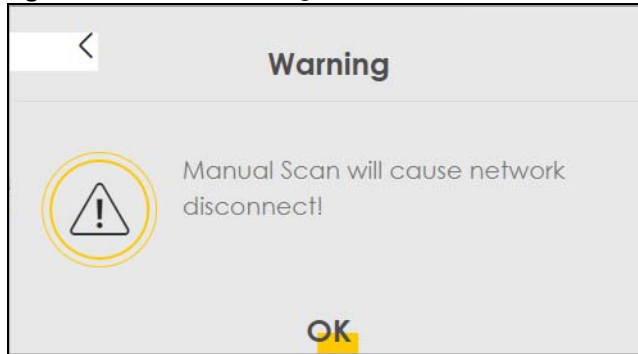
Click **Scan** to check for available PLMNs in the area surrounding the Zyxel Device, and then display them in the network list. Select from the network list and click **Apply**.

Figure 82   Network Setting > Broadband > Cellular PLMN > PLMN Management

The following table describes the labels in this screen.

Table 41   Network Setting > Broadband > Cellular PLMN > PLMN Management

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

7.11 Cellular IP Passthrough

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

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

Note: This screen is not available when the fourth LAN port acts as an Ethernet WAN port.

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

Note: This screen is not available if Ethernet WAN is enabled at **Network Setting** > **Broadband** > **Ethernet WAN** > **State**.

Figure 83   Network Setting > Broadband > Cellular IP Passthrough

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

Figure 84   Network Setting > Broadband > Cellular IP Passthrough > Enable Warning

The following table describes the fields in this screen.

Table 42   Network Setting > Broadband > Cellular IP Passthrough

LABEL	DESCRIPTION
IP Passthrough Management	
IP Passthrough	IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
Passthrough Mode	Select **Dynamic** to allow traffic to be forwarded to the first LAN computer on the local network of the Zyxel Device. Select **Fixed** to allow traffic to be forwarded to a specific computer (for example, Client A) by entering its MAC address. Note: This field will show after enabling **IP Passthrough** in the previous field.
Passthrough to fixed MAC	Enter the MAC address of a LAN computer on the local network of the Zyxel Device upon selecting **Fixed** in the previous field. Note: This field will show after selecting **Fixed** in the previous field.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

7.12 Cellular Lock Overview

Cellular Lock (PCI Lock) locks the Zyxel Device to the base station that it is currently connected to. This is useful if the Zyxel Device is within range of multiple base stations, and you would prefer the Zyxel Device to connect to one base station over the others.

For Zyxel Devices using 4G LTE connections, identify the base station to lock to by Physical Cell ID.

For Zyxel Devices using 5G NR connections, identify the base station to lock to by Physical Cell ID and the frequency band.

To see the currently connected base station's Physical Cell ID and RFCN, go to **Connection Status** > **Cellular Info** and check the **Service Information** section.

7.12.1 Cellular Lock (LTE)

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

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

Figure 85   Network Setting > Broadband > Cellular Lock (LTE)

Broadband	Cellular WAN	Cellular APN	Cellular SIM	Cellular Band	Cellular PLMN	**Cellular Lock(LTE)**

Cellular Lock(5G)

Cellular Lock Configuration (LTE)

LTE(4G) Lock Management

PCI Lock

＋ Add New Rule

Physical Cell ID	RFCN	Delete
172	3550	🗑
		🗑

Cancel   Apply

The following table describes the fields in this screen.

Table 43   Network Setting > Broadband > Cellular Lock (LTE)

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

7.12.2 Cellular Lock (5G)

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

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

Note: Enabling/Disabling Cellular Lock will make the WAN connection to be temporarily disconnected.

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

Figure 86 Network Setting > Broadband > Cellular Lock (5G)

The following table describes the fields in this screen.

Table 44   Network Setting > Broadband > Cellular Lock (5G)

LABEL	DESCRIPTION
NR(5G) Lock Management	
PCI_Enable	Click the switch button (to the right) to enable PCI (Physical Cell Identifier) Lock on a base station when the Zyxel Device has a 5G NR connection.
Band	Enter the band number to which you choose to connect. Note: Make sure to select the same band in the **Network Setting** > **Broadband** > **Cellular Band** screen so as the Zyxel Device can connect to that band.
PCI	Use this to enter the PCI number of the base station you want the Zyxel Device to connect to (0 – 504).
RFCN	Enter the RFCN (Radio Frequency Channel Number) for the 5G NR frequency of the specified PCI (1 – 65535).
SCS	Select the Subcarrier Spacing (SCS) from the drop-down list. Subcarriers are small signal carriers that divide a frequency channel, which is the main carrier wave. Subcarrier spacing is the space between each subcarrier. At the time of writing, SCS ranges from 15-120 KHz.You should select the same SCS that is used by the ISP.
Cancel	Click this to exit this screen without saving.
Apply	Click this to save your changes.

7.13 Cellular SMS

Use this screen to send and receive SMS messages using the SIM card installed in the Zyxel Device.

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

Figure 87 Network Setting > Broadband > Cellular SMS

The following table describes the fields in this screen.

Table 45   Network Setting > Broadband > Cellular SMS

LABEL	DESCRIPTION
Add New Message	Click this button to open the Send New Message screen and send an SMS message from the Zyxel Device.
Storage Status	
Used Capacity	This displays the used storage capacity of the Zyxel Device to receive SMS messages. Note: The Zyxel Device will stop receiving SMS messages when **Used Capacity** is the same as **Total Capacity**. To continue receiving SMS messages, delete old message(s) by clicking the delete icon in **Modify**, or click **Delete All Messages**.
Total Capacity	This displays **100**. This is the maximum capacity to receive SMS messages on the Zyxel Device.
SMS Inbox	
SMS Inbox Enable	Click this to enable or disable the SMS Inbox. When enabled, the Zyxel Device can receive and display SMS messages.

Table 45   Network Setting > Broadband > Cellular SMS (continued)

LABEL	DESCRIPTION
#	This displays the index number of the received message.
From	This displays the phone number that sent the message.
Time Stamp	This displays the time and date that the Zyxel Device received the message.
Content	This displays the content of the message.
Modify	This allows you to delete the message.

7.13.1 Send New Message Screen

Use this screen to send an SMS message from the Zyxel Device. Go to **Network Setting** > **Broadband** > **Cellular SMS** and click Add New Message to view this screen.

Figure 88   Network Setting > Broadband > Cellular SMS > Send New Message

The following table describes the fields in this screen.

Table 46   Network Setting > Broadband > Cellular SMS

LABEL	DESCRIPTION
Character Set	Select whether you want to send the SMS message using GSM-7 encoding or unicode. • **GSM default alphabet**: Use standard ASCII numbers, letters, and special characters. The maximum length of the message is 140 characters. • **Unicode alphabet**: Use any non-English Unicode characters. The maximum length of the message is 70 characters.
Mobile Number	Specify the cellphone number that you want to send the message to.
Text Message	Specify the content of the message.

Table 46   Network Setting > Broadband > Cellular SMS

LABEL	DESCRIPTION
OK	Click this button to send the message.
Cancel	Click this button to close the window without sending the message.

CHAPTER 8
Wireless

8.1 Wireless Overview

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

8.1.1 What You Can Do in this Chapter

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

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the WiFi security mode (Section 8.2 on page 163)
- Use the **Guest/More AP** screen to set up multiple WiFi networks on your Zyxel Device (Section 8.3 on page 168).
- Use the **MAC Authentication** screen to allow or deny WiFi clients based on their MAC addresses from connecting to the Zyxel Device (Section 8.4 on page 171).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 8.5 on page 173).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 8.6 on page 175).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 8.7 on page 176).
- Use the **Channel Status** screen to scan the number of accessing points and view the results (Section 8.8 on page 179).
- Use the **WLAN Scheduler** screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces (Section 8.9 on page 180).

8.1.2 What You Need to Know

Wireless Basics

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

WiFi 6 / IEEE 802.11ax

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

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

Table 47   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	

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

Finding Out More

See Section 8.10 on page 182 for advanced technical information on WiFi networks.

8.2 Wireless General Settings

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

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

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

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

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

Figure 89   Network Setting > Wireless > General

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

Table 48   Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
WiFi	Select **Keep the same settings for 2.4G and 5G WiFi networks** and the 2.4 GHz / 5 GHz WiFi networks will use the same SSID and WiFi security settings.
Wireless/WiFi Network Setup	
Band	This shows the WiFi band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax WiFi clients, **5GHz** is used by IEEE 802.11a/n/ac/ax WiFi clients.
Wireless/WiFi	Click this switch to enable or disable WiFi in this field. When the switch turns blue, the function is enabled. Otherwise, it is not.

Table 48   Network Setting > Wireless > General (continued)

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

8.2.1 No Security

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

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

Figure 90   Wireless > General: No Security
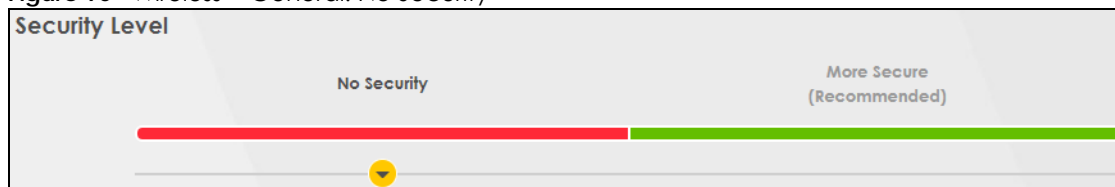
The following table describes the labels in this screen.

Table 49   Wireless > General: No Security

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

8.2.2 More Secure (Recommended)

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

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. **WPA2-PSK** is the default **Security Mode**.

Figure 91 Wireless > General: More Secure: WPA2-PSK

The following table describes the labels in this screen.

Table 50   Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	Select **Generate password automatically** or enter a **Password**. The password has two uses. 1. Manual. Manually enter the same password on the Zyxel Device and the client. You can use 8 – 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: More than 63 hexadecimal characters are not accepted for WPS. Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it is hidden.
Click this to show more fields in this section. Click this to hide them.	
Encryption	**AES** is the default data encryption type, which uses a 128-bit key. Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your WiFi clients can all use AES. Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. Note: Not all models support **TKIP+AES** encryption.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

8.3 Guest/More AP Screen

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

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

The following table introduces the supported WiFi networks.

Table 51   Supported WiFi Networks

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

The following screen displays.

Figure 92   Network Setting > Wireless > Guest/More AP

The following table describes the labels in this screen.

Table 52   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 WiFi profile on the network. When a WiFi client scans for an AP to associate with, this is the name that is broadcast and seen in the WiFi 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. A **Home Guest** can access the Internet, LAN wired devices connected to the Zyxel Device, and other Home Guest WiFi clients. An **External Guest** can just access the Internet through the Zyxel Device. **N/A** displays if guest WLAN is disabled.
Modify	Click the **Edit** icon of an SSID profile to configure the SSID profile.

8.3.1 The Edit Guest/More AP Screen

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

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

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

Figure 93 Network Setting > Wireless > More AP > Edit

The following table describes the fields in this screen.

Table 53   Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
WiFi/Wireless Network Setup	
WiFi/Wireless	Click this switch to enable or disable the WiFi in this field. When the switch turns blue 🔵, the function is enabled; otherwise, it is not.
WiFi/Wireless Network Settings	
WiFi/Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for the WiFi. You can use up to 32 printable characters, including spaces.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the **Access Scenario** field.
Access Scenario	Select **Home Guest** or **External Guest** to provide different levels of access to the Zyxel Device and the other WiFi clients. A **Home Guest** can access the Internet, LAN wired devices connected to the Zyxel Device, and other Home Guest WiFi clients. An **External Guest** can just access the Internet through the Zyxel Device.
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 WiFi interface on the Zyxel Device when WiFi 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 WiFi clients. This option cannot be used if **Keep 2.4G and 5G wireless network name the same** is enabled 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 WiFi clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 8.2.1 on page 166 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.

Table 53   Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. 1. If you did not select **Generate password automatically**, you can manually enter a pre-shared key at least 8 characters long, including one uppercase letter, one lowercase letter, one number, and one special character. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed ⊘, you will see the password in plain text. Otherwise, it is hidden.
Strength	This displays the current password strength – **weak**, **medium**, **strong**.
Click this ▾ to show more fields in this section. Click again to hide them.	
Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your WiFi clients can all use AES. Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. Not all models support the **TKIP+AES** option.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.4 MAC Authentication

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

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

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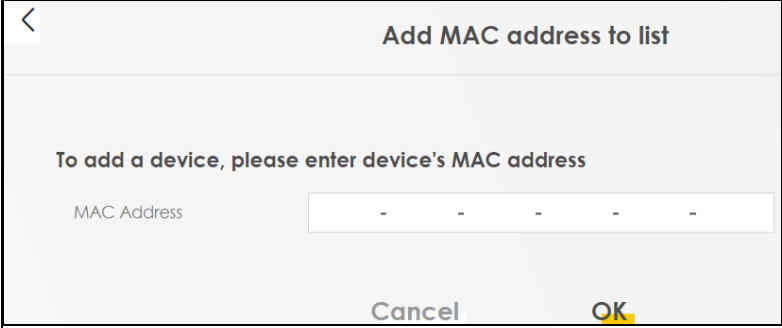
The following table describes the labels in this screen.

Table 54   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 54   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.

8.5 WPS

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

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

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS WiFi connection (see Section 8.2.2 on page 166).

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection (see Section 8.2.2 on page 166). Some models support more than one SSID profile, check the supported number on the **Network Setting** > **Wireless** > **General** screen.

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

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

Figure 95 Network Setting > Wireless > WPS

WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your wireless client supports it.

General

WPS   ⊂▢

Add a new device with WPS Method

Method 1 PBC	Method 2 PIN	Method 3
Step1. Click WPS button [WPS]	**Step1.** Enter the PIN of your new wireless client device and then click Register	Enter AP's PIN Number in wireless Client **Current state** Configured
Step2. Press the WPS button on your new wireless client device within 120 seconds	[ ] Register	1. Please release configuration if you want to configure the wireless settings Release Configuration
	Step2. Press the WPS button on your new wireless client device within 120 seconds	2. Enter current PIN number on your wireless client Generate New PIN

Note

(1) If WPS is Enabled, UPnP will automatically be turned on.
(2) The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile.
(3) The WPS switch is grayed out when wireless LAN is disabled.

Cancel   Apply

The following table describes the labels in this screen.

Table 55   Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Slide this to the right to enable and have the Zyxel Device activate WPS. Otherwise, it is disabled.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS 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 WiFi 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.
Method 2 PIN	Use this section to set up a WPS WiFi network by entering the PIN of the client into the Zyxel Device. Click this switch to make it turn blue. Click **Apply** to activate WPS method 2 on the Zyxel Device.
Register	Enter the PIN of the WiFi device that you are setting up a WPS connection with and click **Register** to authenticate and add the WiFi device to your WiFi network.
	You can find the PIN either on the outside of the WiFi device, or by checking the WiFi device's settings.
	Note: You must also activate WPS on that WiFi device within 2 minutes to have it present its PIN to the Zyxel Device.

Table 55   Network Setting > Wireless > WPS (continued)

LABEL	DESCRIPTION
Method 3	Use this section to set up a WPS WiFi network by entering the PIN of the Zyxel Device into the client. Click this switch to make it turn blue. Click **Apply** to activate WPS method 3 on the Zyxel Device.
Release Configuration	The default WPS status is **configured**. Click this button to remove all configured WiFi and WiFi security settings for WPS connections on the Zyxel Device.
Generate New PIN	If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the WiFi device you want to connect to using WPS. The PIN is not necessary when you use the WPS push-button method. Click the **Generate New PIN** button to have the Zyxel Device create a new PIN.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.6 WMM

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

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

Figure 96   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 56   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. SSID1 is the **General** WiFi SSID; SSID2-SSID4 are the **Guest** WiFi SSIDs. 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.

8.7 Others

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

See for detailed definitions of the terms listed here.

Figure 97 Network Setting > Wireless > Others

The following table describes the labels in this screen.

Table 57   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 57   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 8.10.6 on page 186 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Auto Switch Off	Click this to enable **Auto Switch Off** and configure the next field.
Auto Switch Off Interval	Select **0**,**15**, **30**, **45** or **60** minutes from the drop down menu. The default setting is **30** minutes. Select **0** minute to disable the **Auto Switch Off Interval**.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.8 Channel Status

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

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

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

Figure 98   Network Setting > Wireless > Channel Status
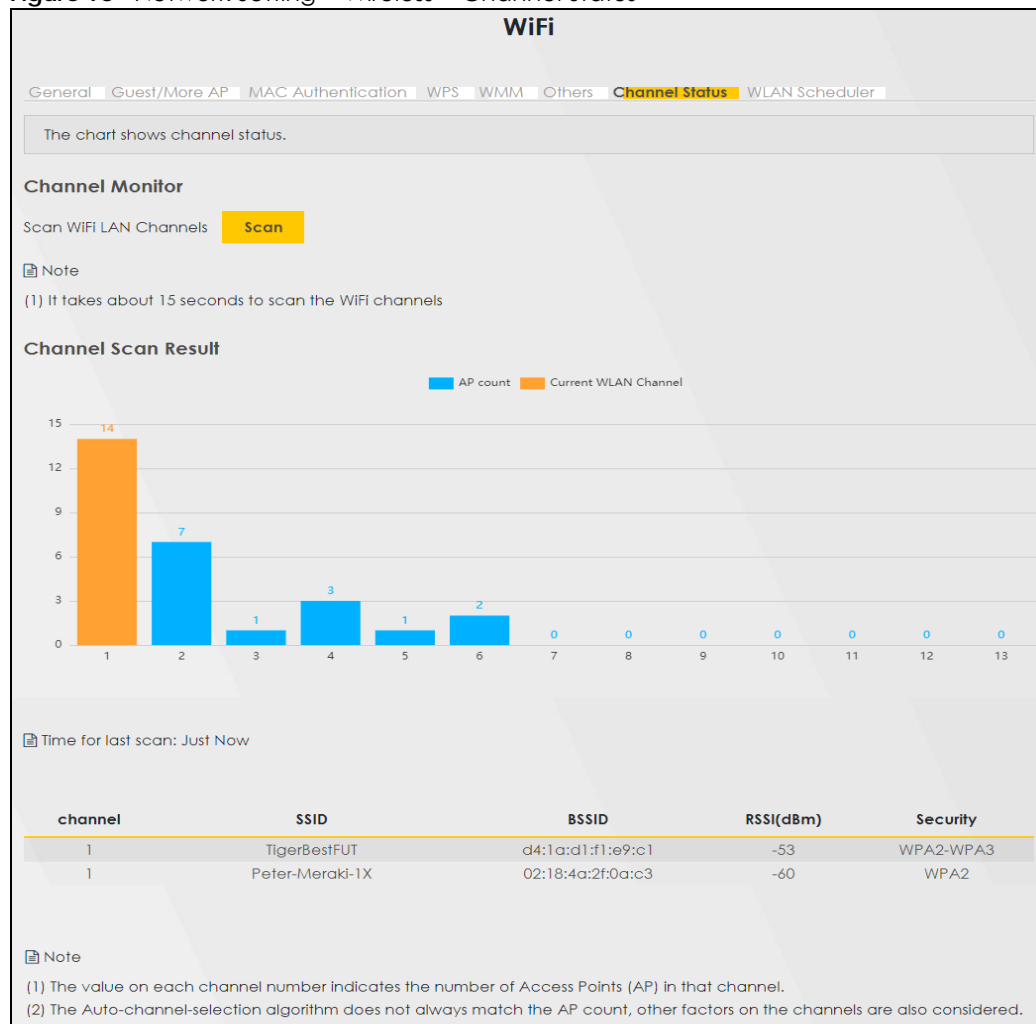
The following table describes the labels in this screen.

Table 58   Network Setting > Wireless > Channel Status

LABEL	DESCRIPTION
Channel Monitor	
Scan wireless LAN Channels	Click the **Scan** button to scan WiFi channels.
Channel Scan Result	This displays the results of the channel scan. The blue bar displays the number of access points (**AP count**) in the WiFi channel. The orange bar displays the WiFi channel that the Zyxel Device is now using.

8.9 WLAN Scheduler

Use the **WLAN Scheduler** screen to create rules to schedule the times to permit Internet traffic from each WiFi network interfaces. Select a specific time and day of a week for scheduling. You can also create a rule to automatically switch off all the WLAN together.

Click **Network Setting** > **Wireless** > **WLAN Scheduler**.

Figure 99   Network Setting > Wireless > WLAN Scheduler

The following table describes the labels in this screen.

Table 59   Network Setting > Wireless > WLAN Scheduler

LABEL	DESCRIPTION
WLAN Scheduler Access	Click this switch to enable the WLAN scheduler function. This serves as the main switch to allow the individual rules to function.
Add New Rule	Click this to configure a new WLAN scheduler rule.
#	This is the index number of the entry.

Table 59   Network Setting > Wireless > WLAN Scheduler (continued)

LABEL	DESCRIPTION
Active	Click the checkbox to enable individual rules. Note: Make sure to enable the **WLAN Scheduler Access** switch for the individual rules to work.
Rule Name	This field displays the name of the rule.
SSID	This is the descriptive name used to identify the wireless network interface that this rule applies to. Will show **ALL WLAN** if you select **All wireless networks** in the **Add New Rule** screen.
Day	This field displays the days of the week that you wish to apply this rule.
Time	This field displays the time of the day that you wish to apply this rule.
Description	This field shows a description of the rule, usually to help identify it.
Modify	Click the **Edit** icon to configure the rule. Click the **Delete** icon to remove the rule.

Note: If you enable a rule for a specific SSID, you will not be able to connect to other wireless networks.

8.9.1 Add or Edit Rules

Click **Add New Rule** in the **WLAN Scheduler** screen, or click the **Edit** icon next to a scheduling rule, and the following screen displays.

Use this screen to create a scheduling rule to permit Internet traffic from each wireless network interface.

Figure 100   Network Setting > Wireless > WLAN Scheduler > Add New Rule

The following table describes the labels in this screen.

Table 60   Network Setting > Wireless > WLAN Schedule > Add New Rule

LABEL	DESCRIPTION
Active	Click this switch to enable this WLAN scheduler rule.
SSID	Select **All wireless networks** if you want the rule to apply to all WiFi network interfaces or select a WiFi network interface to apply the rule to.
Rule Name	Enter a descriptive name for the rule.
Day	Select the days of the week that you wish to apply this rule.
Time of Day Range	Specify the time of the day that you wish to apply to this rule (format **hh:mm**). Note: Click the checkbox for **All days** if you wish to apply the rule for the whole day (24 hours).
Description	Enter a description of the rule, usually to help identify it (its purpose).
OK	Click **OK** to save the changes back to the Zyxel Device.
Cancel	Click **Cancel** to close the window with changes unsaved.

8.10 Technical Reference

This section discusses WiFi in depth.

8.10.1 WiFi Network Overview

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

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

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

The following figure provides an example of a WiFi network.

Figure 101   Example of a WiFi Network
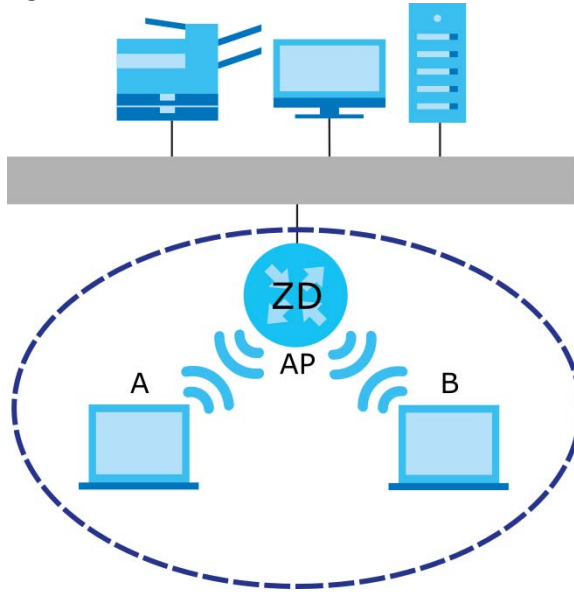
The WiFi network is the part in the blue circle. In this WiFi network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

Every WiFi network must follow these basic guidelines.

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

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

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

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

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

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

8.10.2 Additional WiFi Terms

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

Table 61   Additional WiFi Terms

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

8.10.3 WiFi Security Overview

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

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

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

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

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is

Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

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

8.10.3.1 SSID

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

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

8.10.3.2 MAC Address Filter

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

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

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

8.10.3.3 Encryption

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

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

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

8.10.4 Signal Problems

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

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

---

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.

coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

8.10.5 BSS

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

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

Figure 102   Basic Service Set
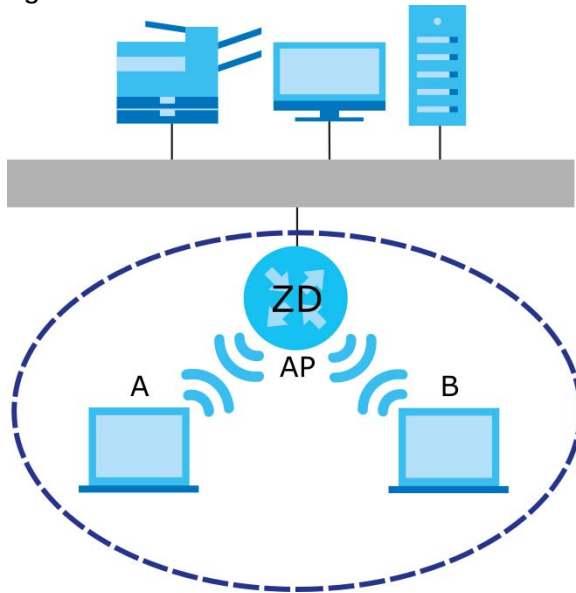
8.10.6 Preamble Type

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

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

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

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

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

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

8.10.7 WiFi Protected Setup (WPS)

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

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

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

8.10.7.1 Push Button Configuration

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

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

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

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

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

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

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

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

8.10.7.2 PIN Configuration

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

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

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

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

1 Ensure WPS is enabled on both devices.

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

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide on how to find the WPS PIN – for the Zyxel Device, see Section 8.5 on page 173).

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

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

6 Start WPS on both devices within two minutes.

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

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

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

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

Figure 103 Example WPS Process: PIN Method
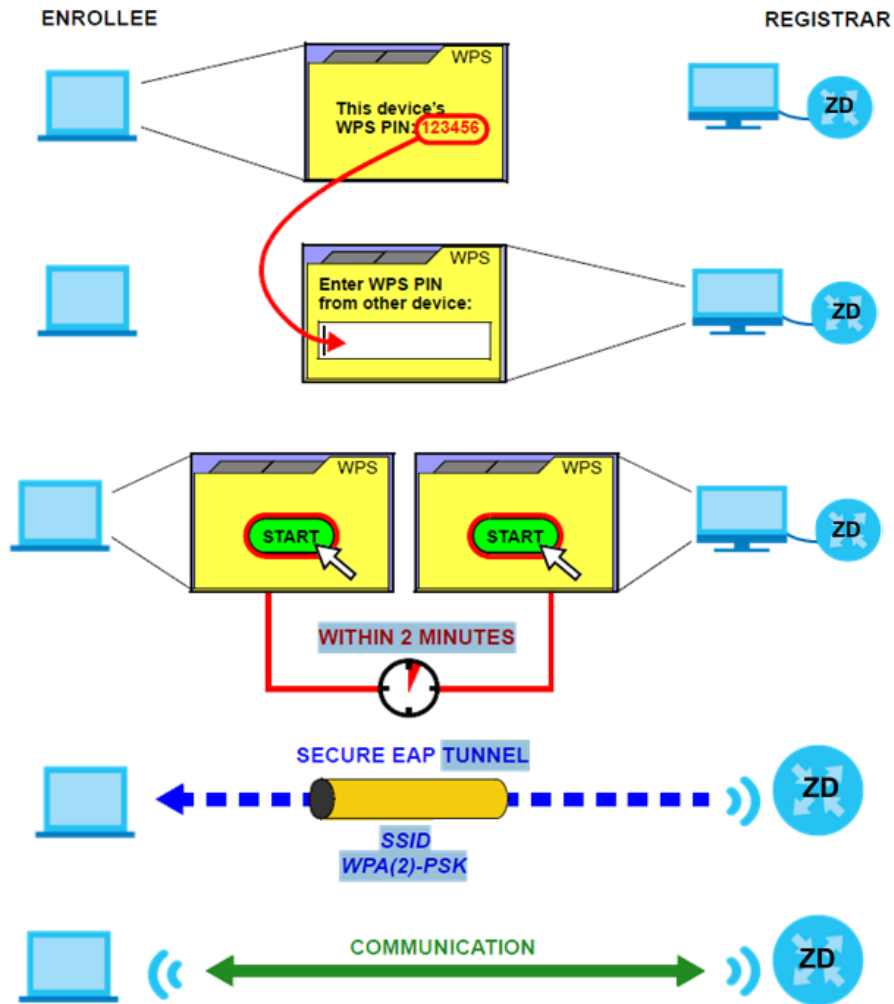
8.10.7.3 How WPS Works

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

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

Figure 104   How WPS Works
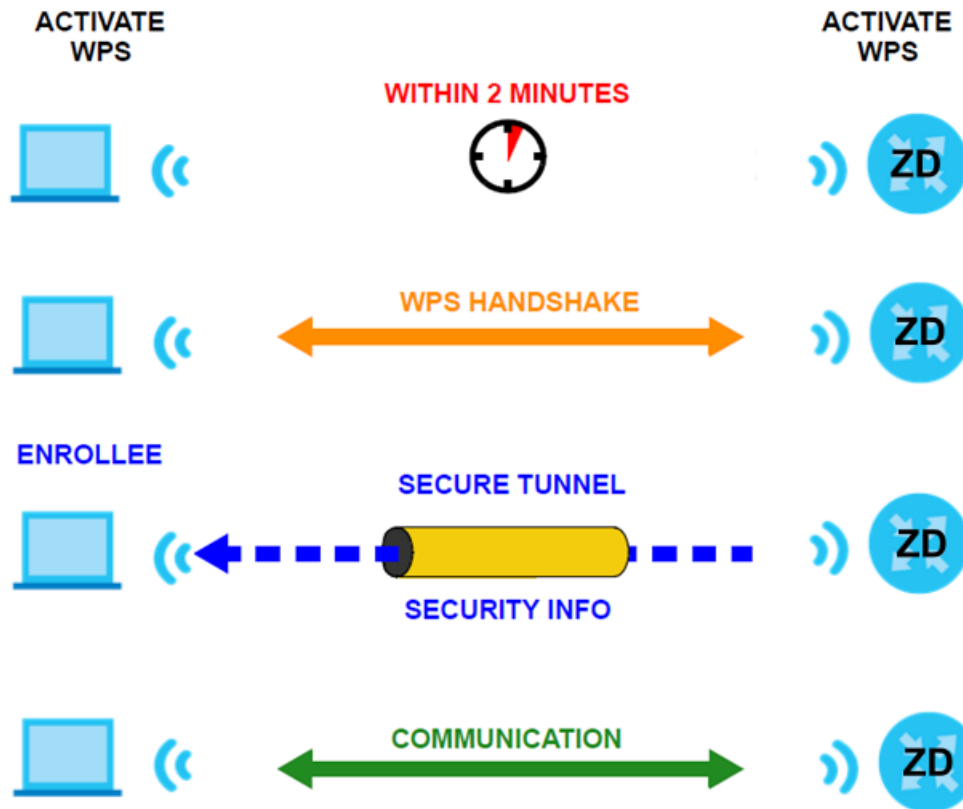
The roles of registrar and enrollee last only as long as the WPS setup process is active (2 minutes). The next time you use WPS, a different device can be the registrar if necessary.

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

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

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

8.10.7.4 Example WPS Network Setup

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

The following figure shows a sample network. In step 1, both **AP1** and **Client 1** are 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 105   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 106   WPS: Example Network Step 2
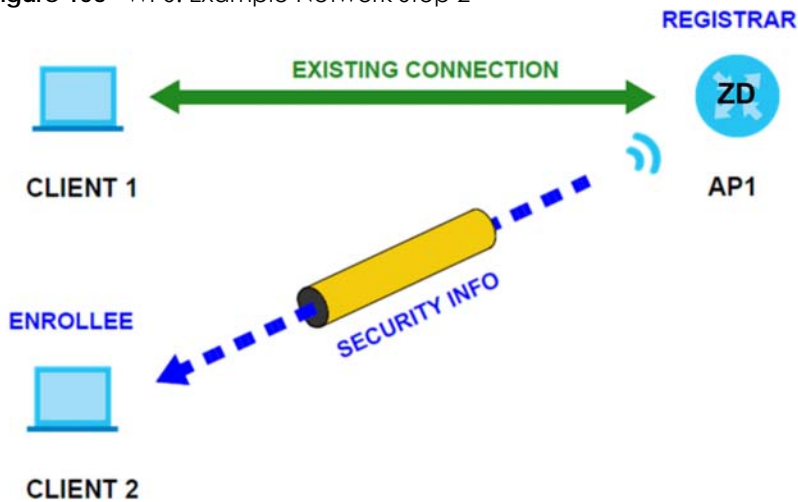
In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 107   WPS: Example Network Step 3
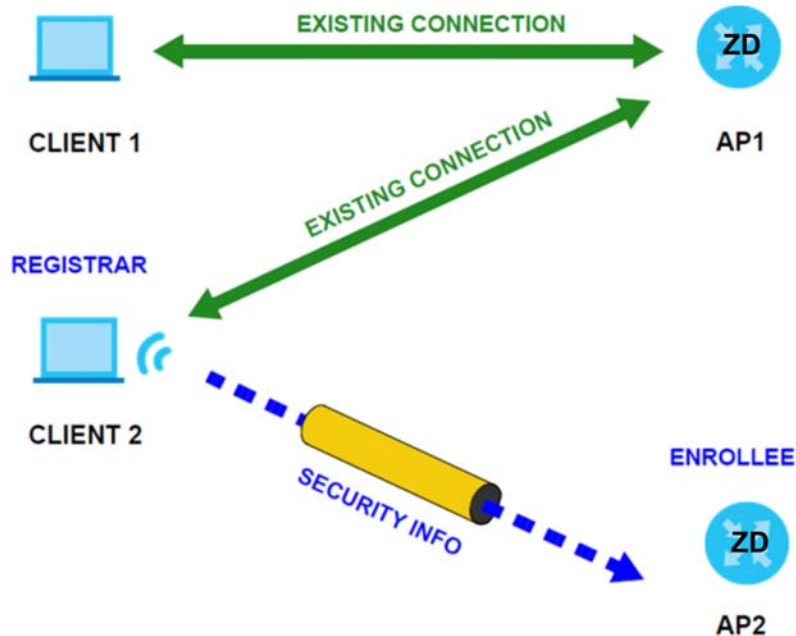
8.10.7.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

Home Networking

9.1 Home Networking Overview

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

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

Figure 108   Local Area Network of the Zyxel Device
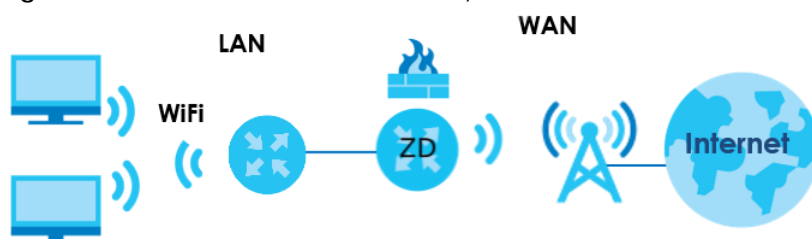
9.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 9.2 on page 195).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 9.3 on page 201).
- Use the **UPnP** screen to enable UPnP (Section 9.4 on page 203).
- Use the **Custom DHCP** screen to set additional DHCP options (Section 9.5 on page 204).

9.1.2 What You Need To Know

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

9.1.2.1 About LAN

IP Address

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

Subnet Mask

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

DHCP

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

DNS

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

RADVD (Router Advertisement Daemon)

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

9.1.2.2 About UPnP

How do I know if I am using UPnP?

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

NAT Traversal

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

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

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

Cautions with UPnP

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

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

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

UPnP and Zyxel

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

See Section 9.7 on page 208 for examples on installing and using UPnP.

9.1.3 Before You Begin

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

9.2 LAN Setup

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

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

Follow these steps to configure your LAN settings.

1 Select the **Interface Group** you want to set up the LAN. To configure an interface group, go to **Network Setting** > **Interface Grouping**. See Chapter 14 for more details about interface group.

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

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

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

Figure 109   Network Setting > Home Networking > LAN Setup

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.

Interface Group

Group Name   Default ▼

LAN IP Setup

IP Address   172 . 21 . 41 . 125

Subnet Mask   255 . 255 . 255 . 0

DHCP Server State

DHCP   ● Enable   ○ Disable   ○ DHCP Relay

IP Addressing Values

Beginning IP Address   192 . 168 . 1 . 2

Ending IP Address   192 . 168 . 1 . 254

Auto reserve IP for the same host   ⬤◯

DHCP Server Lease Time

1   days   0   hours   0   minutes

DNS Values

DNS   ● DNS Proxy   ○ Static   ○ From ISP

Figure 110 Network Setting > Home Networking > LAN Setup (continued)

LAN IPv6 Address Assign Setup

> Stateful ▼

LAN IPv6 DNS Assign Setup

> From Router Advertisement ▼

DHCPv6 Configuration

DHCPv6 Active   DHCPv6 Disable

IPv6 Router Advertisement State

RADVD Active   Enable

IPv6 Address Values

IPv6 Start Address

IPv6 End Address

IPv6 Domain Name

Client IAPD Setup

IAPD Enable

IPv6 Prefix

IPv6 Address

IPv6 DNS Values

IPv6 DNS Server 1   User Defined ▼

IPv6 DNS Server 2   User Defined ▼

IPv6 DNS Server 3   User Defined ▼

DNS Query Scenario

> IPv4/IPv6 DNS Server ▼

Cancel   Apply

Figure 111   Network Setting > Home Networking > LAN Setup

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.

Interface Group

Group Name   Default ▼

LAN IP Setup

IP Address   172 . 21 . 41 . 125

Subnet Mask   255 . 255 . 255 . 0

DHCP Server State

DHCP   ● Enable   ○ Disable   ○ DHCP Relay

IP Addressing Values

Beginning IP Address   192 . 168 . 1 . 2

Ending IP Address   192 . 168 . 1 . 254

Auto reserve IP for the
same host

DHCP Server Lease Time

1 days   0 hours   0 minutes

DNS Values

DNS   ● DNS Proxy   ○ Static   ○ From ISP

Figure 112

The following table describes the fields in this screen.

Table 62   Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group that you want to configure for the LAN settings. You must enable DHCP.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your in dotted decimal notation, for example, (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	

Table 62   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DHCP	Select **Enable** to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.
	If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN.
	If you select **DHCP Relay**, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
DHCP Relay Server Address	
This field is only available when you select **DHCP Relay** in the **DHCP** field.	
IP Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.
IP Addressing Values	
The **IP Addressing Values** fields appear only when you select **Enable** in the **DHCP** field.	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
DHCP Server Lease Time	
This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.	
This field is only available when you select **Enable** in the **DHCP** field.	
Days/Hours/Minutes	DHCP server leases an address to a new client device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different client device.
DNS Values	
This field appears only when you select **Enable** in the **DHCP** field.	
DNS	The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client.
	Select **DNS Proxy** to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.
	Select **Static** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.
	Select **From ISP** if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).
LAN IPv6 Mode Setup	
IPv6 Active	Use this to enable or disable IPv6 on the Zyxel Device.
	When IPv6 is used, the following fields need to be set.

Table 62   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
Link Local Address Type	A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows. Select **EUI64** to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select **Manual**. Link-local Unicast Address Format | 1111 1110 10	0	Interface ID
---	---	---
10 bits	54 bits	64 bits	
EUI64	Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format.
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.
LAN Global Identifier Type	Select **EUI64** to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select **Manual** to manually enter an interface ID for the LAN interface's global IPv6 address.
EUI64	Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address.
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Prefix Setup	Select **Delegate prefix from WAN** to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select **Static** to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: **Stateless**: The Zyxel Device uses IPv6 stateless auto-configuration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. **Stateful**: The Zyxel Device uses IPv6 stateful auto-configuration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6. **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. **From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. **DHCP Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 Address Values	
IPv6 Start Address	This field specifies the first of the contiguous addresses in the IPv6 address pool.

Table 62   Network Setting > Home Networking > LAN Setup (continued)

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

9.3 Static DHCP

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

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

9.3.1 Before You Begin

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

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

Figure 113 Network Setting > Home Networking > Static DHCP

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

➕ Static DHCP Configuration

#	Status	MAC Address	IP Address	Modify

The following table describes the labels in this screen.

Table 63 Network Setting > Home Networking > Static DHCP

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

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

Figure 114 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

Static DHCP Configuration

Active	🔵
Group Name	Default ▼
IP Type	IPv4
Select Device Info	Manual Input ▼
MAC Address	- - - - -
IP Address	. . .

Cancel   OK

The following table describes the labels in this screen.

Table 64   Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

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

9.4 UPnP

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

See 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 115 Network Setting > Home Networking > 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.

UPnP State

UPnP

UPnP NAT-T State

UPnP NAT-T

Note

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

#	Description	Destination IP Address	External Port	Internal Port	Protocol

Cancel   Apply

The following table describes the labels in this screen.

Table 65 Network Settings > Home Networking > UPnP

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

9.5 Custom DHCP

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

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

Figure 116   Network Setting > Home Networking > Custom DHCP

The following table describes the labels in this screen.

Table 66   Network Settings > Home Networking > Custom DHCP

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

9.5.1 Custom DHCP Configuration

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

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

Figure 117 Network Setting > Home Networking > Custom DHCP

The following table describes the labels in this screen.

Table 67   Network Settings > Home Networking > Custom DHCP

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

9.6 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.

9.6.1 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Zyxel Device as a DHCP server or

disable it. When configured as a server, the Zyxel Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

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

9.6.2 DNS Server Addresses

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

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

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

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

9.6.3 LAN TCP/IP

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

IP Address and Subnet Mask

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

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

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

reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

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

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

Private IP Addresses

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

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

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

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

9.7 Turn on UPnP in Windows 10 Example

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

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

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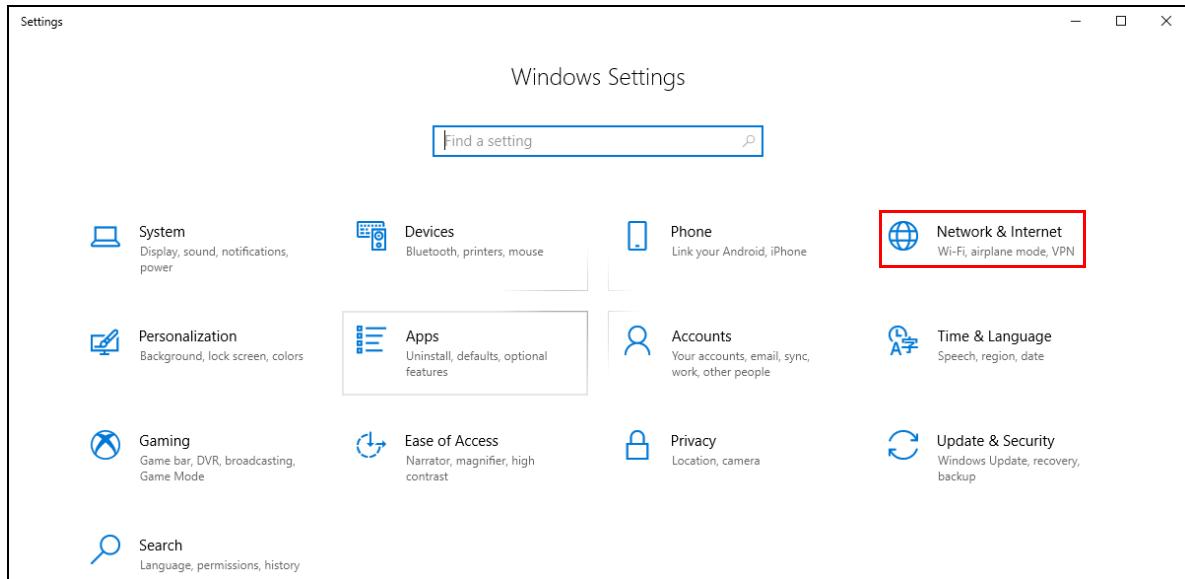
2 Click **Network and Sharing Center**.
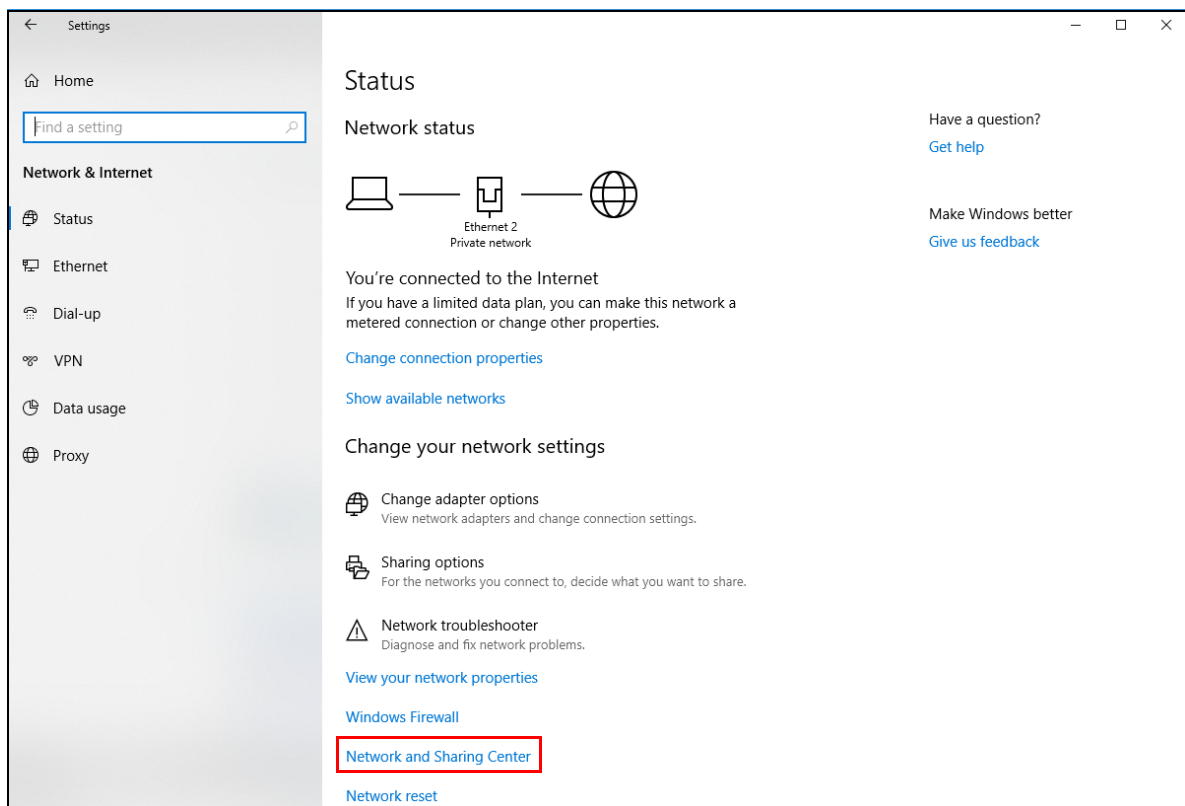
3 Click **Change advanced sharing settings.**
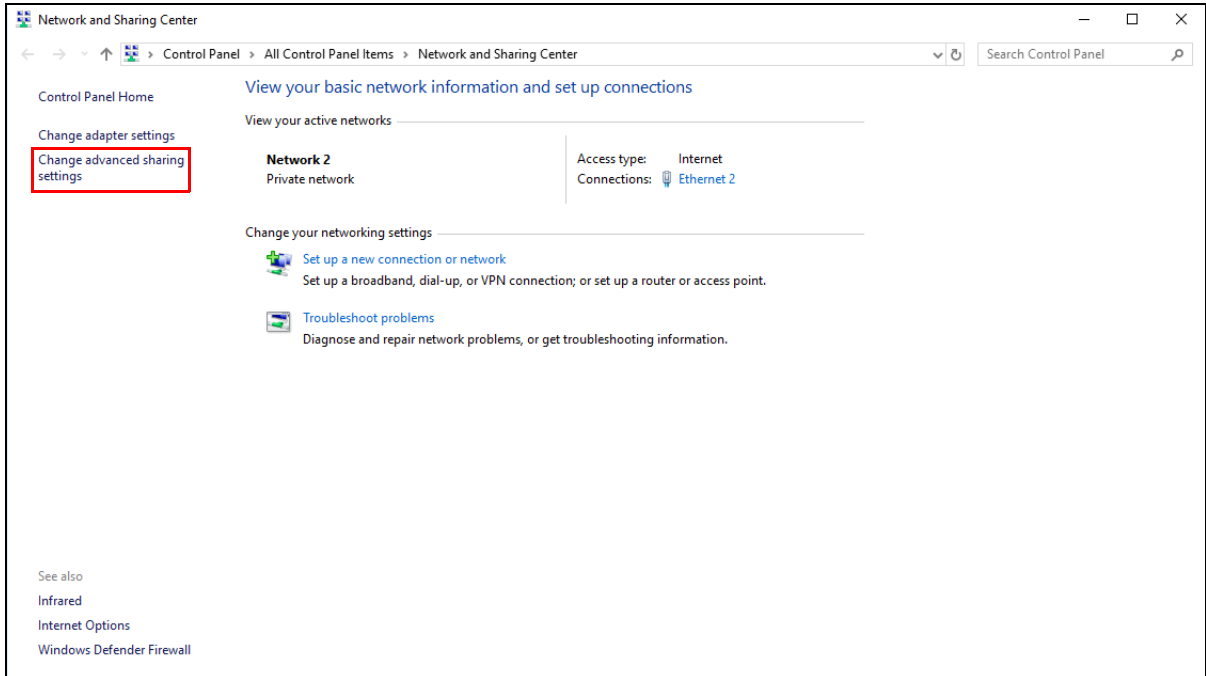
4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.
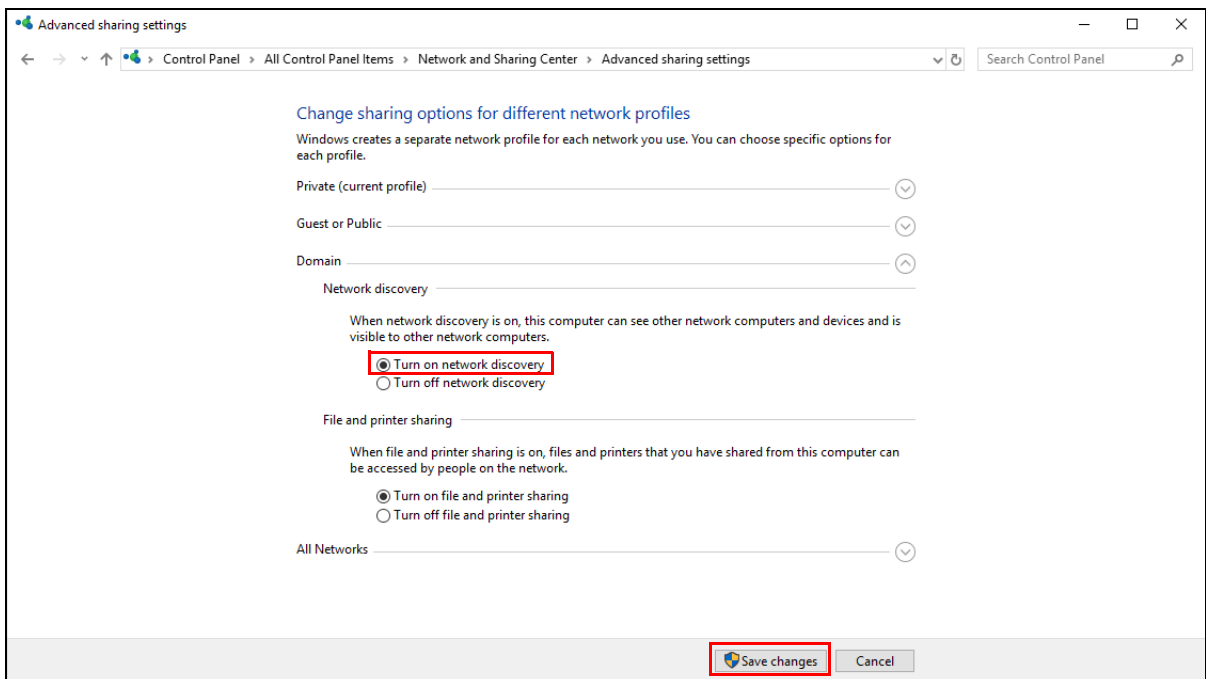
9.7.1 Auto-discover Your UPnP-enabled Network Device

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

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

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

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

Figure 118 Network Connections
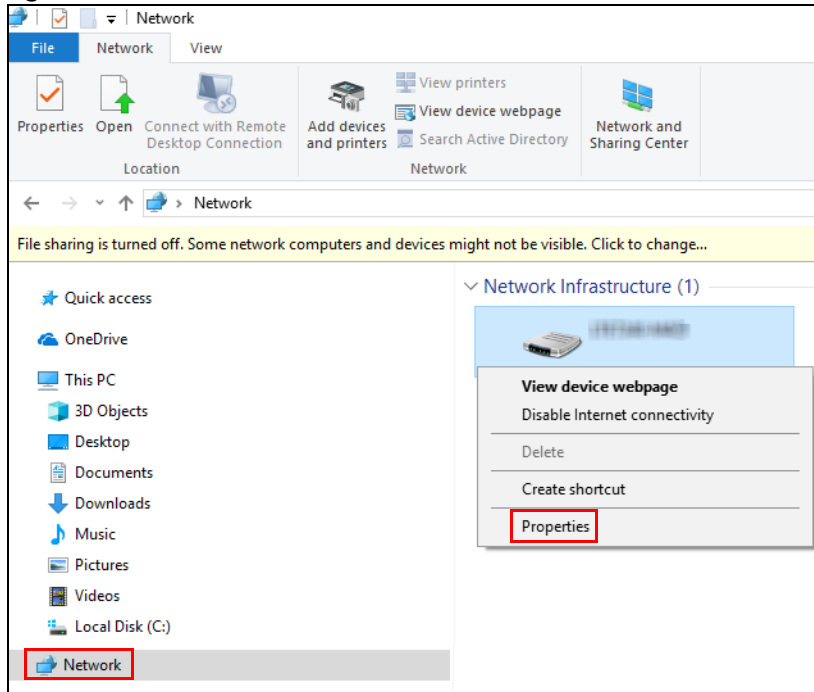
3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 119 Internet Connection Properties
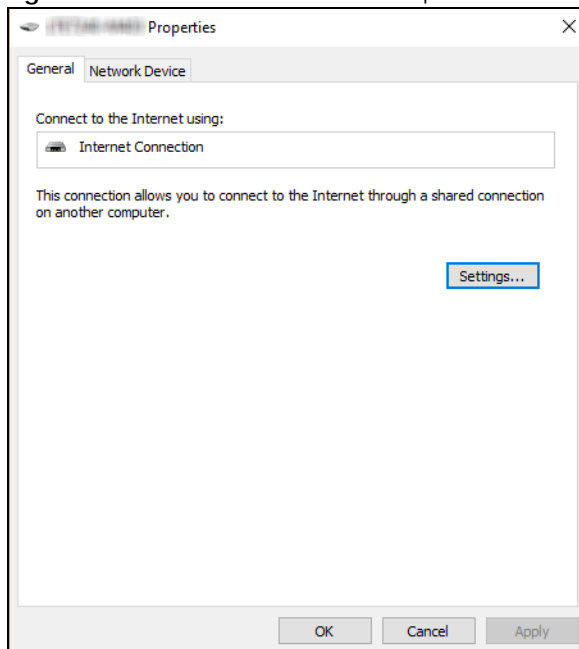
4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 120 Internet Connection Properties: Advanced Settings
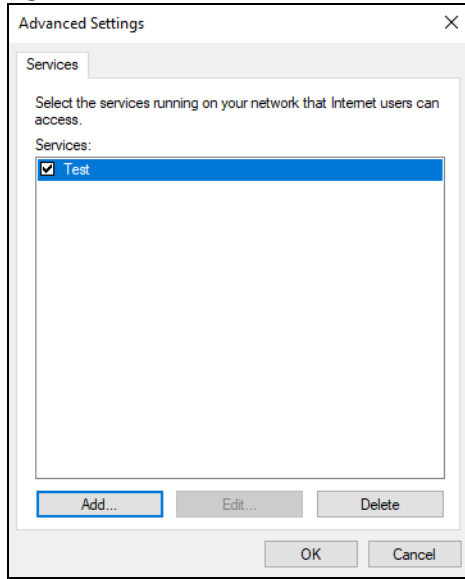
Figure 121 Internet Connection Properties: Advanced Settings: Add
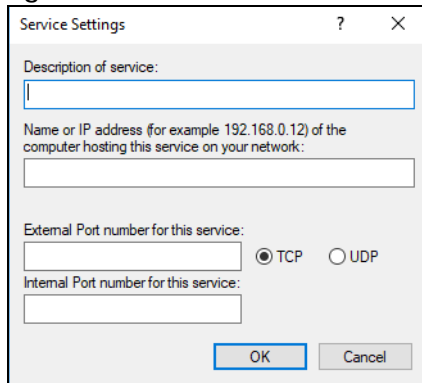
Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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

Figure 122 System Tray Icon
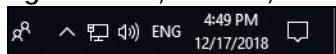
6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 123   Internet Connection Status
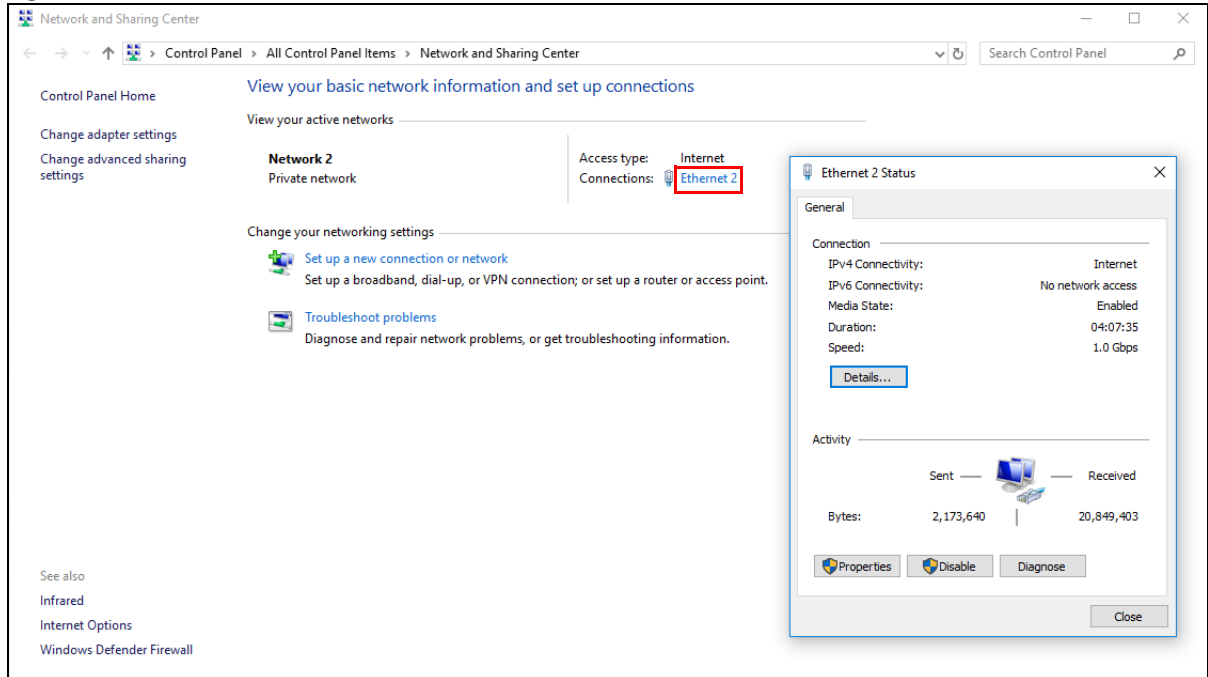
9.8 Web Configurator Access with UPnP in Windows 10

Follow the steps below to access the Web Configurator.

1   Open **File Explorer**.

2   Click **Network**.

Figure 124 Network Connections
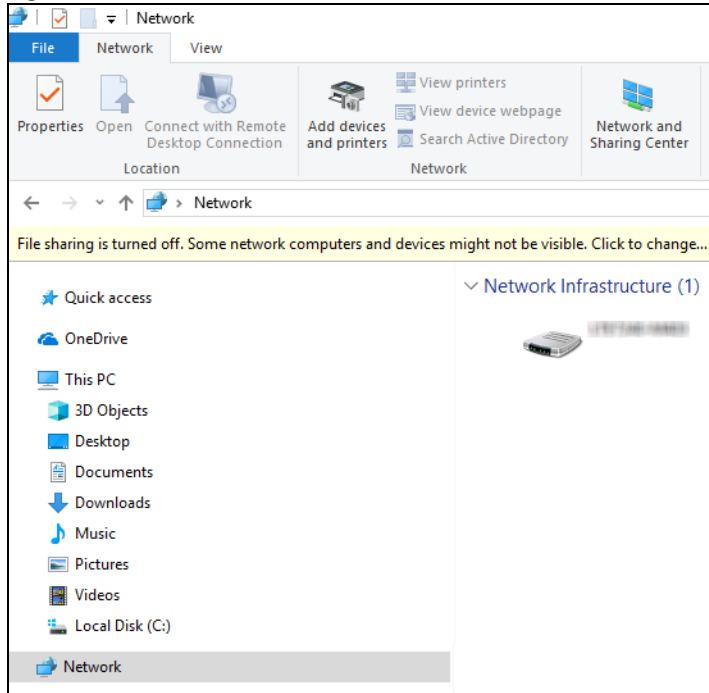
3 An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.

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

Figure 125 Network Connections: Network Infrastructure
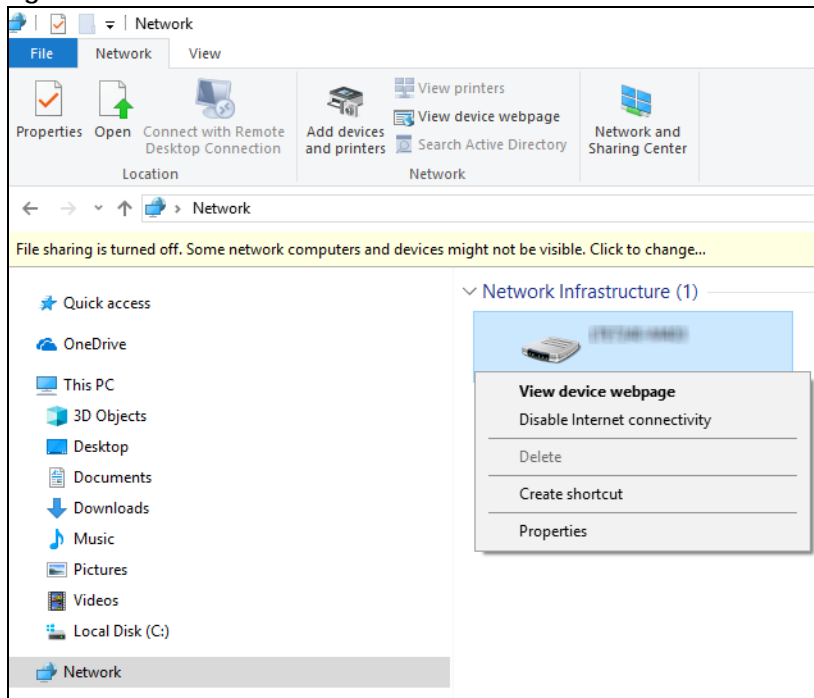
5 Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays information about the Zyxel Device.

Figure 126   Network Connections: Network Infrastructure: Properties: Example
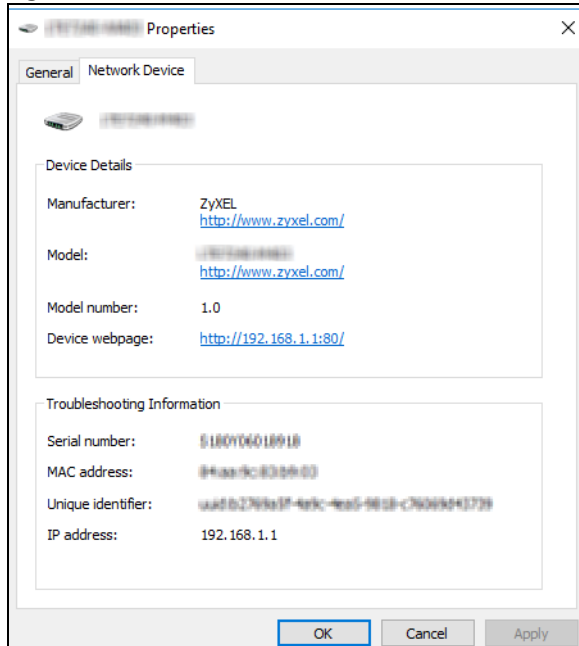
CHAPTER 10
Routing

10.1 Routing Overview

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

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

Figure 127   Example of Static Routing Topology
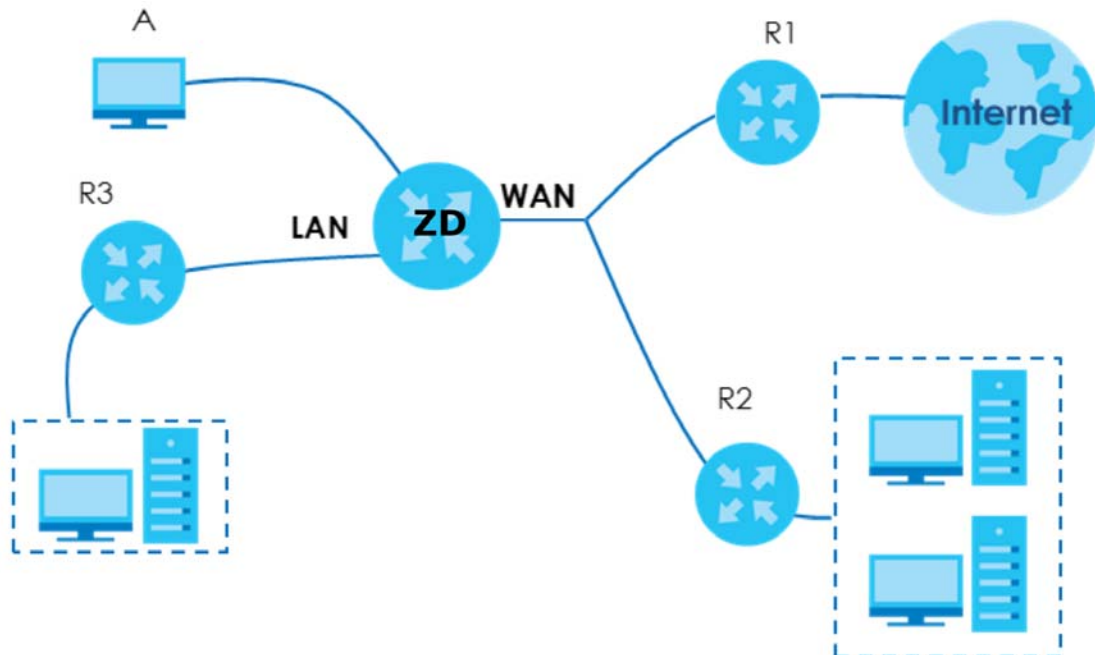
10.2 Configure Static Route

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

Figure 128 Network Setting > Routing > Static Route

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

＋ Add New Static Route

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

The following table describes the labels in this screen.

Table 68   Network Setting > Routing > Static Route

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

10.2.1 Add or Edit Static Route

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

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

Figure 129 Network Setting > Routing > Static Route > Add New Static Route

The following table describes the labels in this screen.

Table 69   Network Setting > Routing > Static Route > Add New Static Route

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

Table 69   Network Setting > Routing > Static Route > Add New Static Route (continued)

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

10.2.1.1 An Example of Adding a Static Route

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

In the following figure, router **R** is connected to the Zyxel Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Zyxel Device's WAN default gateway by default. In this case, **B** will never receive the traffic.
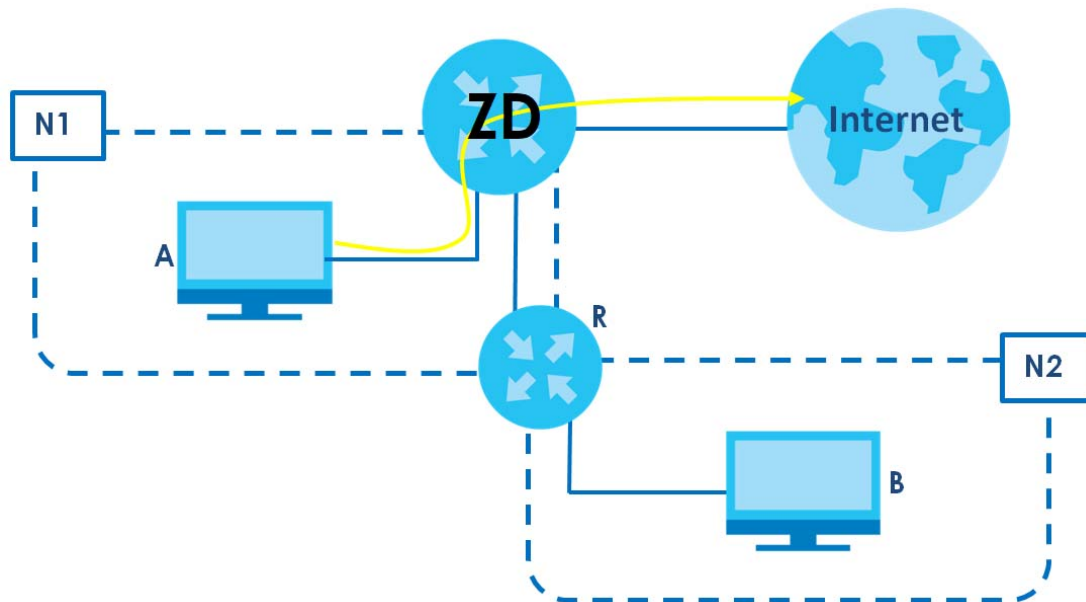
You need to specify a static routing rule on the Zyxel Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Zyxel Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.
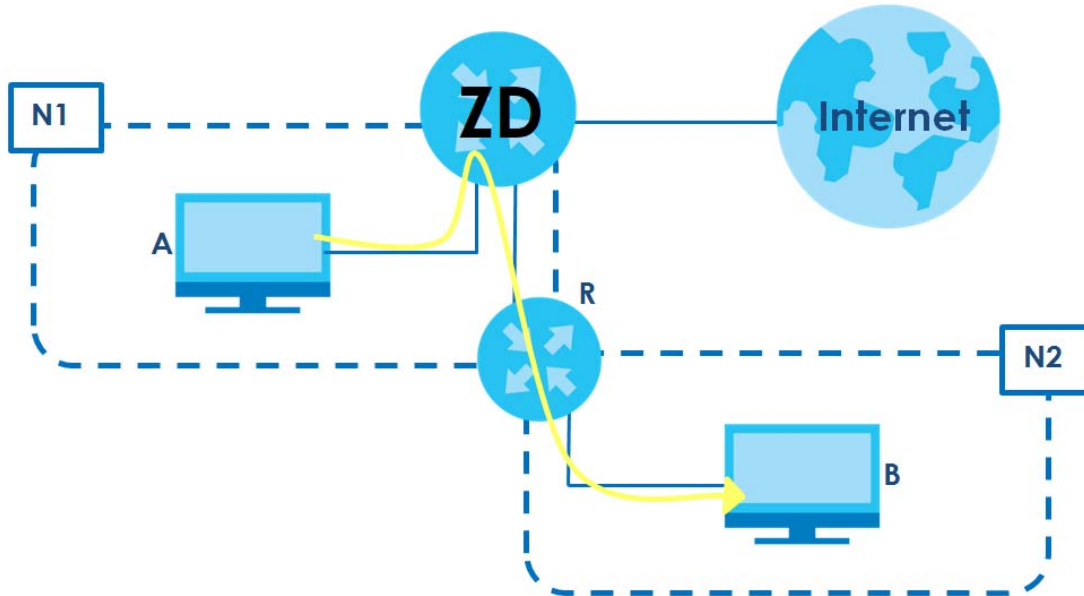
This tutorial uses the following example IP settings:

Table 70   IP Settings in this Tutorial

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

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

1   Log into the Zyxel Device's Web Configurator.

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

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

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

- Click the **Active** button to enable this static route. When the switch goes to the right, the function is enabled. Enter the **Route Name** as **R**.

- Set **IP Type** to **IPv4**.

- Enter the **Destination IP Address 192.168.10.1** and **IP Subnet Mask 255.255.255.0** for the destination, **N2**.

- Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right, the function is enabled. Enter **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.

- Select **Default** as the **Use Interface**.

- Click **OK**.

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

10.3 DNS Route

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface. Click **Network Setting** > **Routing** > **DNS Route** to open the **DNS Route** screen.

Figure 130 Network Setting > Routing > DNS Route

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface.

+ Add New DNS Route

#	Status	Domain Name	WAN Interface	Subnet Mask	Modify

Note

Maximum of 20 entries can be added.

The following table describes the labels in this screen.

Table 71   Network Setting > Routing > DNS Route

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

10.3.1 Add or Edit DNS Route

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

Figure 131 Network Setting > Routing > DNS Route > Add New DNS Route

Add New DNS Route

Active

Domain Name

Subnet Mask

WAN Interface   Cellular WAN

Cancel   OK

Figure 132 Network Setting > Routing > DNS Route > Add New DNS Route

The following table describes the labels in this screen.

Table 72   Network Setting > Routing > DNS Route > Add New DNS Route

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

10.4 Policy Route

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

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

Figure 133 Network Setting > Routing > Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address.

For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.

Add New Policy Route

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

The following table describes the labels in this screen.

Table 73   Network Setting > Routing > Policy Route

LABEL	DESCRIPTION
Add New Policy Route	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.
Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Source MAC	This is the source MAC address.
Source Interface	This is the interface from which the matched traffic is sent.
WAN Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to edit this policy.

Click the **Delete** icon to remove a policy from the Zyxel Device. A window displays asking you to confirm that you want to delete the policy. |

10.4.1 Add or Edit Policy Route

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

Figure 134 Network Setting > Routing > Policy Route: Add or Edit

The following table describes the labels in this screen.

Table 74   Network Setting > Routing > Policy Route: Add or Edit

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

10.5 RIP Overview

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

10.5.1 RIP

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

Figure 135 Network Setting > Routing > RIP

The following table describes the labels in this screen.

Table 75 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). **RIPv1** is universally supported but **RIPv2** carries more information. **RIPv1** is probably adequate for most networks, unless you have an unusual network topology. When set to **Both**, the Zyxel Device will broadcast its routing table periodically and incorporate the RIP information that it receives
Operation	Select **Passive** to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface.
	Select **Active** to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the checkbox to activate the settings.
Disable Default Gateway	Select the checkbox to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 11
Network Address Translation (NAT)

11.1 NAT Overview

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

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the servers on your local network (Section 11.2 on page 228).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings (Section 11.3 on page 231).
- Use the **DMZ** screen to configure a default server (Section 11.4 on page 235).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 11.5 on page 235).

11.1.2 What You Need To Know

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

Inside/Outside and Global/Local

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

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

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

11.2 Port Forwarding

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

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

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

Configure Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example), a default server IP address of 192.168.1.35 to a third (**C** in the example), and a default server IP address of 192.168.1.36 to a fourth (**D** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 136   Multiple Servers Behind NAT Example
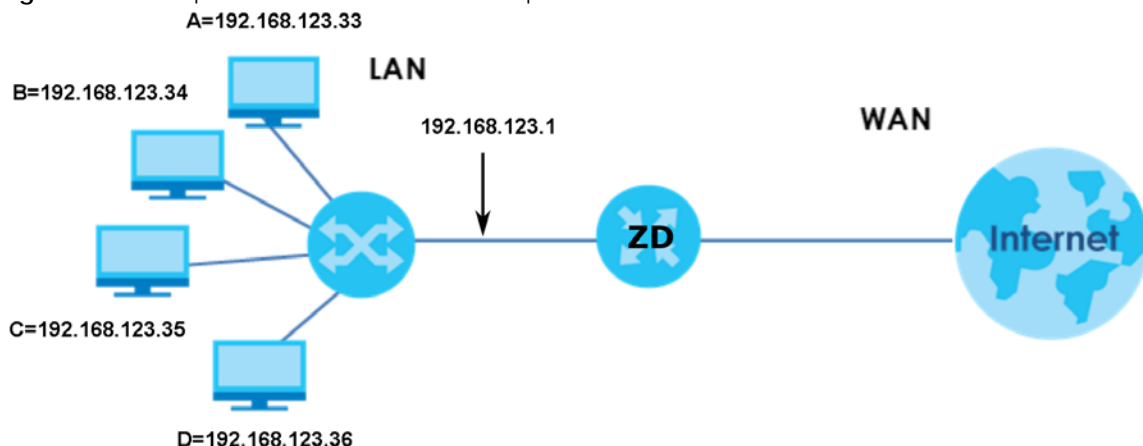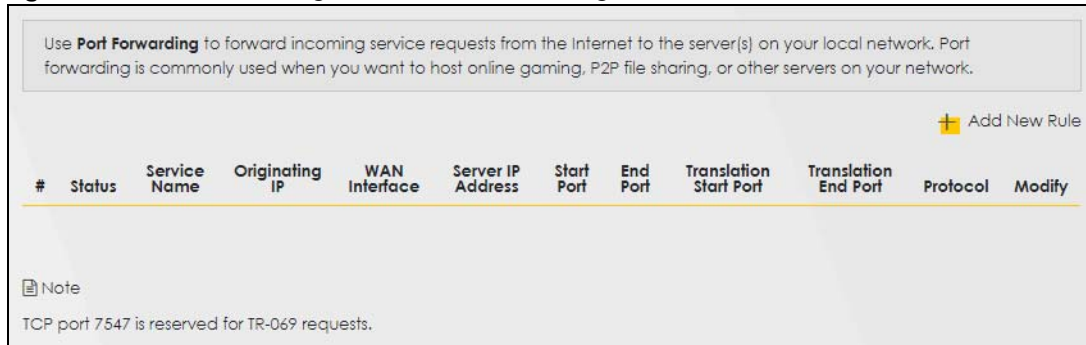
11.2.1 Port Forwarding

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

Note: TCP port 7547 is reserved for system use.

Figure 137 Network Setting > NAT > Port Forwarding

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

➕ Add New Rule

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

📄 Note

TCP port 7547 is reserved for TR-069 requests.

The following table describes the fields in this screen.

Table 76   Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
Originating IP	This is the source's IP address.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP) used to transport the packets for which you want to apply the rule.
Modify	Click the **Edit** icon to edit the port forwarding rule. Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

11.2.2 Add or Edit Port Forwarding

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

Figure 138 Network Setting > NAT > Port Forwarding: Add or Edit

Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
Here is an example to configure port translation. Configure **Start Port** to 100, **End Port** to 120, **Translation Start Port** to 200, and **Translation End Port** to 220.

Note: TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 77   Network Setting > NAT > Port Forwarding: Add or Edit

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

Table 77   Network Setting > NAT > Port Forwarding: Add or Edit (continued)

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

11.3 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service.

The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a \"trigger\" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol (\"open\" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 139 Trigger Port Forwarding Process: Example
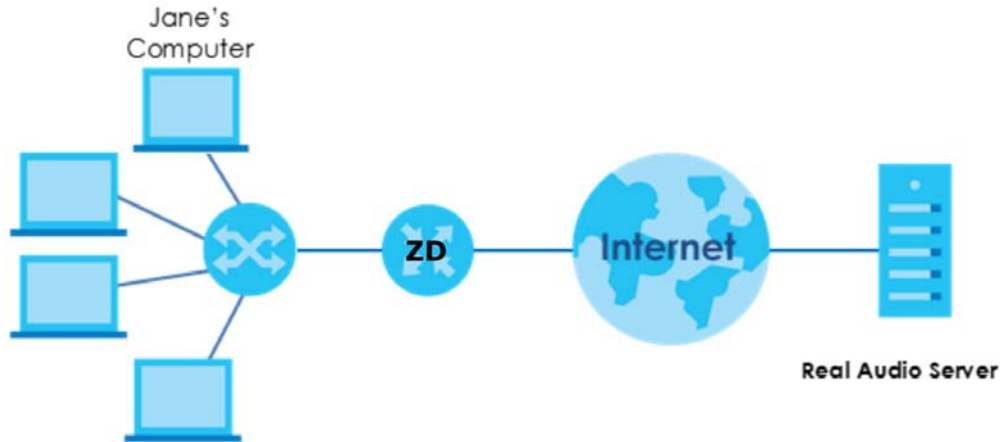
1 Jane requests a file from the Real Audio server (port 7070).

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

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

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

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

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

Note: TCP port 7547 is reserved for system use.

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

Figure 140 Network Setting > NAT > Port Triggering

The following table describes the labels in this screen.

Table 78   Network Setting > NAT > Port Triggering

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

11.3.1 Add or Edit Port Triggering Rule

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

Figure 141 Network Setting > NAT > Port Triggering: Add or Edit

The following table describes the labels in this screen.

Table 79   Network Setting > NAT > Port Triggering: Add or Edit

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

11.4 DMZ

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

You can put public servers, such as email and web servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host. Click **Network Setting** > **NAT** > **DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address of the default server in the **Default Server Address** field, and click **Apply** to activate the DMZ host. Otherwise, clear the IP address in the **Default Server Address** field, and click **Apply** to deactivate the DMZ host.

Figure 142   Network Setting > NAT > DMZ

The following table describes the fields in this screen.

Table 80   Network Setting > NAT > DMZ

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

11.5 ALG

Application Layer Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain applications such as Session Initiation Protocol (SIP) or file transfer in Instant Messaging (IM) applications. It allows SIP calls to pass through the Zyxel Device. When the Zyxel Device

registers with the SIP register server, the SIP ALG translates the Zyxel Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Zyxel Device is behind a SIP ALG.

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

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

Figure 143   Network Setting > NAT > ALG
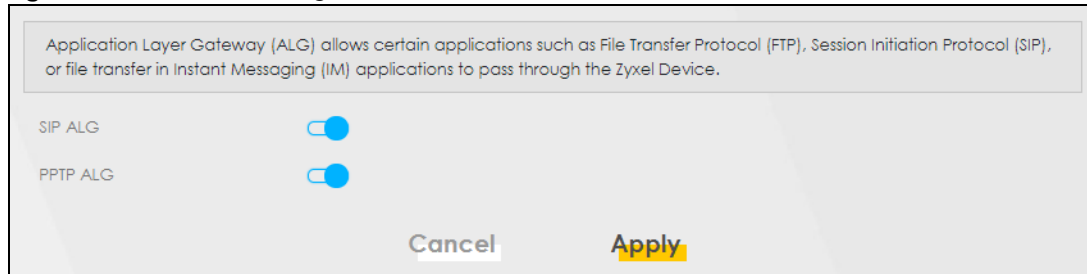
The following table describes the fields in this screen.

Table 81   Network Setting > NAT > ALG

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

11.6 Technical Reference

This part contains more information regarding NAT.

11.6.1 NAT Definitions

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

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

Note that inside or outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the

same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 82   NAT Definitions

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

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

11.6.2 What NAT Does

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

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

11.6.3 How NAT Works

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

Figure 144 How NAT Works
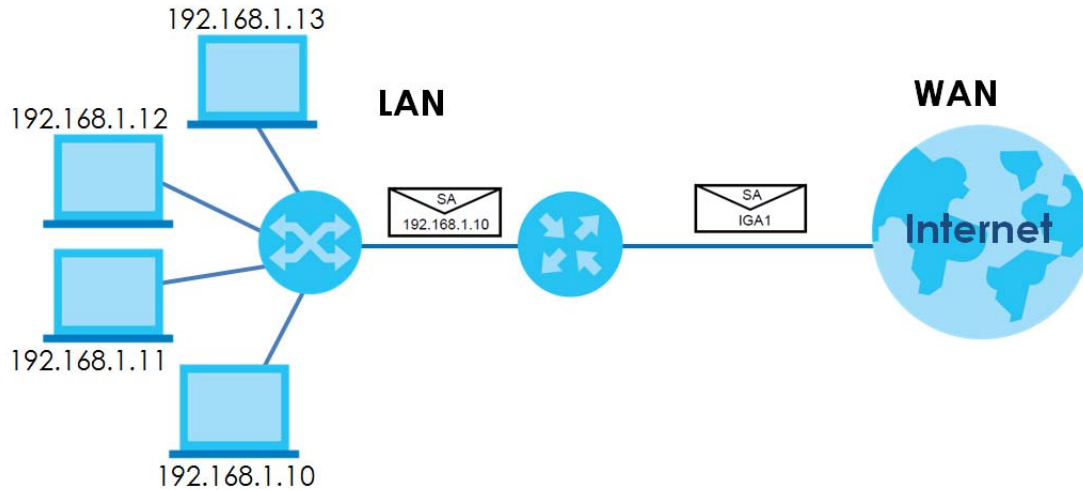
11.6.4 NAT Application

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

Figure 145 NAT Application With IP Alias
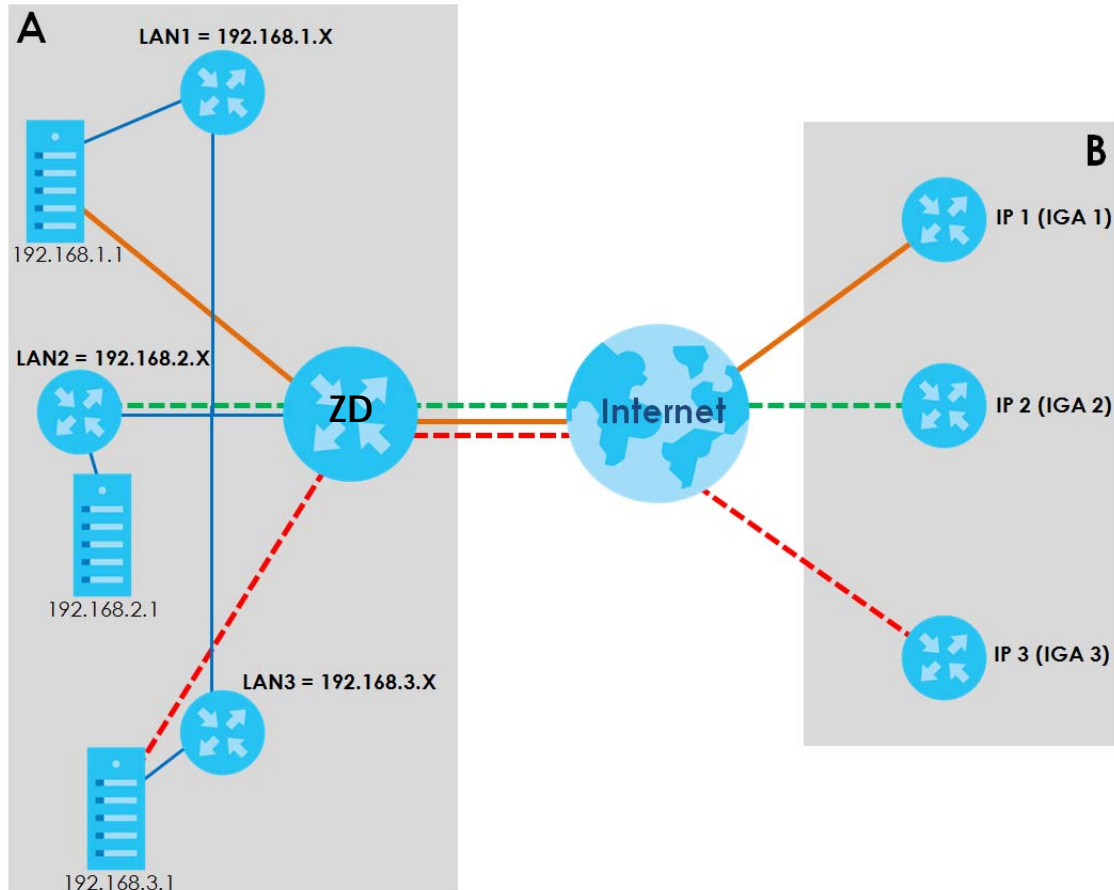
Port Forwarding: Services and Port Numbers

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

Table 83   Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

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

Figure 146   Multiple Servers Behind NAT Example
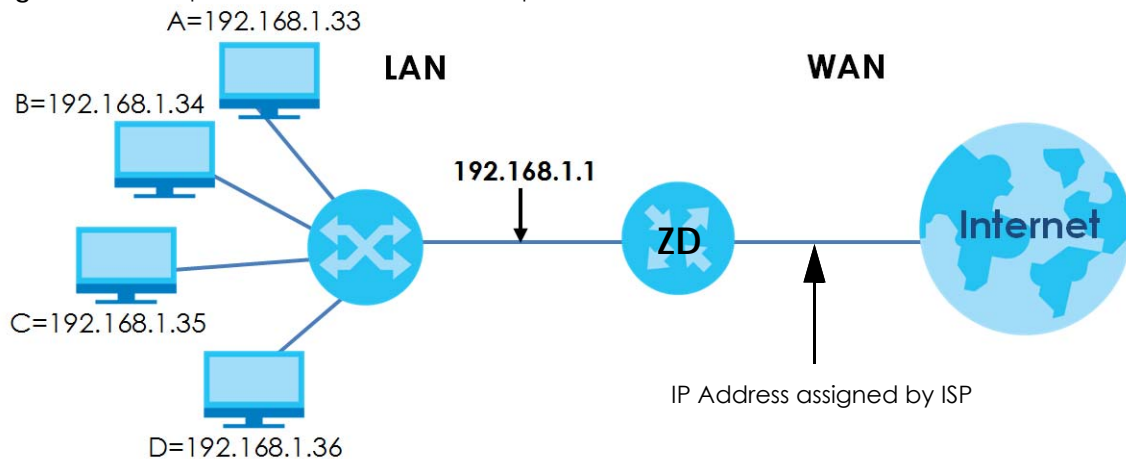
CHAPTER 12
DNS

12.1 DNS Overview

DNS

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

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

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, and so on). You can also access your Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they do not know your IP address.

You first need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 What You Can Do in this Chapter

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

12.1.2 What You Need To Know

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

12.2 DNS Entry (DNS)

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

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

Figure 147   Network Setting > DNS > DNS Entry

The following table describes the fields in this screen.

Table 84

LABEL	DESCRIPTION
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
HostName	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the **Edit** icon to edit the rule.
	Click the **Delete** icon to delete an existing rule.

12.2.1 Add or Edit DNS Entry

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

Figure 148   Network Setting > DNS > DNS Entry: Add

The following table describes the labels in this screen.

Table 85   Network Setting > DNS > DNS Entry: Add or Edit

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

12.3 Dynamic DNS

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Configure a DDNS service provider on your Zyxel Device. Click **Network Setting** > **DNS** > **Dynamic DNS**. The screen appears as shown.

Figure 149 Network Setting > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 86   Network Setting > DNS > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Enter the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the checkbox to enable DynDNS Wildcard.
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	
User Authentication Result	This shows **Success** if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.

Table 86   Network Setting > DNS > Dynamic DNS (continued)

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

CHAPTER 13
VLAN Group

13.1 VLAN Group Overview

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

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

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

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

Figure 150   VLAN Group Example
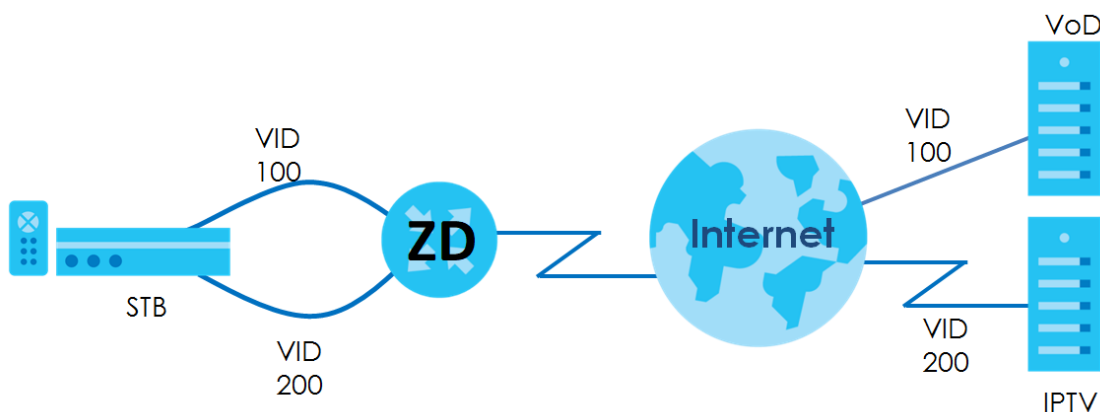
13.1.1 What You Can Do in this Chapter

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

13.2 VLAN Group Settings

This screen shows the VLAN groups created on the Zyxel Device. Click **Network Setting** > **VLAN Group** to open the following screen.

Figure 151   Network Setting > VLAN Group

The following table describes the fields in this screen.

Table 87   Network Setting > VLAN Group

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

13.2.1 Add or Edit a VLAN Group

Click the **Add New VLAN Group** button in the **VLAN Group** screen to open the following screen. Use this screen to create a new VLAN group.

Figure 152 Network Setting > VLAN Group > Add New VLAN Group/Edit

The following table describes the fields in this screen.

Table 88   Network Setting > VLAN Group > Add New VLAN Group/Edit

LABEL	DESCRIPTION
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify this VLAN group. Outgoing traffic is tagged with this ID if **TX Tagging** is selected below.
LAN	Select **Include** to add the associated LAN interface to this VLAN group. Note: Select **TX Tagging** to tag outgoing traffic from the associated LAN port with the **VLAN ID** number entered above.

CHAPTER 14
Interface Grouping

14.1 Interface Grouping Overview

By default, all LAN and WAN interfaces on the Zyxel Device are in the default group. Client devices in the default group can communicate with all devices in the default and other groups. Create interface groups to have the Zyxel Device assign IP addresses in different domains. Each group acts as an independent network on the Zyxel Device. Client devices in the same group can communicate with each other directly. Interfaces that do not belong to any user-defined group belong to the default group.

14.1.1 What You Can Do in this Chapter

The **Interface Grouping** screen lets you create multiple networks on the Zyxel Device (Section 14.2 on page 248).

14.2 Interface Grouping

You can manually add a LAN interface to a new group. Alternatively, you can have the Zyxel Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN Setup** screen to configure the private IP addresses the DHCP server on the Zyxel Device assigns to the clients in the default and/or user-defined groups. If you set the Zyxel Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 9 on page 193 for more information.

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 153   Interface Grouping Application
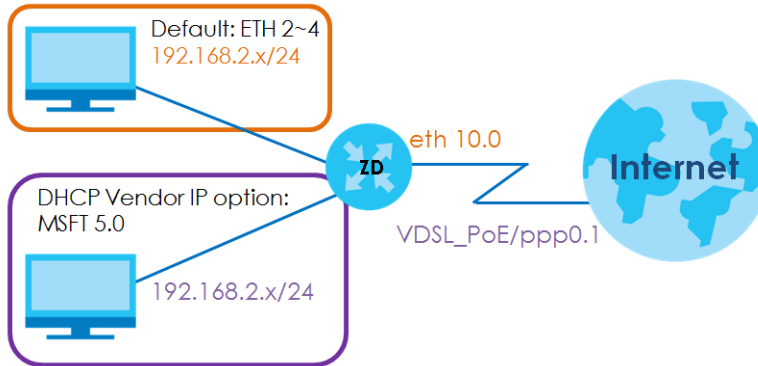
You can use this screen to create new user-defined interface groups or modify existing ones. Interfaces that do not belong to any user-defined group always belong to the default group.

Click **Network Setting** > **Interface Grouping** to open the following screen.

Figure 154   Network Setting > Interface Grouping

The following table describes the fields in this screen.

Table 89   Network Setting > Interface Grouping

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

14.2.1 Interface Group Configuration

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

Note: An interface can belong to only one group at a time.

Note: After configuring a vendor ID, reboot the client device attached to the Zyxel Device to obtain an appropriate IP address.

Note: You can have up to 15 filter criteria.

Figure 155   Network Setting > Interface Grouping > Add New Interface Group/Edit

The following table describes the fields in this screen.

Table 90   Network Setting > Interface Grouping > Add New Interface Group/Edit

LABEL	DESCRIPTION
Group Name	Enter a descriptive name for this interface group. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface. Select **None** to not add a WAN interface to this group.
Selected LAN Interfaces Available LAN Interfaces	Select one or more interfaces (Ethernet LAN, wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Selected LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Selected LAN Interfaces**, use the right-facing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	Click **Add** to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 14.2.2 on page 251 for more information.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
WildCard Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the **Edit** icon to change the group setting. Click the **Delete** icon to delete this group from the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click OK to save your changes.

14.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen. Use this screen to automatically add clients to an interface group based on specified criteria. You can choose to define a group based on a MAC address, a vendor ID (DHCP option 60), an Identity Association Identifier (DHCP option 61), vendor specific information (DHCP option 125), or a VLAN group.

Figure 156 Network Setting > Interface Grouping > Interface Group Configuration: Add

The following table describes the fields in this screen.

Table 91 Network Setting > Interface Grouping > Interface Group Configuration: Add

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first 3 bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
VLAN Group	Select this and the VLAN group of the matched traffic from the drop-down list box. A VLAN group can be configured in **Network Setting** > **VLAN Group**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

CHAPTER 15
USB Service

15.1 USB Service Overview

You can share files on a USB memory stick or hard drive connected to your Zyxel Device with users on your network.

The following figure is an overview of the Zyxel Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Zyxel Device.

Figure 157   File Sharing Overview
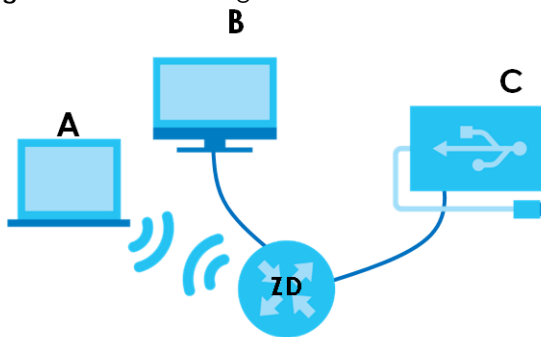
The Zyxel Device will not be able to join a workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

15.1.1 What You Need To Know

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

15.1.2 File Sharing

Workgroup Name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Zyxel Device is given a folder, called a "share". If a USB hard drive connected to the Zyxel Device has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Zyxel Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Zyxel Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Zyxel Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

15.1.3 Before You Begin

1 Make sure the Zyxel Device is connected to your network and turned on.

2 Connect the USB device to one of the Zyxel Device's USB port. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source.

3 The Zyxel Device detects the USB device and makes its contents available for browsing.

Note: If your USB device cannot be detected by the Zyxel Device, see the troubleshooting for suggestions.

15.2 USB Service

Use this screen to set up file sharing through the Zyxel Device. The Zyxel Device's LAN users can access the shared folder (or share) from the USB device inserted in the Zyxel Device. To access this screen, click **Network Setting** > **USB Service**.

Figure 158 Network Setting > USB Service

Note: The **Share Directory List** is only visible when you connect a USB device.

Each field is described in the following table.

Table 92   Network Setting > USB Service

LABEL	DESCRIPTION
Information	
Volume	This is the volume name the Zyxel Device gives to an inserted USB device.
Capacity	This is the total available memory size (in megabytes) on the USB device.
Used Space	This is the memory size (in megabytes) already used on the USB device.
Server Configuration	
File Sharing Services	Click this switch to enable file sharing through the Zyxel Device.
Share Directory List	
This only appears when you have inserted a USB device.	
Add New Share	Click this to set up a new share on the Zyxel Device.
Active	Select this to allow the share to be accessed.

Table 92   Network Setting > USB Service (continued)

LABEL	DESCRIPTION
Status	This field shows the status of the share : The share is not activated. : The share is activated.
Share Name	This field displays the name of the file you shared.
Share Path	This field displays the location in the USB of the file you shared.
Share Description	This field displays a description of the file you shared.
Modify	Click the **Edit** icon to change the settings of an existing share. Click the **Delete** icon to delete this share in the list.
Account Management	
Add New User	Click this button to create a user account to access the secured shares. This button redirects you to **Maintenance** > **User Account**.
Status	This field shows the status of the user. : The user account is not activated for the share. : The user account is activated for the share.
User Name	This is the name of a user who is allowed to access the secured shares on the USB device.
Cancel	Click this to restore your previously saved settings.
Apply	Click this to save your changes to the Zyxel Device.

15.2.1 Add New Share

Use this screen to set up a new share or edit an existing share on the Zyxel Device. Click **Add New Share** in the **File Sharing** screen or click the **Edit** or **Modify** icon next to an existing share.

Please note that you need to set up shared folders on the USB device before enabling file sharing in the Zyxel Device. Spaces and the following special characters, ["], [`], ['], [<], [>], [^], [$], [|], [&], [;], are not allowed for the USB share name.

Figure 159 Network Setting > USB Service > Add New Share

The following table describes the labels in this menu.

Table 93   Network Setting > USB Service > Add New Share

LABEL	DESCRIPTION
Volume	Select the volume in the USB storage device that you want to add as a share in the Zyxel Device.
	This field is read-only when you are editing the share.
Share Path	Manually enter the file path for the share, or click the **Browse** button and select the folder that you want to add as a share.
	This field is read-only when you are editing the share.
Description	You can either enter a short description of the share, or leave this field blank. You can use up to 128 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed.
Access Level	Select **Public** if you want the share to be accessed by users connecting to the Zyxel Device. Otherwise, select **Security**.
Allowed	If **Security** is selected in the **Access Level** field, select this checkbox to allow/prohibit access to the share.
User Name	This field specifies the user for which the **Allowed** setting applies. Users can be added or modified in **Maintenance** > **User Account**.
Cancel	Click **Cancel** to return to the previous screen.
OK	Click **OK** to save your changes.

15.2.2 Add New User Screen

Once you click the **Add New User** button, you will be directed to the **User Account** screen. To create a user account that can access the secured shares on the USB device, click the **Add New Account** button in the **Network Setting** > **USB Service** > **User Account screen**.

Please see Chapter 26 on page 303, for detailed information about **User Account** screen.

CHAPTER 16
Nebula

16.1 Nebula Overview

You can manage the Zyxel Device through the Nebula Control Center (NCC), see Section 1.2 on page 21 for more information.

16.2 Nebula

Use this screen to:

• Enable **Nebula Discovery** to have the Zyxel Device to try to connect to the NCC.

• Configure the proxy server settings if the Zyxel Device is behind a proxy server.

To access this screen, click **Network Setting** > **Nebula**.

Figure 160 Network Setting > Nebula

If the Zyxel Device is connected and registered with the Nebula Control Center, the screen appears as below.

Figure 161 Network Setting > Nebula (with registration in the Nebula Control Center)

Each field is described in the following table.

Table 94   Network Setting > Nebula

LABEL	DESCRIPTION
Nebula Discovery	Slide the switch to the right to enable **Nebula Discovery** to have the Zyxel Device try to connect to the NCC. Once the Zyxel Device is connected to and has registered in the NCC, it'll go into the Nebula cloud management mode.
	If **Nebula Discovery** is disabled, the Zyxel Device will not discover the NCC and remain in standalone operation.
	This is not configurable and will only display **ON** when your Zyxel Device is being managed by NCC. See Figure 161 on page 259.
Use Proxy to Access to NCC	If the Zyxel Device is behind a proxy server, slide the switch to the right to enable this feature. Configure the proxy server settings so the Zyxel Device can access the NCC through the proxy server.
Proxy Server	Enter the IP address of the proxy server.
Proxy Port	Enter the service port number used by the proxy server.
Authentication	Enable this if the proxy server requires authentication before it grants access to the NCC.
User Name	Enter you proxy user name.
Password	Enter your proxy password.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to set the settings in this screen back to default.

CHAPTER 17
Firewall

17.1 Firewall Overview

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

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

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

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

Figure 162   Default Firewall Action
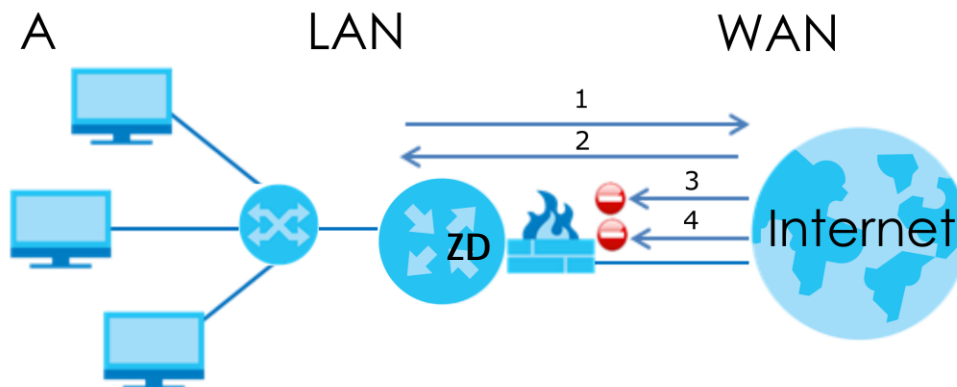
17.1.1 What You Need to Know About Firewall

SYN Attack

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

DoS

Denial-of-Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access

to network resources. The Zyxel Device is pre-configured to automatically detect and thwart all known DoS attacks.

DoS Thresholds

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

DDoS

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

ICMP

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

LAND Attack

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

Ping of Death

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

SPI

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

17.2 Firewall

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

17.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device (Section 17.3 on page 262).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 17.4 on page 263).

- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules (Section 17.5 on page 264).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 17.6 on page 266).

17.3 General

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

Figure 163 Security > Firewall > General
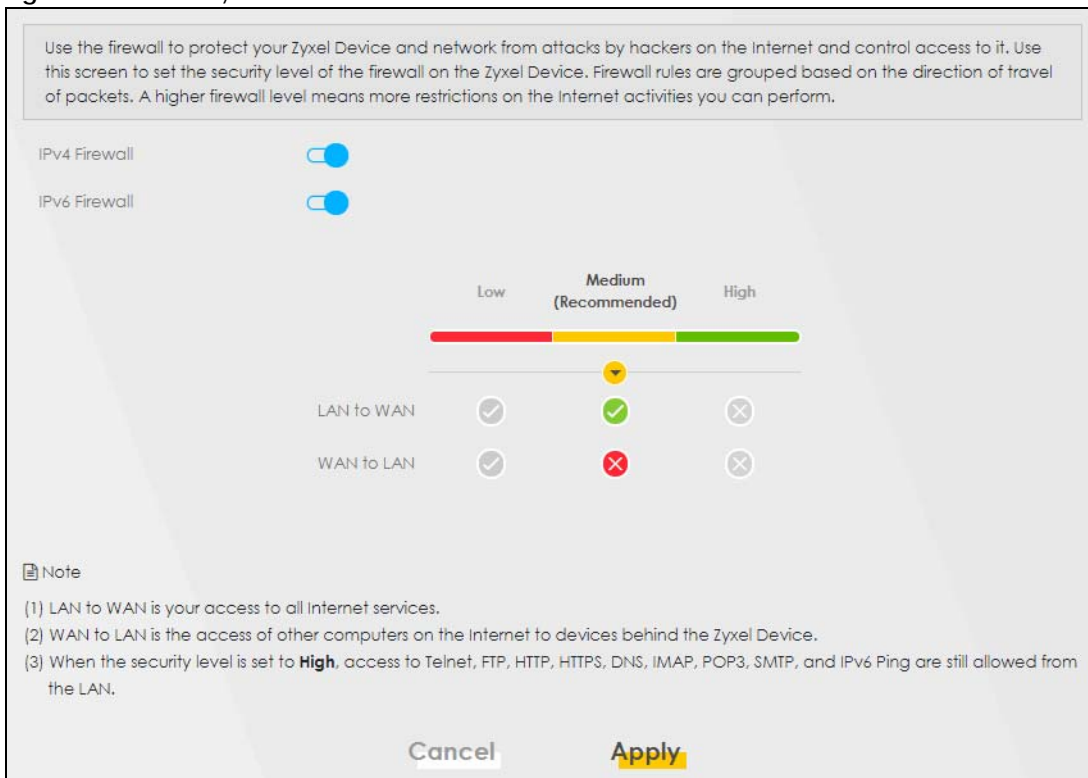
Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.
When the security level is set to **High**, Telnet, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

The following table describes the labels in this screen.

Table 95   Security > Firewall > General
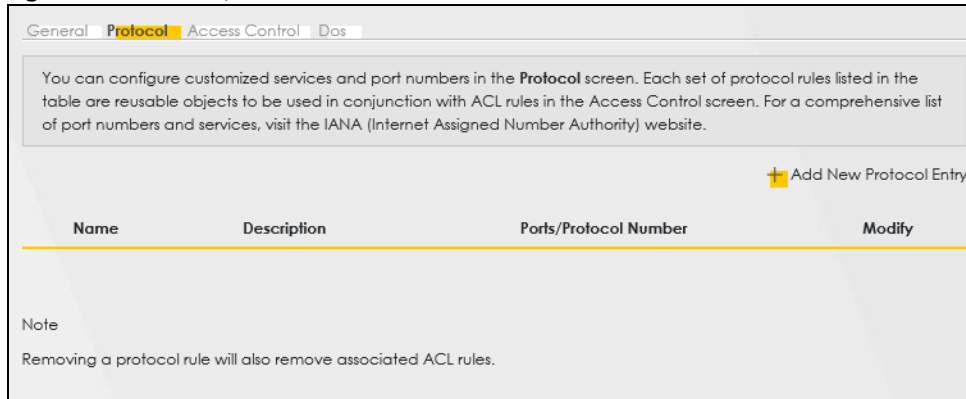
LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using **IPv4** (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using **IPv6** (Internet Protocol version 6).
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.
Medium	This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.
Low	This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

17.4 Protocol (Customized Services)

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security** > **Firewall** > **Protocol** to display the following screen.

Note: Removing a protocol rule will also remove associated ACL rules.

Figure 164   Security > Firewall > Protocol

The following table describes the labels in this screen.

Table 96   Security > Firewall > Protocol

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

Table 96   Security > Firewall > Protocol (continued)

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

17.4.1 Add Customized Service

Add a customized rule or edit an existing rule by specifying the protocol and the port numbers. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

Figure 165   Security > Firewall > Protocol: Add New Protocol Entry

The following table describes the labels in this screen.

Table 97   Security > Firewall > Protocol: Add New Protocol Entry

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

17.5 Access Control (Rules)

An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed. Click **Security** > **Firewall** > **Access Control** to display the following screen.

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

Figure 166   Security > Firewall > Access Control

The following table describes the labels in this screen.

Table 98   Security > Firewall > Access Control

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

17.5.1 Add New ACL Rule

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

The following table describes the labels in this screen.

Table 99   Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name for your filter rule. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed.
Order	Assign the order of your rules as rules are applied in turn.
Source IP Address	If you selected **Specific IP Address** in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select **Specific IP Address**. If not, select a detected device.
Destination IP Address	If you selected **Specific IP Address** in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.
IP Type	Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4/IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD).
Select Service	Select a service from the **Select Service** box.
Protocol	Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN).

This appears when you select **TCP/UDP** or **TCP** in the **Protocol** field. |
Policy	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule.
Direction	Select **WAN to LAN** to apply the rule to traffic from WAN to LAN. Select **LAN to WAN** to apply the rule to traffic from LAN to WAN. Select **WAN to Router** to apply the rule to traffic from WAN to router. Select **LAN to Router** to apply the rule to traffic from LAN to router.
Enable Rate Limit	Click this switch to enable the setting of maximum number of packets per maximum number of minute or second to limit the throughput of traffic that matches this rule. If not, the next item will be disabled.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by clicking **Add New Rule**. This will bring you to the **Security** > **Scheduler Rules** screen.
packet(s) per (1–512)	Enter the maximum number of packets (1 – 512) per minute or second.
Add New Rule	Select a schedule rule for this ACL rule from the drop-down list box. You can configure a new schedule rule by clicking **Add New Rule**.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

17.6 DoS

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Use the **DoS** screen to activate protection against DoS attacks.

Click **Security** > **Firewall** > **DoS** to display the following screen.

Figure 167   Security > Firewall > DoS
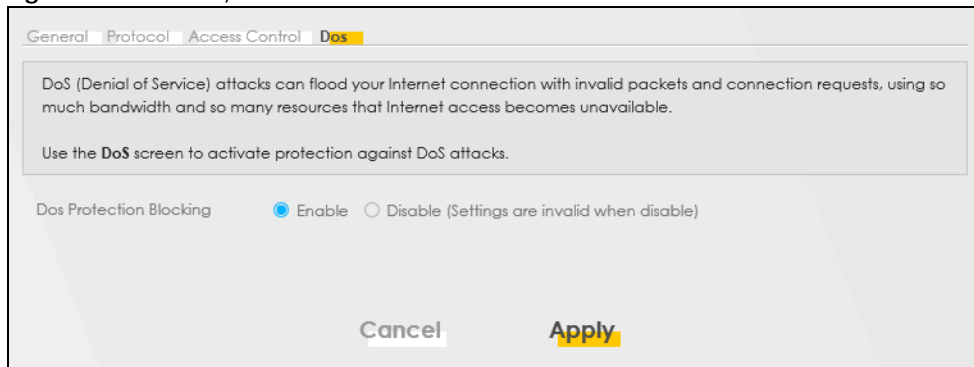
The following table describes the labels in this screen.

Table 100   Security > Firewall > DoS

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

17.7 Firewall Technical Reference

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

17.7.1 Firewall Rules Overview

Your customized rules take precedence and override the Zyxel Device's default settings. The Zyxel Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the Zyxel Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to Router
- WAN to LAN
- LAN to WAN
- WAN to Router

By default, the Zyxel Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to Router

  These rules specify which computers on the LAN can manage the Zyxel Device (remote management).

Note: You can also configure the remote management settings to allow only a specific computer to manage the Zyxel Device.

- LAN to WAN

  These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the Zyxel Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN

  These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to Router

  By default the Zyxel Device stops computers on the WAN from managing the Zyxel Device. You could configure one of these rules to allow a WAN computer to manage the Zyxel Device.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the Zyxel Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the Zyxel Device's default rules.

17.7.2 Guidelines For Security Enhancement With Your Firewall

1 Change the default password through the Web Configurator.

2 Think about access control before you connect to the network in any way.

3 Limit who can access your router.

4 Do not enable any local service (such as telnet) that you do not use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

17.7.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Zyxel Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC (Internet Relay Chat) is blocked, are there users that require this service?

2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

3 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the Web Configurator screens.

Figure 168   Security > MAC Filter

MAC Filter

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** scree wired connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is a factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the M the LAN client to configure this screen.

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

MAC Restrict Mode   ● Allow   ○ Deny

Set	Active	Host Name	MAC Address

Note

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

CHAPTER 18
Certificates

18.1 Certificates Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

18.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Zyxel Device's CA-signed (Certification Authority) certificates ().
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer ().

18.2 What You Need to Know

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

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Zyxel Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

18.3 Local Certificates

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

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

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

Figure 169 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

Table 101   Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by password	Select the checkbox and enter the private key into the text box to store it on the Zyxel Device. You can use up to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
Choose File/ Browse	Click this button to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Zyxel Device.
Create Certificate Request	Click this button to go to the screen where you can have the Zyxel Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have a unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.

Table 101   Security > Certificates > Local Certificates (continued)

LABEL	DESCRIPTION
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate. For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

18.3.1 Create Certificate Request

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

Figure 170   Security > Certificates > Local Certificates: Create Certificate Request

The following table describes the labels in this screen.

Table 102   Security > Certificates > Local Certificates: Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Enter a descriptive name to identify this certificate. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed.
Common Name	Select **Auto** to have the Zyxel Device configure this field automatically. Or select **Customize** to enter it manually. Enter the IP address (in dotted decimal notation), domain name or email address in the field provided. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Enter a descriptive name to identify the company or group to which the certificate owner belongs. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed.

Table 102   Security > Certificates > Local Certificates: Create Certificate Request (continued)

LABEL	DESCRIPTION
State/Province Name	Enter a descriptive name to identify the state or province where the certificate owner is located. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

18.3.2 View Certificate Request

Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

Click the **View** icon in the **Local Certificates** screen to open the following screen.

Figure 171 Security > Certificates > Local Certificates: View Certificate

The following table describes the fields in this screen.

Table 103 Security > Certificates > Local Certificates: View Certificate

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

Table 103   Security > Certificates > Local Certificates: View Certificate (continued)

LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click **Back** to return to the previous screen.

18.4 Trusted CA

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

Figure 172   A maximum of ten certificates can be added.Security > Certificates > Trusted CA

The following table describes the labels in this screen.

Table 104   Security > Certificates > Trusted CA

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

Table 104   Security > Certificates > Trusted CA (continued)

LABEL	DESCRIPTION
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

18.5 Import Trusted CA Certificate

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

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

Figure 173   Security > Certificates > Trusted CA > Import Certificate

The following table describes the labels in this screen.

Table 105   Security > Certificates > Trusted CA > Import Certificate

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

18.6 View Trusted CA Certificate

Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Click **Security** > **Certificates** > **Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 174   Security > Certificates > Trusted CA > View Certificate
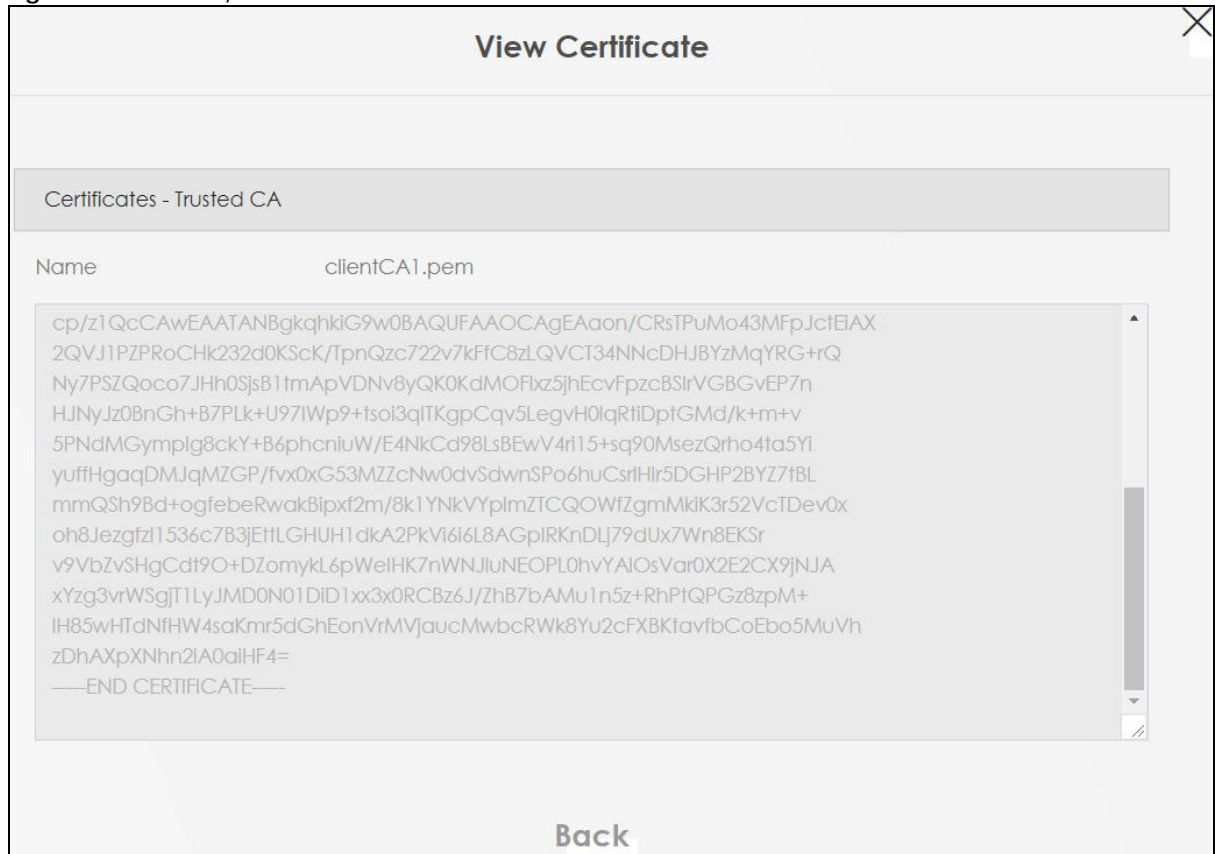
The following table describes the labels in this screen.

Table 106   Security > Certificates > Trusted CA > View Certificate

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

18.7 Certificates Technical Reference

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

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1 Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.

2 Tim keeps the private key and makes the public key openly available.

3 Tim uses his private key to encrypt the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to decrypt it.

5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Advantages of Certificates
- Certificates offer the following benefits.The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Format

The certification authority certificate that you want to import has to be in PEM (Base-64) encoded X.509 file format. This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

18.7.1 Verify a Certificate

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

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

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

Figure 175   Certificates on Your Computer
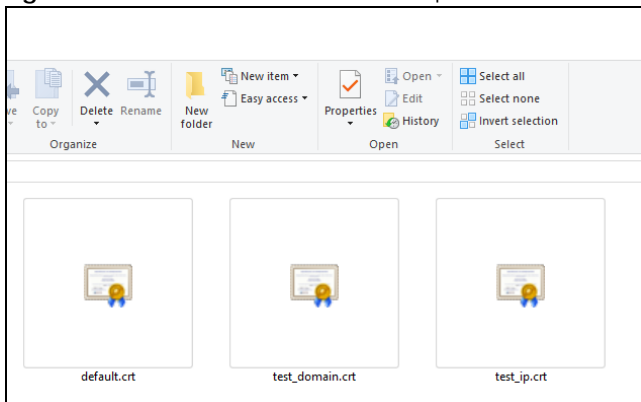
3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 176   Certificate Details
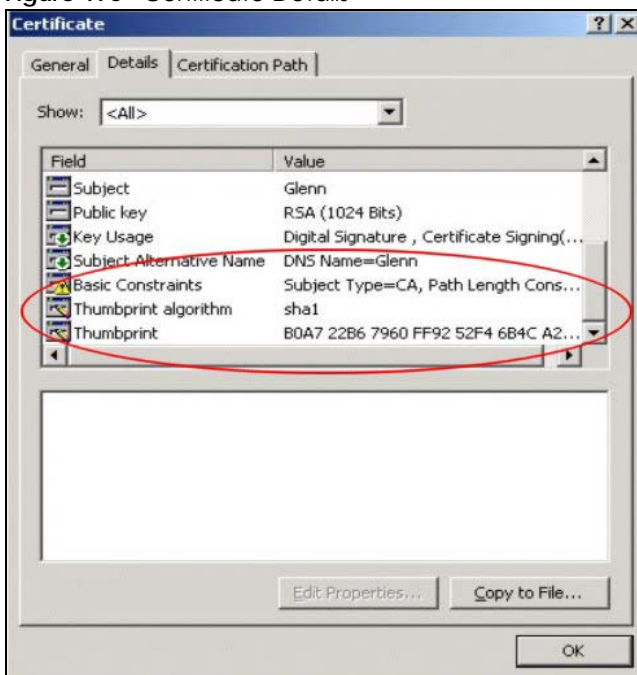
Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

CHAPTER 19
Log

19.1 What You Need To Know

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

Alerts and Logs

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

19.2 System Log

Use the **System Log** screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor** > **Log** to open the **System Log** screen.

Figure 177   System Monitor > Log > System Log

The following table describes the fields in this screen.

Table 107   System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.

Table 107   System Monitor > Log > System Log (continued)

LABEL	DESCRIPTION
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the Zyxel Device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

19.3 Security Log

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

Figure 178   System Monitor > Log > Security Log

The following table describes the fields in this screen.

Table 108   System Monitor > Log > Security Log

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

CHAPTER 20
Traffic Status

20.1 Traffic Status Overview

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

20.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 20.2 on page 284).
- Use the **LAN** screen to view the LAN traffic statistics (Section 20.3 on page 286).

20.2 WAN Status

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

Figure 179 System Monitor > Traffic Status > WAN
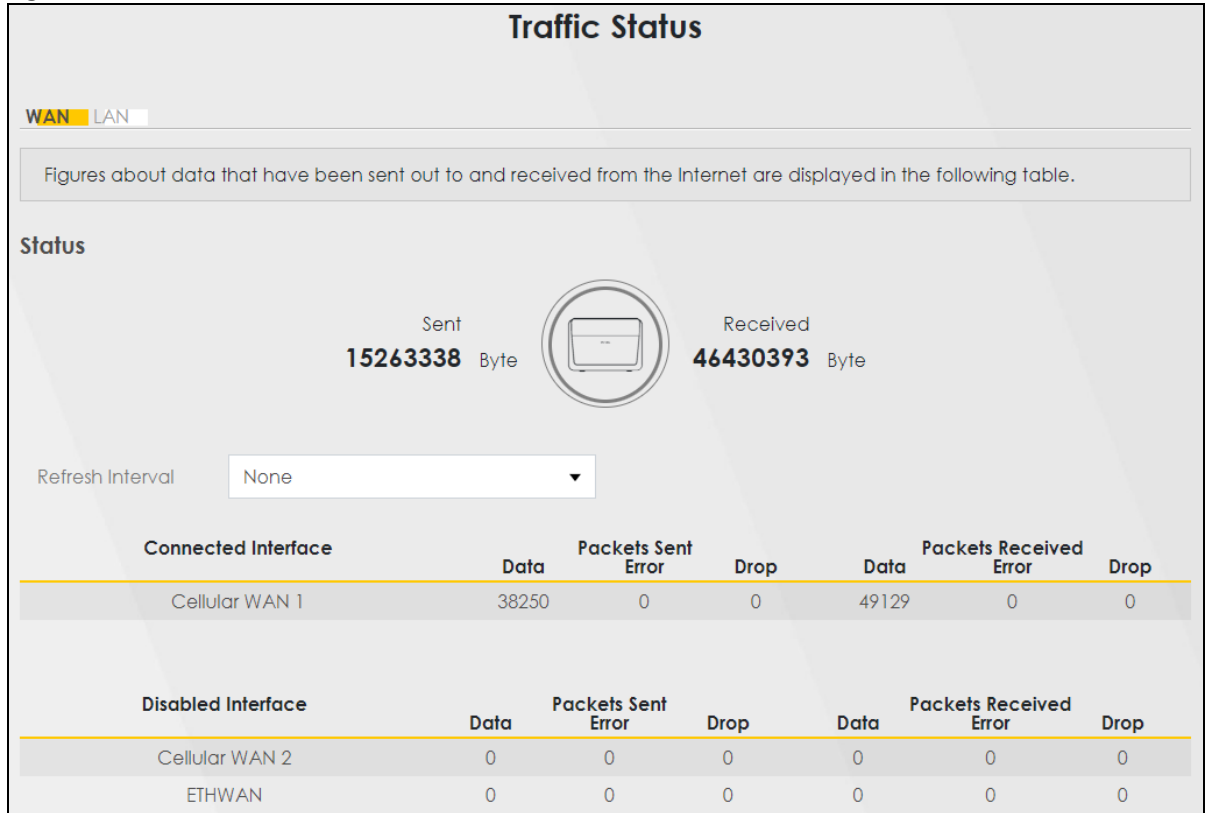
The following table describes the fields in this screen.

Table 109 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disabled.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	

Table 109   System Monitor > Traffic Status > WAN (continued)

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

20.3 LAN Status

Click **System Monitor** > **Traffic Status** > **LAN** to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.

Figure 180   System Monitor > Traffic Status > LAN

The following table describes the fields in this screen.

Table 110   System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interfaces.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	

Table 110   System Monitor > Traffic Status > LAN (continued)

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

CHAPTER 21
ARP Table

21.1 ARP Table Overview

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

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

21.1.1 How ARP Works

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

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP table for future reference and then sends the packet to the MAC address that replied.

21.2 ARP Table

Use the ARP table to view the IPv4-to-MAC address mappings for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mappings of each IPv6 neighbor. To open this screen, click **System Monitor** > **ARP Table**.

Figure 181 System Monitor > ARP Table

The following table describes the labels in this screen.

Table 111 System Monitor > ARP Table

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

C HAPTER 22
Routing Table

22.1 Routing Table Overview

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

22.2 Routing Table

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

Click **System Monitor** > **Routing Table** to open the following screen.

Figure 182 System Monitor > Routing Table

The following table describes the labels in this screen.

Table 112   System Monitor > Routing Table

LABEL	DESCRIPTION
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.
Interface	This indicates the name of the interface through which the route is forwarded. • **brx** indicates a LAN interface where x can be 0 – 3 to represent LAN1 to LAN4 respectively. • **ethx** indicates an Ethernet WAN interface using IPoE or in bridge mode. • **ppp0** indicates a WAN interface using PPPoE. • **wlx** indicates a wireless interface where x can be 0 – 1.

WLAN Station Status

23.1 WLAN Station Status Overview

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

Figure 183   System Monitor > WLAN Station Status

Figure 184   System Monitor > WLAN Station Status

The following table describes the labels in this screen.

Table 113   System Monitor > WLAN Station Status

LABEL	DESCRIPTION
#	This is the index number of an associated WiFi station.
MAC Address	This field displays the MAC address of an associated WiFi station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated WiFi station and the Zyxel Device.

Table 113   System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's WiFi connection. The normal range is –30dBm to –79dBm. If the value drops below –80dBm, try moving the associated WiFi station closer to the Zyxel Device to get better signal strength.
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The greater the number, the better the quality of WiFi. The normal range is 15 to 40. If the value drops below 15, try moving the associated WiFi station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated WiFi station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the Zyxel Device is receiving an excellent WiFi signal. **4** means the Zyxel Device is receiving a very good WiFi signal. **3** means the Zyxel Device is receiving a weak WiFi signal, **2** means the Zyxel Device is receiving a very weak WiFi signal. **1** means the Zyxel Device is not receiving a WiFi signal.

CHAPTER 24
Cellular WAN Status

24.1 Cellular WAN Status Overview

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

24.2 Cellular WAN Status

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

Figure 185   System Monitor > Cellular WAN Status

Cellular WAN Status

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

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

Refresh Interval	None

Module Information

IMEI	358892640000202
Module SW Version	RM502QAEAAR11A02M4G

SIM Status

SIM Card Status	Available
IMSI	466977610432303
ICCID	898869719107669219186
PIN Protection	Disable
PIN Remaining Attempts	3

IP Passthrough Status

IP Passthrough Enable	Disable

Cellular Status

Cellular Status	Up
Data Roaming	Disable
Operator	TW Mobile
PLMN	46697

NR Information

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

Figure 186   System Monitor > Cellular WAN Status (continued)

Service Information	
Access Technology	NR
Band	LTE_BC1
RSSI	-56
Cell ID	76856462
Physical Cell ID	444
UL Bandwidth (MHz)	15
DL Bandwidth (MHz)	15
RFCN	275
RSRP	-82
RSRQ	-12
RSCP	N/A
EcNo	N/A
TAC	22560
LAC	N/A
RAC	N/A
BSIC	N/A
SINR	20
CQI	6
MCS	0
RI	0
PMI	167
SCC Information	
# 1	
Physical Cell ID	444
RFCN	9560
Band	LTE_BC28
RSSI	-54
RSRP	-82
RSRQ	-8
SINR	N/A

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

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

The following table describes the labels in this screen.

Table 114   System Monitor > Cellular WAN Status

LABEL	DESCRIPTION
Refresh Interval	Select the time interval the Zyxel Device will check and refresh the fields shown on this screen. Select **None** to stop detection.
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Module SW Version	This shows the software version of the cellular module.
SIM Status	
SIM Card Status	This displays the SIM card status:
	None – the Zyxel Device does not detect that there is a SIM card inserted.
	Waiting SIM Available – the SIM card is detected but not available yet.
	Available – the SIM card could either have or doesn't have PIN code security.
	Locked – the SIM card has PIN code security, but you did not enter the PIN code yet.
	Blocked – you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card.
	Error - the Zyxel Device detected that the SIM card has errors.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (**ICCID**). This is the serial number of the SIM card.
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.
	Shows **Enable** if the service provider requires you to enter a PIN to use the SIM card and **PIN Protection** is enabled.
	Shows **Disable** if the service provider lets you use the SIM without inputting a PIN.
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
IP Passthrough Enable	This displays if IP Passthrough is enabled on the Zyxel Device.
	IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the first LAN computer on the local network and will not go through NAT.
IP Passthrough Mode	This displays the IP Passthrough mode.
	This displays **Dynamic** and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device.
	This displays **Fixed** and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.

Table 114   System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
Data Roaming	This displays if data roaming is enabled on the Zyxel Device. Data roaming is to use your Zyxel Device in an area which is not covered by your service provider. Enable roaming to ensure that your Zyxel Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.
Operator	This displays the name of the service provider.
PLMN	This displays the PLMN number.
Antenna Status	This displays **Internal** when the **INT EXT** switch is set to **INT**. Use the Zyxel Device's internal antenna to get cellular signal. This displays **External** when the **INT EXT** switch is set to **EXT**. Connect external antennas to the Zyxel Device's to strengthen the cellular signal. See Section 2.2 on page 28 for more information.
Service Information	
Access Technology	This displays the type of the mobile network to which the Zyxel Device is connecting.
Band	This displays the current cellular band of your Zyxel Device.
RSSI (dBm)	This displays the strength of the WiFi signal between an associated wireless station and an AP. The normal range is –30 dBm to –79 dBm. If the value drops below –80 dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting. The value depends on the Current Access Technology: • For GPRS, it is the Cell Identity as specified in 3GPP-TS.25.331. • For UMTS, it is the Cell Identity as defined in SIB3 3GPP-TS.25.331, 3GPP-TS.24.008. • For LTE, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331. The value is '0' (zero) or 'N/A' if there is no network connection.
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Zyxel Device and the mobile network it is connecting to. The normal range is 1 to 504.
UL Bandwidth (MHz)	This shows the cellular channel bandwidth from the Zyxel Device to the base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
DL Bandwidth (MHz)	This shows the cellular channel bandwidth from the base station to the Zyxel Device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting. The value depends on the Current Access Technology: • For GPRS, it is the ARFCN (Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.45.005. • For UMTS, it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. • For LTE, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. The value is '0' (zero) or 'N/A' if there is no network connection.

Table 114   System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
RSRP (dBm)	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133. An undetectable signal is indicated by the lower limit, example –140 dBm. This parameter is for LTE only. The normal range is –30 to –140. The value is –140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSRQ (dB)	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example -240. This parameter is for LTE only. The normal range is –30 to –240. The value is –240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
SINR (dB)	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device. The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example –120 dBm. This parameter is for UMTS only. The normal range is –30 to –120. The value is –120 if the Current Access Technology is not UMTS. The value is 'N/A' if there is no network connection.
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level. The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, for example, –240 dB. This parameter is for UMTS only. The normal range is –30 to –240. The value is –240 if the Current Access Technology is not UMTS or there is no network connection.
Primary Scrambling Code	This displays a unique scrambling code used by the Nebula Device to identify a base station in a cellular network. A primary scrambling code is the product of the scrambling code and 16. Therefore, the primary scrambling code set contains all multiples of 16 from 0 through 8176. This only appears in UMTS mode. Otherwise, this field is blank.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN. The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.

Table 114   System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
RAC	This displays the RAC (Routing Area Code), which is used in mobile network "packet domain service" (PS) to identify a routing area within a location area. In a mobile network, it uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and use RAC to identify the location of data service like HSDPA or LTE. The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station. This parameter is for GPRS only. The value is '0' (zero) if the Current Access Technology is not GPRS. The value is 'N/A' if there is no network connection.
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber. The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101. This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good/bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI). PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer). PMI determines how cellular data are encoded for the antennas to improve the downlink rate.
Neighbour Cells	This displays the type of the neighbor cell's carrier frequency detected by the Zyxel Device. **Intra-Frequency** – when the current cell and target cell operate on the same carrier frequency. **Inter-Frequency** – when the current cell and target cell operate on different carrier frequencies.
#	This is the index number of the entry.
Connection Mode	This displays the connection mode of the detected neighbor cell.
NR Physical Cell ID	This shows the Physical Cell ID (**PCI**), which are queries and replies between the Zyxel Device and the 5G mobile network it is connecting to. The normal range is 0 to 503.
RFCN	This displays the Radio Frequency Channel Number (**RFCN**) of the detected base station. This is the carrier frequency designated by EARFCN. The range is 0 – 65535.
RSSI	This displays the Received Signal Strength Indicator (**RSSI**) level of the detected base station. RSSI is an indicator of the signal strength, including signals and noises received by the target cell. The normal range is –30 dBm to –79 dBm.

Table 114   System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
NR RSRP	This displays the Reference Symbol Received Power (**RSRP**) level of the detected base station. RSRP is the average signal strength of the target station and is usually measured during a handover. The normal range is –140dBm to –44dBm.
NR RSRQ	This displays the Reference Signal Received Quality (**RSRQ**) level of the detected base station. RSRQ is the indicator of the signal quality of data transmission. The normal range is –24.0 dB to 0 dB. **RSRQ** is defined as **RSRP/RSSI***N. N is the number of resource blocks. A resource block is the smallest unit of radio resources allocated to a user and contains twelve sub-carriers in frequency and 0.5 ms in time.
NR SINR (dBm)	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the 5G network. A negative value means more noise than signal.

CHAPTER 25
System
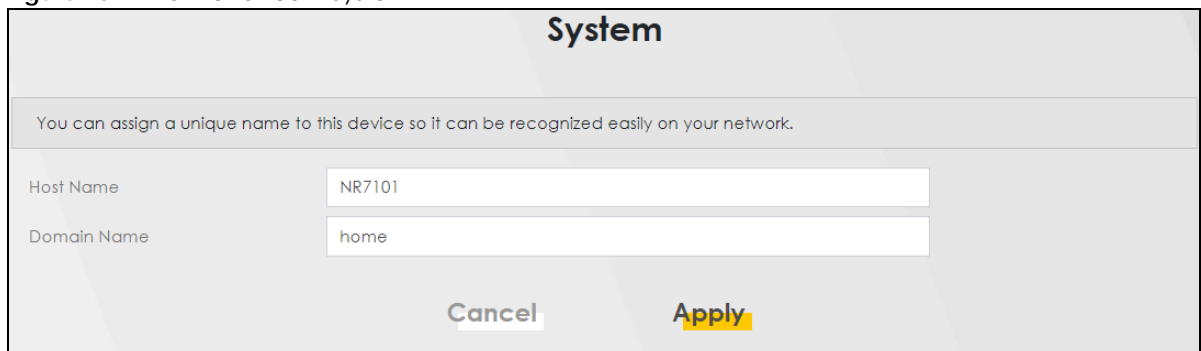
25.1 System Overview

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

25.2 System

Click **Maintenance** > **System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.

Figure 187 Maintenance > System

<div>

System

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

Host Name: NR7101

Domain Name: home

Cancel   Apply

</div>

The following table describes the labels in this screen.

Table 115 Maintenance > System

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

26.1 User Account Overview

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

26.2 User Account

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

Figure 188 Maintenance > User Account

The following table describes the labels in this screen.

Table 116 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account (up to four **Administrator** accounts and four **User** accounts).
#	This is the index number.
Active	This indicates whether the user account is active or not. The checkbox is selected when the user account is enabled. It is cleared when it is disabled.
User Name	This displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.

Table 116   Maintenance > User Account (continued)

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

26.2.1 User Account Add or Edit

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

Figure 189   Maintenance > User Account: Edit

Figure 190 Maintenance > User Account > Add

The following table describes the labels in this screen.

Table 117 Maintenance > User Account > User Account Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (switch turns blue) or disable (switch turns gray) to activate or deactivate the user account.
User Name	Enter a name for this account. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed.
Verify Password	Enter the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	Specify whether this user will have **Administrator** or **User** privileges. An **Administrator** account can access all Web Configurator menus. A **User** account can only access **Monitor** and **Maintenance** menus. The maximum account number of **Administrator** and **User** are both four. The total number of the users allowed to log in the Zyxel Device at the same time is eight. **The Administrator** privileges are the following: • **Quick Start** setup. • The following screens are visible for setup: **Broadband**, **Wireless**, **Home Networking**, **Routing**, **NAT**, **DNS**, **Firewall**, **MAC Filter**, **Voice**, **Log**, **Traffic Status**, **ARP Table**, **Routing Table**, **Cellular WAN Status**, **System**, **User Account**, **Remote Management**, **TR-069 Client**, **Time**, **Email Notification**, **Log Setting**, **Firmware Upgrade**, **Backup/Restore**, **Reboot**, **Diagnostic**. **The User** privileges are the following: • The following screens are visible for setup: **Log**, **Traffic Status**, **ARP Table**, **Routing Table**, **Cellular WAN Status**, **User Account**, **Remote Management**, **Time**, **Email Notification**, **Log Setting**, **Firmware Upgrade**, **Backup/Restore**, **Reboot**, **Diagnostic**.

Table 117   Maintenance > User Account > User Account Add/Edit (continued)

LABEL	DESCRIPTION
Remote Privilege	Select whether this user can access the Zyxel Device with HTTP, Telnet or SSH through the **WAN**, **LAN** or **LAN/WAN**. Only the **Administrator** is allowed to use Telnet and SSH for remote management.
Cancel	Click **Cancel** to restore your previously saved settings.
OK	Click **OK** to save your changes.

CHAPTER 27
Remote Management

27.1 Remote Management Overview

Remote management controls through which interfaces, which web services (such as HTTPS, SSH, SNMP, and Ping) can access the Zyxel Device.

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

27.1.1 What You Can Do in this Chapter

- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 27.2 on page 307).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 27.3 on page 309).
- Use **MGMT Services for IP Passthrough** to configure which interfaces you can use to access the Zyxel Device for a given service (Section 27.4 on page 310).
- Use **Trust Domain for IP Passthrough** to view a list of public IP addresses and complete domain names which are allowed to access the Zyxel Device (Section 27.5 on page 312),

27.2 MGMT Services

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

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

Figure 191 Maintenance > Remote Management > MGMT Services

The following table describes the fields in this screen.

Table 118   Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
Service Control	
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up.
	Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Cellular WAN	Enable the cellular WAN connection configured in **Network Setting** > **Broadband** > **Cellular WAN** to access the service on the Zyxel Device.
	If there are multiple cellular WANs configured on the Zyxel Device, you can select which to use for the Zyxel Device management.
ETHWAN	Enable the Ethernet WAN connection configured in **Network Setting** > **Broadband** > **Ethernet WAN** to access the service on the Zyxel Device.
GPON	Enable the Gigabit Ethernet Passive Optical Network WAN connection configured in **Network Setting** > **Broadband** > **Add New WAN Interface** or **Modify** to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN/WLAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the LAN or WLAN.

Table 118   Maintenance > Remote Management > MGMT Services (continued)

LABEL	DESCRIPTION
WAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Redirect	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server. For example, if you enter http://192.168.1.1 in your browser to access the Web Configurator, then the Zyxel Device will automatically change this to the more secure https://192.168.1.1 for access.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

27.3 Trust Domain

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** > **MGMT Services** screen. Click **Maintenance** > **Remote Management** > **Trust Domain** to open the following screen.

Note: Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Figure 192   Maintenance > Remote Management > Trust Domain

The following table describes the fields in this screen.

Table 119   Maintenance > Remote Management > Trust Domain

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

27.3.1 Add Trust Domain

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

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

Figure 193   Maintenance > Remote Management > Trust Domain > Add Trust Domain

The following table describes the fields in this screen.

Table 120   Maintenance > Remote Management > Trust Domain > Add Trust Domain

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

27.4 MGMT Services for IP Passthrough

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

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

Figure 194   Maintenance > Remote Management > MGMT Services for IP Passthrough

Remote Management

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

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

Service Control

WAN Interface used for services

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

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

Cancel   Apply

Figure 195   Maintenance > Remote Management > MGMT Services for IP Passthrough

The following table describes the fields in this screen.

Table 121   Maintenance > Remote Management > MGMT Services for IP Passthrough

LABEL	DESCRIPTION
Service	This is the service you may use to access the Zyxel Device.
WAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

27.5 Trust Domain for IP Passthrough

Use this screen to view a list of public IP addresses/complete domain names which are allowed to access the Zyxel Device when **IP Passthrough** is enabled. IP Passthrough allows Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT. Make sure to enable IP Passthrough in **Network Setting** > **Broadband** > **Cellular IP Passthrough**.

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

Figure 196 Maintenance > Remote Management > Trust Domain for IP Passthrough

The following table describes the fields in this screen.

Table 122 Maintenance > Remote Management > Trust Domain for IP Passthrough

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

27.5.1 Add Trust Domain

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

Figure 197 Maintenance > Remote Management > Trust Domain for IP Passthrough > Add Trust Domain

The following table describes the fields in this screen.

Table 123   Maintenance > Remote Management > Trust Domain for IP Passthrough > Add Trust Domain

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

CHAPTER 28
TR-069 Client

28.1 TR-069 Overview

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

28.1.1 TR-069 Client

TR-069 is a protocol that defines how your Zyxel Device can be managed via a management server. TR-069 is based on sending Remote Procedure Calls (RPCs) between an (Auto-Configuration Server) ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS. You can use a management server to remotely set up the Zyxel Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Zyxel Device.

28.1.2 XMPP

If a remotely-managed Zyxel Device is behind a NAT router and has a private IP address, then the ACS cannot communicate directly with the Zyxel Device. In this case, the Zyxel Device needs to communicate with the ACS through an XMPP server.

Figure 198 XMPP Connection Request

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

Figure 199 Maintenance > TR-069 Client

The following table describes the fields in this screen.

Table 124   Maintenance > TR-069 Client

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

Table 124   Maintenance > TR-069 Client (continued)

LABEL	DESCRIPTION
XMPP Server Address	Enter the IP address of the XMPP server. The Zyxel Device will use the address to connect to the XMPP server.
XMPP Server Port	Enter the TCP port reserved for the XMPP server. The default is 5222. (1 – 65535)
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore the screen's last saved settings.

CHAPTER 29
Time Settings

29.1 Time Settings Overview

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

29.2 Time

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

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

Figure 200 Maintenance > Time

The following table describes the fields in this screen.

Table 125 Maintenance > Time

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

Table 125   Maintenance > Time (continued)

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

Email Notification

30.1 Email Notification Overview

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

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

30.2 Email Notification

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

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

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

Figure 201 Maintenance > E-mail Notification

The following table describes the labels in this screen.

Table 126   Maintenance > E-mail Notification

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

30.2.1 E-mail Notification Edit

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

Figure 202   Maintenance > E-mail Notification > Add

The following table describes the labels in this screen.

Table 127   Maintenance > E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the email address specified in the **Account e-mail Address** field.
	If this field is left blank, reports, logs or notifications will not be sent through email.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [	], [&], or [;]. Spaces are allowed. This is usually the user name of a mail account you specified in the **Account email Address** field.
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the email address that you want to be in the from or sender line of the email notification that the Zyxel Device sends.
	If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well.
Connection Security	Select **SSL** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device.
	Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS.
	Select **NONE** to disable the connection security.
Cancel	Click this button to begin configuring this screen afresh.
OK	Click this button to save your changes and return to the previous screen.

C HAPTER 31
Log Setting

31.1 Log Setting Overview

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

31.2 Log Setting

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

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

Figure 203 Maintenance > Log Setting

The following table describes the fields in this screen.

Table 128   Maintenance > Log Setting

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

31.2.1 Example Email Log

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

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- 'End of Log' message shows that a complete log has been sent.

Figure 204   Email Log Example

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

End of Firewall Log
```

Firmware Upgrade

32.1 Firmware Upgrade Overview

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

32.2 Firmware Upgrade

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

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

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

<p style="color:red; font-weight:bold; text-align:center">Do NOT turn off the Zyxel Device while firmware upload is in progress!</p>

Figure 205 Maintenance > Firmware Upgrade

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

Upgrade Firmware

Restore Default Settings After Firmware Upgrade ☐

Current Firmware Version: V1.15(ACGC.1)C0

File Path   Choose File | No file chosen   Upload

The following table describes the labels in this screen.

Table 129   Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select this to reset all your configurations, including Mesh WiFi settings, to the factory defaults after firmware upgrade. Otherwise, make sure this is cleared if you do not want the Zyxel Device to lose all its current configurations and return to the factory defaults. Note: Make sure to back up the Zyxel Device's configuration settings first in case the reset all settings process is not successful.

Table 129   Maintenance > Firmware Upgrade (continued)

LABEL	DESCRIPTION
File Path	Enter the location of the file you want to upload in this field or click **Choose File/Browse** to find it.
Choose File/ Browse	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to 3 minutes. Note: Only use firmware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device. For example, if the Zyxel Device's current firmware version is V5.70(ACDZ.0)B4, you must upload the firmware file containing "ACDZ".

After you see the firmware updating screen, wait a few minutes before logging into the Zyxel Device again.

Figure 206   Firmware Uploading

The Zyxel Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 207   Network Temporarily Disconnected
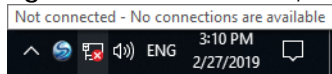
After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

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

Figure 208   Error Message
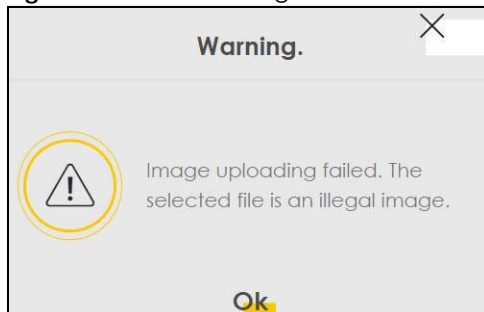
32.3 Module Upgrade

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

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

Figure 209   Maintenance > Firmware Upgrade > Module Upgrade

The following table describes the labels in this screen.

Table 130   Maintenance > Firmware Upgrade > Module Upgrade

LABEL	DESCRIPTION
Upgrade Cellular Module Firmware	
Current Module Version	This is the current module firmware version.
Choose file...	Enter the location of the file you want to upload in this field or click **Choose File/Browse** to find it.
Choose File/ Browse	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take more than 3 minutes.

After you see the module updating screen, wait about 20 minutes before logging into the Zyxel Device again.

The Zyxel Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 210   Network Temporarily Disconnected
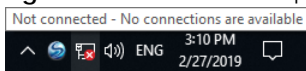
After two minutes, log in again and check your new firmware version in the **Status** screen.

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

CHAPTER 33
Backup/Restore

33.1 Backup/Restore Overview

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

33.2 Backup/Restore

Click **Maintenance** > **Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 211 Maintenance > Backup/Restore

Backup/Restore

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

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once the Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

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

Backup Configuration

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

[Backup]

Restore Configuration

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

File Path   [Choose File] No file chosen   [Upload]

Back to Factory Default Settings

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

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

- LAN IP address will be 192.168.1.1

- DHCP will be reset to default setting

[Reset]

Backup Configuration

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Zyxel Device's current configuration to your computer.

Restore Configuration

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

Table 131   Maintenance > Backup/Restore: Restore Configuration

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

Do not turn off the Zyxel Device while configuration file upload is in progress.

After the Zyxel Device configuration has been restored successfully, the login screen appears. Login again to restart the Zyxel Device.

The Zyxel Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 212   Network Temporarily Disconnected
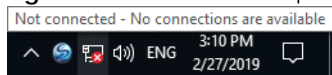
If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default Zyxel Device IP address (192.168.1.1 – 192.168.225.225).If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 213   Configuration Upload Error
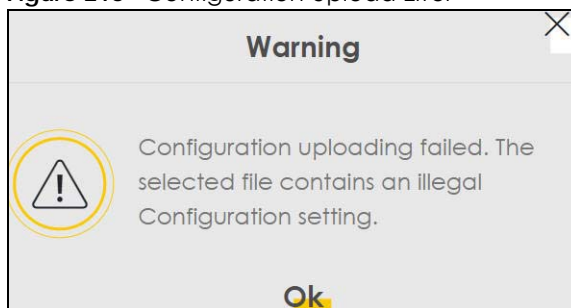
Back to Factory Default Settings

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

Figure 214 Reset Warning Message
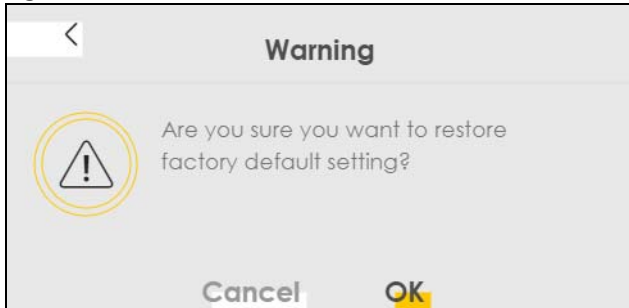
Figure 215 Reset In Progress
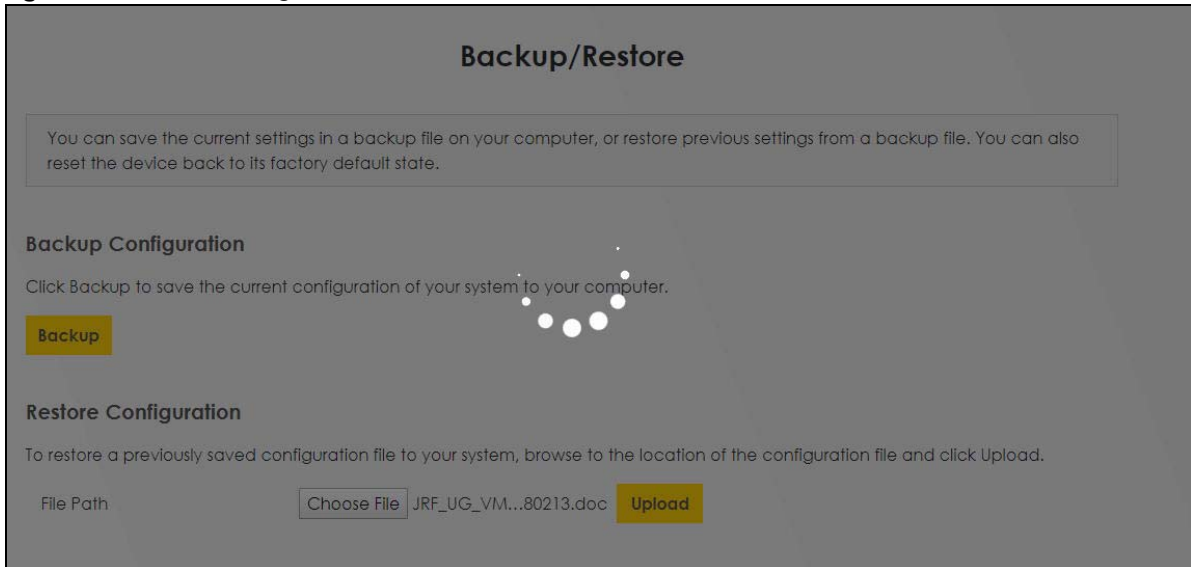
You can also press the **RESET** button on the panel to reset the Zyxel Device to the factory defaults.

33.3 Reboot

System **Reboot** allows you to restart the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example. This does not affect the Zyxel Device's configuration.

Click **Maintenance** > **Reboot**. Click **Reboot** to have the Zyxel Device restart.

Figure 216 Maintenance > Reboot
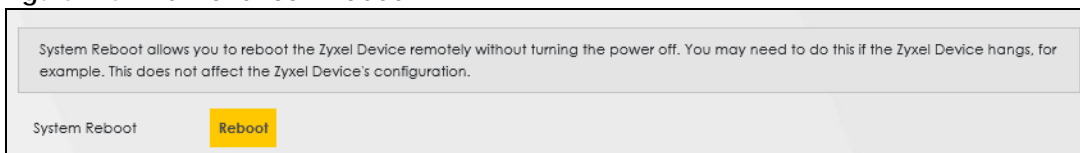
33.4 Schedule Reboot

Use the **Schedule Reboot** screen to schedule the date and time to reboot the Zyxel Device remotely without turning the power off. You can also select a specific day of the week and time to periodically reboot the Zyxel Device remotely.

Click **Maintenance** > **Reboot** > **Schedule Reboot** to open the following screen.

Figure 217   Maintenance > Reboot > Schedule Reboot

The following table describes the labels in this screen.

Table 132   Maintenance > Reboot > Schedule Reboot

LABEL	DESCRIPTION
Periodicity	Select this to have the Zyxel Device to reboot periodically.
Day of Week	Select the day of the week to apply periodic rebooting. **Day of Week** is not available when the previous field **Periodically** is not selected.
Time of Date	Select the date of the year that you plan to reboot the Zyxel Device remotely.
Time of Day	Select the time of the day that you plan to reboot the Zyxel Device remotely.
Cancel	Click **Cancel** to close the window with changes unsaved.
Apply	Click **Apply** to save the changes back to the Zyxel Device.

CHAPTER 34
Diagnostic

34.1 Diagnostic Overview

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

34.1.1 What You Can Do in this Chapter

34.2 Diagnostic

Use this screen to ping, traceroute or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking one of the buttons to start a test, the results will be shown in the screen. Use nslookup to find the IP address for a host name and the host name for an IP address.

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

Figure 218 Maintenance > Diagnostic

The following table describes the fields in this screen.

Table 133   Maintenance > Diagnostic

LABEL	DESCRIPTION
Ping/TraceRoute Test	The result of tests is shown here in the info area.
Select Test Method	
Ping	Select this to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area.
Ping 6	Select this to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area.
Trace Route	Select this to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Select this to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Select this to perform a DNS lookup on the IP address or host name.
TCP/IP	
Address	Enter the IP address of a computer that you want to perform ping, trace route or nslookup in order to test a connection.

Legal and Regulatory

35.1 Overview

Use this screen to view the regulatory information for your Zyxel Device.

35.2 The Regulatory Information Screen

Go to **Maintenance** > **Legal and Regulatory** to check the applicable regulatory information for your Zyxel Device.

Figure 219   Maintenance > Legal and Regulatory > Regulatory Information

The following table describes the labels in this screen.

Table 134   Maintenance > Legal and Regulatory > Regulatory Information

LABEL	DESCRIPTION
Regulatory Information	
NCC	This field displays the certification from the National Communications Commission (NCC).

PART III
Troubleshooting and Appendices

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

CHAPTER 36
Troubleshooting

36.1 Troubleshooting Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Accessibility and Compatibility Problems
- Power and Hardware Problems
- Device Access Problems
- Cellular Problems
- Internet Problems
- WiFi Problems
- USB Problems
- UPnP Problems

36.2 Accessibility and Compatibility Problems

Screen reader not reading content.

- Ensure the latest version of the screen reader is installed.
- Check if the screen reader's accessibility settings are enabled.

Web browser not displaying correctly.

- Clear your web browser cache.
- Ensure that JavaScript is enabled.
- Try using a different supported web browser.

36.3 Power and Hardware Problems

The Zyxel Device does not turn on.

Non-PoE Devices

1 Make sure you are using the power adapter included with the Zyxel Device.

2 Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.

3 Disconnect and re-connect the power adapter to the Zyxel Device.

4 Make sure you have pressed the **POWER** button to turn on the Zyxel Device.

5 If the problem continues, contact the vendor.

PoE Devices

1 Make sure you are using the power adapter included with the Zyxel Device.

2 Make sure the PoE is connected to the Zyxel Device and plugged in to an appropriate power source.

3 Make sure the power source is turned on.

4 Turn the Zyxel Device off and on.

5 If the problem continues, contact the vendor.

The LED does not behave as expected.

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

2 Check the hardware connections.

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

4 Turn the Zyxel Device off and on.

5 If the problem continues, contact the vendor.

36.4 Device Access Problems

I do not know the IP address of the Zyxel Device.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address, you might be able to find the IP address of the Zyxel Device by looking up the IP address of your computer's default gateway. To do this in Microsoft Windows, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device, depending on your network environment.

3 If this does not work, reset the Zyxel Device to its factory defaults.

  - Locate a small hole labeled **RESET** on the Zyxel Device.
  - Use a paperclip or a similar tool to press and hold the **RESET** button.
  - Release the button, and the Zyxel Device will reset to its default settings, including the default IP address, user name, and password.

  Note: Resetting the Zyxel Device will erase all your custom settings, so you need to reconfigure it.

I forgot the admin password.

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

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

I cannot access the Web Configurator login screen.

1 Make sure you are using the correct IP address.

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

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

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. Clear the Internet browser cache and try accessing the Web Configurator login screen again. Outdated browser data can cause login issues. If the problem persists, try logging into the web configurator using a different browser. (e.g., Chrome, Firefox, Edge)

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance** > **Remote Management**).

5 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

I cannot log into the Zyxel Device.

1 For first-time Zyxel Device logins, after using the label password to access the web configurator, ensure your new password meets the requirements on the screen. For example, some models require the new password to be at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character.

2 Make sure you have entered the user name and password correctly. The default user name is **admin**. These both user name and password are case-sensitive, so make sure [Caps Lock] is not on.

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

4 Turn the Zyxel Device off and on.

5 If this does not work, you have to reset the Zyxel Device to its factory default. To reset the Zyxel Device, press the **RESET** button until the POWER LED begins to blink and then release it.

I cannot log into the Zyxel Device using DDNS.

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the Zyxel Device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.
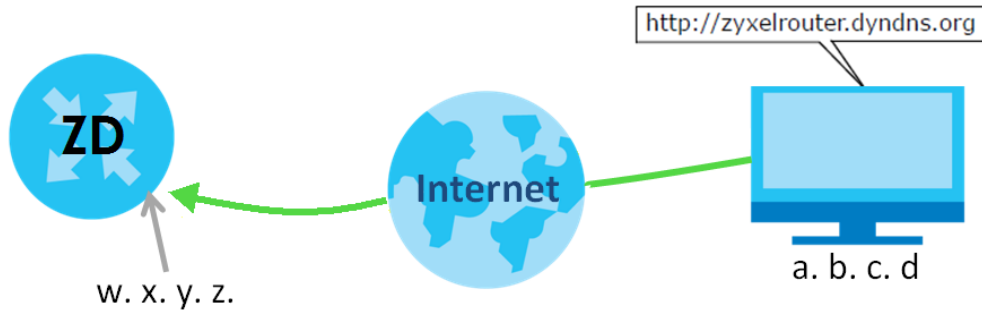
To use this feature, you have to apply for DDNS service at www.dyndns.org.

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

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

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

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

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

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

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

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

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

Step 2 Configure DDNS on Your Zyxel Device

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

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

Step 3 Test the DDNS Setting

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

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

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

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

I cannot connect to the Zyxel Device using Telnet, SSH, or Ping.

1 See the Remote Management section for details on allowing web services (such as HTTPS, Telnet, SSH and Ping) to access the Zyxel Device.

2 Check the server **Port** number field for the web service in the **Maintenance** > **Remote Management** screen. You must use the same port number in order to use that web service for remote management.

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

I cannot access the Zyxel Device from outside the network (WAN).

To test if this is due to CGNAT, follow these steps:

1 Log in to your Zyxel Device's Web Configurator using the default IPv4 address (for example, 192.168.1.1).

2 Locate the WAN IP address on the **Dashboard** screen. You can find this information in the Network or WAN settings.

3 Go to a website that can show you the public IP address of your network (for example, https://whatsmyip.com). When you access this site, it will display your public IP address.

4 Compare the WAN IP address displayed on the **Dashboard** screen with the public IP address shown on the https://whatsmyip.com website.

- If both IP addresses are the same, your ISP is not using Carrier-Grade NAT, and you should be able to access your Zyxel Device from the WAN (outside).
- If the IP addresses are different, it indicates that your ISP is using Carrier-Grade NAT, and your Zyxel Device has a shared public IP address. As a result, remote access to your Zyxel Device from the WAN will not be possible.

If you discover that your Zyxel Device is behind a Carrier-Grade NAT and you need remote access, you must contact your ISP and request a public IP address for your SIM card or Zyxel Device.

I cannot use my Zyxel Device to assign IP addresses.

There are two modes you can select for the Zyxel Device: **Router Mode** and **IP Passthrough Mode**. In **Router Mode**, the Zyxel Device can assign IP addresses to LAN clients. In **IP Passthrough Mode**, the Zyxel Device passes the public IP address assigned by the ISP directly to LAN clients.

If you want the Zyxel Device to assign IP addresses, you need to set the Zyxel Device to **Router Mode** and enable **DHCP**.

1 Checking **Router Mode**

To check if your Zyxel Device is in **Router Mode**, go to the **Home** screen. In the **Cellular Info** section, check if the **Mode** field displays **Router Mode**. If the **Mode** field displays **IP Passthrough Mode**, follow the steps below to change to **Router Mode**:

- Click the menu icon (☰) and go to **Network Setting** > **Broadband** > **Cellular APN**.
- Click the **Modify** icon in the row of the APN that is enabled and currently active. The **Edit APN** screen will appear.
- Click the **IP Passthrough** switch to the left to turn off **IP Passthrough Mode**. Click **OK**.
- Go to the **Home** screen and check the **Cellular Info** section. The **Mode** field should now display **Router Mode**.

2 Enabling **DHCP**

DHCP (Dynamic Host Configuration Protocol) is a protocol that automatically assigns IP addresses to LAN clients. To enable **DHCP** on your Zyxel Device:

- Go to **Network Setting** > **Home Networking** > **LAN Setup**.
- Select **Enable** in the **DHCP Server State**. Click **Apply**.

Your Zyxel Device should now be able to assign IP addresses to LAN clients on your network.

36.5 Cellular Problems

The SIM card cannot be detected.

1 Disconnect the Zyxel Device from the power supply.

2 Remove the SIM card from its slot.

3 Clean the SIM card slot of any loose debris using compressed air.

4 Clean the gold connectors on the SIM card with a clean lint-free cloth.

5 Insert the SIM card into its slot and connect the Zyxel Device to the power supply to restart it.

I get an **Invalid** SIM card alert.

1 Make sure you have an active plan with your ISP.

2 Make sure that the Zyxel Device is in the coverage area of a cellular network.

3 Enable **Data Roaming** in **Network Setting** > **Broadband** > **Cellular WAN** to keep the Zyxel Device connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered, such as a different country. Then, restart the Zyxel Device.

I get a weak cellular signal.

1 Check the signal strength. Look at the LEDs, and check the LED section for more information. If the signal strength is low, try moving the Zyxel Device closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (such as microwaves, other wireless networks).

2 Select **Auto** in **Network Setting** > **Broadband** > **Cellular Band**: **Preferred Access Technology** and slide the switch to the right to enable **Band Auto Selection**.

3 Find the location of your nearest cellular base stations, then install the Zyxel Device towards the direction of those sites. The nearest site or site with a direct line-of-sight is usually preferred.

   Note: It is best to test towards more than one cellular site, as the nearest site / line-of-sight is not always the best due to the terrain, interference, density of usage, and so on. All of these factors influence the stability, availability and throughput of the link to the Zyxel Device.

4 Conduct test measurements using the Web Configurator's **System Monitor** > **Cellular WAN Status** screen to obtain a report of the cellular network signal strength and quality at various test positions.

   Note: It is best to reboot the Zyxel Device before each test measurement is taken to ensure that it is not camping on the previous cellular site. This is because the Zyxel Device can 'lock' onto the previous cellular site even when the new cellular site is at a much better signal level and quality.

5 Although installing the Zyxel Device as high as possible is the usual rule of thumb, it is sometimes possible that the Zyxel Device is in a weak coverage spot at that specific height. Adjust the height to achieve the best service possible. Use app to determine the best location for your Zyxel Device.

   It is possible that the current serving cellular site has become over utilized or is out-of-service. In this case, you may need to reposition the Zyxel Device to the direction with the strongest cellular signal. Use app to determine the best location for your Zyxel Device.

I don't want to enter the SIM card PIN code every time I reboot the Zyxel Device.

A PIN (Personal Identification Number) code is the key to a SIM card. The PIN code for your SIM card protects against unauthorized users. When the Internet connection is down, users may need to reboot the Zyxel Device. Enabling **PIN Protection** allows the Zyxel Device to prompt you for the PIN code every

time the Zyxel Device reboots. If you don't want to enter the PIN code every time the Zyxel Device reboots, follow the steps below:

1   Click the menu icon (☰) and go to **Broadband > Cellular SIM > PIN Management**.

2   Click the **Auto Unlock PIN** switch to the right to enable **Auto Unlock PIN**. Enter the PIN code and click **Apply**. For more details about **Auto Unlock PIN**, please refer to Section 7.7 on page 148.

Now, you don't need to enter the PIN code every time you reboot the Zyxel Device.

I forget the PIN code.

If you forget the PIN code of your SIM card, follow the steps below:

1   Check your SIM card packaging or documents from your service provider.

2   Try common default PIN codes (for example, 0000 or 1234 – but be careful, as multiple wrong attempts can lock your SIM card).

3   Contact your service provider for assistance.

Note: If your SIM card is locked, you may need the PUK (Personal Unlocking Key), which is also provided by your service provider.

36.6 Internet Problems

I cannot access the Internet.

1   Check the hardware connections and make sure the LEDs are behaving as expected. See the **Quick Start Guide**.

2   Check the SIM card. Maybe it has wrong settings, the account has expired, it needs to be removed and reinserted (refer to the Quick Start Guide), or it is missing. See Section 36.8 on page 353 for possible SIM card problems.

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

4   Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting** > **Interface Group**).

5   Make sure you have the Ethernet WAN port connected to a Modem or Router.

6 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **Network Setting** > **Home Networking** > **LAN Setup** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

7 For models that have optional dual LAN/WAN ports, make sure you converted the LAN port to a WAN port by clicking **Enable** on the **Network Setting** > **Broadband** > **Ethernet WAN** screen. Then make sure you have the Ethernet WAN port connected to a modem or router.

8 If you are trying to access the Internet wirelessly, make sure that you enabled the WiFi in the Zyxel Device and your WiFi client and that the WiFi settings in the WiFi client are the same as the settings in the Zyxel Device.

9 Disconnect all the cables from your Zyxel Device and reconnect them.

10 Check that the network monitoring feature of the Zyxel Device is enabled. Network monitoring helps identify issues with Internet connection and allows the Zyxel Device to attempt reconnection to the base station if the cellular connection is lost. To enable **Network Monitoring**, Go to **Network Settings > Broadband > Cellular WAN**. See Section 7.5 on page 141 for more information about network monitoring.

11 If you want to use the 5 Ghz WiFi network, check with your ISP for the 5G bands supported in your area. Go to **Networking** > **Broadband** > **Cellular Band** > **Band Management**, switch **Band Auto Selection** to the left to manually select the cellular bands. Choose the specific 5G bands provided by your ISP for a stable Internet connection, and click **Apply**. For example, you might select n77, n78, and n79 for 5G. Note that cellular bands vary by country.

12 If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet connection.

1 Make sure you have the Ethernet WAN port connected to a Modem or Router.

2 Make sure you configured a proper Ethernet WAN interface (**Network Setting** > **Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

3 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting** > **Interface Group**).

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **Network Setting** > **Home Networking** > **LAN Setup** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2   For models that support external antennas, see Section 1.1 on page 20Section 1.1.1 on page 18. Connect two external antennas to improve the cellular WAN signal strength. Then, set the **INT/EXT / INT EXT / EXT INT** switch to **EXT**. Point the antennas to the base stations directions if you know where they are, or try pointing the antennas in different directions and check which provides the strongest signal to the Zyxel Device. Use app to determine the best location for your Zyxel Device.

3   If your Zyxel Device keeps alternating between ISPs, then choose a fixed ISP. Go to the **Network Setting** > **Cellular PLMN** screen, disable **PLMN Auto Selection** and then choose your preferred ISP.

4   Turn the Zyxel Device off and on.

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

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

What should I do if my Zyxel Device is under attack?

A slow Internet speed, a web browser that keeps redirecting you, suspicious activity alerts from your ISP, and increased pop-ups on the Zyxel Device; could be signs that your Zyxel Device is under attack. If you suspect that your Zyxel Device is under attack, do the following:

1   Create an ACL (Access Control List) rule to block the ports being targeted. See Section 17.5 on page 264 for more information on using ACL. See also Section 5.7.1 on page 100 for more information on configuring a firewall rule. Go to **System Monitor** > **Log** > **Security Log** to view the security-related logs to determine which ports are being targeted. See Section 19.3 on page 283 for more information on security logs.

2   Contact your ISP to report the attack and seek assistance.

3   When possible, turn off the Zyxel Device for 24 hours, then turn it on again.

4   Request the ISP to change your IP address.

My 5G connection is not available.

1   Check with your ISP to see if your SIM card supports 5G service.

2   Check the local 5G signal using the *nPerf website* by selecting your country, choosing your carrier, and entering your address. You can also ask your ISP about the availability of 5G signals in your area.

3   Go to **Networking** > **Broadband** > **Cellular Band** > **Access Technology**. Make sure that the **Preferred Access Technology** includes the 5G option. For example, choose NR5G. See Section 7.9 on page 151 for more information about cellular band configuration.

4 Go to **Networking** > **Broadband** > **Cellular Band** > **Band Management**. Switch the **Band Auto Selection** to the right to enable automatic band selection. If you want to manually select specific 5G bands provided by your ISP, switch the **Band Auto Selection** to the left. For example, you might select n77, n78, and n79 for 5G. Note that cellular bands vary by country. See Section 7.9 on page 151 for more information about cellular band configuration.

36.7 WiFi Problems

I cannot connect to the Zyxel Device WiFi.

1 Check the WiFi LED status to make sure the Zyxel Device WiFi is on.

2 Make sure your WiFi client is within transmission range of the Zyxel Device.

3 Make sure you entered the correct SSID and password. See the Zyxel Device back label for the default SSID and password.

4 Make sure your WiFi client is using the same WiFi security type (WPA2-PSK, WPA3-SAE, or none) as the Zyxel Device.

5 Make sure the WiFi adapter on your WiFi client is working properly. Right-click your computer's network adapter then select **Properties** to check your network adapter status.

6 Make sure the WiFi adapter on your WiFi client is IEEE 802.11-compatible and supports the same WiFi standard as the Zyxel Device radio.

Note: To check if it is your Zyxel Device that is causing the problem and not your WiFi connection, try using a wired connection.

The WiFi connection is slow and intermittent.

The following factors may cause interference:

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

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

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

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

36.8 USB Problems

The Zyxel Device fails to detect my USB device.

1 Disconnect the USB device.

2 Reboot the Zyxel Device.

3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

4 Reconnect your USB device to the Zyxel Device.

36.9 UPnP Problems

My computer cannot detect UPnP settings from the Zyxel Device.

1 Make sure that UPnP is enabled in your computer.

2 On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings** > **Home Networking** > **UPnP** screen.

3 Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.

4 Reconnect the Ethernet cable.

5 Restart your computer.

36.10 Getting More Troubleshooting Help

Search for support information for your model at *support.zyxel.com* and *community.zyxel.com* for more troubleshooting suggestions.

APPENDIX A
Customer Support

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

Zyxel

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

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

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

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

Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

Europe

Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria
- *https://www.zyxel.com/bg/bg*

Czech Republic

- Zyxel Communications Czech s.r.o.

- *https://www.zyxel.com/cz/cs*

Denmark

- Zyxel Communications A/S
- *https://www.zyxel.com/dk/da*

Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

France

- Zyxel France
- *https://www.zyxel.com/fr/fr*

Germany

- Zyxel Deutschland GmbH.
- *https://www.zyxel.com/de/de*

Hungary

- Zyxel Hungary & SEE
- *https://www.zyxel.com/hu/hu*

Italy

- Zyxel Communications Italy S.r.l.
- *https://www.zyxel.com/it/it*

Norway

- Zyxel Communications A/S
- *https://www.zyxel.com/no/no*

Poland

- Zyxel Communications Poland
- *https://www.zyxel.com/pl/pl*

Romania

- Zyxel Romania
- *https://www.zyxel.com/ro/ro*

Russian Federation

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Slovakia

- Zyxel Slovakia
- *https://www.zyxel.com/sk/sk*

Spain

- Zyxel Iberia
- *https://www.zyxel.com/es/es*

Sweden

- Zyxel Communications A/S
- *https://www.zyxel.com/se/sv*

Switzerland

- Studerus AG
- *https://www.zyxel.com/ch/de-ch*
- *https://www.zyxel.com/fr/fr*

Turkey

- Zyxel Turkey A.S.
- *https://www.zyxel.com/tr/tr*

UK

- Zyxel Communications UK Ltd.
- *https://www.zyxel.com/uk/en-gb*

Ukraine

- Zyxel Ukraine
- *https://www.zyxel.com/ua/uk-ua*

South America

Argentina

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Brazil

- Zyxel Communications Brasil Ltda.
- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.

- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX B
Wireless LANs

Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 220 Peer-to-Peer Communication in an Ad-hoc Network

BSS
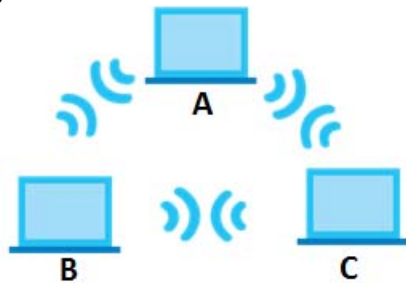
A Basic Service Set (BSS) exists when all communications between WiFi clients or between a WiFi client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between WiFi clients in the BSS. When Intra-BSS is enabled, WiFi client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, WiFi client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 221 Basic Service Set
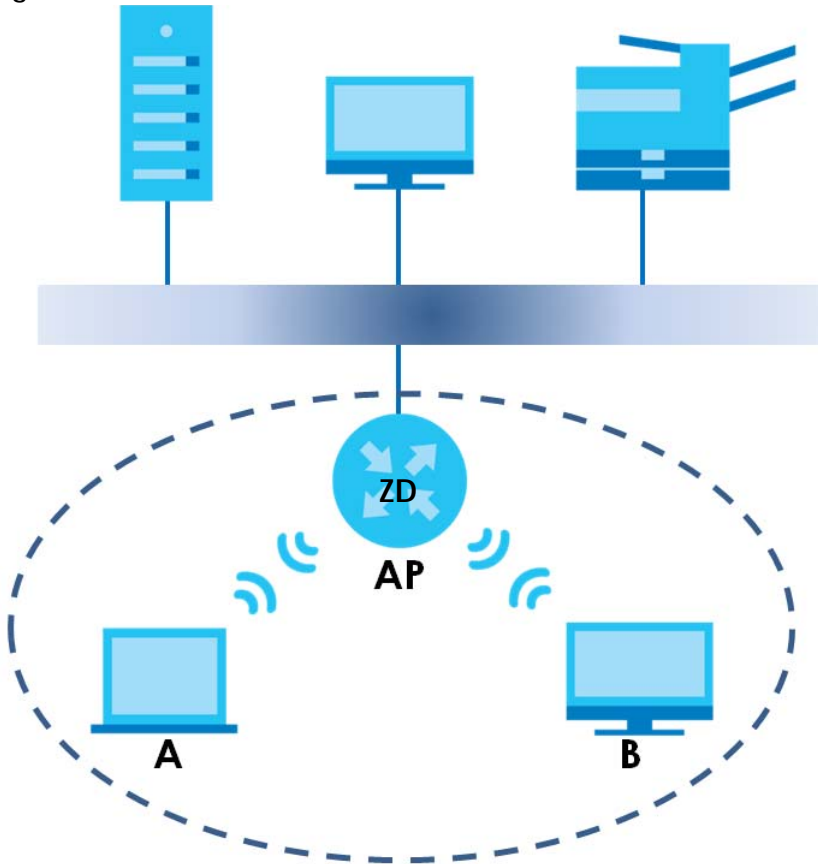
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated WiFi clients within the same ESS must have the same ESSID in order to communicate.

Figure 222 Infrastructure WLAN
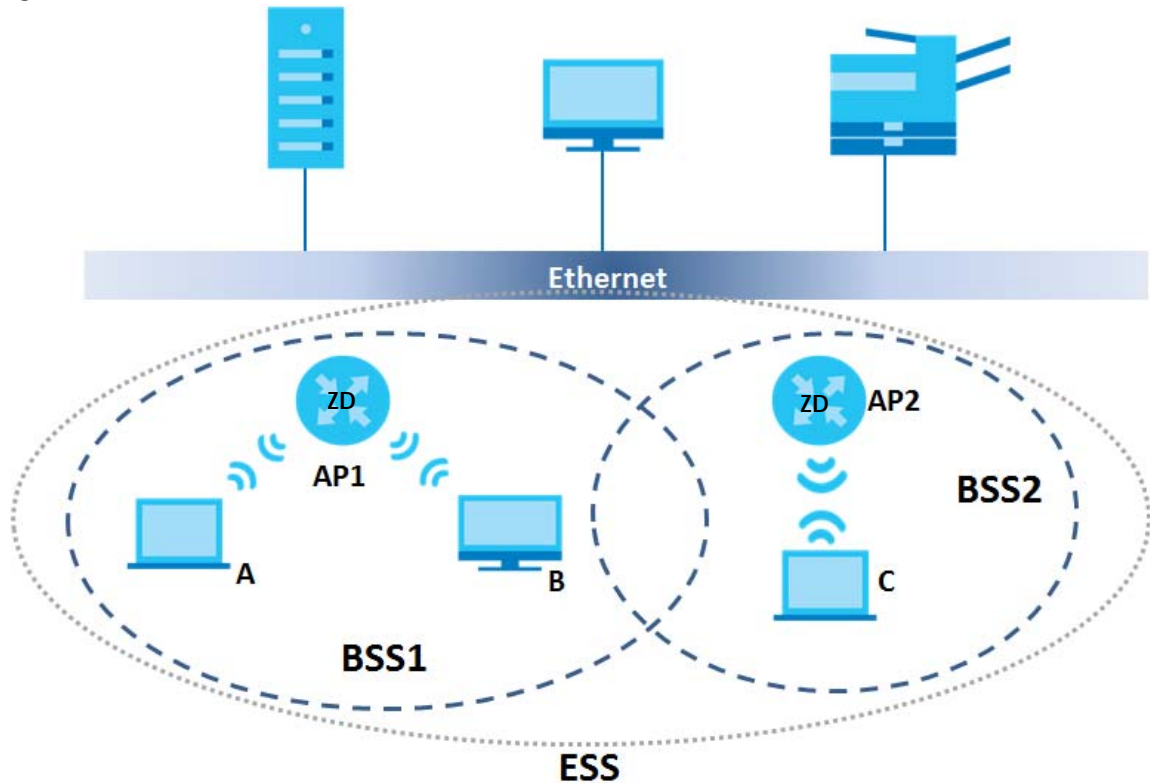
Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 223 RTS/CTS
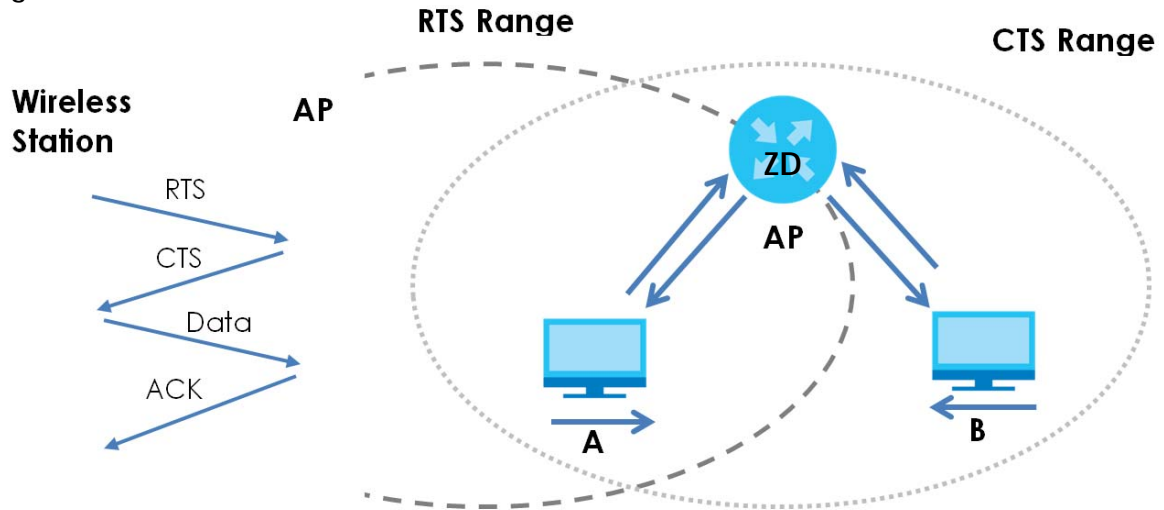
When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 135   IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between WiFi clients, access points and the wired network.

Wireless security methods available on the Zyxel Device are data encryption, WiFi client authentication, restricting access by device MAC address and hiding the Zyxel Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Zyxel Device.

Table 136   Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	WiFi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the Zyxel Device and on all WiFi clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

• User based identification that allows for roaming.

- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the WiFi clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the WiFi client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the WiFi client. The WiFi client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the WiFi clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2

and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 137   Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

WiFi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the WiFi clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and WiFi client. As long as the passwords match, a WiFi client will be granted access to a WLAN.

If the AP or the WiFi clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or WiFi clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice..

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a WiFi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP).

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate WiFi clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a WiFi client to store the PMK it derived through a successful authentication with an AP. The WiFi client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the WiFi client (already connected to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WiFi Client WPA Supplicants

A WiFi client supplicant is the software that runs on an operating system instructing the WiFi client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" WiFi client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1 The AP passes the WiFi client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients.

**Figure 224** WPA(2) with RADIUS Application Example
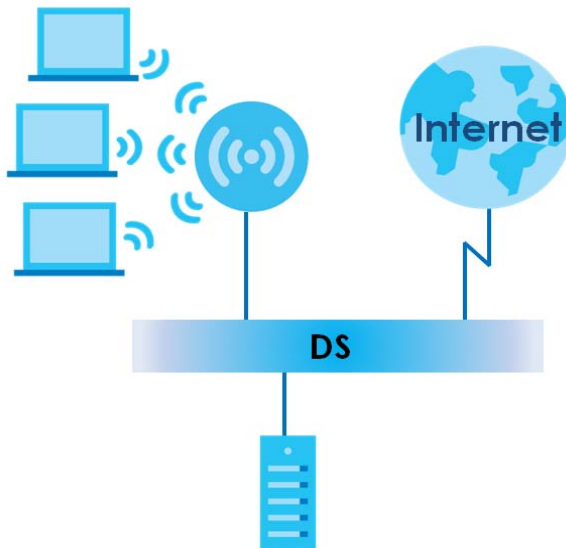
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1 First enter identical passwords into the AP and all WiFi clients. The Pre-Shared Key (PSK) must consist of between 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.

2 The AP checks each WiFi client's password and allows it to join the network only if the password matches.

3 The AP and WiFi clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and WiFi clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 225 WPA(2)-PSK Authentication
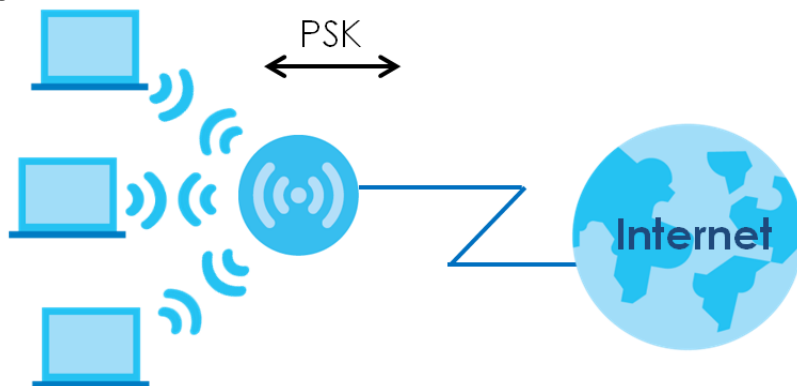
Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 138   Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4 GHz (IEEE 802.11b and IEEE 802.11g) or 5 GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WiFi

There are two types of antennas used for WiFi applications.

• Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
• Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

APPENDIX C
IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

Prefix and Prefix Length

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

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

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

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 139   Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, Multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A Multicast address allows a host to send packets to all hosts in a Multicast group.

Multicast scope allows you to determine the size of the Multicast group. A Multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined Multicast addresses.

Table 140   Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the Multicast addresses which are reserved and cannot be assigned to a Multicast group.

Table 141   Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

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

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 142

MAC	00	:	13	:	49	:	12	:	34	:	56

Table 143

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.
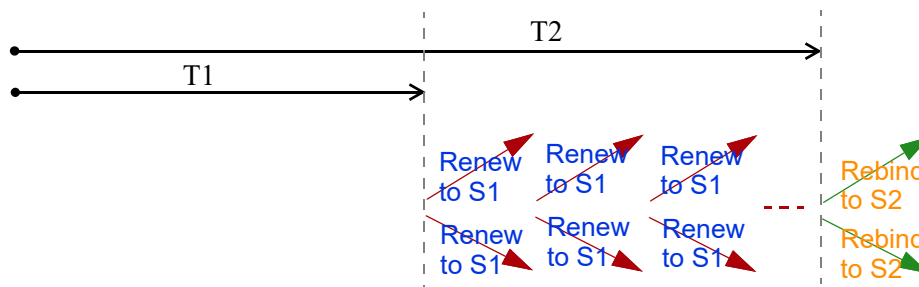
DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by Multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical Multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device

receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive Multicast packets and the IP addresses of Multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which Multicast groups a port can join.

MLD Messages

A Multicast router or switch periodically sends general queries to MLD hosts to update the Multicast forwarding table. When an MLD host wants to join a Multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a Multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 10 computer.

To enable IPv6 in Windows 10:

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

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.
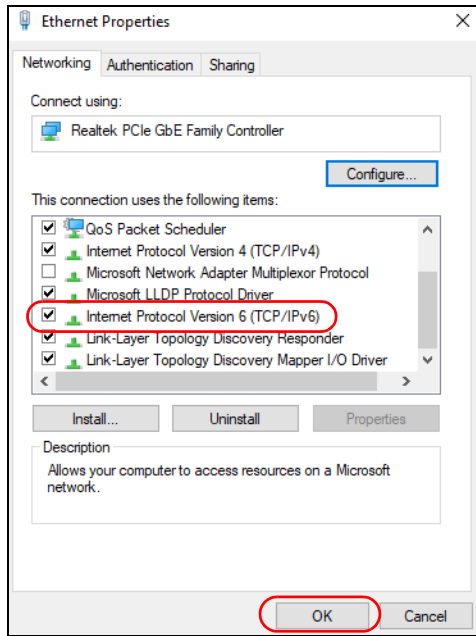
4 Click the Search icon (⌕) and then enter "cmd" in the search box.

5 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:f
```

APPENDIX D
Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 144   Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance *www.zyxel.com*) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for email.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.

Table 144   Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get email from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).

Table 144   Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX E
Legal Information

Copyright

Copyright © 2025 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America (Nebula LTE7461-M602)

The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 30 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

Canada (Nebula LTE7461-M602)

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 Statement

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

- This radio transmitter (2468C-LTE7461M602) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list that have, a gain greater than the maximum gain indicated for any type listed, are strictly prohibited for use with this device.

Antenna Information

Type	Antenna Type	Frequency Range	WiFi Gain (dBi)	LTE Gain (dBi)	Connector
WLAN-ANT0	PIFA	2.4 – 2.4835 GHz	6	N.A.	iPEX
WLAN-ANT1	PIFA	2.4 – 2.4835 GHz	5	N.A.	iPEX
WWAN	Dipole	2500 – 2570 MHz	N.A.	9	iPEX
		698 – 716 MHz	N.A.	3.5	iPEX
		777 – 787 MHz	N.A.	3	iPEX
		1850 – 1915 MHz	N.A.	8	iPEX
		814 – 849 MHz	N.A.	3.6	iPEX
		2305 – 2315 MHz	N.A.	9	iPEX
		1710 – 1780 MHz	N.A.	6	iPEX

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,
- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna models(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-LTE7461M602) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

informations antenne

Chaîne NB.	Antenne Type	Gamme de fréquences	WiFi Gain (dBi)	LTE Gain (dBi)	Connecteur
WLAN-ANT0	PIFA	2.4 – 2.4835 GHz	6	N.A.	iPEX
WLAN-ANT1	PIFA	2.4 – 2.4835 GHz	5	N.A.	iPEX
WWAN	Dipole	2500 – 2570 MHz	N.A.	9	iPEX
		698 – 716 MHz	N.A.	3.5	iPEX
		777 – 787 MHz	N.A.	3	iPEX
		1850 – 1915 MHz	N.A.	8	iPEX
		814 – 849 MHz	N.A.	3.6	iPEX
		2305 – 2315 MHz	N.A.	9	iPEX
		1710 – 1780 MHz	N.A.	6	iPEX

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes
- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with ISED radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 30 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 30 cm de distance entre la source de rayonnement et votre corps.

Europe and the United Kingdom

The following information applies if you use the product within the European Union and United Kingdom.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Regulation

- Compliance information for wireless products relevant to the EU, United Kingdom and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU, United Kingdom and other European countries, the 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz wireless LANs.
- If this device for operation in the band 5150 – 5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20 cm between the radio equipment and your body. For the NR7101, the minimum distance between radio equipment and body is 22cm.
- The maximum RF power operating for each band as follows:

Nebula LTE3301-PLUS

- WCDMA
  - The band 880 – 915 MHz is 24 dBm
  - The band 1710 – 1785 MHz is 24 dBm
  - The band 1920 – 1980 MHz is 24 dBm
- LTE
  - The band 703 – 748 MHz is 23 dBm
  - The band 832 – 862 MHz is 23 dBm
  - The band 880 – 915 MHz is 23 dBm
  - The band 1710 – 1785 MHz is 23 dBm
  - The band 1920 – 1980 MHz is 23 dBm
  - The band 2300 – 2400 MHz is 23 dBm
  - The band 2500 – 2570 MHz is 23 dBml
  - The band 2570 – 2620 MHz is 23 dBm
- WiFi
  - The band 2400 – 2483.5 MHz is 81.28 mW
  - The band 5150 – 5350 MHz is 180.30 mW
  - The band 5470 – 5725 MHz is 612.35 mW

Nebula NR5101

- WCDMA
  - The band 880 – 915 MHz is 24 dBm
  - The band 1710 – 1785 MHz is 24 dBm
  - The band 1920 – 1980 MHz is 24 dBm
- LTE
  - The band 703 – 748 MHz is 23 dBm
  - The band 832 – 862 MHz is 23 dBm
  - The band 880 – 915 MHz is 23 dBm
  - The band 1452 – 1496 MHz is 23 dBm
  - The band 1710 – 1785 MHz is 23 dBm
  - The band 1920 – 1980 MHz is 23 dBm
  - The band 2010 – 2025 MHz is 23 dBm
  - The band 2300 – 2400 MHz is 23 dBm
  - The band 2500 – 2570 MHz is 23 dBm
  - The band 2570 – 2620 MHz is 23 dBm
  - The band 3400 – 3600 MHz is 23 dBm
  - The band 3600 – 3800 MHz is 23 dBm
- NR
  - The band 2496 – 2690 MHz is 26 dBm

- • The band 3300 – 3800 MHz is 26 dBm
- • The band 3300 – 4200 MHz is 26 dBm
- • WiFi
  - • The band 2400 – 2483.5 MHz is 90.16 mW
  - • The band 5150 – 5350 MHz is 177.42 mW
  - • The band 5470 – 5725 MHz is 451.86 mW

Nebula NR7101

- • WCDMA
  - • The band 880 – 915 MHz is 24 dBm
  - • The band 1710 – 1785 MHz is 24 dBm
  - • The band 1920 – 1980 MHz is 24 dBm
- • LTE
  - • The band 703 – 748 MHz is 23 dBm
  - • The band 832 – 862 MHz is 23 dBm
  - • The band 880 – 915 MHz is 23 dBm
  - • The band 1710 – 1785 MHz is 23 dBm
  - • The band 1920 – 1980 MHz is 23 dBm
  - • The band 2010 – 2025 MHz is 23 dBm
  - • The band 2300 – 2400 MHz is 23 dBm
  - • The band 2500 – 2570 MHz is 23 dBm
  - • The band 2570 – 2620 MHz is 23 dBm
  - • The band 3400 – 3600 MHz is 23 dBm
- • NR
  - • The band 2496 – 2690 MHz is 26 dBm
  - • The band 3300 – 3800 MHz is 26 dBm
  - • The band 3300 – 4200 MHz is 26 dBm
- • WiFi
  - • The band 2400 – 2483.5 MHz is 86.10 mW

Nebula FWA505

- • LTE
  - • The band 703 – 748 MHz is 23 dBm
  - • The band 832 - 862 MHz is 23 dBm
  - • The band 880 - 915 MHz is 23 dBm
  - • The band 1710 - 1785 MHz is 23 dBm
  - • The band 1920 - 1980 MHz is 23 dBm
  - • The band 2300 - 2400 MHz is 23 dBm
  - • The band 2500 - 2570 MHz is 23 dBm
  - • The band 2570 - 2620 MHz is 23 dBm
  - • The band 3400 - 3600 MHz is 23 dBm
- • NR
  - • The band 703 - 748 MHz is 23 dBm
  - • The band 832 - 862 MHz is 23 dBm
  - • The band 880 - 915 MHz is 23 dBm
  - • The band 1710 - 1785 MHz is 23 dBm
  - • The band 1920 - 1980 MHz is 23 dBm
  - • The band 2300 - 2400 MHz is 23 dBm
  - • The band 2500 - 2570 MHz is 23 dBm
  - • The band 2570 - 2620 MHz is 23 dBm
  - • The band 3300 - 3800 MHz is 26 dBm
  - • The band 3300 - 4200 MHz is 26 dBm
- • WiFi
  - • The band 2400 - 2483.5 MHz is 90.99 mW
  - • The band 5150 - 5350 MHz is 140.60 mW
  - • The band 5470 - 5725 MHz is 244.91mW

Nebula FWA510

- • WCDMA
  - • The band 880 – 915 MHz is 24 dBm
  - • The band 1920 – 1980 MHz is 24 dBm
- • LTE
  - • The band 703 – 748 MHz is 23 dBm
  - • The band 832 – 862 MHz is 23 dBm
  - • The band 880 – 915 MHz is 23 dBm
  - • The band 1452 – 1496 MHz is 23 dBm
  - • The band 1710 – 1785 MHz is 23 dBm
  - • The band 1920 – 1980 MHz is 23 dBm
  - • The band 2300 – 2400 MHz is 23 dBm
  - • The band 2500 – 2570 MHz is 23 dBm
  - • The band 2570 – 2620 MHz is 23 dBm

- • The band 3400 – 3600 MHz is 23 dBm
- • NR
  - • The band 703 – 748 MHz is 20.25 dBm
  - • The band 3300 – 3800 MHz is 21.92 dBm
- • WiFi
  - • The band 2400 – 2483.5 MHz is 90.16 mW
  - • The band 5150 – 5350 MHz is 174.58 mW
  - • The band 5470 – 5725 MHz is 857.04 mW

Nebula FWA710

- • WCDMA
  - • The band 880 – 915 MHz is 24 dBm
  - • The band 1920 – 1980 MHz is 24 dBm
- • LTE
  - • The band 703 – 748 MHz is 23 dBm
  - • The band 832 – 862 MHz is 23 dBm
  - • The band 880 – 915 MHz is 23 dBm
  - • The band 1452 – 1496 MHz is 23 dBm
  - • The band 1710 – 1785 MHz is 23 dBm
  - • The band 1920 – 1980 MHz is 23 dBm
  - • The band 2300 – 2400 MHz is 23 dBm
  - • The band 2500 – 2570 MHz is 23 dBm
  - • The band 2570 – 2620 MHz is 23 dBm
  - • The band 3400 – 3600 MHz is 23 dBm
- • NR
  - • The band 703 – 748 MHz is 20.25 dBm
  - • The band 3300 – 3800 MHz is 21.92 dBm
- • WiFi
  - • The band 2400 – 2483.5 MHz is 77.98 mW

Belgium (English) / België (Flemish) / Belgique (French)	**National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie *http://www.bipt.be* voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez *http://www.ibpt.be* pour de plus amples détails.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. National Restrictions • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check *https://www.mise.gov.it/it/* for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare *https://www.mise.gov.it/it/* per maggiori dettagli.

Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕC.

Notes:
- Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty or has extreme temperatures as these conditions may harm your device.

- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- The Power Supply is not waterproof, avoid contact with liquid. Handle the Power Supply with care; do not pry open, nor pull or press the pins on it.
- Do not expose your Zyxel Device to dampness, dust or corrosive liquids.
- Do not store things on the Zyxel Device.
- Do not obstruct the Zyxel Device ventilation slots as insufficient airflow may harm your Zyxel Device. For example, do not place the Zyxel Device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this Zyxel Device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the Zyxel Device.
- Do not open the Zyxel Device or unit. Opening or removing the Zyxel Device covers can expose you to dangerous high voltage or other risks.
- Only qualified service personnel should service or disassemble this Zyxel Device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this Zyxel Device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adapter first before connecting it to a power outlet.
- Do not allow anything to rest on the power adapter or cord and do NOT place the product where anyone can walk on the power adapter or cord.
- Please use the provided or designated connection cables/power cables/adapters. Connect it to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adapter or cord is damaged, it might cause electrocution. Remove it from the Zyxel Device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- The following warning statements apply, where the disconnect device is not incorporated in the Zyxel Device or where the plug on the power supply cord is intended to serve as the disconnect device,

  – For a permanently connected Zyxel Device, a readily accessible disconnected device shall be incorporated externally to the Zyxel Device;

  – For a pluggable device, the socket-outlet shall be installed near the Zyxel Device and shall be easily accessible.

Environment Statement

ErP

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless settings, please refer to the chapter about wireless settings for more detail.)

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區
- 取得審驗證明之低功率射頻器材，非經核准，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
  前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區
- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

以下訊息僅適用於產品屬於行動通信電信終端設備並銷售至台灣地區
- 減少電磁波影響，請妥適使用
- Nebula NR5101
- 電波功率密度 MPE 標準值 : 1 mW/ cm2，送測產品實測值 : 0.116 mW/ cm2，建議使用時設備天線至少距離人體 20 公分
- Nebula LTE3301-PLUS
- 電波功率密度 MPE 標準值 : 1 mW/ cm2，送測產品實測值 : 0.141 mW/ cm2，建議使用時設備天線至少距離人體 20 公分

安全警告 - 為了您的安全，請先閱讀以下警告及指示 :
- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸 :
  – 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  – 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 (如 : 台灣供應電壓 110 伏特)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用 :
  – 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  – 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
$\sim$	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
= = =	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
⏚	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
▣	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to *www.zyxel.com* to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the Zyxel Device at *https://www.zyxel.com/global/en/support/warranty-information*.

Registration

Register your product online at *www.zyxel.com* to receive email notices of firmware upgrades and related information.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses please go to: *https://www.zyxel.com/form/gpl_oss_software_notice.shtml*

Index