

User's Guide

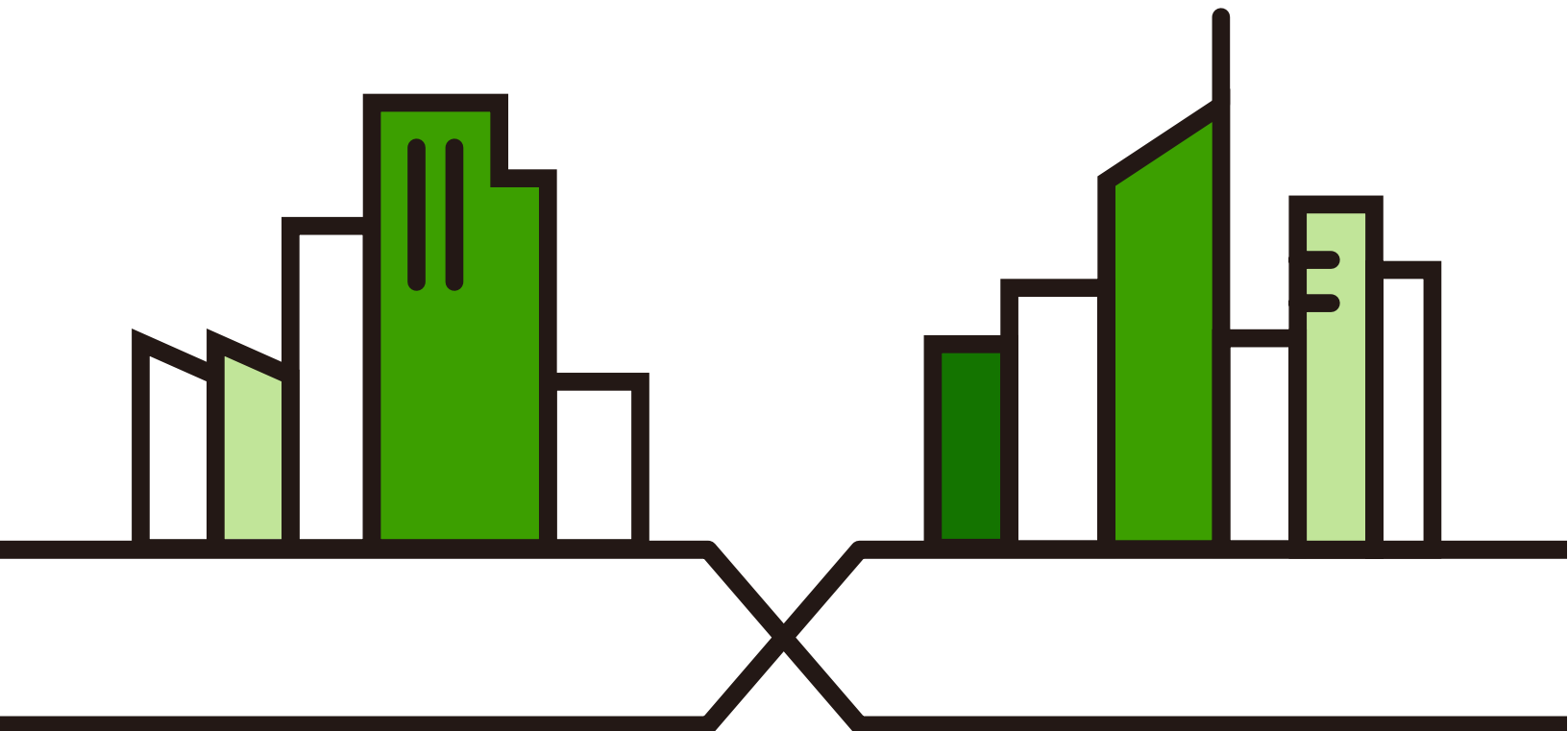
Nebula Mobile Router

Nebula LTE3301-PLUS/Nebula NR5101/Nebula NR7101/Nebula LTE7461-M602

Default Login Details

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

Version 1.00 Ed 2, 7/2022



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

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

- The Nebula CC help portal

Go to <https://nebula.zyxel.com/> 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

- The LTE or NR (5G) device in this user's guide will be referred to as the "Zyxel Device".
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting > Routing > DNS Route** means you first click **Network Setting** in the navigation panel, then the **Routing** submenu, and then finally the **DNS Route** tab to get to that screen.

Icons Used in Figures

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

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

Contents Overview

User's Guide	15
Introduction	16
Hardware Panels	24
Web Configurator	35
Quick Start	45
Tutorials	48
Technical Reference	86
Connection Status	87
Broadband	101
Wireless	123
Home Networking	153
Routing	175
Network Address Translation (NAT)	185
DNS	198
VLAN Group	202
Interface Grouping	205
USB Service	210
Nebula	215
Firewall	217
MAC Filter	229
Parental Control	231
Certificates	237
Log	246
Traffic Status	249
ARP Table	252
Routing Table	254
WLAN Station Status	257
Cellular WAN Status	259
System	264
User Account	266
Remote Management	269
TR-069 Client	275
Time Settings	278
Email Notification	281
Log Setting	284
Firmware Upgrade	288
Backup/Restore	292

Diagnostic 296

Troubleshooting and Appendices298

 Troubleshooting 299

Document Conventions	3
Contents Overview	4
Part I: User's Guide.....	15
Chapter 1	
Introduction	16
1.1 Overview	16
1.1.1 Feature Differences	16
1.1.2 NCC Management	17
1.1.3 Register Your Zyxel Device Using the Nebula Web Portal	18
1.2 Applications for the Zyxel Device	21
1.3 How to Manage your Zyxel Device	23
1.4 Good Habits for Managing the Zyxel Device	23
Chapter 2	
Hardware Panels.....	24
2.1 Overview	24
2.2 LEDs	24
2.3 Panel Ports and Buttons	27
2.3.1 WiFi/WPS Button	30
2.3.2 RESET Button	33
Chapter 3	
Web Configurator.....	35
3.1 Overview	35
3.1.1 Access the Web Configurator	35
3.2 Web Configurator Layout	37
3.2.1 Settings Icon	38
3.2.2 Widget and Check Icons	43
Chapter 4	
Quick Start.....	45
4.1 Overview	45
4.2 Quick Start Setup	45
4.3 Quick Start Setup – Time Zone	45
4.4 Quick Start Setup – WiFi	46
4.5 Quick Start Setup – Finish	47
Chapter 5	
Tutorials	48

5.1 Overview	48
5.2 Wired Network Setup	48
5.2.1 Setting Up an Ethernet Connection	48
5.3 WiFi Network Setup	50
5.3.1 Changing Security on a WiFi Network	51
5.3.2 Connecting to the Zyxel Device's WiFi Network Using WPS	53
5.3.3 Setting Up a Guest Network	57
5.3.4 Setting Up Two Guest WiFi Networks on Different WiFi Bands	61
5.4 Cellular Network Setup	66
5.4.1 Setting up a Cellular Network Connection	66
5.5 USB Applications	66
5.5.1 File Sharing	66
5.6 Network Security	71
5.6.1 Configuring a Firewall Rule	71
5.6.2 Parental Control	72
5.6.3 Configuring a MAC Address Filter	77
5.7 Internet Calls	78
5.7.1 Configuring VoIP	78
5.7.2 Adding a SIP Service Provider	78
5.7.3 Adding a SIP Account	79
5.7.4 Configuring a Phone	80
5.7.5 Making a VoIP Call	81
5.7.6 Making a VoLTE Phone Call	82
5.8 Device Maintenance	82
5.8.1 Upgrading the Firmware	82
5.8.2 Backing up the Device Configuration	83
5.8.3 Restoring the Device Configuration	84

Part II: Technical Reference..... 86

Chapter 6 Connection Status.....87

6.1 Connection Status Overview	87
6.1.1 Connectivity	87
6.1.2 Icon and Device Name	88
6.1.3 System Info	88
6.1.4 Cellular Info	90
6.1.5 Cloud Control Status	95
6.1.6 WiFi Settings	96
6.2 Guest WiFi Settings	97
6.2.1 LAN	99

Chapter 7	
Broadband	101
7.1 Overview	101
7.1.1 What You Can Do in this Chapter	101
7.1.2 What You Need to Know	102
7.1.3 Before You Begin	102
7.2 Broadband	102
7.2.1 Add or Edit Internet Connection	103
7.3 Ethernet WAN	107
7.4 Cellular WAN	107
7.5 Cellular APN	109
7.5.1 Edit Cellular APN1/APN2	110
7.5.2 Using Separate APNs for Data and Management Traffic	112
7.6 Cellular SIM Configuration	114
7.7 Cellular Band Configuration	116
7.8 Cellular PLMN Configuration	117
7.9 Cellular IP Passthrough	119
7.10 Cellular Lock	120
7.11 Cellular SMS	121
7.11.1 Send New Message Screen	122
Chapter 8	
Wireless	123
8.1 Overview	123
8.1.1 What You Can Do in this Chapter	123
8.1.2 What You Need to Know	123
8.2 Wireless General Settings	124
8.2.1 No Security	126
8.2.2 More Secure (Recommended)	127
8.3 Guest/More AP Screen	129
8.3.1 The Edit Guest/More AP Screen	130
8.4 MAC Authentication	133
8.5 WPS	134
8.6 WMM	136
8.7 Others Screen	137
8.8 WLAN Scheduler	141
8.8.1 Add or Edit Rules	142
8.9 Technical Reference	143
8.9.1 WiFi Network Overview	143
8.9.2 Additional Wireless Terms	144
8.9.3 WiFi Security Overview	144
8.9.4 Signal Problems	146
8.9.5 MBSSID	146

8.9.6 WiFi Protected Setup (WPS)	147
--	-----

Chapter 9

Home Networking	153
------------------------------	------------

9.1 Overview	153
9.1.1 What You Can Do in this Chapter	153
9.1.2 What You Need To Know	153
9.2 LAN Setup	154
9.3 Static DHCP	159
9.3.1 Before You Begin	159
9.4 UPnP	161
9.5 Technical Reference	162
9.5.1 DHCP Setup	163
9.5.2 DNS Server Addresses	163
9.5.3 LAN TCP/IP	164
9.6 Turn on UPnP in Windows 10 Example	165
9.6.1 Auto-discover Your UPnP-enabled Network Device	167
9.7 Web Configurator Easy Access in Windows 10	170
9.7.1 DHCP Setup	172
9.7.2 DNS Server Addresses	172
9.7.3 LAN TCP/IP	173

Chapter 10

Routing	175
----------------------	------------

10.1 Overview	175
10.2 Configure Static Route	175
10.2.1 Add or Edit Static Route	176
10.3 DNS Route	180
10.3.1 Add or Edit DNS Route	181
10.4 Policy Route	181
10.4.1 Add or Edit Policy Route	182
10.5 RIP Overview	184
10.5.1 RIP	184

Chapter 11

Network Address Translation (NAT)	185
--	------------

11.1 Overview	185
11.1.1 What You Can Do in this Chapter	185
11.1.2 What You Need To Know	185
11.2 Port Forwarding	186
11.2.1 Port Forwarding	186
11.2.2 Add or Edit Port Forwarding	187
11.3 Port Triggering	189

11.3.1 Add or Edit Port Triggering Rule	191
11.4 DMZ	192
11.5 ALG	193
11.6 Technical Reference	194
11.6.1 NAT Definitions	194
11.6.2 What NAT Does	195
11.6.3 How NAT Works	195
11.6.4 NAT Application	196
Chapter 12	
DNS	198
12.1 DNS Overview	198
12.1.1 What You Can Do in this Chapter	198
12.1.2 What You Need To Know	199
12.2 DNS Entry	199
12.2.1 Add or Edit DNS Entry	200
12.3 Dynamic DNS	200
Chapter 13	
VLAN Group	202
13.1 Overview	202
13.1.1 What You Can Do in this Chapter	202
13.2 VLAN Group Settings	203
13.2.1 Add or Edit a VLAN Group	203
Chapter 14	
Interface Grouping	205
14.1 Interface Grouping Overview	205
14.1.1 What You Can Do in this Chapter	205
14.2 Interface Grouping	205
14.2.1 Interface Group Configuration	206
14.2.2 Interface Grouping Criteria	208
Chapter 15	
USB Service	210
15.1 USB Service Overview	210
15.1.1 What You Need To Know	210
15.1.2 Before You Begin	211
15.2 USB Service	211
15.2.1 Add New Share	213
15.2.2 Add New User Screen	214
Chapter 16	
Nebula	215

16.1 Nebula Overview	215
16.2 Nebula	215
Chapter 17	
Firewall.....	217
17.1 Overview	217
17.1.1 What You Need to Know About Firewall	217
17.2 Firewall	218
17.2.1 What You Can Do in this Chapter	218
17.3 Firewall General Settings	219
17.4 Protocol (Customized Services)	220
17.4.1 Add Customized Service	221
17.5 Access Control (Rules)	221
17.5.1 Add New ACL Rule	222
17.6 DoS	225
17.7 Firewall Technical Reference	226
17.7.1 Firewall Rules Overview	226
17.7.2 Guidelines For Security Enhancement With Your Firewall	227
17.7.3 Security Considerations	227
Chapter 18	
MAC Filter	229
18.1 MAC Filter Overview	229
18.2 MAC Filter	229
18.2.1 Add New Rule	230
Chapter 19	
Parental Control	231
19.1 Parental Control Overview	231
19.2 Parental Control Schedule and URL Filter	231
19.2.1 Add or Edit a Parental Control Profile	232
Chapter 20	
Certificates	237
20.1 Certificates Overview	237
20.1.1 What You Can Do in this Chapter	237
20.2 What You Need to Know	237
20.3 Local Certificates	237
20.3.1 Create Certificate Request	239
20.3.2 View Certificate Request	239
20.4 Trusted CA	241
20.5 Import Trusted CA Certificate	242
20.6 View Trusted CA Certificate	243

20.7 Certificates Technical Reference	243
20.7.1 Verify a Certificate	244
Chapter 21	
Log	246
21.1 Log Overview	246
21.1.1 What You Can Do in this Chapter	246
21.1.2 What You Need To Know	246
21.2 System Log	247
21.3 Security Log	248
Chapter 22	
Traffic Status	249
22.1 Traffic Status Overview	249
22.1.1 What You Can Do in this Chapter	249
22.2 WAN Status	249
22.3 LAN Status	250
Chapter 23	
ARP Table	252
23.1 ARP Table Overview	252
23.1.1 How ARP Works	252
23.2 ARP Table	252
Chapter 24	
Routing Table	254
24.1 Routing Table Overview	254
24.2 Routing Table	254
Chapter 25	
WLAN Station Status	257
25.1 WLAN Station Status Overview	257
Chapter 26	
Cellular WAN Status	259
26.1 Cellular WAN Status Overview	259
26.2 Cellular WAN Status	259
Chapter 27	
System	264
27.1 System Overview	264
27.2 System	264

Chapter 28	
User Account	266
28.1 User Account Overview	266
28.2 User Account	266
28.2.1 User Account Add or Edit	267
Chapter 29	
Remote Management	269
29.1 Overview	269
29.1.1 What You Can Do in this Chapter	269
29.2 MGMT Services	269
29.3 MGMT Services for IP Passthrough	270
29.4 Trust Domain	271
29.5 Add Trust Domain	272
29.6 Trust Domain for IP Passthrough	273
29.7 Add Trust Domain	273
Chapter 30	
TR-069 Client	275
30.1 Overview	275
30.2 TR-069 Client	275
Chapter 31	
Time Settings	278
31.1 Time Settings Overview	278
31.2 Time	278
Chapter 32	
Email Notification	281
32.1 Email Notification Overview	281
32.2 Email Notification	281
32.2.1 E-mail Notification Edit	282
Chapter 33	
Log Setting	284
33.1 Log Setting Overview	284
33.2 Log Setting	284
33.2.1 Example Email Log	286
Chapter 34	
Firmware Upgrade	288
34.1 Overview	288
34.2 Firmware Upgrade	288

34.3 Module Upgrade	290
Chapter 35	
Backup/Restore	292
35.1 Backup/Restore Overview	292
35.2 Backup/Restore	292
35.3 Reboot	294
35.4 Schedule Reboot	295
Chapter 36	
Diagnostic.....	296
36.1 Diagnostic Overview	296
36.1.1 What You Can Do in this Chapter	296
36.2 Ping/TraceRoute/Nslookup Test/ Speed Test	296
 Part III: Troubleshooting and Appendices.....	 298
Chapter 37	
Troubleshooting.....	299
37.1 Overview	299
37.2 Power and Hardware Problems	299
37.3 Device Access Problems	300
37.4 Cellular Problems	303
37.5 Internet Problems	304
37.6 WiFi Problems	306
37.7 USB Problems	306
37.8 UPnP Problems	307
Appendix A Customer Support	308
Appendix B IPv6.....	313
Appendix C Legal Information	319
Appendix D Legal Information	327
Index	335

PART I

User's Guide

CHAPTER 1

Introduction

1.1 Overview

Zyxel Device refers to the following models:

- Nebula LTE3301-PLUS (4G LTE-A Indoor Router)
- Nebula NR5101 (5G NR Indoor IAD)
- Nebula NR7101 (5G New Radio Outdoor Router)
- Nebula LTE7461-M602 (4G LTE-A 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

FEATURE/MODEL	NEBULA LTE3301-PLUS	NEBULA NR5101	NEBULA NR7101	NEBULA LTE7461-M602
2.4G WiFi	Y	Y	Y	Y
5G WiFi	Y	Y	N	N
External Antennas	Y	N	N	N
Module Upgrade	N	N	Y	N
Schedule Reboot	N	N	Y	N
VLAN Group	N	N	Y	N
Ethernet WAN	Y	Y	N	N
Cellular Backup	N	Y	N	N
Cellular IP Passthrough	Y	Y	N	Y
Guest/More AP	Y	Y	N	N
More AP Edit	Y	Y	N	N
WAN Scheduler	Y	Y	N	N
File Sharing	Y	Y	N	N
Parental Control	Y	Y	N	N
System	Y	Y	N	Y
Network Monitoring	Y	Y	Y	Y
Proxy ARP	N	N	Y	N
FQ_Codel (Fair Queuing with Controlled Delay)	N	N	Y	N
PIN Modification	N	N	Y	Y
Preferred Service Domain	N	N	Y	N

Table 1 Feature Differences (continued)

FEATURE/MODEL	NEBULA LTE3301-PLUS	NEBULA NR5101	NEBULA NR7101	NEBULA LTE7461-M602
IGMP Proxy	N	Y	Y	Y
MLD Proxy	N	Y	Y	Y
Fullcone NAT	N	Y	Y	N
Latency Settings	N	N	Y	N
DHCPv6	Y	Y	N	Y
Neighbor Cells	N	N	Y	Y
Speed Test	N	N	Y	Y
XMPP	N	N	Y	N
TR-069 Client	Y	Y	Y	N

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

1.1.2 NCC Management

You can manage the Zyxel Device with the Zyxel Nebula Cloud Center. The Zyxel Nebula Cloud 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 myZyxel account to log into the NCC for management first. You can access the NCC through the NCC web portal via a web browser on your computer or the NCC Mobile app on your smartphone, see [Section 1.3 on page 23](#) for more information.

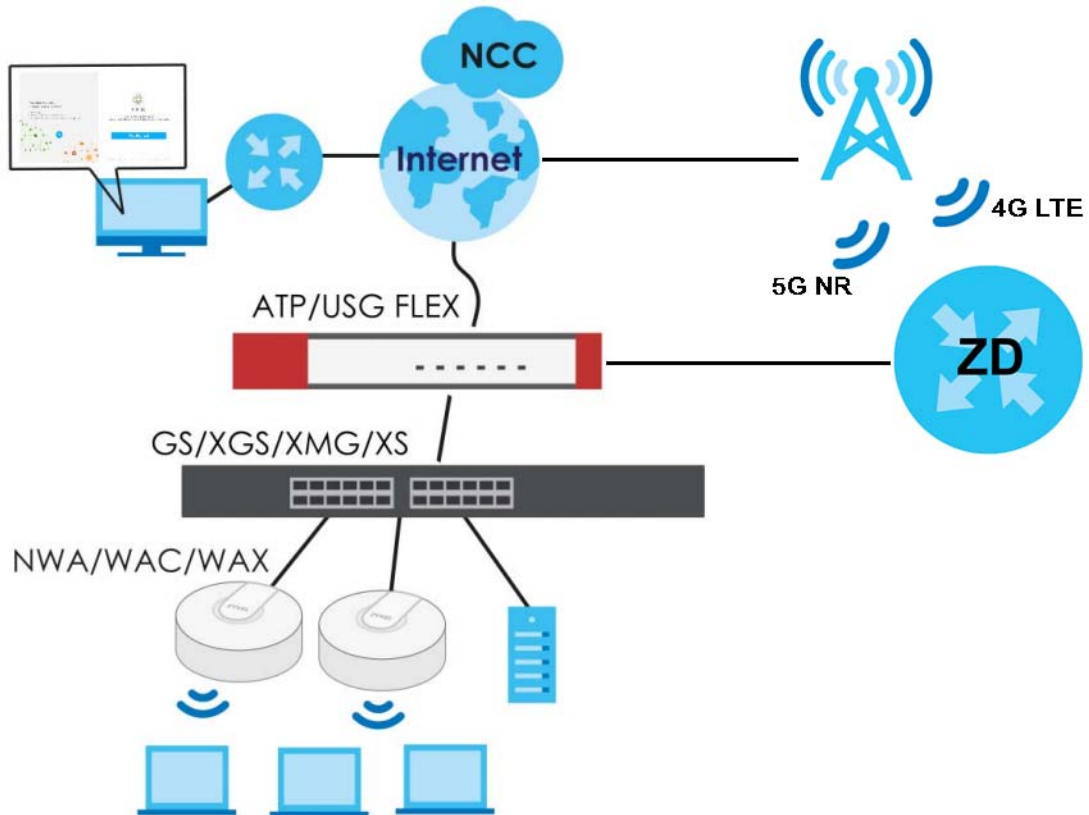
For advanced configurations, such as configuring WAN settings, wireless LAN settings and firewall settings, use the Zyxel Device web configurator. To find the best place for your Zyxel Device to receive the optimal cellular signal or perform a signal strength test, use the Zyxel Air app.

Table 2 Management Methods

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

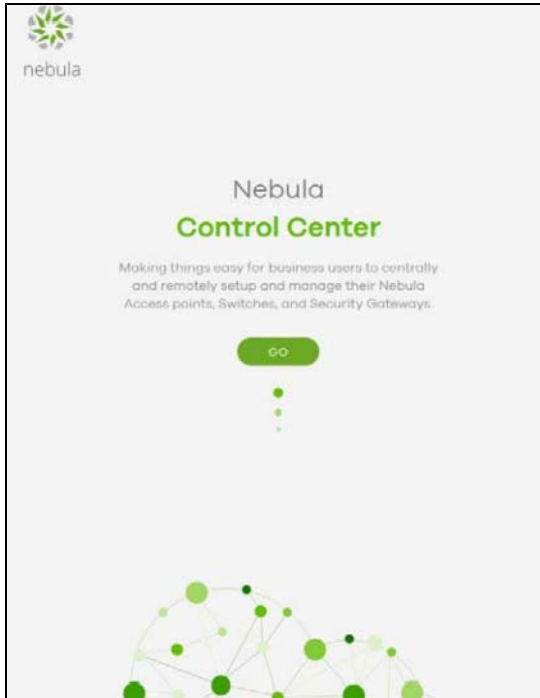
Note: The configurations you make in the NCC have priority over the configurations in the web configurator and the Zyxel Air app.

Figure 1 NCC Example Network Topology

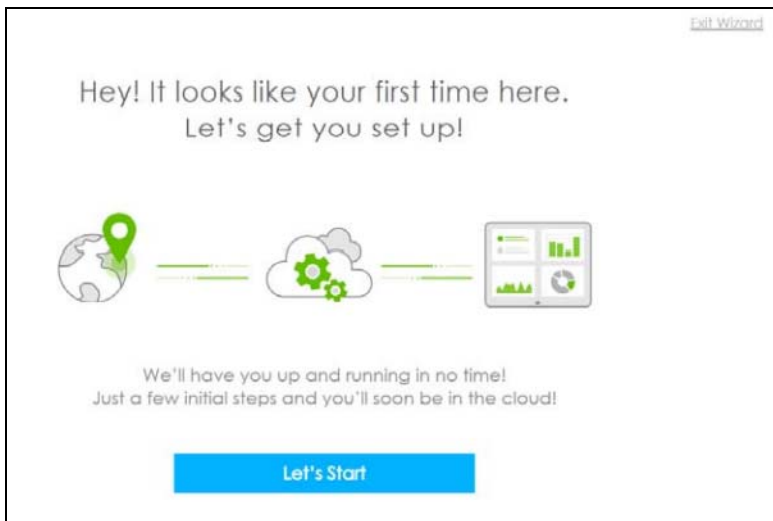


1.1.3 Register Your Zyxel Device Using the Nebula Web Portal

- 1 After logging into <https://nebula.zyxel.com>, the following screen appears. Click **GO** to start the NCC wizard.



- 2 The welcome screen displays when you are creating the first organization under your account. Click **Let's Start** to begin.



- 3 Enter a descriptive name for your organization and site. Both names must consist of 1 to 64 characters.
- 4 Select the time zone of your location. This will set the time difference between your time zone and Coordinated Universal Time (UTC).
- 5 Click **Next** to continue.

01 — — —

Nebula is organized into Organizations, for example, "YourCompany" or "YourClient", and Sites, for example, "London Branch" or "Factory". You can create as many Organizations and Sites as you need once you're up and running. The country allows us to set the correct time zone for your site and the legal requirements for settings like radio power on access points.

Please enter your Organization and Site names and select the correct Country and Time Zone.

Organization

Site

Country
Taiwan

Timezone
Asia - Taipei (UTC +8.0)

Next

[Exit Wizard](#)

- 6 Enter your Zyxel Device MAC address and serial number.
- 7 Click the **+Add** button to register and add the Zyxel Device to the site. You can register multiple Zyxel Device at a time.

02 — — —

To add your device(s) you will need to input the MAC address, which is the number that looks like this: 7C:99:DD:39:AC:F0, and the Serial Number that looks similar to: S891345239054. These are located on the box and at the bottom of each device, it may appear as:

Serial Number
MAC address

You might just click Next to skip this step.

Let's now add your device(s) to Nebula

MAC Address

Serial Number

+ Add

Name	MAG	Serial Number
Please click Add button after filling in the MAC address and Serial Number		

Back Next

[Exit Wizard](#)

- 8 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.

1.2 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.

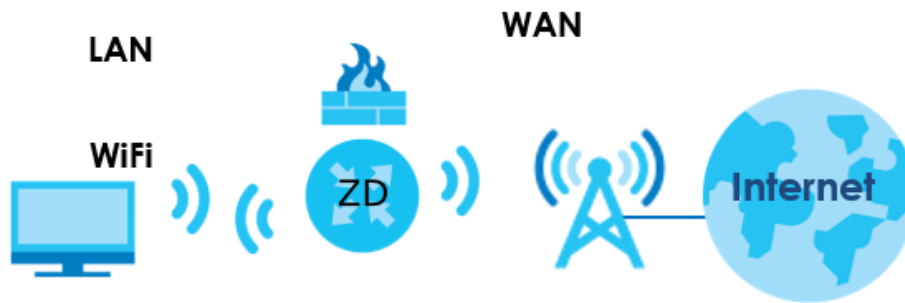
You can also install external antennas to improve your wireless WAN signal strength, see [Table 1 on page 16](#) for more information.

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.

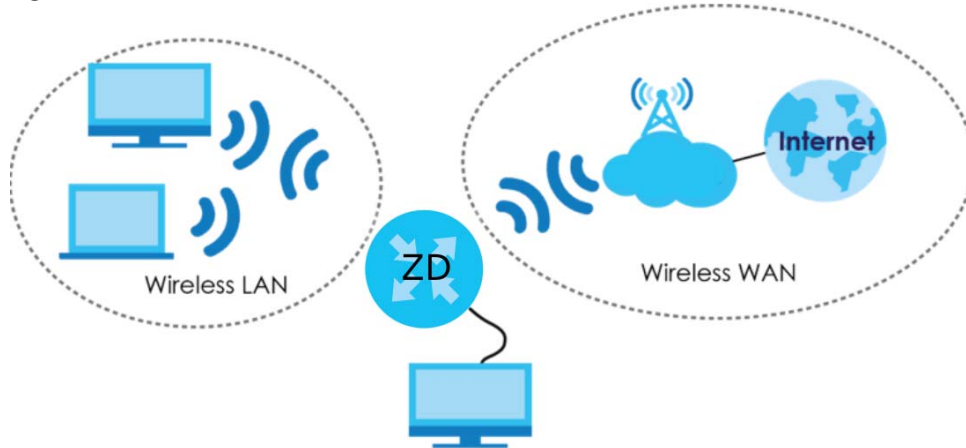
Figure 2 Zyxel Device's Internet Access Application



Wireless LAN (WiFi)

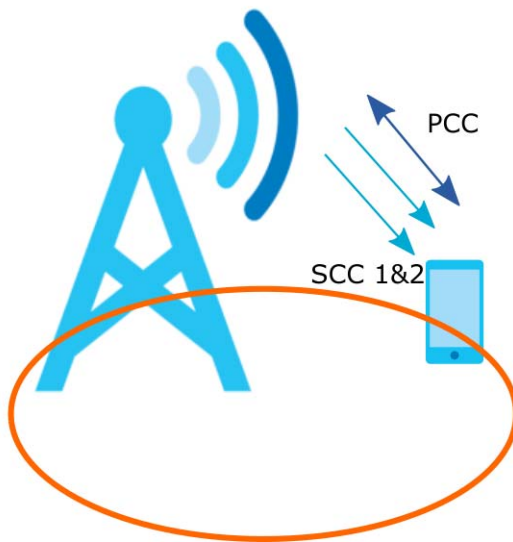
WiFi clients can connect to the Zyxel Device to access network resources and the Internet. The Zyxel Device supports WiFi Protected Setup (WPS), which allows you to quickly set up a WiFi network with strong security.

Your Zyxel Device WiFi may only be for configuration, see [Table 1 on page 16](#) for more information.

Figure 3 Zyxel Device's Wireless LAN

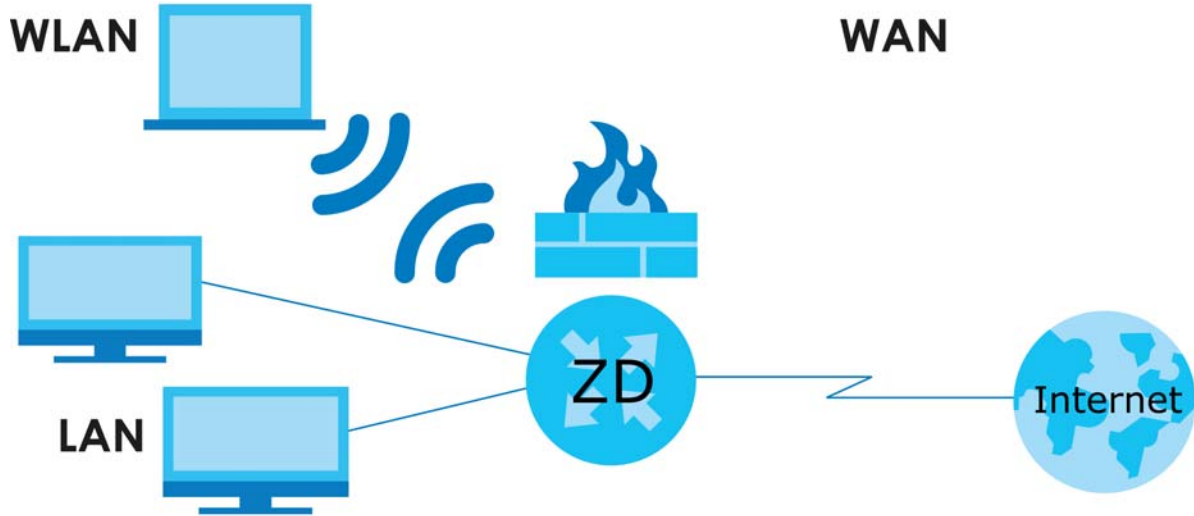
Carrier Aggregation

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

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.

Figure 5 Zyxel Device's Internet Access Application: Ethernet WAN

1.3 How to Manage your Zyxel Device

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

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

1.4 Good Habits for Managing the Zyxel Device

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

- **Change the password.** Use a password that is not easy to guess and that consists of different types of characters, such as numbers and letters.
- **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.

Figure 6 Nebula LTE3301-PLUS

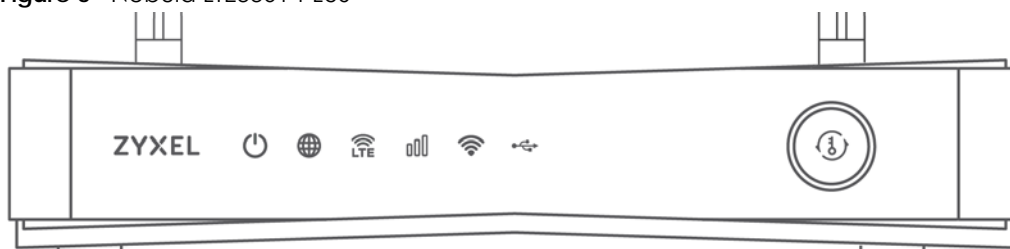


Figure 7 Nebula NR5101

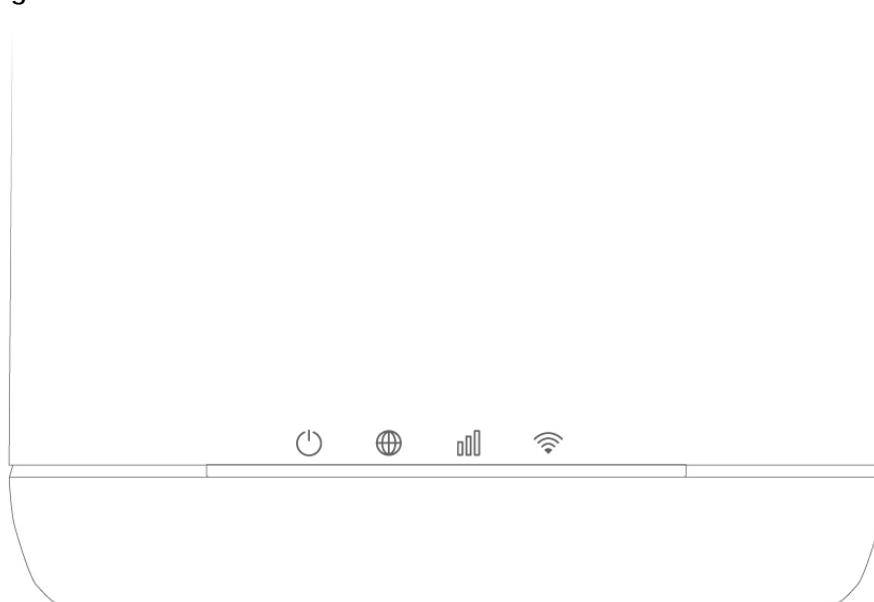
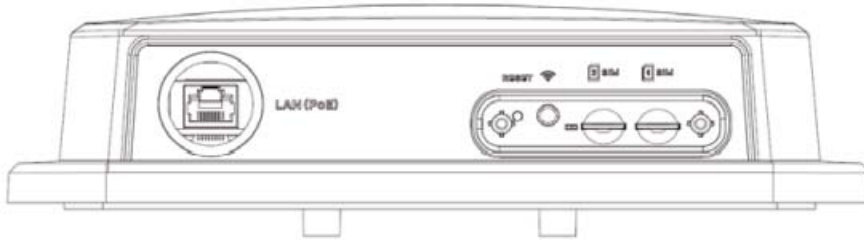


Figure 8 Nebula NR7101**Figure 9** Nebula LTE7641-M602

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

Table 3 Nebula LTE3301-PLUS LED Behavior

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.

Table 3 Nebula LTE3301-PLUS LED Behavior (continued)

LED	COLOR	STATUS	DESCRIPTION
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.

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

Table 4 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.

Table 5 Nebula NR7101 LED Behavior

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

Table 6 Nebula LTE7461-M602 LED Behavior

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.

2.3 Panel Ports and Buttons

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

Figure 10 Nebula LTE3301-PLUS

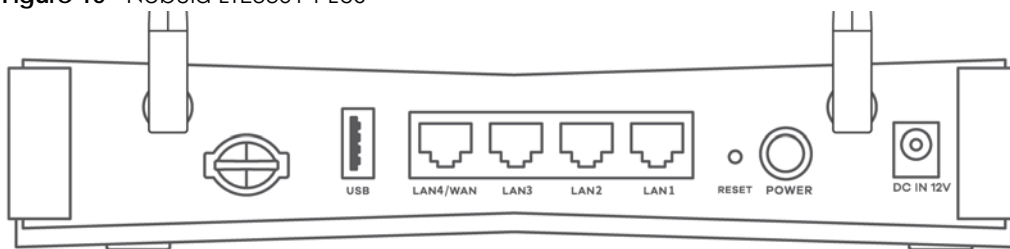


Figure 11 Nebula NR5101

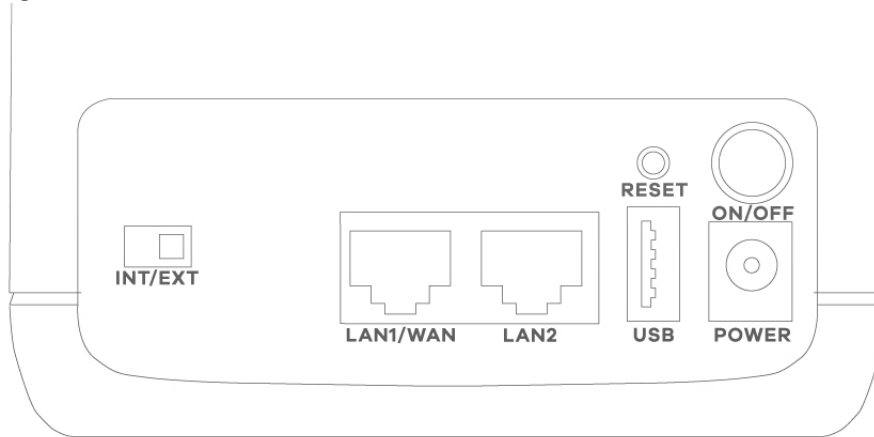


Figure 12 Nebula NR7101

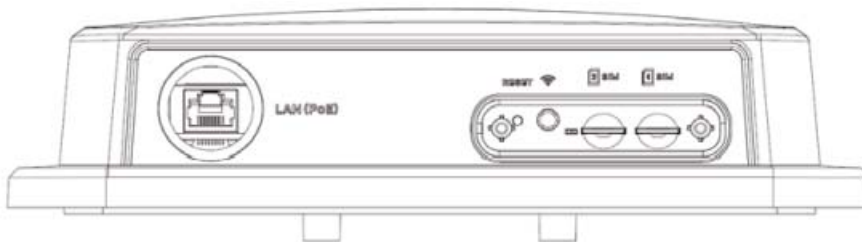


Figure 13 Nebula LTE7461-M602



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

Table 7 Nebula LTE3301-PLUS Panel Ports and Buttons

LABELS	DESCRIPTION
ANT1-ANT2	Install the external antennas to strengthen the cellular signal.
LAN/Ethernet	Connect a computer to the LAN using an RJ45 cable.
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.
RESET	Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults.
POWER Button	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.
Reboot	Press the RESET button for more than 2 seconds but less than 5 seconds, it will cause the system to reboot.
SIM card	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.

Table 8 Nebula NR5101 Panel Ports and Buttons

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.
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	Press for 1 second: Enable or disable WiFi. Press for more than 5 seconds: Activate WPS connection process.
RESET	Press for 2 seconds: Reboot the Zyxel Device. Press for 5 seconds: Restore the Zyxel Device to its factory default settings.
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.
INT/EXT	Select between the internal or external cellular antennas.

Table 9 Nebula NR7101 Panel Ports and Buttons

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

Table 10 Nebula LTE7461-M602 Panel Ports and Buttons

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.
SIM card	Insert a micro-SIM card into the slot with the chip facing down and the beveled corner in the top left corner.

2.3.1 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.

2.3.1.1 Nebula LTE3301-PLUS

Follow the steps below to activate WiFi or WPS for Nebula LTE3301-PLUS.

Activating WiFi

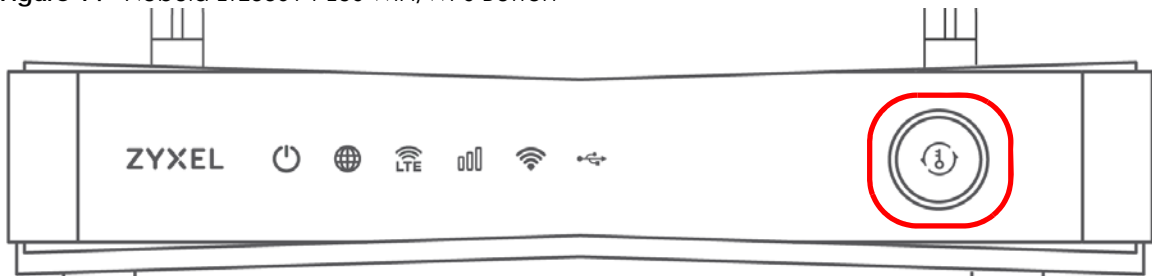
- 1 Make sure the power is on.
- 2 Press the WPS button for more than 5 seconds then release it.
- 3 The WLAN LED turns green/white.

Activating WPS

You can quickly set up a secure wireless 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 for more than 1 second but less than 5 seconds and release it. Please note that pressing more than 5 seconds will turn off WiFi.
- 3 Press the WPS button on another WPS-enabled device that is within range of the Zyxel Device.
- 4 After a WiFi connection is established, the **WLAN** LED turns green/white.

Figure 14 Nebula LTE3301-PLUS WiFi/WPS Button



2.3.1.2 Nebula NR5101

Follow the steps below to activate WiFi or WPS for Nebula NR5101.

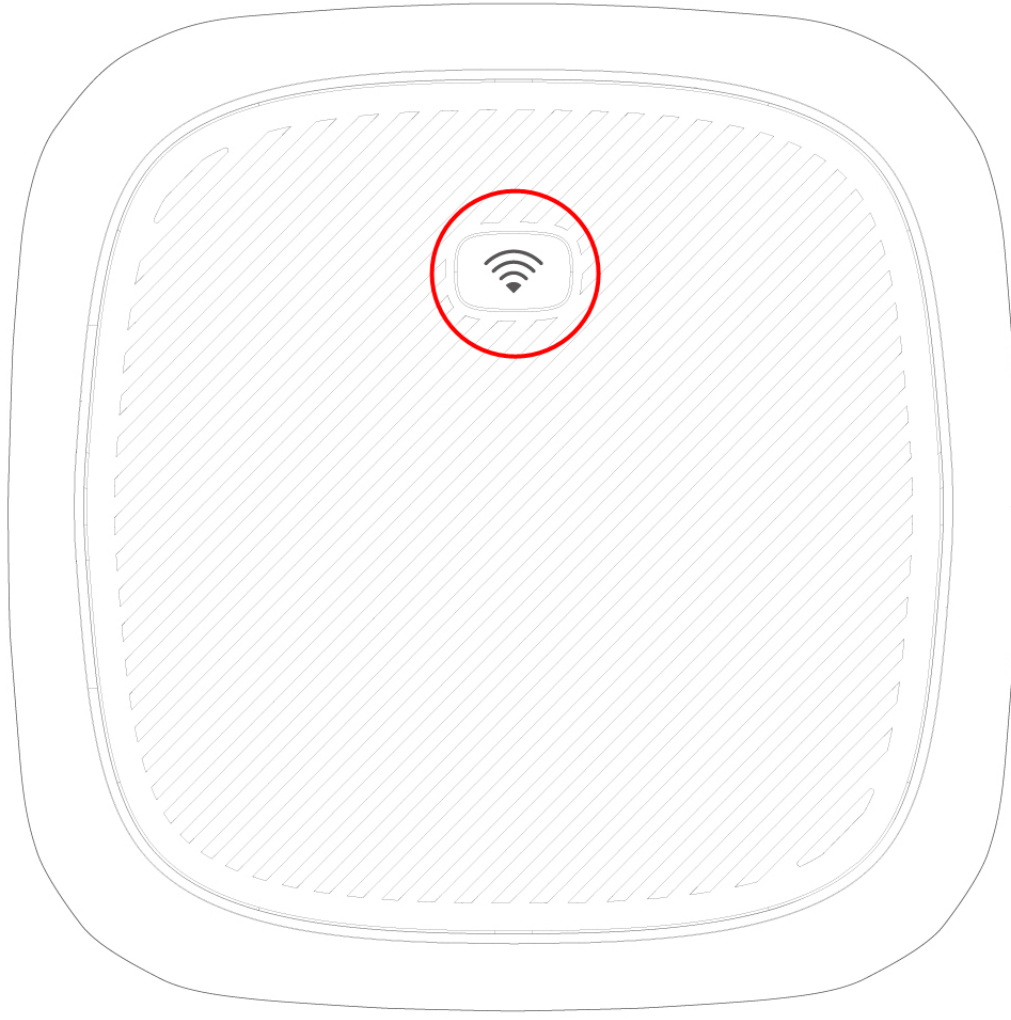
Activating WPS

You can quickly set up a secure wireless 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 for more than 5 seconds and release it.
- 3 Press the WPS button on another WPS-enabled device that is within range of the Zyxel Device.
- 4 After a WiFi connection is established, the **WiFi/WPS** LED blinks green.

Figure 15 Nebula NR5101 WiFi/WPS Button



2.3.1.3 Nebula NR7101

Follow the steps below to activate WiFi or WPS for Nebula NR7101.

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

Activating WiFi

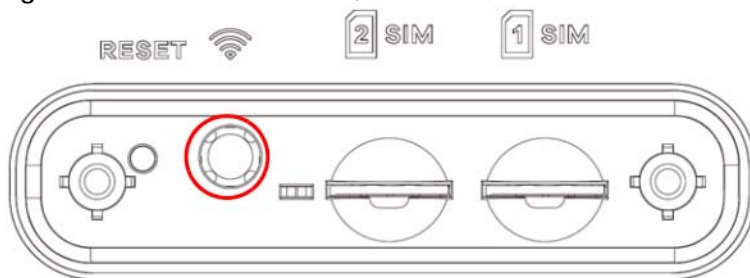
- 1 Make sure the LED is on and not blinking.
- 2 Press the **WiFi/WPS** button for more than 5 seconds and release it. Once WiFi is on, the LED blinks amber.

Activating WPS

You can quickly set up a secure wireless 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 for more than 1 second but less than 5 seconds and release it. Please note that pressing more than 5 seconds will turn off WiFi.
- 3 Press the WPS button on another WPS-enabled device that is within range of the Zyxel Device.
- 4 After a WiFi connection is established, the LED blinks amber.

Figure 16 Nebula NR7101 WiFi/WPS Button



2.3.1.4 Nebula LTE7461-M602

Follow the steps below to activate WiFi or WPS for the Nebula LTE7461-M602.

Use the WiFi button on the Zyxel Device to turn on or turn off WiFi.

Note: WiFi is for the local management use only.

Figure 17 Nebula LTE7461-M602



Activating WiFi

- 1 Make sure the power is on.
- 2 Press the WiFi button for more than 5 seconds and release it. Once WiFi is on, the LED blinks amber.

Activating WPS

You can quickly set up a secure wireless 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 button for more than 1 second but less than 5 seconds and release it. Please note that pressing more than 5 seconds will turn off WiFi.
- 3 Press the WPS button on another WPS-enabled device that is within range of the Zyxel Device.
- 4 After a WiFi connection is established, the LED blinks amber.

2.3.2 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 18 Nebula LTE3301-PLUS)

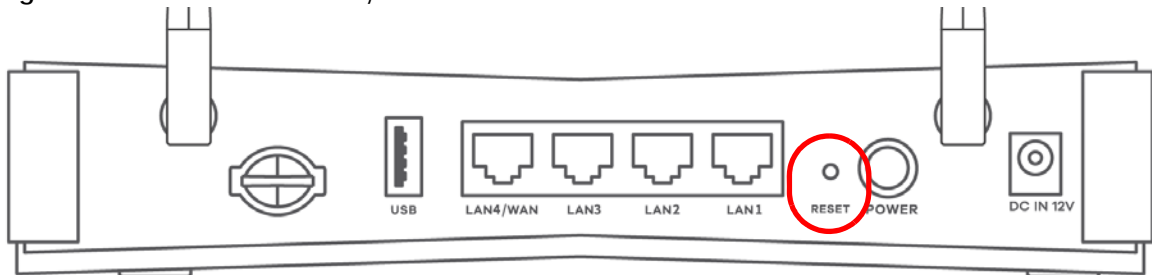


Figure 19 Nebula NR5101

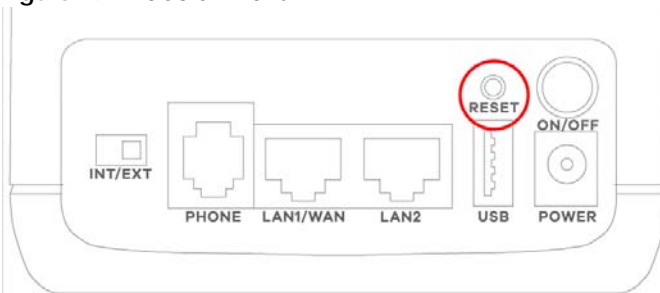


Figure 20 Nebula NR7101

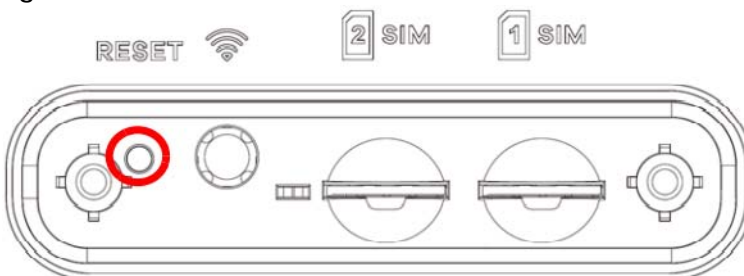


Figure 21 Nebula LTE7461-M602



- 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, Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

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

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

3.1.1 Access the Web Configurator

- 1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254.
- 3 Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to <http://192.168.1.1>.
- 4 A login screen displays. Select the language you prefer (upper right).
- 5 To access the administrative Web Configurator and manage the Zyxel Device, type the default user name **admin** and the randomly assigned default password (see the Zyxel Device label) in the **Login** screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 22 Password Screen

ZYXEL | NR5101 ENG ▼

Login

User Name

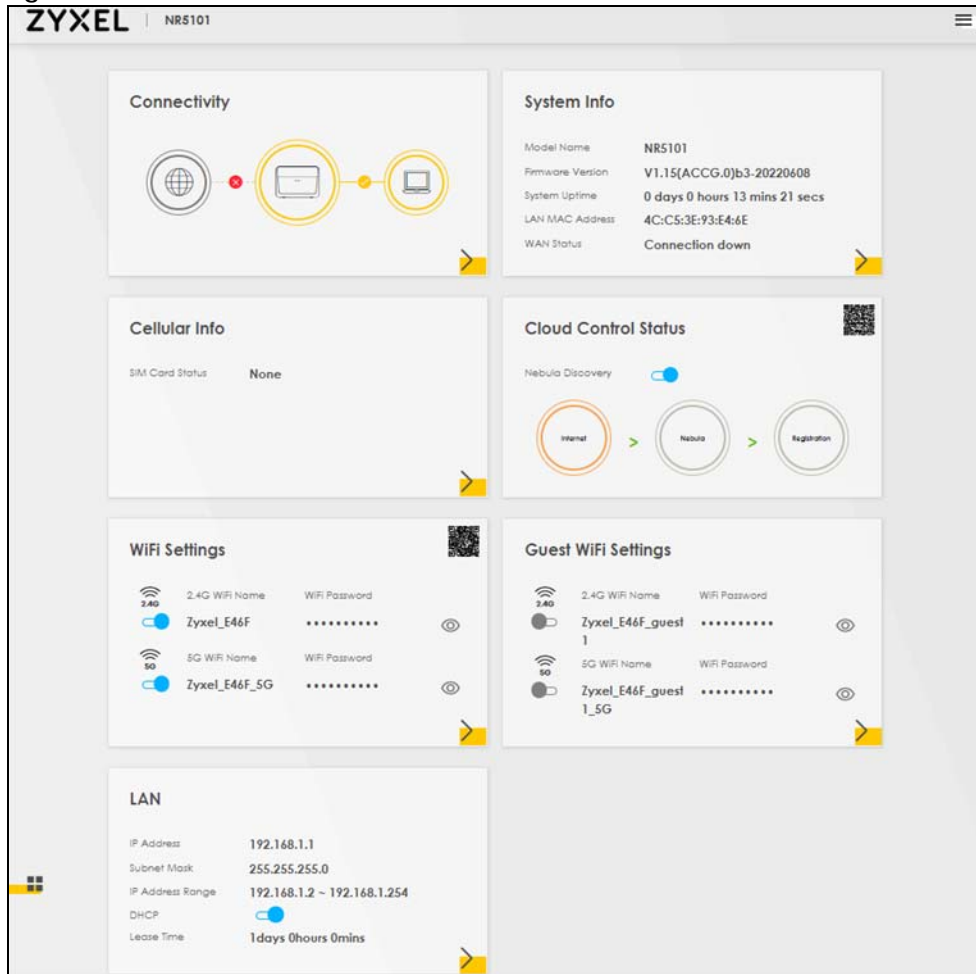
Password
 👁

Login

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

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

Figure 23 Connection Status

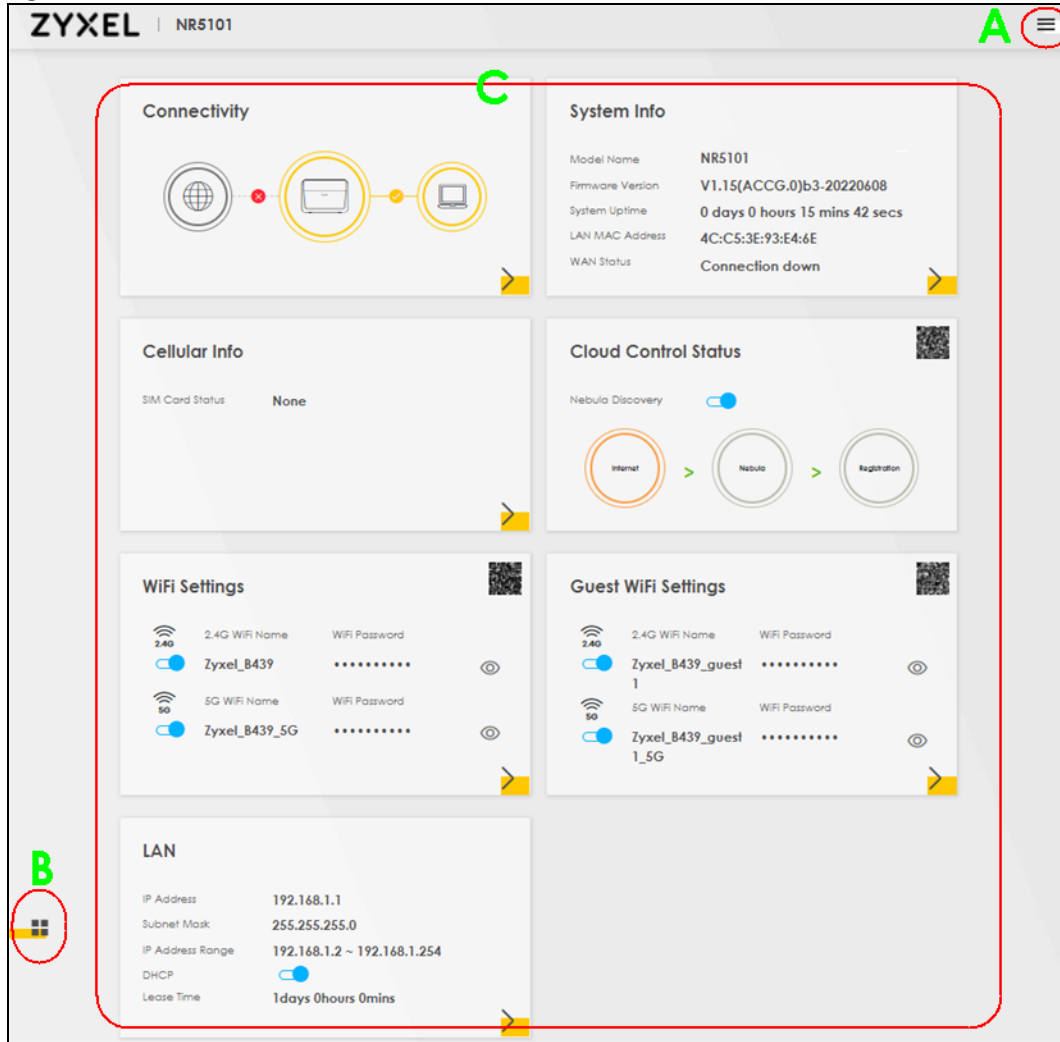


3.2 Web Configurator Layout

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

Figure 24 Screen Layout

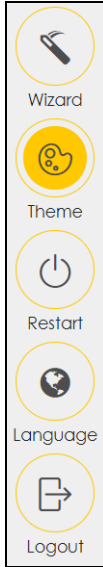


3.2.1 Settings Icon

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

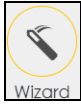
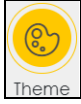

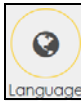

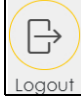
3.2.1.1 Side Bar

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

Figure 25 Side Bar

The icons provide the following functions.

Table 11 Web Configurator Icons in the Title Bar

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

3.2.1.2 Navigation Panel

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

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

Figure 26 Navigation Panel

Home
Network Setting
Broadband
Wireless
Home Networking
Routing
NAT
DNS
USB Service
Nebula
Security
System Monitor
Maintenance

Table 12 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.
	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 a cellular WAN connection that includes the Access Point Name (APN) provided by your service provider.
	Cellular SIM	Use this screen to enter a PIN for your SIM card to prevent others from using it.
	Cellular Band	Use this screen to configure the cellular frequency bands that can be used for Internet access as provided by your service provider.
	Cellular PLMN	Use this screen to view available PLMNs and select your preferred network.
	Cellular IP Passthrough	Use this screen to enable IP Passthrough mode.
	Cellular Lock	Use this screen to enable or disable PCI Lock.
	Cellular SMS	Use this screen to enable SMS Inbox and receive SMS messages.

Table 12 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication or security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the Zyxel Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
	WLAN Scheduler	Use this screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS 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	USB Service	Use this screen to enable file sharing through the Zyxel Device.
Nebula	Nebula	Use this screen to enable Nebula Discovery and configure proxy server settings.
VLAN Group	VLAN Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to map a port to create multiple networks on the Zyxel Device.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.

Table 12 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
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.
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: <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: <ul style="list-style-type: none"> • 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 wireless LAN.
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.
	MGMT Services for IP Passthrough	Use this screen to enable various approaches to access this Zyxel Device remotely from a WAN and/or LAN connection.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the Maintenance > Remote Management > MGMT Services screen.
	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.

Table 12 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
TR-069 Client	TR-069 Client	Use this screen to configure your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.
Time	Time	Use this screen to change your Zyxel Device's time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Settings	Log Settings	Use this screen to change your Zyxel Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
	Module Upgrade	Use this screen to upload new module firmware to your Zyxel Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.
	Schedule Reboot	Use this screen to set the time to reboot the Zyxel Device without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems.

3.2.1.3 Dashboard

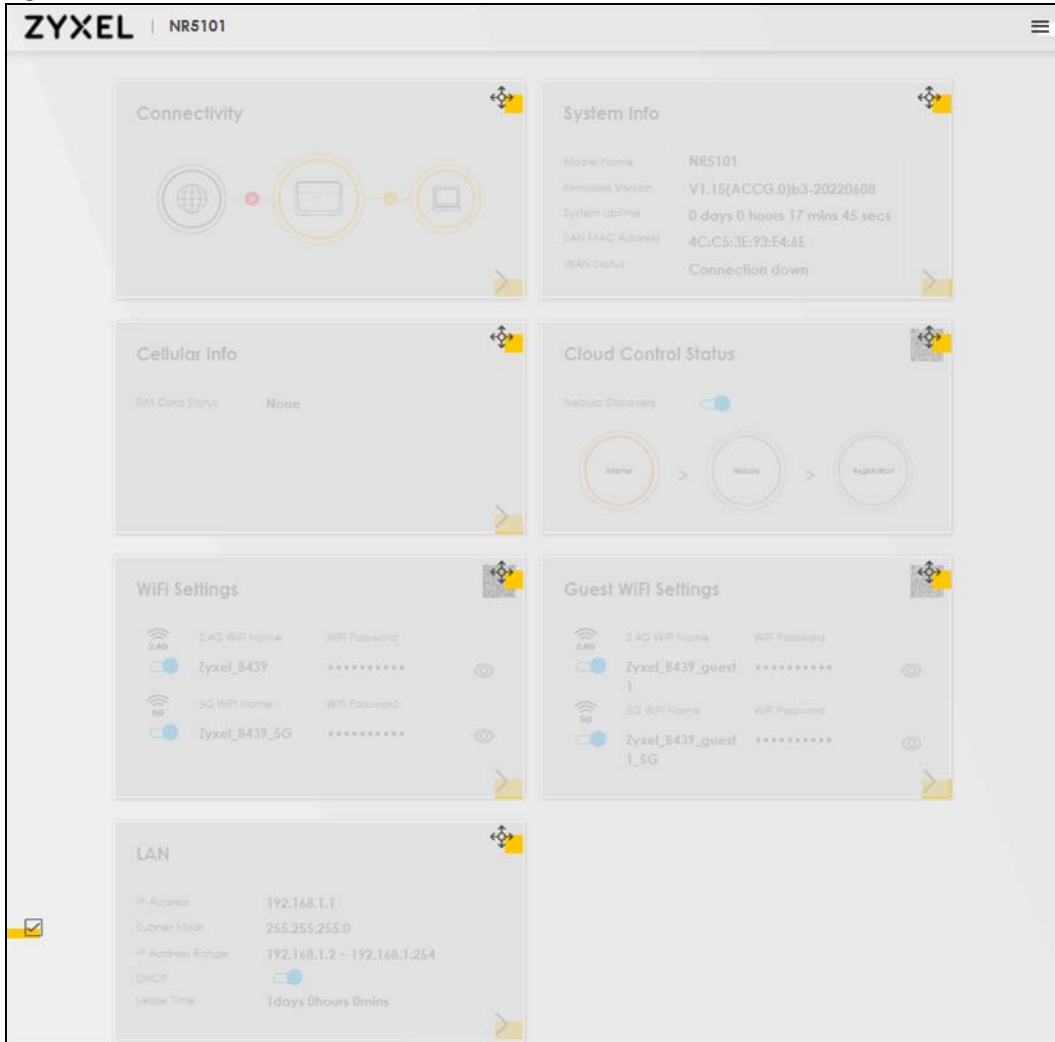
Use the menu items in the navigation panel on the right to open screens to configure the Zyxel Device's features.

3.2.2 Widget and Check Icons

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 27 Widget and Check Icons



CHAPTER 4

Quick Start

4.1 Overview

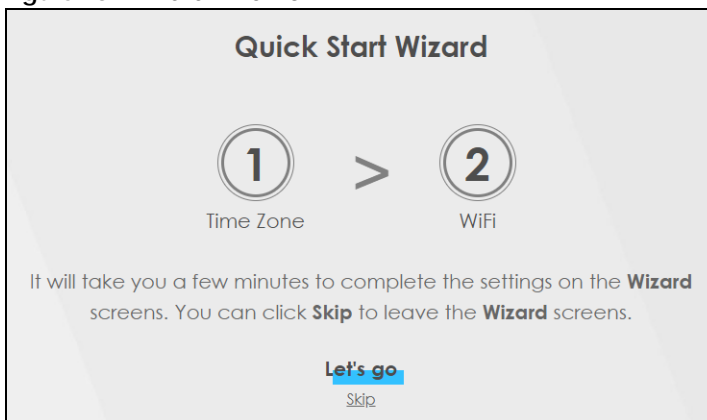
Use the **Wizard** screens to configure the Zyxel Device's time zone and wireless settings.

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

4.2 Quick Start Setup

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

Figure 28 Wizard – Home



4.3 Quick Start Setup – Time Zone

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

Figure 29 Wizard – Time Zone

The screenshot shows a configuration wizard with two steps: '1 Time zone' and '2 WiFi'. The 'Time zone' step is active, and the 'Next' button is highlighted in blue. Below the step indicators, there is a 'Time Zone' label and a dropdown menu currently displaying '(GMT-05:00) Eastern Time'. At the bottom, there are 'Back' and 'Next' buttons.

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 wireless clients to connect to the Zyxel Device. If you want to show or hide your WiFi password, click the Eye icon (👁).

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

Figure 30 Wizard – Wireless

The screenshot shows the 'WiFi' configuration screen, which is step 2 of 2 in the wizard. The 'WiFi' step is active, and the 'Done' button is highlighted in yellow. At the top, there are two sections: '2.4G WiFi' and '5G WiFi', each with a blue toggle switch turned on. Below each section are fields for 'WiFi Name' and 'WiFi Password'. The 2.4G WiFi name is 'ZyxeI_B439' and the 5G WiFi name is 'ZyxeI_B439_5G'. Both password fields are masked with asterisks and have an eye icon to toggle visibility. Below the password fields are signal strength indicators labeled 'Strength' with a yellow bar and the word 'medium'. At the bottom, there is a 'Country' dropdown menu set to 'Default' and a 'Done' button.

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.

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

4.5 Quick Start Setup – Finish

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

CHAPTER 5

Tutorials

5.1 Overview

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

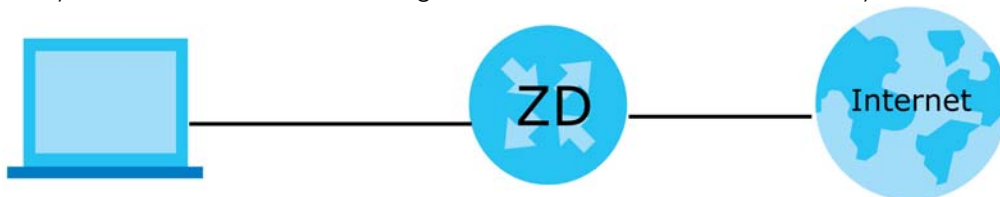
- [Wired Network Setup](#)
- [WiFi Network Setup](#)
- [Cellular Network Setup](#)
- [USB Applications](#)
- [Network Security](#)
- [Internet Calls](#)
- [Device Maintenance](#)

5.2 Wired Network Setup

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

5.2.1 Setting Up an Ethernet Connection

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



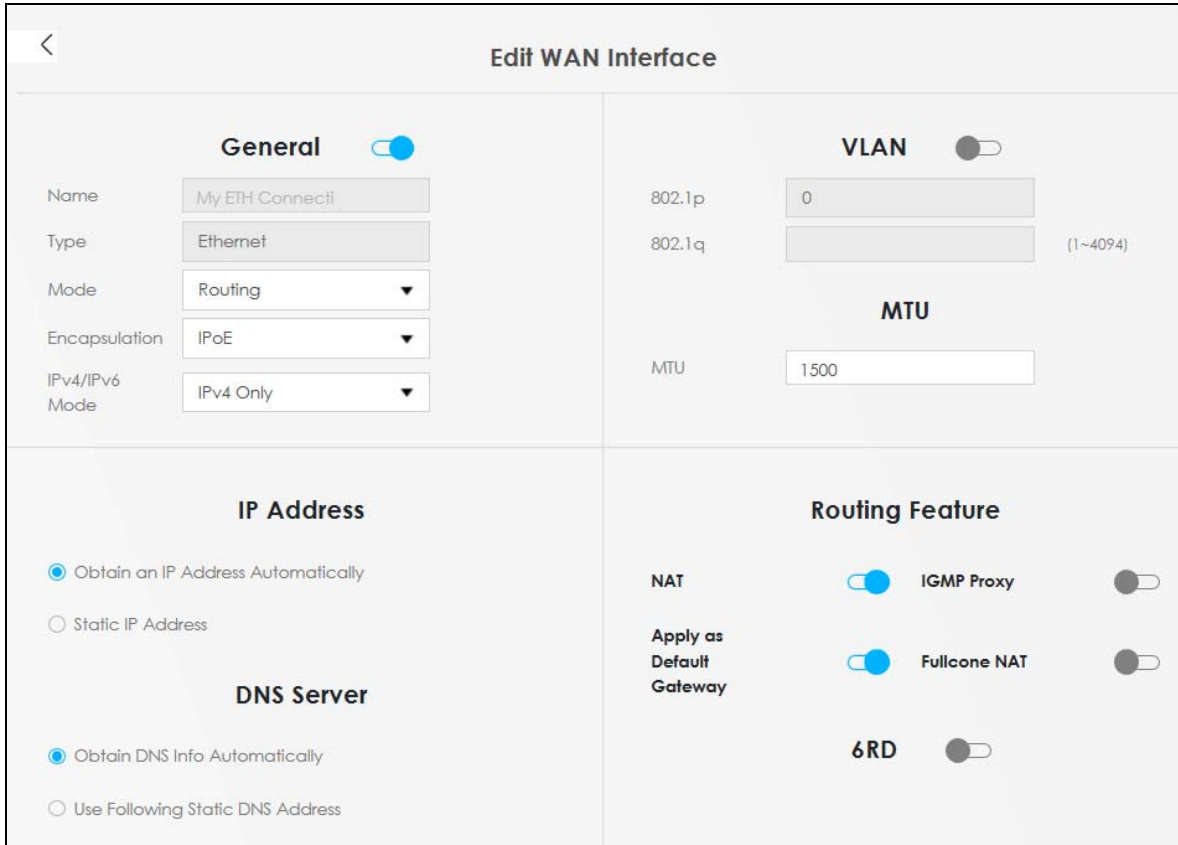
- 1 Make sure you have the Ethernet WAN port connect to a modem or router.
- 2 Go to **Network Setting > Broadband** and then the following screen appears. Click **Add New WAN Interface** to add a WAN connection.

#	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 In this example, configure the following information for the Ethernet connection.

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

- 4 Enter the **General** settings provided by your Internet service provider.
- 4a Enter a **Name** to identify your WAN connection.
- 4b Set the **Type** to **Ethernet**.
- 4c Set your Ethernet connection **Mode** to **Routing**.
- 4d Choose the **Encapsulation** specified by your Internet service provider. For this example, select **IPoE** or **PPPoE** as the WAN encapsulation type.
- 4e Set the **IPv4/IPv6 Mode** to **IPv4 Only**.
- 5 Under **Routing Feature**, enable **NAT** and **Apply as Default Gateway**.
- 6 For the rest of the fields, use the default settings.
- 7 Click **Apply** to save your settings.



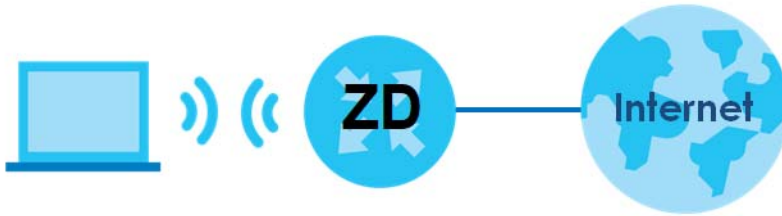
- 8 Go to the **Network Setting > Broadband** screen to view the established Ethernet connection. The new connection is displayed on the **Broadband** screen.

#	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	N	Y	Y	N	N	 

5.3 WiFi Network Setup

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

Figure 31 WiFi Network Setup



See the label on the Zykel Device for the WiFi network settings and then connect manually to the Zykel Device. Alternatively, you can set up a WiFi network using WPS. See [Section 5.3.2 on page 53](#).

5.3.1 Changing Security on a WiFi Network

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

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

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

Wireless

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

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

Wireless

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

Wireless Network Setup

Band: 2.4GHz

Wireless:

Channel: Auto Current : 7 / 40 MHz

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Example

Max Clients: 32

Hide SSID ⓘ

Multicast Forwarding

Max. Upstream Bandwidth:

Max. Downstream Bandwidth:

Note

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

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

Security Level

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: DoNotStealMyWirelessNetwork ⓘ

Encryption: AES

Timer: 3600 sec

- 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	<input type="text" value="2347"/>
Fragmentation Threshold	<input type="text" value="2346"/>
Output Power	<input type="text" value="100%"/>
Beacon Interval	<input type="text" value="100"/> ms
DTIM Interval	<input type="text" value="1"/> ms
802.11 Mode	<input type="text" value="802.11b/g/n Mixed"/>
802.11 Protection	<input type="text" value="Auto"/>
Preamble	<input type="text" value="Long"/>
Protected Management Frames	<input type="text" value="Capable"/>

You can now use the WPS feature to establish a WiFi connection between your notebook and the Zyxel Device (see [Section 5.3.2 on page 53](#)). Now use the new security settings to connect to the Internet through the Zyxel Device using WiFi.

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

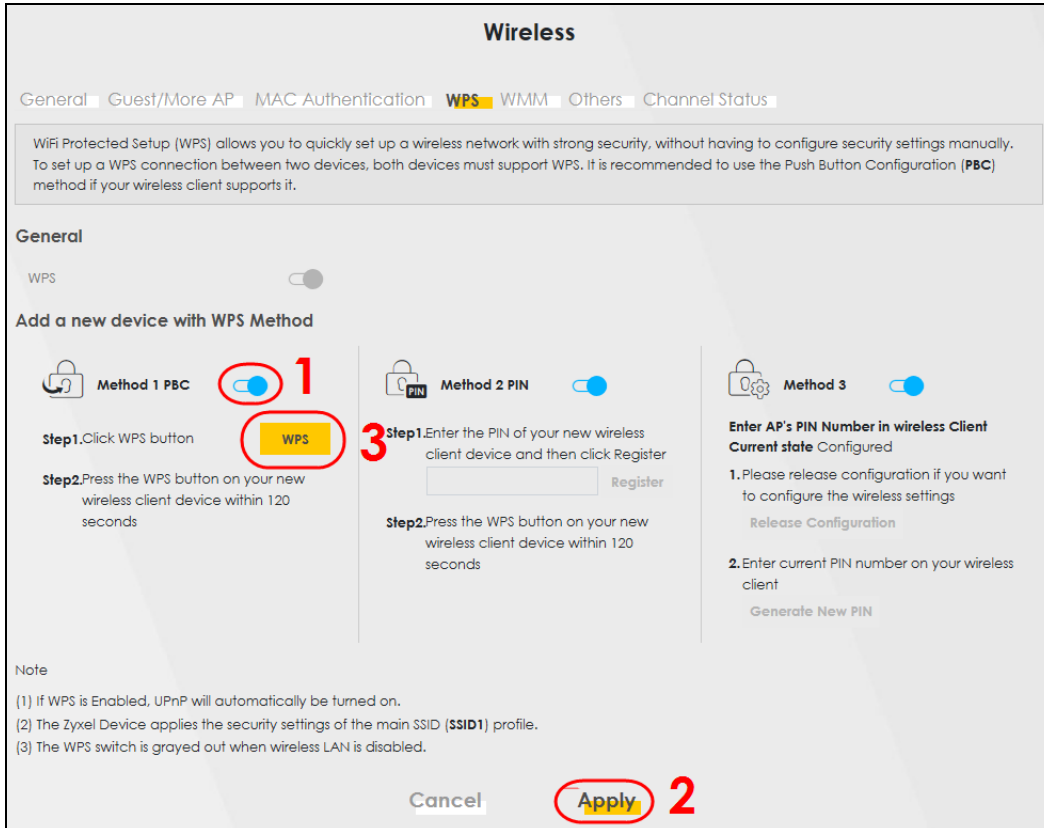
This section shows you how to connect a WiFi device to the Zyxel Device's WiFi network using WPS. WPS (Wi-Fi Protected Setup) is a security standard that allows devices to connect to a router securely without you having to enter a password. There are two methods:

- **Push Button Configuration (PBC)** – Connect to the WiFi network by pressing a button. See [Section 5.3.2.1 on page 53](#). This is the simplest method.
- **PIN Configuration** – Connect to the WiFi network by entering a PIN (Personal Identification Number) from a WiFi-enabled device in the Zyxel Device's Web Configurator. See [Section 5.3.3 on page 57](#). This is the more secure method, because one device can authenticate the other.

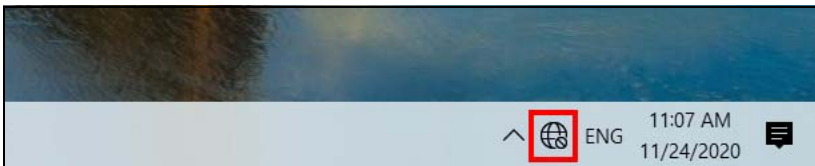
5.3.2.1 WPS Push Button Configuration (PBC)

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

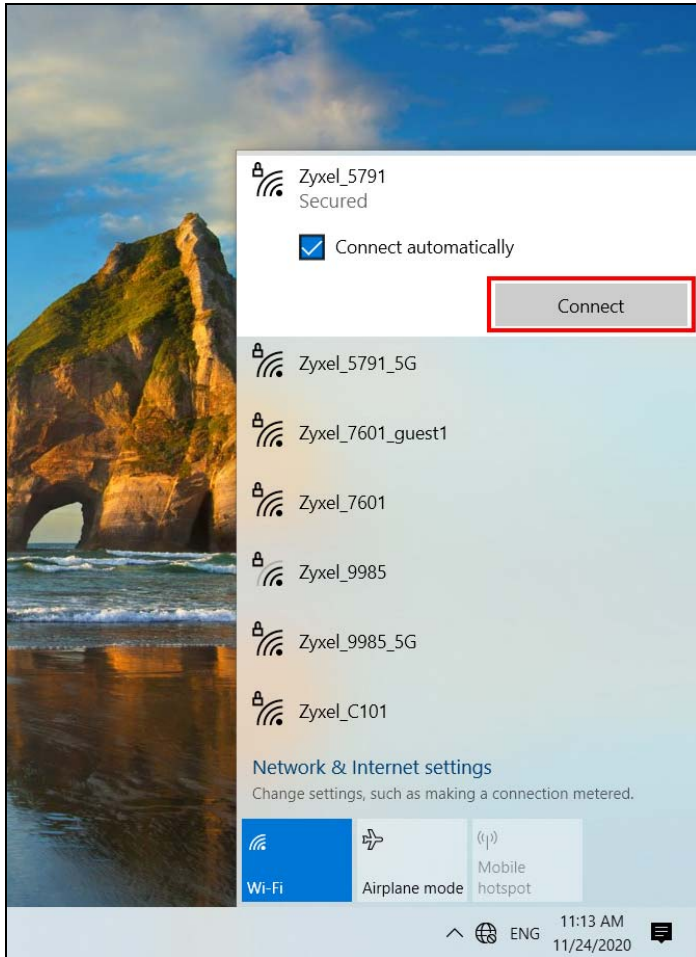
- 1 Make sure that your Zyxel Device is turned on, and your notebook is within range of the Zyxel Device's WiFi signal.
- 2 Push and hold the **WPS** button located on the Zyxel Device until the **WiFi** or **WPS** LED starts blinking slowly. Alternatively, log into the Zyxel Device's Web Configurator, and then go to the **Network Setting > Wireless > WPS** screen. Enable **WPS** and **Method 1 PBC**, click **Apply**, and then click the **WPS button**.



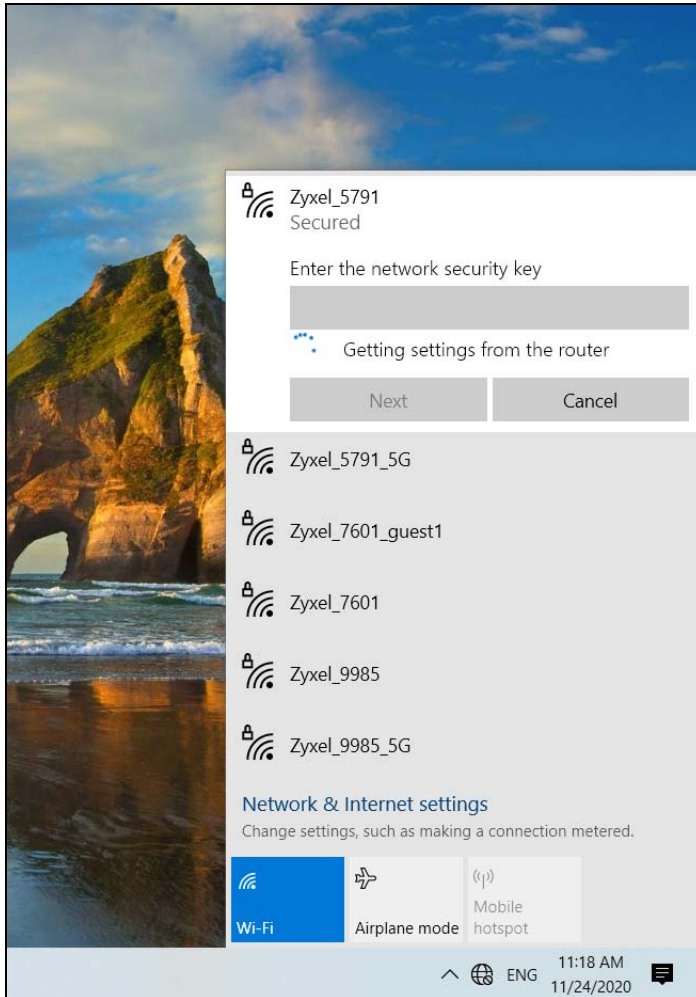
- 3** In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.



- 4** Locate the WiFi network of the Zyxel Device. The default WiFi network name is "Zyxel_XXXX" (2.4G) or "Zyxel_XXXX_5G" (5G). Then click **Connect**.



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



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

5.3.2.2 WPS PIN Configuration

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

- 1 Enable WiFi on the device you want to connect to the WiFi network. Then, note down the WPS PIN in the device's WiFi settings.
- 2 Log into Zyxel Device's Web Configurator, and then go to the **Network Setting > Wireless > WPS** screen. Enable **WPS**, and then click **Apply**.
- 3 Enable **Method 2 PIN**, and then click **Apply**. Enter the PIN of the WiFi device, and then click **Register**.

WiFi Protected Setup (WPS) allows you to quickly set up a 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

Step1. Click WPS button

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

Method 2 PIN **1**

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

Register **3**

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

Method 3

Enter AP's PIN Number in wireless Client

Current state Configured

Please release configuration if you want to configure the wireless settings

2 Enter current PIN number on your wireless client

Release Configuration

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 **SSID1** profile. If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA2-PSK** or **No Security**.
- (3) The WPS switch is grayed out when wireless LAN is disabled.

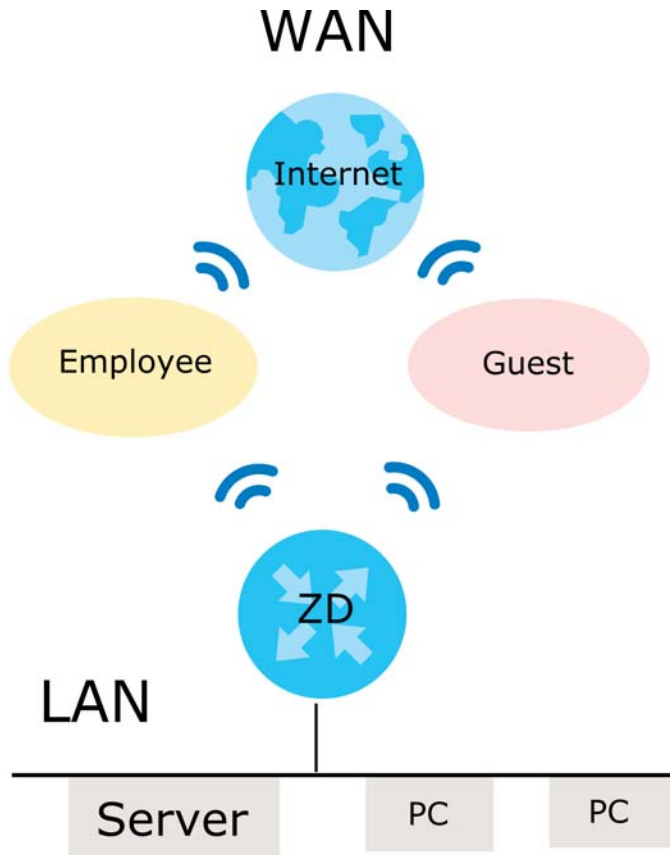
Cancel **Apply** **2**

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

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

5.3.3 Setting Up a Guest Network

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

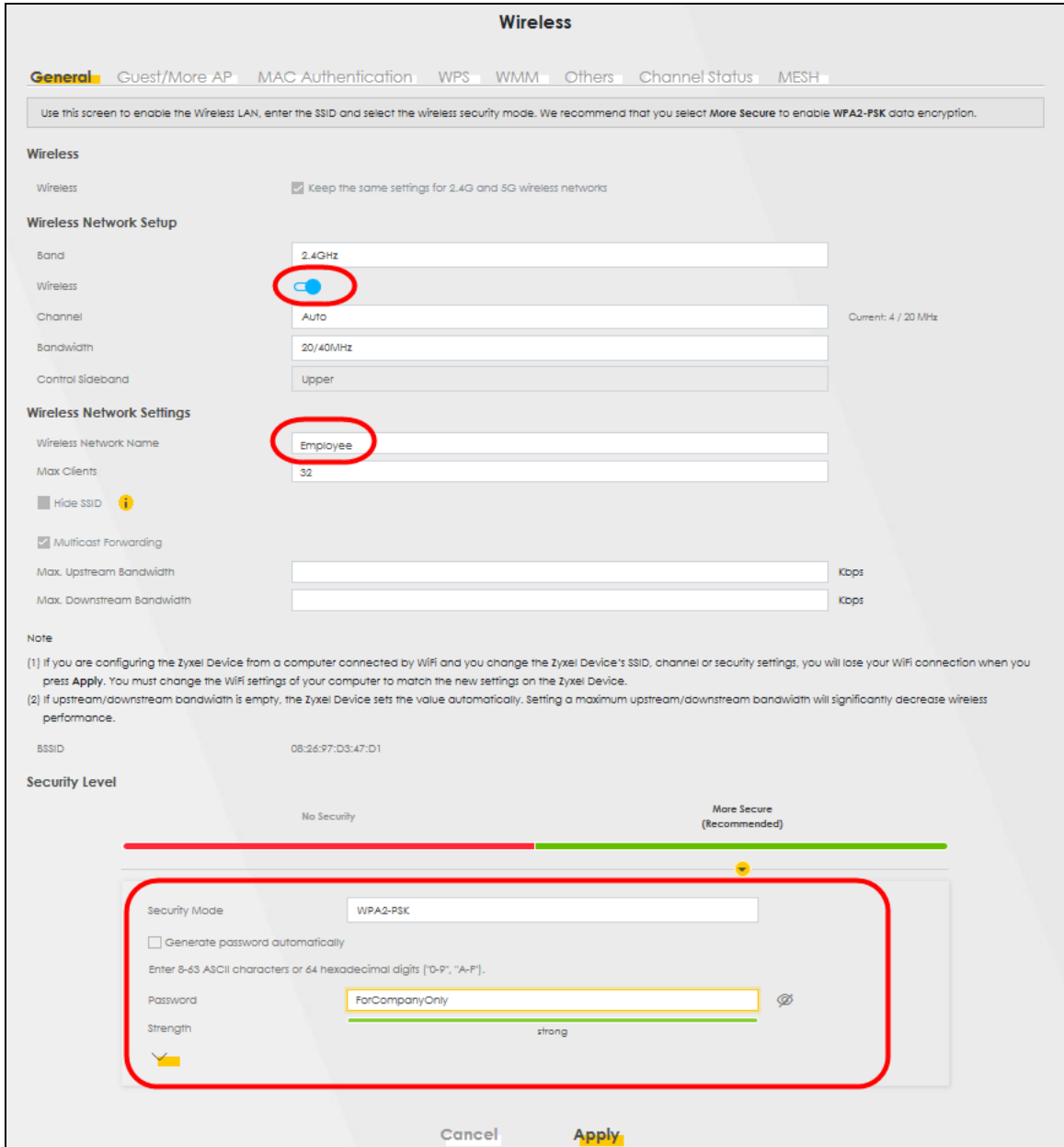


- Employees using the **General** WiFi network group will have access to the local network and the Internet.
- Visitors using the **Guest** WiFi network group with a different SSID and password will have access to the Internet only.

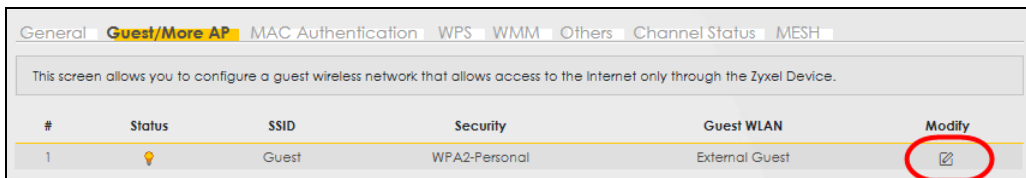
Use the following parameters to set up the WiFi network groups.

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

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



- 2 Go to the **Network Setting > Wireless > Guest/More AP** screen. Click the **Modify** icon to configure the second WiFi network group.



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

✕

More AP Edit

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless

Security Level

Wireless Network Name:

Hide SSID

Guest WLAN

Access Scenario:

Max. Upstream Bandwidth:

Max. Downstream Bandwidth:

Note

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

BSSID:

SSID Subnet:

Security Level

No Security
More Secure (Recommended)

Security Mode:

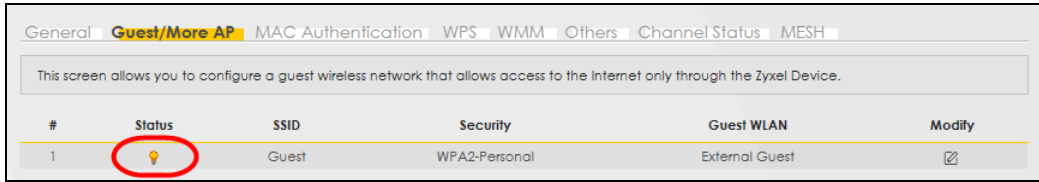
Generate password automatically
 Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password: 👁

💡

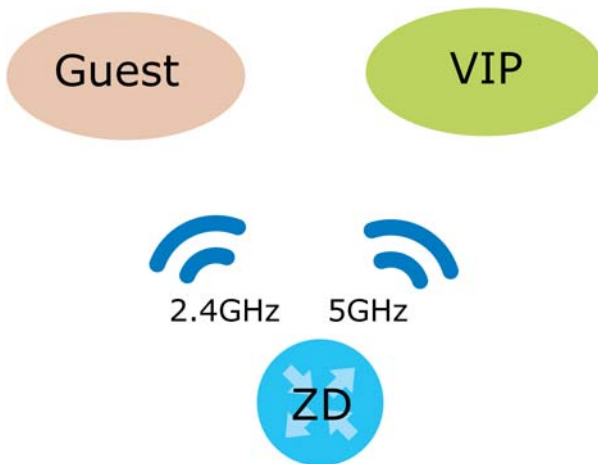
Cancel
OK

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



5.3.4 Setting Up Two Guest WiFi Networks on Different WiFi Bands

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



- The **Guest** group will use the 2.4G band.
- The **VIP** group will use the 5G band.

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

Table 13 WiFi Settings Parameters Example

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

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

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

Wireless

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

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA2-PSK** data encryption.

Wireless

Keep the same settings for 2.4G and 5G wireless networks

Wireless Network Setup

Band

Wireless

Channel Current: 3 / 20 MHz

Bandwidth

Control Sideband

Wireless Network Settings

Wireless Network Name

Max Clients

Hide SSID ⓘ

Multicast Forwarding

Max. Upstream Bandwidth Kbps

Max. Downstream Bandwidth Kbps

- 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

Hide SSID

Guest WLAN

Access Scenario

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 0A:26:97:D3:47:D1

SSID Subnet

Security Level

No Security More Secure (Recommended)

Security Mode

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

Password

Strength

Cancel

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

Wireless

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	

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

Wireless

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

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA2-PSK** data encryption.

Wireless

Keep the same settings for 2.4G and 5G wireless networks

Wireless Network Setup

Band: 5GHz

Wireless:

Channel: Auto Current: 60 / 160 MHz

Bandwidth: 20/40/80/160MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Zyxel_7601

Max Clients: 32

Hide SSID ⓘ

Multicast Forwarding

Max. Upstream Bandwidth: _____ Kbps

Max. Downstream Bandwidth: _____ Kbps

- 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**.

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

Hide SSID

Guest WLAN

Access Scenario

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 0A:26:97:D3:47:D2

SSID Subnet

Security Level

No Security More Secure (Recommended)

Security Mode

Generate password automatically

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

Password

Strength medium

Cancel OK

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

Wireless

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		VIP	WPA2-Personal	External Guest	

5.4 Cellular Network Setup

5.4.1 Setting up a Cellular Network Connection

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

- 1 Insert a SIM Card into your Zyxel Device SIM slot. Make sure this SIM has an active data plan with your Internet Service Provider (ISP).
- 2 Connect your Zyxel Device to your computer, and log into the Web Configurator.
- 3 If your SIM has a PIN Code, enter this code in the **Broadband > Cellular SIM** screen.

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

5.5 USB Applications

This section shows you how to set up a cellular backup network, access shared folders and play files through Window Media using a USB device.

5.5.1 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.

5.5.1.1 Setting 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

- 5 The **Add New Share** screen appears.
- 5a Select your USB device from the **Volume** drop-down list box.
- 5b Enter a **Description** name for the added share to identify the device.
- 5c Click **Browse** and the **Browse Directory** screen appears.

Add New Share

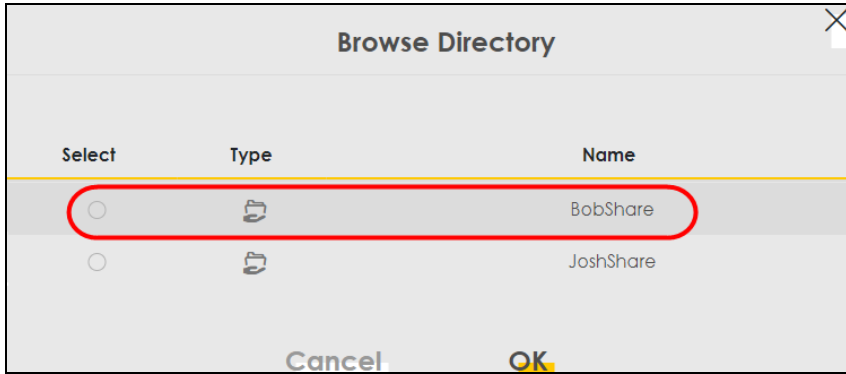
Volume: usb1_sda1

Share Path: BobShare

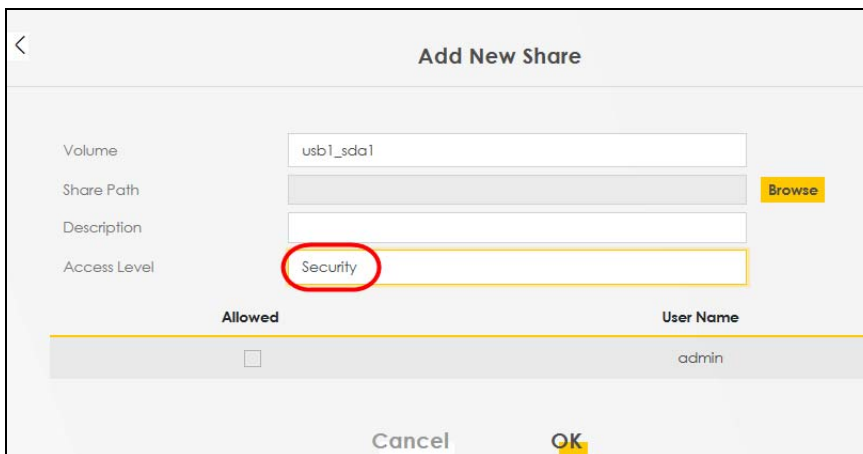
Description: Bob

Access Level: Public

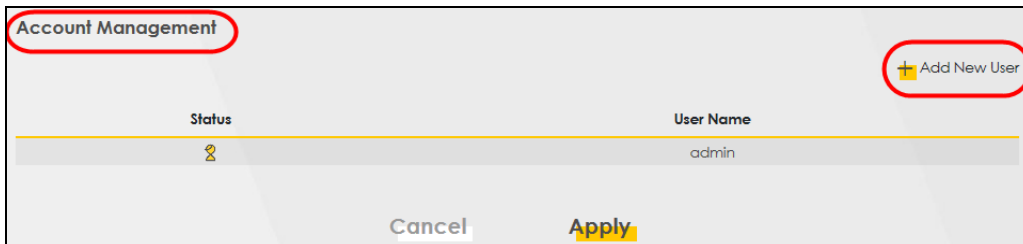
- 5d On the **Browse Directory** screen, select the folder that you want to add as a share. In this example, select **BobShare** and then click **OK**.



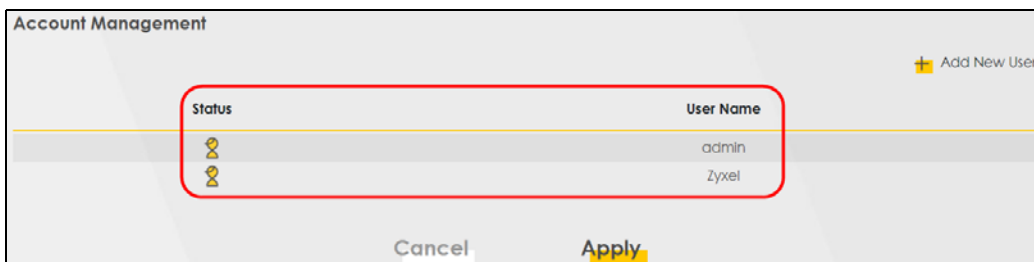
5e In **Access Level**, select **Public** to let the share to be accessed by all users connected to the Zyxel Device. Otherwise, select **Security** to let the share to be accessed by specific users to access only. Click **OK** to save the settings.



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.



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

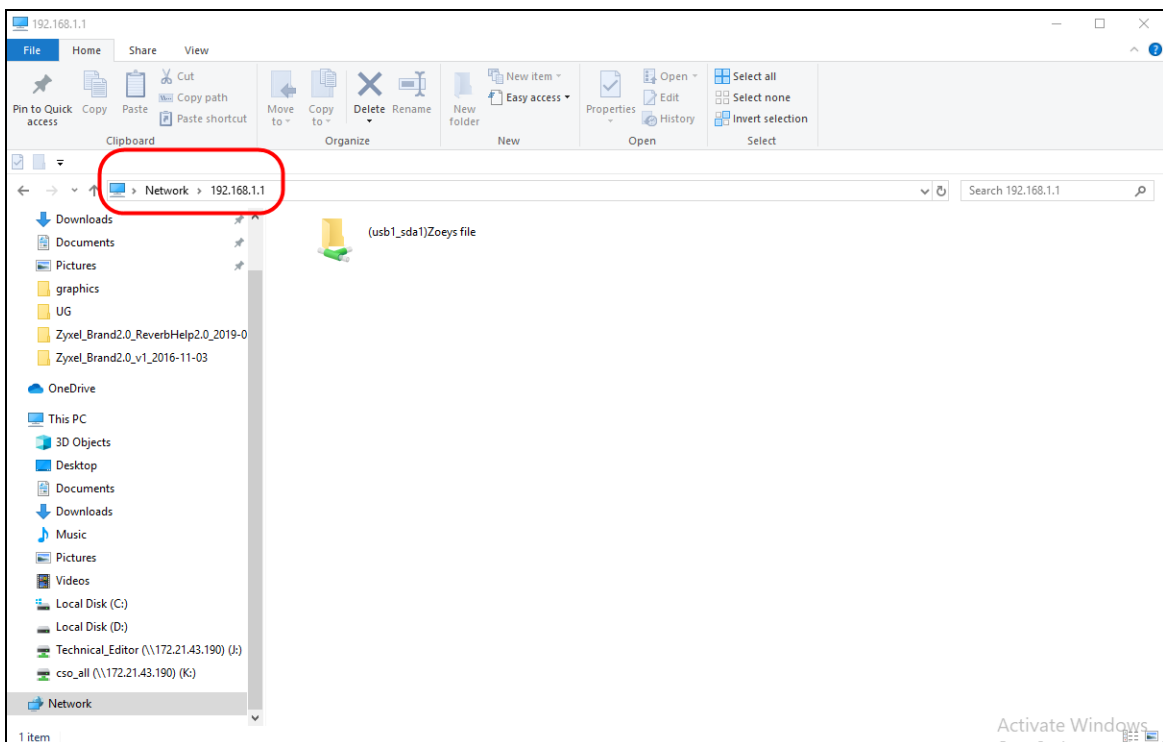
Share Directory List						
Active	Status	Share Name	Share Path	Share Description	Modify	
<input checked="" type="checkbox"/>		BobShare	/mnt/usb1_sda1/BobShare	Bob		
<input checked="" type="checkbox"/>		JoshShare	/mnt/usb1_sda1/JoshShare	Josh		

5.5.1.2 Accessing 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)Zoey's 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)Zoey's file**, and then enter the share's username and password if prompted.
- 4 After you access **(usb1_sda)Zoey's file** through your Zyxel Device, you do not have to log in again unless you restart your computer.

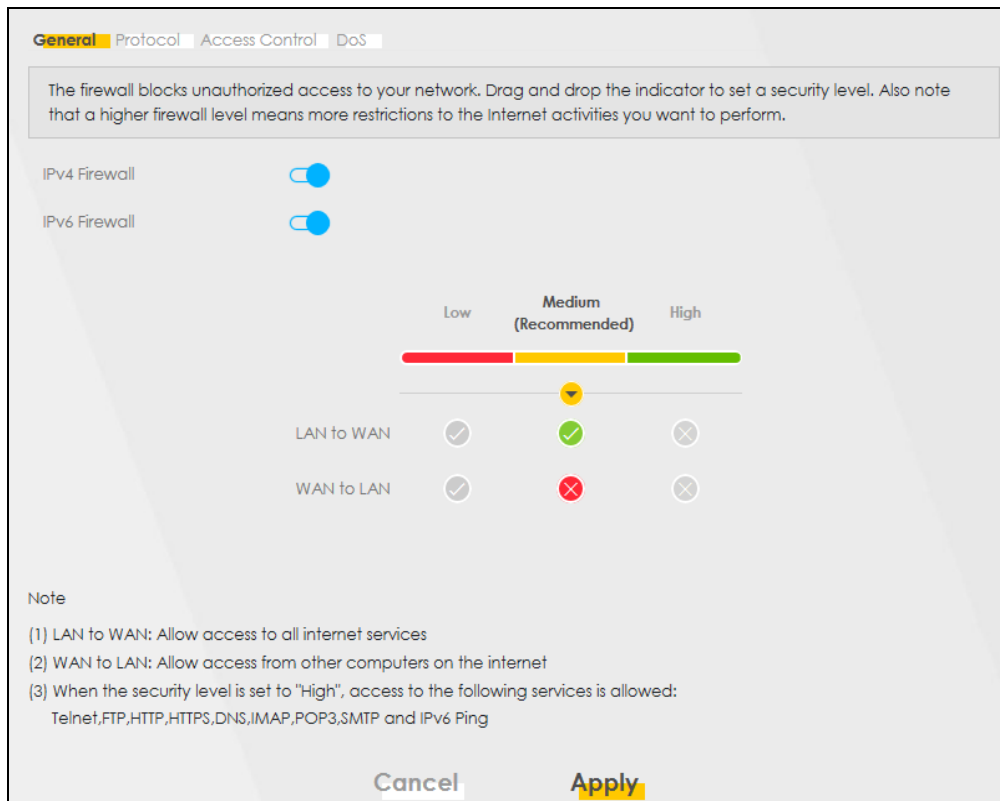
5.6 Network Security

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

5.6.1 Configuring a Firewall Rule

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

- 1 Go to the **Security > Firewall > General** screen.
- 2 Select **IPv4 Firewall/IPv6 Firewall** to enable the firewall, and then click **Apply**.



- 3 Open the **Access Control** screen to create a rule.

The screenshot shows the 'Add New ACL Rule' configuration interface. The fields are as follows:

- Filter Name: [Empty text box]
- Order: 1
- Select Source IP Address: Specific IP Address
- Source IP Address: [Empty text box] [prefix length]
- Select Destination Device: Specific IP Address
- Destination IP Address: [Empty text box] [prefix length]
- IP Type: IPv4
- Select Service: Specific Service
- Protocol: ALL
- Custom Source Port: Range [1] - [1]
- Custom Destination Port: Range [1] - [1]
- Policy: ACCEPT
- Direction: WAN to LAN
- Enable Rate Limit: [Off]
- Rate Limit: [Empty] packet(s) per [Minute] (1-512)
- Scheduler Rules: [Dropdown menu]

Buttons: Cancel, OK, Add New Rule

- 4 Click **Add New Rule** and use the following fields to configure and apply a new ACL (Access Control List) rule.
 - 4a **Filter Name:** Enter a name to identify the firewall rule.
 - 4b **Source IP Address:** Enter the IP address of the computer that initializes traffic for the application or service.
 - 4c **Destination IP Address:** Enter the IP address of the computer to which traffic for the application or service is entering.
 - 4d **Protocol:** Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP** or **ICMPv6**) used to transport the packets.
 - 4e **Policy:** Select whether to (**ACCEPT**, **DROP**, or **REJECT**) the packets.
 - 4f **Direction:** Select the direction (**WAN to LAN**, **LAN to WAN**, **WAN to ROUTER**, or **LAN to ROUTER**) of the traffic to which this rule applies.
- 5 Select **Enable Rate Limit** to activate the rules you created. Click **OK**.

5.6.2 Parental Control

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

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

5.6.2.1 Configuring Parental Control Schedule and Filter

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

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

Use this feature to:

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

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

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

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

Parental Control Screen

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

Parental Control

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

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities. These rules are defined in a Parental Control Profile (PCP).

General

Parental Control Enable Disable (Settings are invalid when disable)

Parental Control Profile(PCP) + Add New PCP

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

Add New PCP Screen

1 Under **General**:

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

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

1c Select an user this rule applies to in **Home Network User**, then click **Add**. You will see the MAC address of the user you just select in **Rule List**.

General

Active Enable Disable (Settings are invalid when disable)

Parental Control Profile Name

Home Network User Add

Rule List

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

2 Under **Internet Access Schedule**:

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

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

Internet Access Schedule

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

+ Add New Time

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

3 Under **Network Service**:

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

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

Network Service

Network Service Setting: Block

+ Add New Service

#	Service Name	Protocol:Port	Modify
1	http	TCP:80	[Edit] [Delete]

4 Under **Site / URL Keyword**:

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

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

4c 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.

Site/URL Keyword

Block or Allow the Web Site: Block the web URLs

+ Add

#	Website	Modify
1	gambling	[Edit] [Delete]

Redirect blocked site to Zyxel Family Safety page Zyxel Family Safety page will replace any sites from the above list in the browser.

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

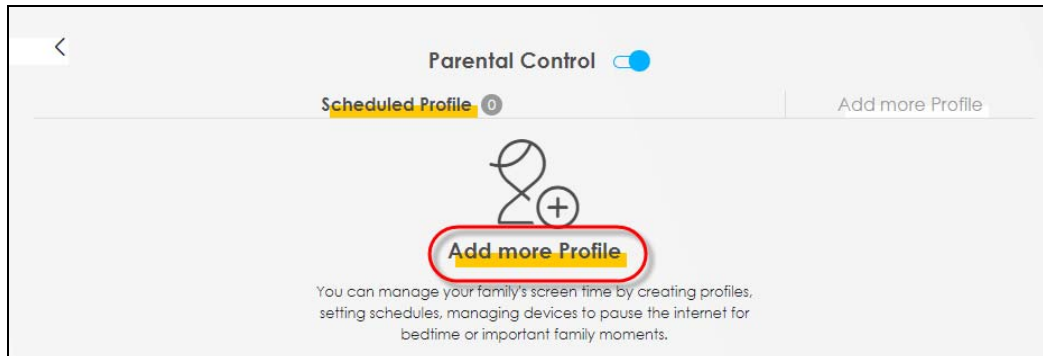
5.6.2.2 Configuring a Parental Control Schedule

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

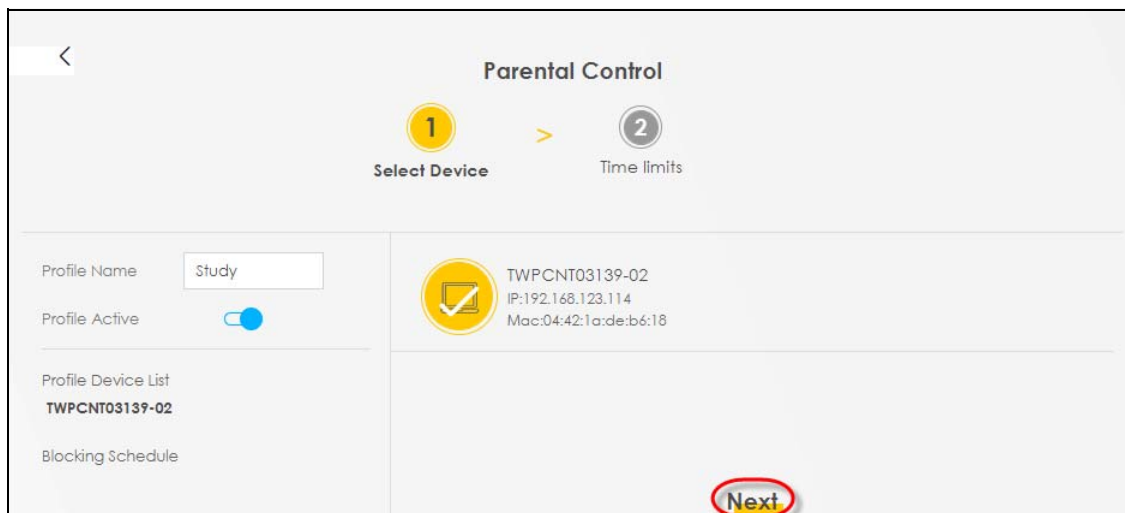
This example shows you how to block an user from accessing the Internet during time for studying. Use the parameter below to configure a schedule rule.

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

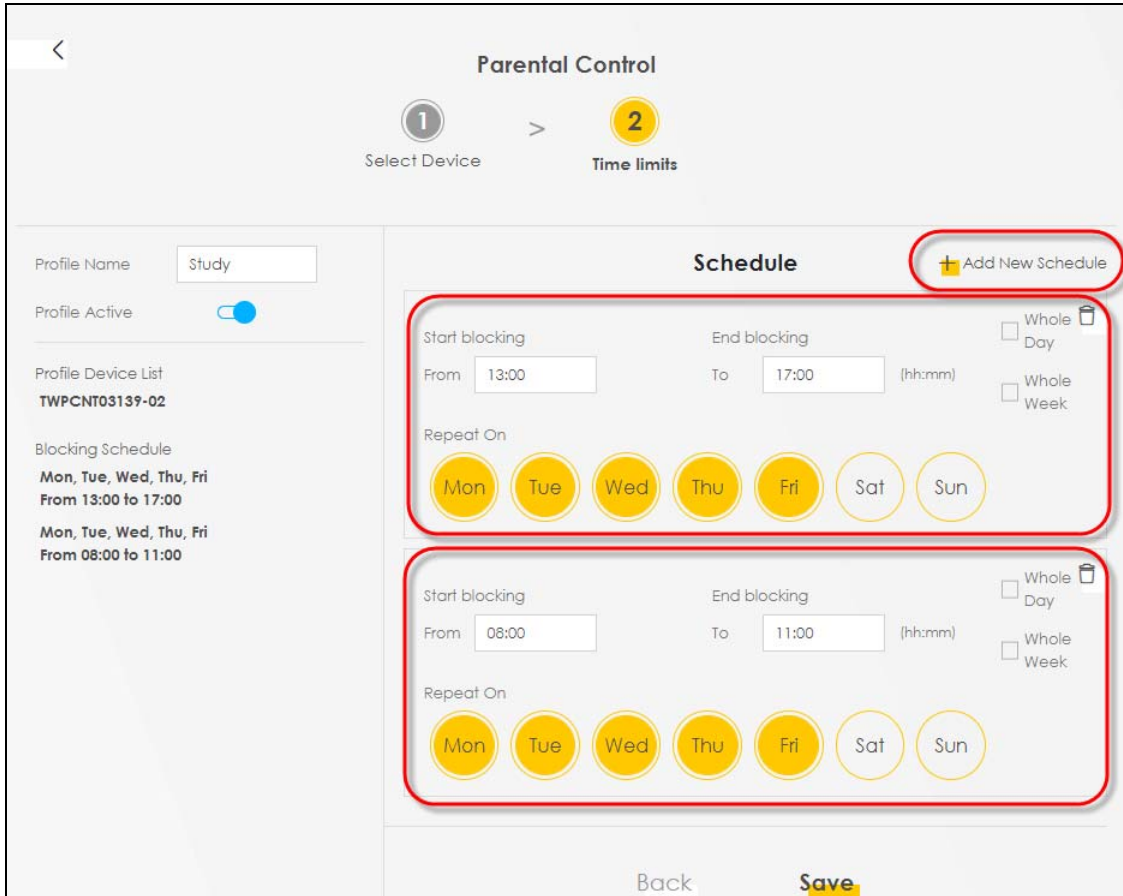
- 1 Click **Add more Profile** to open the **Parental Control** screen.



- 2 Use this screen to add a Parental Control rule.
 - 2a Enter the **Profile Name** given in the above parameter.
 - 2b Click on the switch to enable **Profile Active**.
 - 2c Select a device, and then click **Next** to proceed.



- 3 Use this screen to edit the Parental Control schedule.
 - 3a Click **Add New Schedule** to add a second schedule.
 - 3b Use the parameter given above to configure the time settings of your schedules.
 - 3c Click **Save** to save the settings.

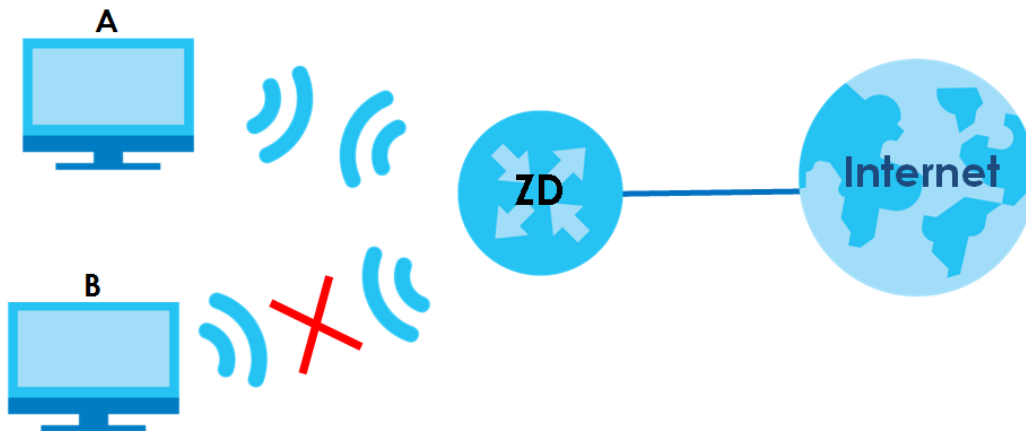


5.6.3 Configuring a MAC Address Filter

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

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

Figure 32 Configure a MAC Address Filter Example



- 1 Go to the **Security > MAC Filter > MAC Filter** screen. Under **MAC Address Filter**, select **Enable**.
- 2 Click **Add New Rule** to add a new entry. Select **Active**, and then enter the **Host Name** and **MAC Address** of computer B. Click **Apply**.

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	<input checked="" type="checkbox"/>	B	00 - 24 - 21 - AB - 1F - 00	

Cancel Apply

5.7 Internet Calls

This section shows you how to make Internet calls.

5.7.1 Configuring VoIP

To make voice calls over the Internet, you must set up a Session Initiation Protocol (SIP) provider and SIP account on the Zyxel Device. You should have an account with a SIP service provider already set up.

5.7.2 Adding a SIP Service Provider

Follow the steps below to add a SIP service provider.

- 1 Make sure your Zyxel Device is connected to the Internet.
- 2 Open the Web Configurator.
- 3 Go to the **VoiceVoIP > SIP > SIP Service Provider** screen. Click the **Add New Provider** button to add the SIP Service Provider.

SIP Account SIP Service Provider

Use this screen to view the SIP service provider information on the Zyxel Device. A SIP provider offers Internet call services using VoIP technology. You may need to consult your SIP service provider for the following settings.

+ Add New Provider

#	SIP Service Provider Name	SIP Proxy Server Address	REGISTER Server Address	SIP Service Domain	Modify
1	Verizon	sip.infostrada.it	sip.infostrada.it	sip.infostrada.it	

- 4 On the **Add New Provider** screen, select **Enable SIP Service Provider**.

- 5 Enter **SIP Service Provider Name** of up to 64 ASCII printable characters.
- 6 Enter **SIP Proxy Server Address**, **SIP REGISTRAR Server Address**, and **SIP Service Domain** provided by your SIP service provider. Click **OK** to save your settings.

Add New Provider

SIP Service Provider Selection

Service Provider Selection ADD_NEW

General

SIP Service Provider Enable SIP Service Provider

SIP Service Provider Name

SIP Local Port (1025~65535)

SIP Proxy Server Address

SIP Proxy Server Port (1025~65535)

SIP REGISTRAR Server Address

SIP REGISTRAR Server Port (1025~65535)

SIP Service Domain

Cancel **OK**

5.7.3 Adding a SIP Account

The SIP account must be associated with the SIP service provider configured above. You may configure several SIP accounts for the same service provider. Follow the steps below to set up your SIP account:

- 1 Make sure your Zyxel Device is connected to the Internet.
- 2 Open the Web Configurator.
- 3 Go to the **VoiceVoIP > SIP > SIP Account** screen.
- 4 Click the **Add New Account** button on the **SIP Account** screen to add a SIP account and map it to a phone port.

SIP Account SIP Service Provider

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider.

The Zyxel Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's VoIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account and map it to a phone port. The SIP account contains information that allows your Zyxel Device to connect to your VoIP service provider.

+ Add New Account

#	Enable	SIP Account	Service Provider	Account Number	Modify
1	Enabled	SIP1	Verizon	Account1	
2	Enabled	SIP2	Verizon	Account2	
3	Disabled	SIP3	Verizon	Account3	

- Under **General**, select **Enable SIP Account**, and then enter the **SIP Account Number**.
- Under **Authentication**, enter **Username** and **Password**. Leave the other settings as default. Click **OK** to save your settings.

SIP Account Entry Edit

SIP Account Selection

SIP Account Selection SIP1

SIP Service Provider Association

SIP Account Associated with Verizon

General

Enable SIP Account

SIP Account Number Account1

Authentication

Username User1

Password *****

URL Type

URL Type SIP

5.7.4 Configuring a Phone

You must now configure the phone port to use the SIP account you just configured.

- Go to the **VoiceVoIP > Phone > Phone Device** screen.

- Click the **Modify** icon of **PHONE1** to configure PHONE1 on your Zyxel Device. The following screen appears.

Phone Device Region

Use this screen to view detailed information on phones used for Internet phone calls (SIP). You can define which phone(s) will ring when a specific SIP address receives an incoming call, and which SIP address will be used when an outgoing call is made with a specific phone.

Analog Phone

#	Phone ID	Internal Number	Incoming SIP Number	Outgoing SIP Number	Modify
1	PHONE1	**11	Account1	Account1	
2	PHONE2	**12	Account2	Account2	

- Under **SIP1 SIP Account to Make Outgoing Call**, select **SIP1** to have the phone connected to the first phone port use the registered SIP1 account to make outgoing calls.
- Under **SIP Account(s) to Receive Incoming Call**, select **SIP1** to have the phone connected to the first phone port receive phone calls for the SIP1 account. Click **OK** to save your changes.

Phone Device Edit

SIP Account to Make Outgoing Call

SIP Account SIP1 SIP2

SIP Number ChangeMe ChangeMe

SIP Account(s) to Receive Incoming Call

SIP Account SIP1 SIP2

directoryNumber ChangeMe ChangeMe

Immediate Dial Enable

Immediate Dial Enable

Cancel **OK**

5.7.5 Making a VoIP Call

Follow these steps to make a phone calling using Voice over IP (VoIP).

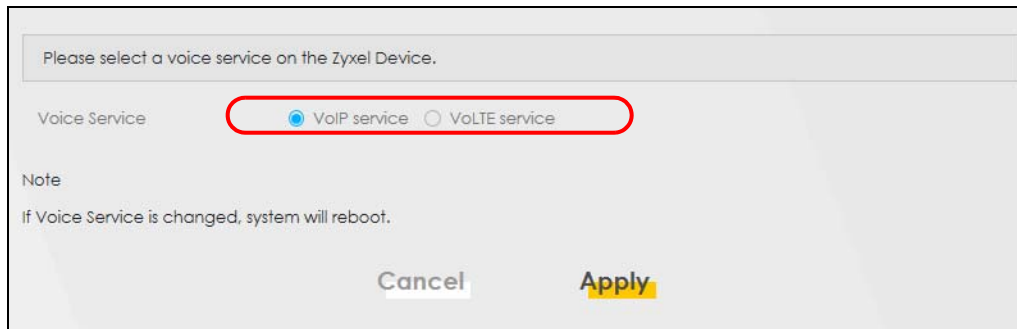
- Make sure you connect a telephone to phone port 1 on the Zyxel Device.
- Make sure the Zyxel Device is turned on and connected to the Internet.

- 3 Pick up the phone receiver.
- 4 Dial the VoIP phone number you want to call.

5.7.6 Making a VoLTE Phone Call

Follow these steps to make a phone calling using Voice over LTE (VoLTE).

- 1 Make sure that your SIM card supports VoLTE or Vo3G.
- 2 Log into the Web Configurator.
- 3 Go to the **Configuration > Voice > Voice Mode** screen.
- 4 On the **Voice Mode** screen, select **VoLTE service**, and then click **Apply**. The Zyxel Device restarts.



- 5 Connect an analog telephone to a **PHONE** port on the Zyxel Device.
- 6 Pick up the phone receiver.
- 7 Dial the phone number you want to call.

5.8 Device Maintenance

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

5.8.1 Upgrading the Firmware

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

- 1 Download the correct firmware file from the download library at the Zyxel website. The model code for the Zyxel Device in this example is ABLZABVY. Note the model code for your device. Unzip the file.
- 2 Go to the **Maintenance > Firmware Upgrade** screen.
- 3 Click **Browse/Choose File** and select the file with a ".bin" extension to upload. Click **Upload**.

Firmware Upgrade 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: **V5.13(ABLZ.1)b4**

File Path No file chosen

Upgrade WWAN Package

Current WWAN Package Version: **1.16**

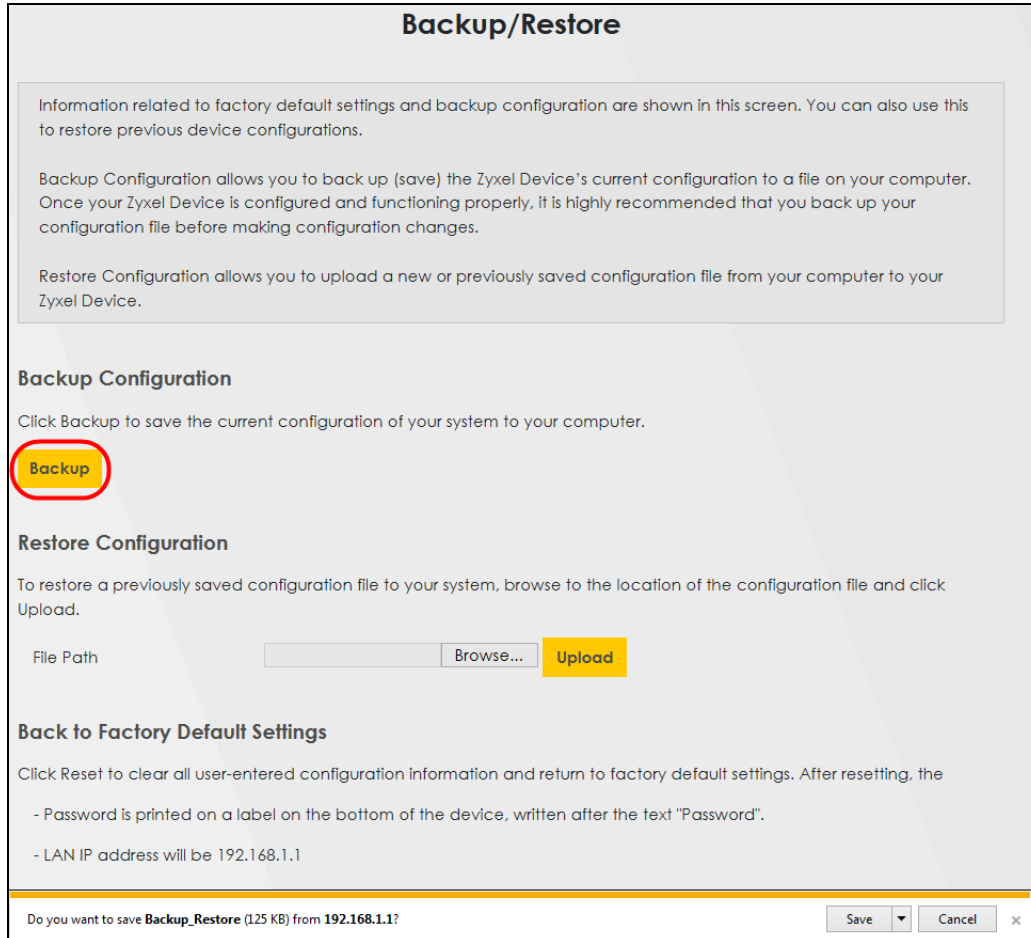
File Path No file chosen

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

5.8.2 Backing up the Device Configuration

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

- 1 Go to the **Maintenance > Backup/Restore** screen.
- 2 Under **Backup Configuration**, click **Backup**. A configuration file is saved to your computer. In this case, the **Backup/Restore** file is saved.



5.8.3 Restoring the Device Configuration

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

- 1 Go to the **Maintenance > Backup/Restore** screen.
- 2 Under **Restore Configuration**, click **Browse/Choose File**, and then select the configuration file that you want to upload. Click **Upload**.

Backup/Restore

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

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

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

Backup Configuration

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

Backup

Restore Configuration

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

File Path

Back to Factory Default Settings

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

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

Reset

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

PART II

Technical Reference

CHAPTER 6

Connection Status

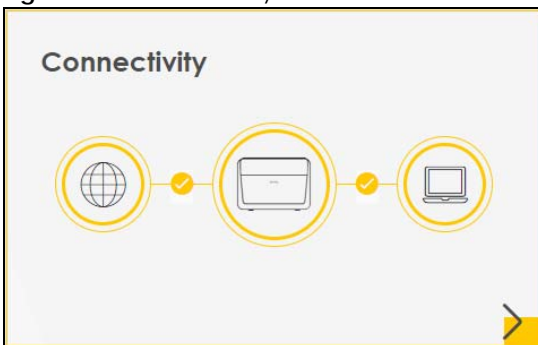
6.1 Connection Status Overview

After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access and wireless 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 33 Connectivity





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

Figure 34 Connectivity: Connected Devices

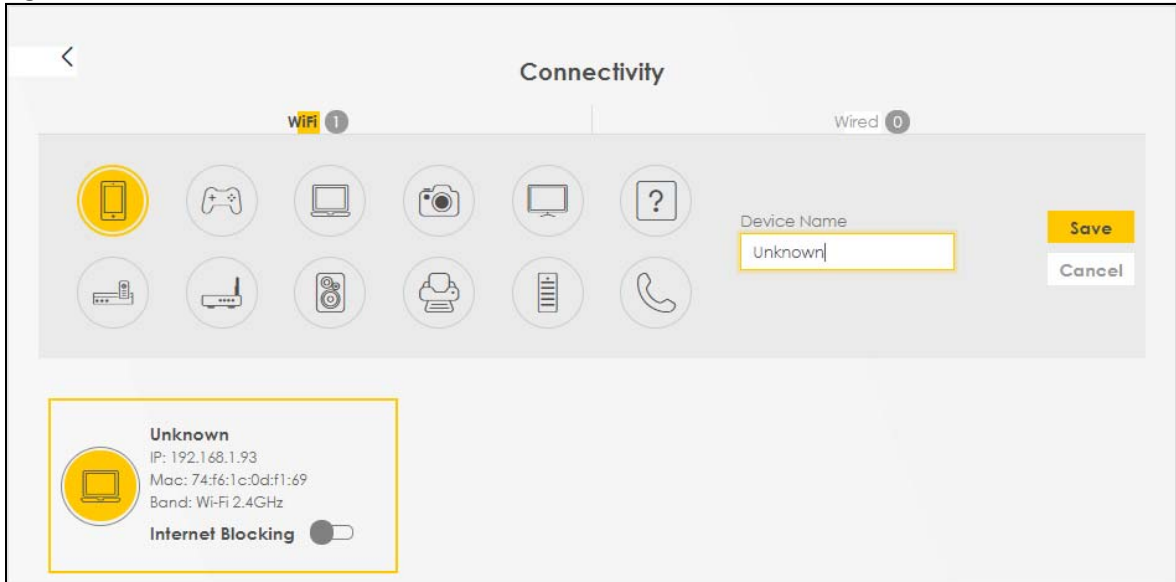


You can change the icon and name of a connected device. Place your mouse within the device block, and an Edit icon () will appear. Click the Edit icon, and you'll see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Click **Save** to save your changes.

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 **Save** to save your changes.

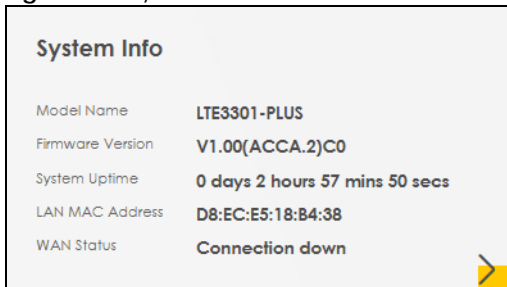
Figure 35 Connectivity: Edit



6.1.3 System Info

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

Figure 36 System Info



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

Figure 37 System Info: Detailed Information

System Info

Host Name: LTE3301-PLUS
 Model Name: LTE3301-PLUS
 Serial number: S210Z42000480
 Firmware Version: V1.00(ACCA.2)C0
 System Uptime: 0 days 3 hours 10 mins 56 secs

Interface Status

LAN1: 100M/Full | LAN2: - | LAN3: - | LAN4: - | Cellular: - | USB: No Device | WLAN 2.4G: 144 Mbps | WLAN 5G: 866 Mbps

WAN Information (No WAN)

LAN Information

IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0
 IPv6 Address: N/A
 IPv6 Link Local Address: fe80::daec:e5ff:fe18:b438
 DHCP: Server
 Security: Firewall Medium

WLAN Information

	2.4GHz	5GHz
MAC Address	D8:EC:E5:18:B4:39	D8:EC:E5:18:B4:3A
Status	On	On
SSID	Zyxel_B439	Zyxel_B439_5G
Channel	Auto(Current 1)	Auto(Current 36)
Security	WPA2-Personal	WPA2-Personal
802.11 Mode	802.11b/g/n Mixed	802.11a/n/ac Mixed
WPS	On	On

Each field is described in the following table.

Table 14 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the Zyxel Device system name. It is used for identification.
Model Name	This shows the model number of your Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This is the current version of the firmware inside the Zyxel Device.
System Uptime	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it.
Interface Status	
Virtual ports are shown here. You can see the ports in use and their transmission rate.	
WAN Information (These fields display when you have an Ethernet WAN connection.)	
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 IP address of the Zyxel Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device in the WAN.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.

Table 14 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 therefore only valid for communication within the local network segment or broadcast domain of the device. Typically, link-local addresses are used for automatic address configuration and neighbor discovery protocols.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: Server – The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay – The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. None – The Zyxel Device is not providing any DHCP services to the LAN.
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 displayed.

Figure 38 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 39 Cellular Info: Detailed Information

Cellular Info			
Module Information		Service Information	
IMEI	351964110000165	Access Technology	LTE
Module SW Version	EG12EAPAR01A05M4G	Band	LTE_BC7
SIM Status		RSSI	-53
SIM Card Status	Available	Cell ID	56410647
IMSI	466011801891892	Physical Cell ID	23
ICCID	89886018157708842319	UL Bandwidth [MHz]	20
PIN Protection	Disable	DL Bandwidth [MHz]	20
PIN Remaining Attempts	3	RFCN	3250
IP Passthrough Status		RSRP	-80
IP Passthrough Enable	Disable	RSRQ	-9
Cellular Status		RSCP	N/A
Cellular Status	Up	EcNo	N/A
Data Roaming	Disable	TAC	59242
Operator	Far EastOne	LAC	N/A
PLMN	46601	RAC	N/A
		BSIC	N/A
		SINR	19

The following table describes the labels in this screen.

Table 15 Cellular Info: Detailed Information

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

Table 15 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
SIM Card Status	This displays the SIM card status: None – the Zyxel Device does not detect that there is a SIM card inserted. Available – the SIM card could either have or does not have PIN code security. Locked – the SIM card has PIN code security, but you did not enter the PIN code yet. Blocked – you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card. Error – the Zyxel Device detected that the SIM card has errors.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (ICCID). This is the serial number of the SIM card.
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. 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.
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
IP Passthrough Enable	This displays if IP Passthrough is enabled on the Zyxel Device. IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
IP Passthrough Mode	This displays the IP Passthrough mode. This displays Dynamic and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device. This displays Fixed and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.
Cellular Status	
Cellular Status	This displays the status of the cellular Internet connection.
Data Roaming	This displays if data roaming is enabled on the Zyxel Device. 4G 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) send position and timing data from high orbit artificial satellites. It works with GPS navigation 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, you can easily locate the Zyxel Device with accurate information.
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.

Table 15 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
Band	This displays the current cellular band of your Zyxel Device (WCDMA2100).
RSSI	This displays the strength of the cellular signal between an associated cellular station and the Zyxel Device.
Cell ID	<p>This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting.</p> <p>The value depends on the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting:</p> <ul style="list-style-type: none"> • 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/5G, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331. <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>
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	<p>This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting.</p> <p>The value depends on the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting:</p> <ul style="list-style-type: none"> • For GPRS, it is the ARFCN (Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.45.005. • For UMTS (3G), it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. • For LTE/5G, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>
RSRP	<p>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.</p> <p>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.</p> <p>An undetectable signal is indicated by the lower limit, example -140 dBm.</p> <p>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.</p>
RSRQ	<p>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.</p> <p>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.</p> <p>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.</p>

Table 15 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
RSCP	<p>This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device.</p> <p>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.</p> <p>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.</p>
EcNo	<p>This displays the ratio (in dB) of the received energy per chip and the interference level.</p> <p>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.</p> <p>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.</p>
TAC	<p>This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber.</p> <p>The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.</p> <p>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.</p>
LAC	<p>This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.</p> <p>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].</p> <p>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.</p>
RAC	<p>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.</p> <p>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.</p> <p>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].</p> <p>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.</p>
BSIC	<p>The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.</p> <p>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.</p>
SINR	<p>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.</p>
CQI	<p>This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good or bad the communication channel quality is.</p>
MCS	<p>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.</p>
RI	<p>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.</p>

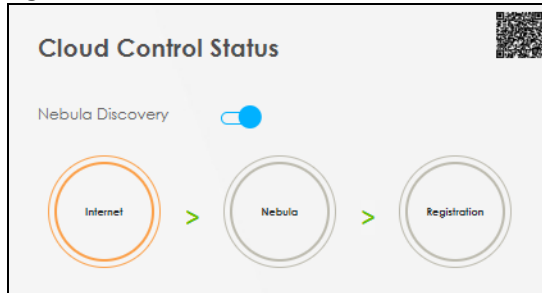
Table 15 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
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).
# Number	This displays the ID of the SCC. Some cellular providers support two or more SCCs.
Physical Cell ID	This displays the Physical Cell ID (PCI) of the SCC.
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.
RSRP	This displays the Received Signal Code Power of the SCC.
RSRQ	This displays the Reference Signal Receive Quality of the SCC.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) of the SCC.

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 40 Cloud Control Status



Each field is described in the following table.

Table 16 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.
Cloud Control Status	<p>This field displays:</p> <ul style="list-style-type: none"> The Zyxel Device Internet connection status. The connection status between the Zyxel Device and the NCC. The Zyxel Device registration status on the NCC. <p>Mouse over the circles to display detailed information.</p> <p>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.</p> <p>Internet</p> <ul style="list-style-type: none"> Green: The Zyxel Device is connected to the Internet. Orange: The Zyxel Device is not connected to the Internet. <p>Nebula</p> <ul style="list-style-type: none"> Green: The Zyxel Device is connected to the NCC. Gray: The Zyxel Device is not connected to the NCC. <p>Registration</p> <ul style="list-style-type: none"> Green: The Zyxel Device is registered on the NCC. Gray: The Zyxel Device is not registered on the NCC. <p>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.</p>
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



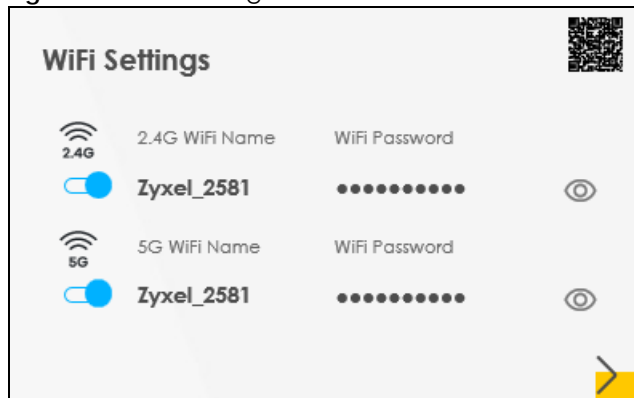
Use this screen to enable or disable the main wireless network. When the switch turns blue (), the function is enabled. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the main wireless networks. If you want to show or hide your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

Figure 41 WiFi Settings

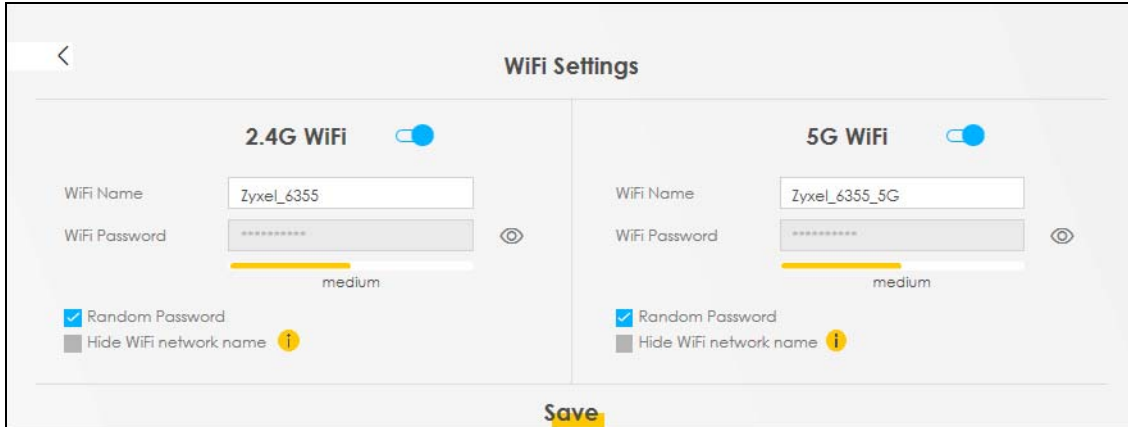


Click the Arrow icon (➤) to configure the SSIDs and/or passwords for your main wireless networks. Click the Eye icon (👁) to display the characters as you enter the WiFi Password.

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



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

Figure 42 WiFi Settings: Configuration




Each field is described in the following table.

Table 17 WiFi Settings: Configuration

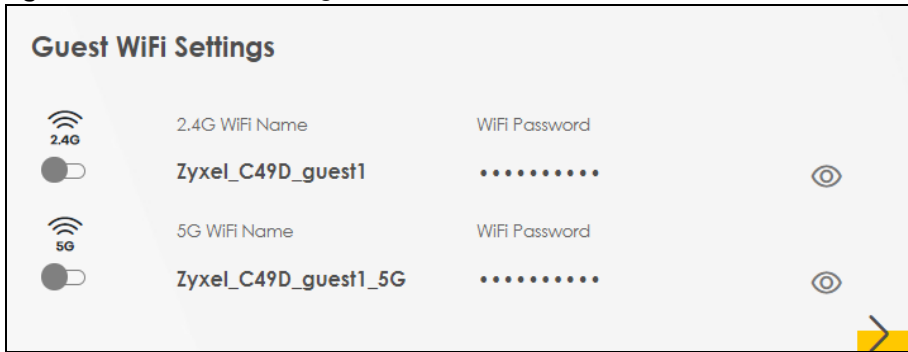
LABEL	DESCRIPTION
2.4 GHz / 5 GHz WiFi	Click this switch to enable or disable the 2.4G / 5G WiFi network. When the switch turns blue  , the function is enabled.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating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

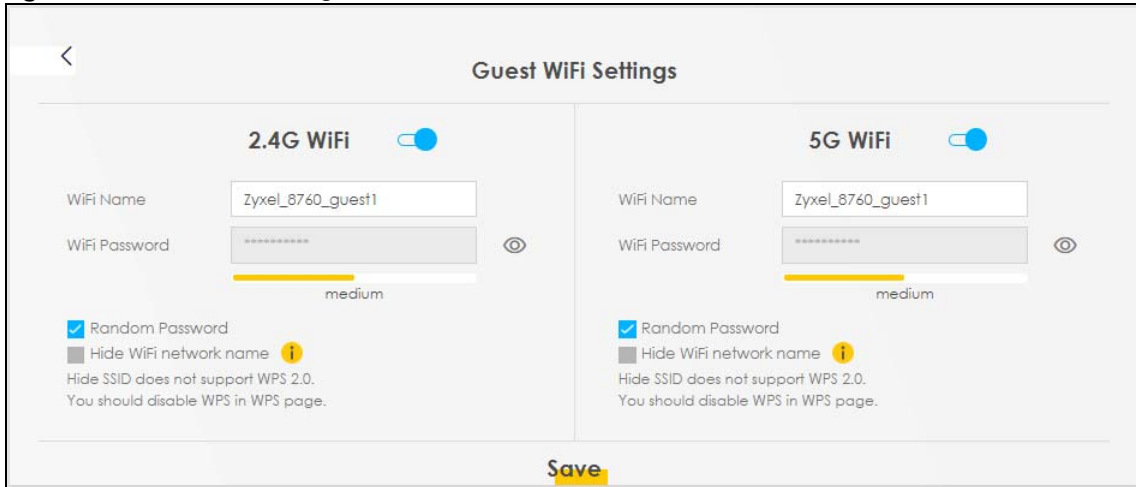
network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the Eye icon.

Figure 43 Guest WiFi Settings



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

Figure 44 Guest WiFi Settings: Different SSIDs



Each field is described in the following table.

Table 18 WiFi Settings: Configuration



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

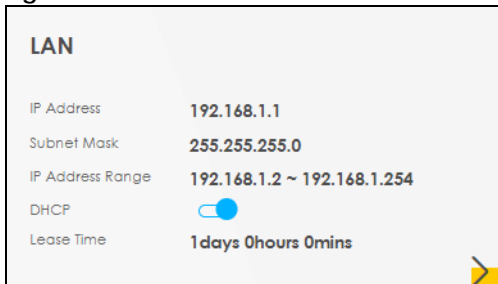
Table 18 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
Hide WiFi network name	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID.
Save	Click Save to save your changes.

6.2.1 LAN

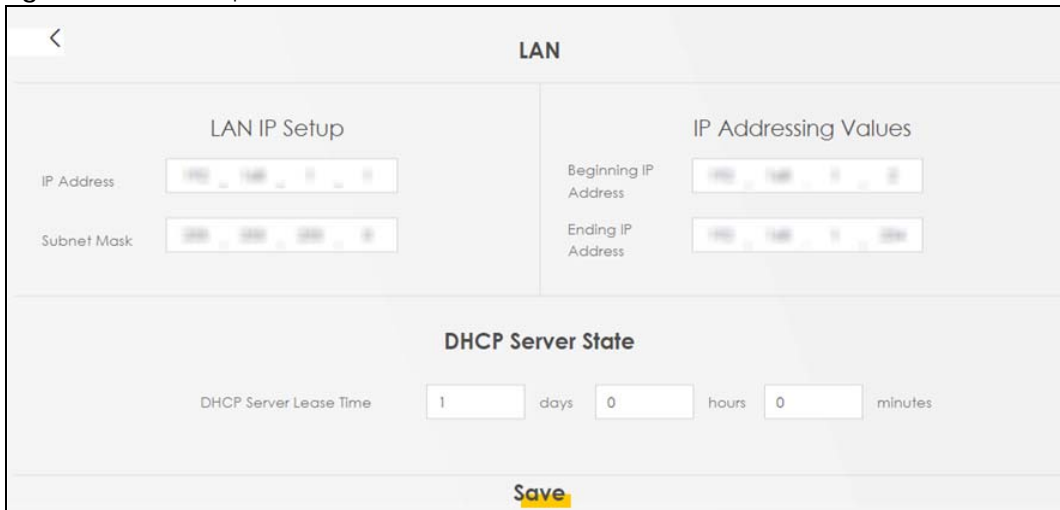
Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device.

Figure 45 LAN



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

Figure 46 LAN Setup



Each field is described in the following table.

Table 19 Status Screen

LABEL	DESCRIPTION
Group Name	Select the interface group you want to use.
LAN IP Setup	
IP Address	Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).

Table 19 Status Screen (continued)

LABEL	DESCRIPTION
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
DHCP Server State	
DHCP Server Lease Time	This is the period of time a DHCP-assigned address is valid, before it expires. When a client connects to the Zyxel Device, DHCP automatically assigns the client an IP addresses from the IP address pool. DHCP leases each addresses for a limited period of time, which means that past addresses are "recycled" and made available for future reassignment to other devices.
Days/Hours/Minutes	Enter the lease time of the DHCP server.
Save	Click Save to save your changes.

CHAPTER 7

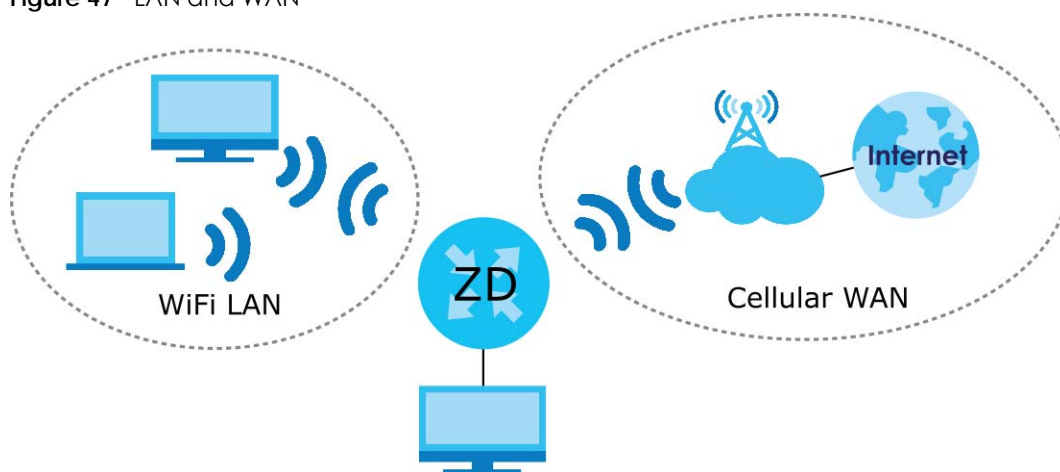
Broadband

7.1 Overview

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

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

Figure 47 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 102](#)).
- 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 107](#)).
- Use the **Cellular WAN** screen to configure a cellular WAN connection ([Section 7.4 on page 107](#)).
- Use the **Cellular APN** screen to configure the APN setting ([Section 7.5 on page 109](#)).
- Use the **Cellular SIM** screen to enter the PIN of your SIM card ([Section 7.6 on page 114](#)).
- 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 7.7 on page 116](#)).
- Use the **Cellular PLMN** screen to display available Public Land Mobile Networks ([Section 7.8 on page 117](#)).
- Use the **Cellular IP Passthrough** screen to configure a cellular WAN connection ([Section 7.9 on page 119](#)).
- Use the **Cellular Lock** screen to configure the base station you choose to connect to ([Section 7.10 on page 120](#)).

- Use the **Cellular SMS** screen to send and receive SMS messages from the Zyxel Device ([Section 7.11 on page 121](#)).

Table 20 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.

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 48 Network Setting > Broadband

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

The following table describes the labels in this screen.

Table 21 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 Edit or 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 49 Network Setting > Broadband > Add or Edit New WAN Interface

The screenshot shows the 'Edit WAN Interface' configuration page. It features a grid of settings sections:

- General:** Includes fields for Name (Cellular WAN), Type, Mode (Routing), Encapsulation (IPoE), and IPv4/IPv6 Mode (IPv4 IPv6 DualStack). A toggle switch is present.
- VLAN:** Includes fields for 802.1p (0) and 802.1q, with a range indicator [1~4094].
- MTU:** Includes a field for MTU (1500).
- IP Address:** Radio buttons for 'Obtain an IP Address Automatically' (selected) and 'Static IP Address'.
- DNS Server:** Radio buttons for 'Obtain DNS Info Automatically' (selected) and 'Use Following Static DNS Address'.
- DHCP Options:** Sections for Request Options (option 43, 120, 121) and Sent Options (option 60, 61, 125) with corresponding text input fields for Vendor ID, IAID, and DUID.
- IPv6 Address:** Radio buttons for 'Obtain an IPv6 Address Automatically' (selected) and 'Static IPv6 Address'.
- IPv6 DNS Server:** Radio buttons for 'Obtain IPv6 DNS Info Automatically' (selected) and 'Use Following Static IPv6 DNS Address'.
- IPv6 Routing Feature:** Toggle switches for MLD Proxy and 'Apply as Default Gateway'.
- NAT and Routing Feature:** Toggle switches for NAT, IGMP Proxy, 'Apply as Default Gateway', and Fullcone NAT.

At the bottom, there are 'Cancel' and 'Apply' buttons. The 'Apply' button is highlighted in yellow.

The following table describes the labels in this screen.

Table 22 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.

Table 22 Network Setting > Broadband > Add or Edit New WAN Interface (continued)






LABEL	DESCRIPTION
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.
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.

Table 22 Network Setting > Broadband > Add or Edit New WAN Interface (continued)

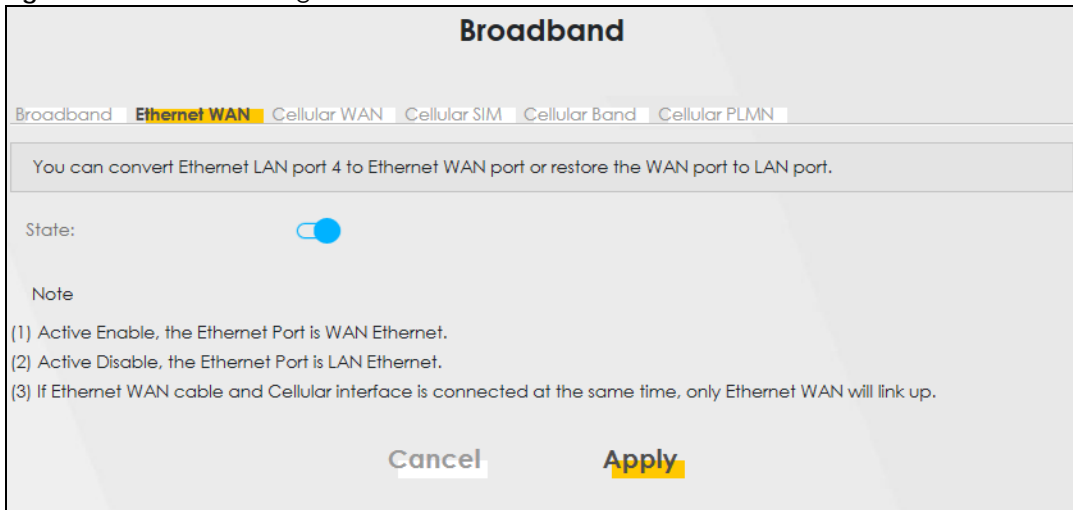
LABEL	DESCRIPTION
DHCP Options	
Request Options	Select Option 43 to have the Zyxel Device get vendor specific information from DHCP packets sent from the DHCP server. Select Option 120 to have the Zyxel Device get an IP address or a fully-qualified domain name of a SIP server from DHCP packets sent from 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.
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 Enable	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.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

7.3 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.

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

Figure 50 Network Setting > Broadband > Ethernet WAN



7.4 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 51 Network Setting > Broadband > Cellular WAN

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

PDP Type

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

The following table describes the fields in this screen.

Table 23 Network Setting > Broadband > Cellular WAN

LABEL	DESCRIPTION
Antenna	
Antenna Select	Select between External or Internal Antenna for your Zyxel Device.
Roaming	
Data Roaming	Click this to enable (<input checked="" type="checkbox"/>) 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	

Table 23 Network Setting > Broadband > Cellular WAN (continued)

LABEL	DESCRIPTION
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.
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 (<input checked="" type="checkbox"/>) 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.

7.5 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. For details, see the features comparison table at [Section 1.1 on page 17](#).

Figure 52 Network Setting > Broadband > Cellular APN

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

The following table describes the labels in this screen.

Table 24 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).
Authentication 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.

7.5.1 Edit Cellular APN1/APN2

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

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

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

Figure 53 Network Setting > Broadband > Cellular APN > Edit APN

Edit APN 1

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

Enable

APN Manual Mode

APN

Username (Optional)

Password (Optional)

Authentication Type

PDP Type

IP Passthrough

Passthrough Mode

Static Gateway Enable

Subnet mask Prefix 0 : keep subnet mask assigned by CM

DHCP Lease Time 0 : keep predefined value, unit: second

Note
APN information can be obtained from the service provider.

Cancel OK

The following table describes the fields in this screen.

Table 25 Network Setting > Broadband > Cellular APN > Edit APN

LABEL	DESCRIPTION
Enable	Click this to enable (<input checked="" type="checkbox"/>) 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 (<input checked="" type="checkbox"/>) 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 25 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 Passthrough 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.

7.5.2 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 > Cellular APN**, 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 ▼

PDP Type ▼

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

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

Remote Management

MGMT Services Trust Domain MGMT Services for IP PassThrough Trust Domain for IP PassThrough

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

Service Control

WAN Interface used for services Any_WAN Multi_WAN

Cellular WAN 1 Cellular WAN 2 ETHWAN

Service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	443
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
PING	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	

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

TR-069 Client

TR-069 is a remote management tool on this device. The operator can upgrade firmware, modify settings, and diagnose problems remotely when TR-069 is enabled.

CWMP Active

Inform

Inform Interval

IP Protocol TR069 on IPv4 Only TR069 on IPv6 Only Auto Select

ACS URL (URL or IPv4 Address / Global IPv6 Address)

ACS User Name

ACS Password

WAN Interface Used by TR-069 Client Any_WAN Multi_WAN

Cellular WAN 1 Cellular WAN 2 ETHWAN

7.6 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 54 Network Setting > Broadband > Cellular SIM

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

PIN Management

PIN Protection

PIN

Attempts remaining: 2

Note

(1) The PIN is automatically saved in the Zyxel Device.
 (2) Entering the wrong PIN exceeding a set number of times will lock the SIM card.

Cancel Apply

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 26 Network Setting > Broadband > Cellular SIM

LABEL	DESCRIPTION
PIN Management	
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. Click to enable () if the service provider requires you to enter a PIN to use the SIM card. Click to disable if the service provider lets you use the SIM without inputting a PIN.
PIN Modification	
more...	Click the icon () to show more 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-digit code to set as the new PIN code. Note: This field will show upon clicking the icon ()
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.

7.7 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 55 Network Setting > Broadband > Cellular Band

The following table describes the fields in this screen.

Table 27 Network Setting > Broadband > Cellular Band

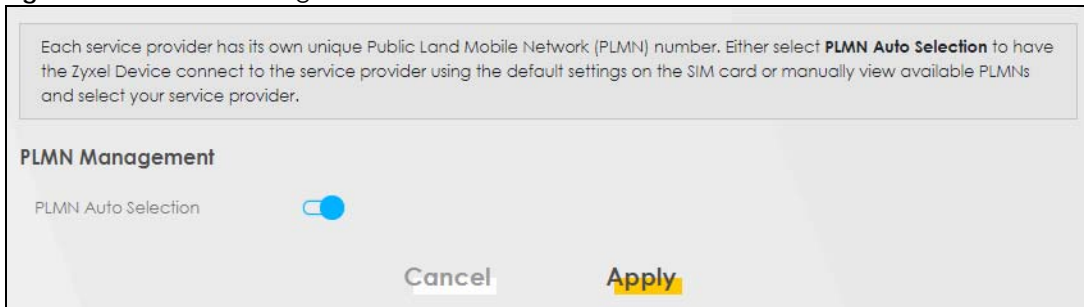
LABEL	DESCRIPTION
Access Technology	
Preferred Access Technology	Select the cellular mode your Zyxel Device supports to which you want the Zyxel Device to connect, and then click Apply to save your settings. Otherwise, select Auto to have the Zyxel Device connect to an available network using the default 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	Select the cellular bands to use for the Zyxel Device's cellular WAN connection. Click to enable (<input checked="" type="checkbox"/>) automatic frequency band selection as provided by the cellular service provider. Otherwise, select disabled.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

7.8 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 56 Network Setting > Broadband > Cellular PLMN



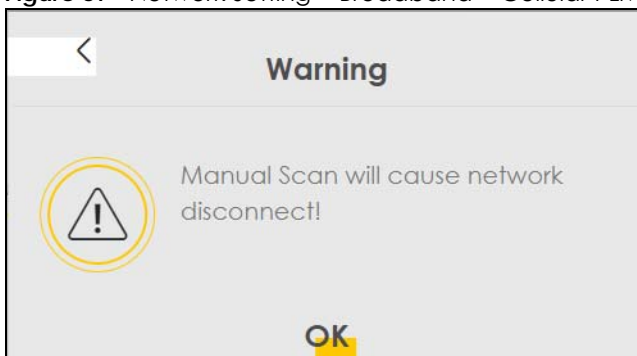
The following table describes the labels in this screen.

Table 28 Network Setting > Broadband > Cellular PLMN

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

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

Figure 57 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 58 Network Setting > Broadband > Cellular PLMN > Manual Scan

Cellular PLMN Configuration

PLMN Management

PLMN Auto Selection

Scan

#	Status	Name	Type	PLMN
<input type="radio"/>	Available	FET	LTE	46601
<input type="radio"/>	Current	FET	UMTS	46601
<input type="radio"/>	Forbidden	TWM	UMTS	46697
<input type="radio"/>	Available	Chunghwa	UMTS	46692
<input type="radio"/>	Available	Chunghwa	LTE	46692
<input type="radio"/>	Forbidden	T Star	LTE	46689
<input type="radio"/>	Forbidden	TWM	LTE	46697
<input type="radio"/>	Forbidden	466 05	GPRS	46605
<input type="radio"/>	Forbidden	466 05	LTE	46605
<input type="radio"/>	Forbidden	T Star	UMTS	46689

Cancel
Apply

The following table describes the labels in this screen.

Table 29 Network Setting > Broadband > Cellular PLMN > Manual Scan

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

7.9 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 if Ethernet WAN is enabled at **Network Setting > Broadband > Ethernet WAN > State**.

Figure 59 Network Setting > Broadband > Cellular IP Passthrough

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

IP Passthrough Management

IP Passthrough

Passthrough Mode Fixed

Passthrough to fixed MAC

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

Cancel Apply

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

Warning

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

OK

The following table describes the fields in this screen.

Table 30 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.

Table 30 Network Setting > Broadband > Cellular IP Passthrough (continued)

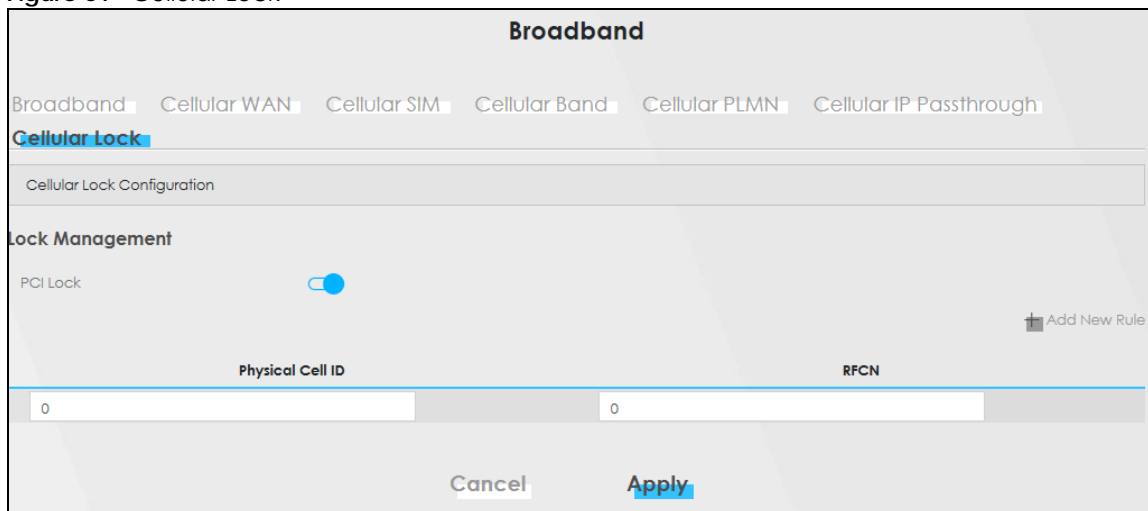
LABEL	DESCRIPTION
Passthrough Mode	Select Dynamic to allow traffic to be forwarded to the first LAN computer on the local network of the Zyxel Device. Select Fixed to allow traffic to be forwarded to a specific computer (for example, Client A) by entering its MAC address. Note: This field will show after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

7.10 Cellular Lock

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

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

Figure 61 Cellular Lock



The following table describes the fields in this screen.

Table 31 Cellular Lock

LABEL	DESCRIPTION
PCI Lock	Select this to enable or disable PCI (Physical Cell Identifier) Lock.
Add New Rule	Select this if you want to add a new rule or to configure cellular lock rules.
Physical Cell ID	Use this to enter the PCI number of the base station you choose to connect to (0 – 504).
RFCN	Use RFCN (Radio Frequency Channel Number) to enter the LTE frequency of the specified PCI number(1 – 65535).

Table 31 Cellular Lock (continued)

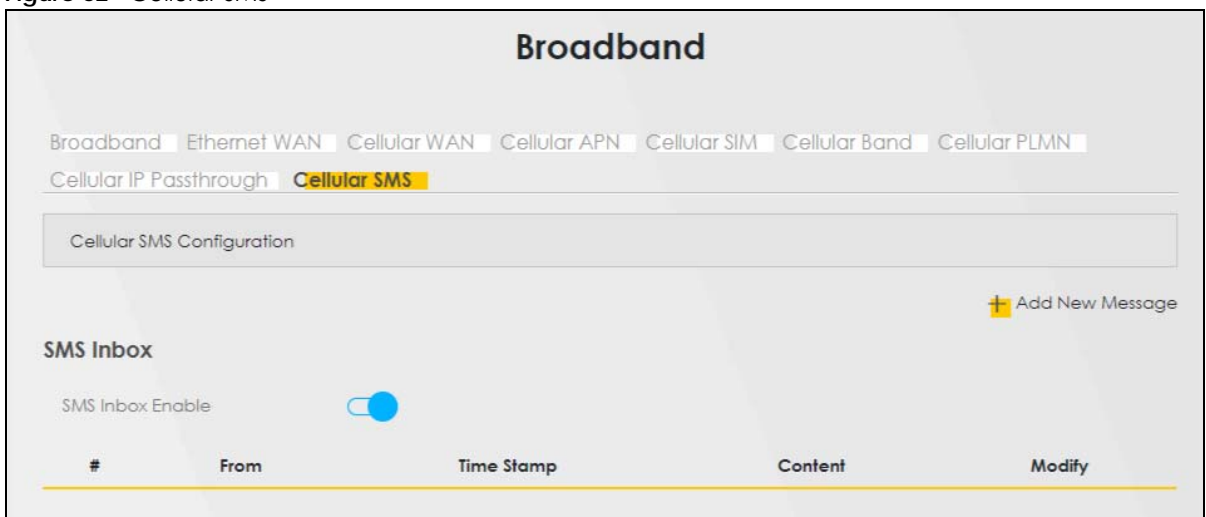
LABEL	DESCRIPTION
Cancel	Click this to exit this screen without saving.
Apply	Click this to save your changes.

7.11 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 62 Cellular SMS



The following table describes the fields in this screen.

Table 32 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.
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.
#	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.

7.11.1 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 63 Send New Message

The following table describes the fields in this screen.

Table 33 Cellular SMS

LABEL	DESCRIPTION
Character Set	Select whether you want to send the SMS message using GSM-7 encoding or unicode. <ul style="list-style-type: none"> 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.
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 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 124](#))
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device ([Section 8.3 on page 129](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device ([Section 8.4 on page 133](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 8.5 on page 134](#)).
- 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 136](#)).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold ([Section 8.7 on page 137](#)).
- Use the **WLAN Scheduler** screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces ([Section 8.8 on page 141](#)).

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.

WiFi6 / IEEE 802.11ax

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

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

Table 34 WiFi Standards Comparison

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

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

Finding Out More

See [Section 8.9 on page 143](#) for advanced technical information on WiFi networks.

8.2 Wireless General Settings

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

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

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 64 Network Setting > Wireless > General

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

Table 35 Network Setting > Wireless > General


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

Table 35 Network Setting > Wireless > General (continued)

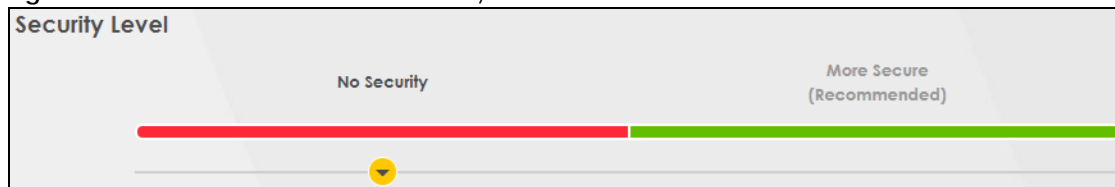
LABEL	DESCRIPTION
Bandwidth	<p>A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps.</p> <p>40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p> <p>Because not all devices support 40 MHz and/or 160 MHz channels, select 20/40MHz or 20/40/80/160MHz to allow the Zyxel Device to adjust the channel bandwidth automatically.</p>
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	<p>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.</p> <p>Enter a descriptive name (up to 32 English keyboard characters) for WiFi.</p>
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	<p>Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.</p> <p>This check box is grayed out if the WPS function is enabled in the Network Setting > Wireless > WPS screen.</p>
Multicast Forwarding	Select this check box 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	<p>Select More Secure (Recommended) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen.</p> <p>Or you can select No Security to allow any client to associate this network without any data encryption or authentication.</p> <p>See the following sections for more details about this field.</p>
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 65 Wireless > General: No Security



The following table describes the labels in this screen.

Table 36 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 WPA-PSK security mode is a more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be. The WPA3-SAE (Simultaneous Authentication of Equals handshake) security mode protects against dictionary attacks (password guessing attempts). It improves security by requiring a new encryption key every time a WPA3 connection is made. A handshake is the communication between the Zyxel Device and a connecting client at the beginning of a WiFi session.

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

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

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

Figure 66 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

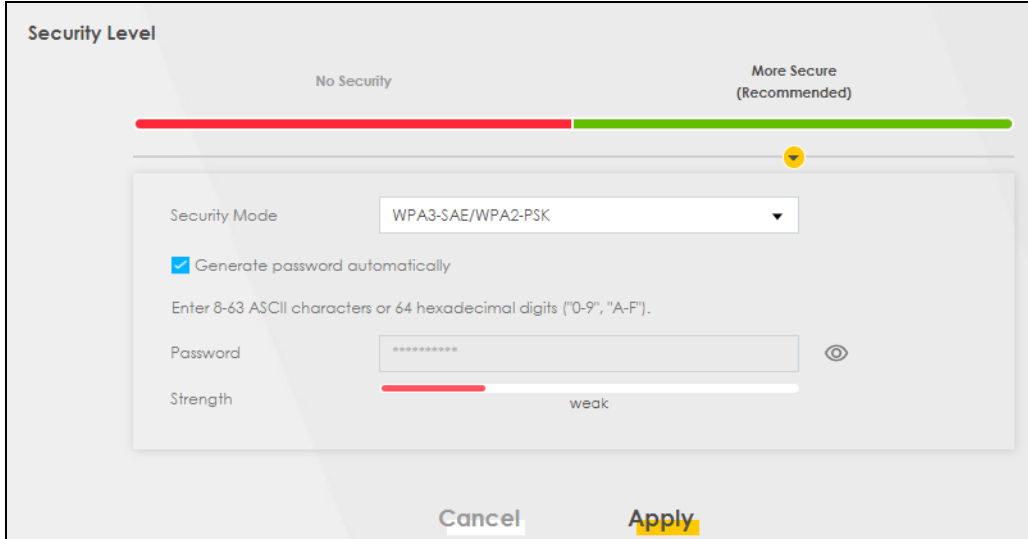
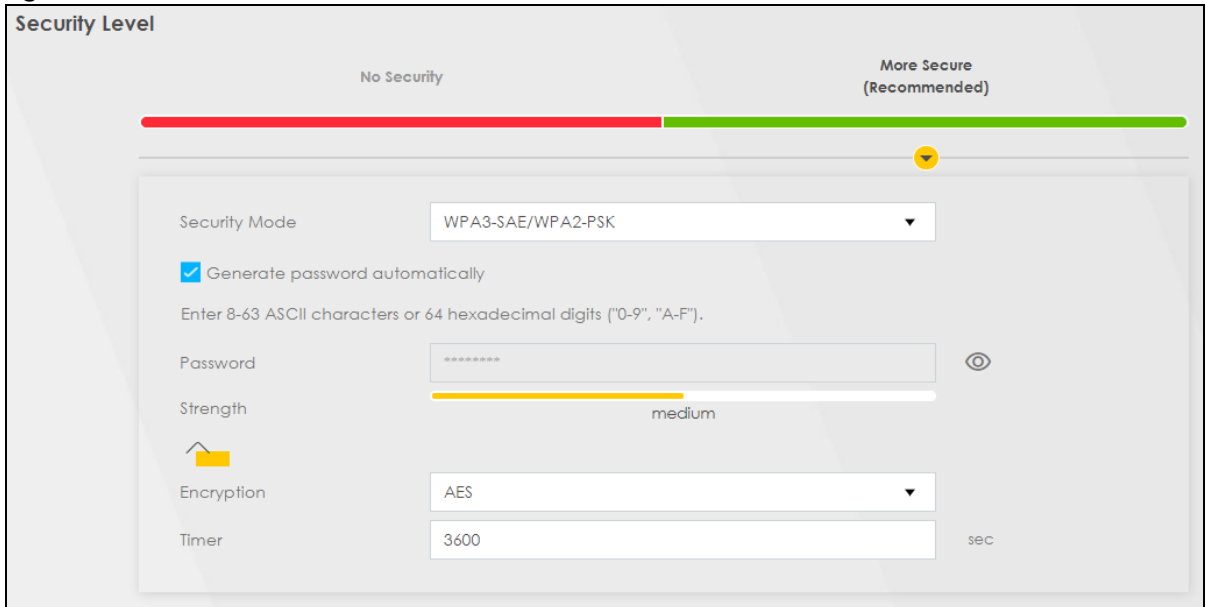


Figure 67 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK




The following table describes the labels in this screen.

Table 37 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK




LABEL	DESCRIPTION
Security Level	Select More Secure to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.

Table 37 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK (continued)

LABEL	DESCRIPTION
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	<p>Select Generate password automatically or enter a Password.</p> <p>The password has two uses.</p> <ol style="list-style-type: none"> 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8 – 63 ASCII characters or exactly 64 hexadecimal ('0 – 9', 'a – f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. <p>Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.</p>

The following table describes the labels in this screen.

Table 38 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select More Secure to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	<p>Select Generate password automatically or enter a Password.</p> <p>The password has two uses.</p> <ol style="list-style-type: none"> 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8 – 63 ASCII characters or exactly 64 hexadecimal ('0 – 9', 'a – f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. <p>Note: Enter 8 – 63 ASCII characters only. 64 hexadecimal characters are not accepted for WPS.</p> <p>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.</p>
more...	Click this  to show more fields in this section. Click this  to hide them.
Encryption	<p>AES is the default data encryption type, which uses a 128-bit key.</p> <p>Select the encryption type (AES or TKIP+AES) for data encryption.</p> <p>Select AES if your wireless clients can all use AES.</p> <p>Select TKIP+AES to allow the wireless clients to use either TKIP or AES.</p>
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 wireless network that allows access to the Internet through the Zyxel Device. You can use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.







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

The following table introduces the supported wireless networks.

Table 39 Supported Wireless Networks

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

Figure 68 Network Setting > Wireless > Guest/More AP

This device can enable up to 4 wireless networks to work at the same time. Assign a name and a security level (if needed) to start the 2nd, 3rd, and 4th wireless network services.					
#	Status	SSID	Security	Guest WLAN	Modify
1		Zyxel_9DE5_guest1	WPA2-Personal	External Guest	
2		Zyxel_9DE5_guest2	WPA2-Personal	External Guest	
3		Zyxel_9DE5_guest3	WPA2-Personal	External Guest	

The following table describes the labels in this screen.

Table 40 Network Setting > Wireless > Guest/More AP

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

8.3.1 The Edit Guest/More AP Screen

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

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

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

Figure 69 Network Setting > Wireless > Guest/More AP > Edit

The following table describes the fields in this screen.

Table 41 Network Setting > Wireless > Guest/More AP > Edit


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

Table 41 Network Setting > Wireless > Guest/More AP > Edit (continued)



LABEL	DESCRIPTION
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the Access Scenario field.
Access Scenario	If you select Home Guest , clients can connect to each other directly. If you select External Guest , clients are blocked from connecting to each other directly.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled.
SSID Subnet	Click on this switch to Enable this function if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients. This option cannot be used if the WPS function is enabled in the Network > Wireless > WPS screen or if the Keep 2.4G and 5G wireless network name the same check box is selected in Network > Wireless > General .
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool. The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	
Security Mode	Select More Secure (WPA2-PSK) to add security on this wireless network. The wireless clients which want to associate to this network must have the same wireless security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See Section 8.2.1 on page 126 for more details about this field.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. If you did not select Generate password automatically , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it's hidden.
	Click this  to show more fields in this section. Click again to hide them.
Encryption	Select the encryption type (AES or TKIP+AES) for data encryption. Select AES if your wireless clients can all use AES. Select TKIP+AES to allow the wireless clients to use either TKIP or AES.
Timer	The Timer is the rate at which the RADIUS server sends a new group key out to all clients.

Table 41 Network Setting > Wireless > Guest/More AP > Edit (continued)

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

8.4 MAC Authentication

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

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

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

Figure 70 Network Setting> Wireless > MAC Authentication

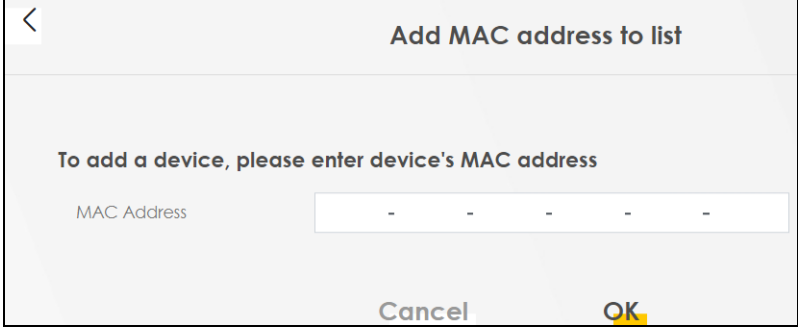
The screenshot shows the MAC Authentication configuration interface. Under the 'General' heading, there is a dropdown menu for 'SSID' currently showing 'Zyxel_IDF1'. Below it, 'MAC Restrict Mode' has three radio buttons: 'Disable', 'Deny', and 'Allow', with 'Allow' selected. The 'MAC address List' section features a table with columns for '#', 'MAC Address', and 'Modify'. A '+ Add new MAC address' button is located to the right of the table. At the bottom of the screen, there are 'Cancel' and 'Apply' buttons.

The following table describes the labels in this screen.

Table 42 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 42 Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
Add new MAC address	<p>This field is available when you select Deny or Allow in the MAC Restrict Mode field.</p> <p>Click this if you want to add a new MAC address entry to the MAC filter list below.</p> <p>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.</p> 
#	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	<p>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).</p> <p>Click the Delete icon to delete the entry.</p>
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 wireless network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection. Your devices must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your device supports it. See [Section 8.9.6.1 on page 147](#) for more information about WPS.

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection (see [Section 8.2.2 on page 127](#)).

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

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

Figure 71 Network Setting > Wireless > WPS

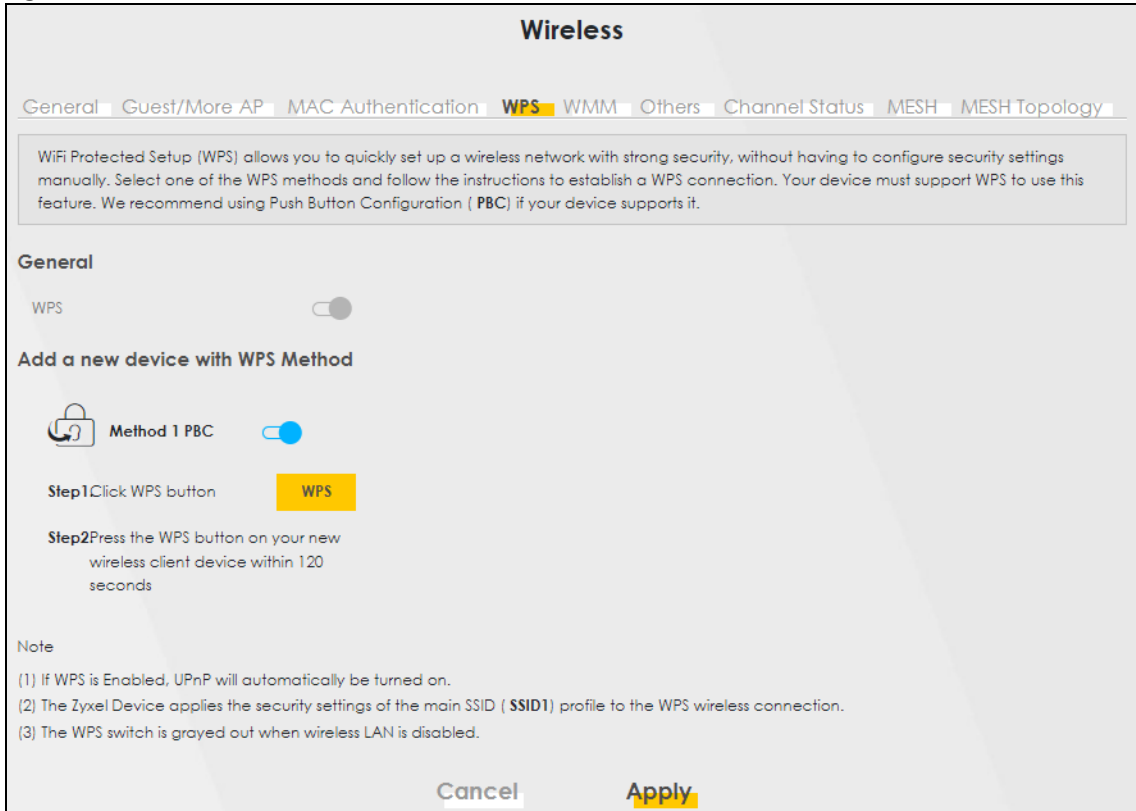
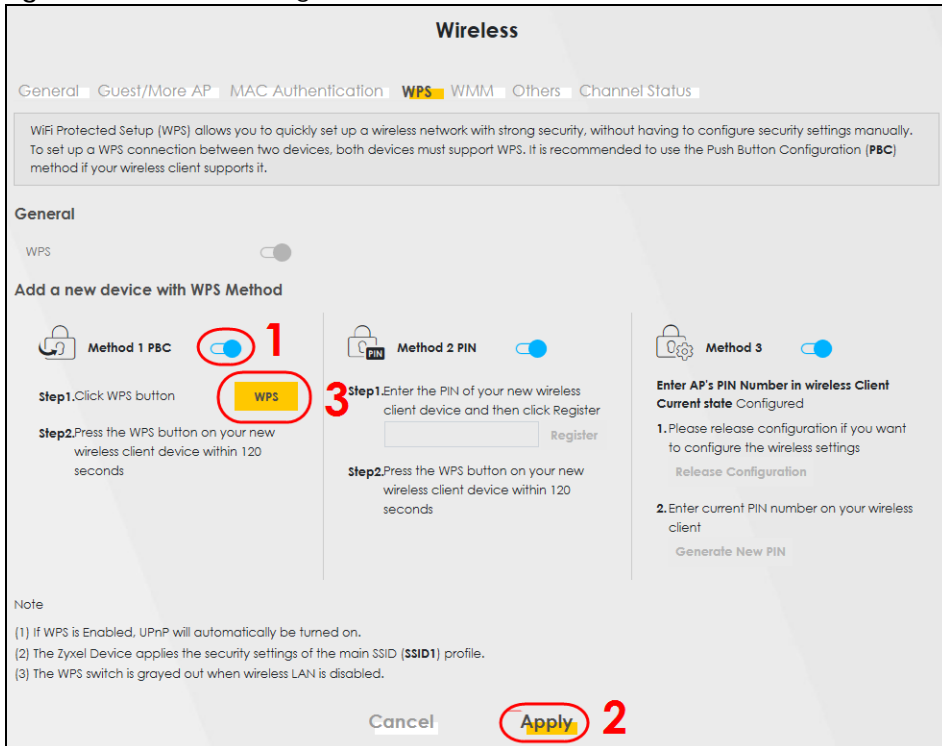



Figure 72 Network Setting > Wireless > WPS



The following table describes the labels in this screen.

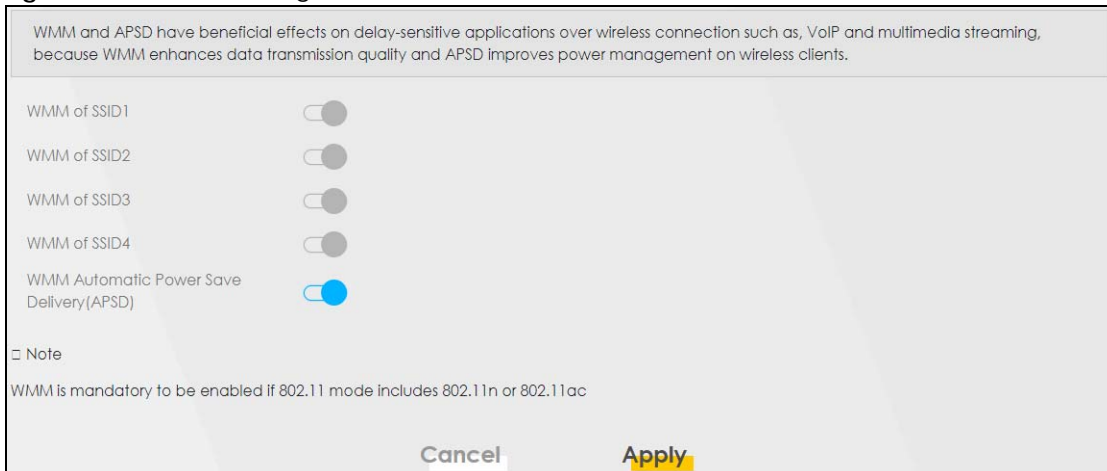
Table 43 Network Setting > Wireless > WPS

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

8.6 WMM

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

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

Figure 73 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 44 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM of SSID	Select On to have the Zyxel Device automatically give the WiFi network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to video, which makes them run more smoothly. If the 802.11 Mode in Network Setting > Wireless > Others is set to include 802.11n or 802.11ac, WMM cannot be disabled.
WMM Automatic Power Save Delivery (APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Zyxel Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Zyxel Device until the Zyxel Device "wakes up." The Zyxel Device wakes up periodically to check for incoming data. Note: This works only if the WiFi device to which the Zyxel Device is connected also supports this feature.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

8.7 Others Screen

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

See [Section 8.9.2 on page 144](#) for detailed definitions of the terms listed here.

Figure 74 Network Setting > Wireless > Others

WiFi

General | MAC Authentication | WPS | WMM | **Others**

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

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

Cancel **Apply**

The following table describes the labels in this screen.

Table 45 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 45 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Mode	<p>For 2.4 GHz frequency WiFi devices:</p> <ul style="list-style-type: none"> • 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. <p>For 5 GHz frequency WiFi devices:</p> <ul style="list-style-type: none"> • 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.

Table 45 Network Setting > Wireless > Others (continued)

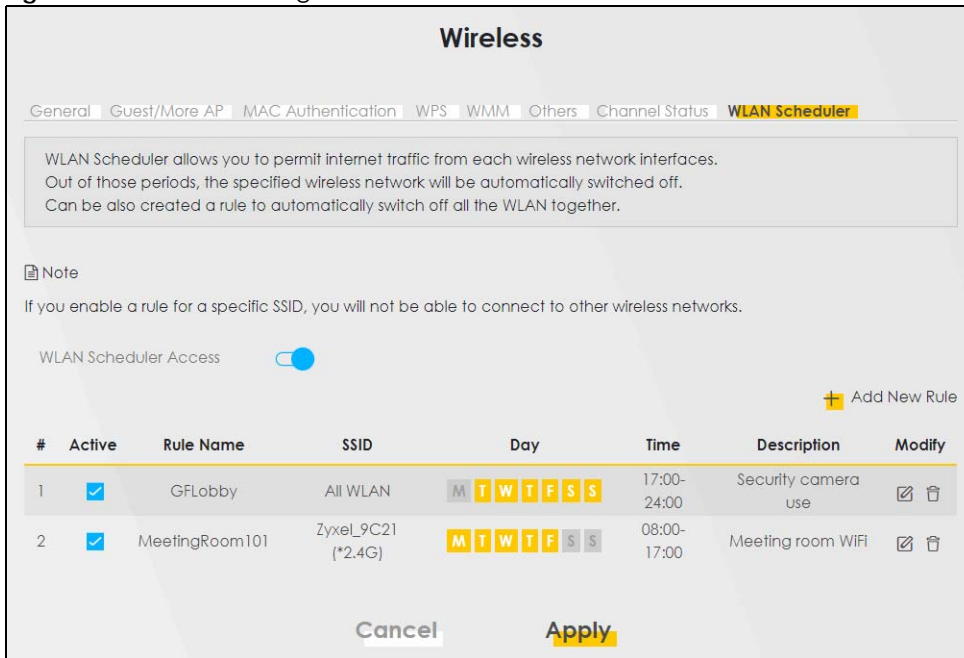
LABEL	DESCRIPTION
802.11 Mode	<p>For 2.4 GHz frequency WiFi devices:</p> <ul style="list-style-type: none"> • Select 802.11b Only to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select 802.11g Only to allow only IEEE 802.11g compliant WiFi devices to associate 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. <p>For 5 GHz frequency WiFi devices:</p> <ul style="list-style-type: none"> • 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.
802.11 Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select Off to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network.</p> <p>This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.</p>
Preamble	<p>Select a preamble type from the drop-down list box. Choices are Long or Short. See Section 8.9.6 on page 147 for more information.</p> <p>This field is configurable only when you set 802.11 Mode to 802.11b.</p>
Protected Management Frames	<p>WiFi with Protected Management Frames (PMF) provides protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging. Select Capable if the WiFi client supports PMF, then the management frames will be encrypted. Select Required to force the WiFi client to support PMF; otherwise the authentication cannot be performed by the Zyxel Device. Otherwise, select Disabled.</p>
Auto Switch Off Interval	<p>Select a time period from the drop list. WiFi will automatically switch off by the time period you selected.</p>
Cancel	<p>Click Cancel to restore your previously saved settings.</p>
Apply	<p>Click Apply to save your changes.</p>

8.8 WLAN Scheduler

Use the **WLAN Scheduler** screen to create rules to schedule the times to permit Internet traffic from each wireless 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 75 Network Setting > Wireless > WLAN Scheduler



The following table describes the labels in this screen.

Table 46 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. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Add New Rule	Click this to configure a new WLAN scheduler rule.
#	This is the index number of the entry.
Active	Click the check box 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.

8.8.1 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 76 Network Setting > Wireless > WLAN Scheduler > Add New Rule

The following table describes the labels in this screen.

Table 47 Network Setting > Wireless > WLAN Schedule > Add New Rule

LABEL	DESCRIPTION
Active	Slide the switch to the right () to enable this WLAN scheduler rule.
SSID	Select All wireless networks if you want the rule to apply to all wireless network interfaces or select a wireless 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 check box 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.

8.9 Technical Reference

This section discusses wireless LANs in depth.

8.9.1 WiFi Network Overview

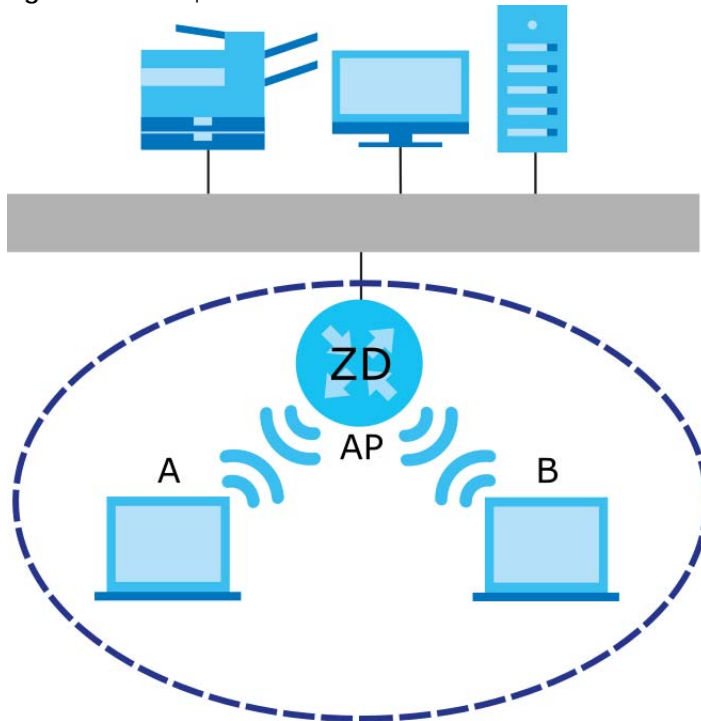
WiFi networks consist of WiFi clients, access points and bridges.

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

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

The following figure provides an example of a WiFi network.

Figure 77 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 Zykel Device is the AP.

Every WiFi network must follow these basic guidelines.

- Every device in the same WiFi network must use the same SSID.
The SSID is the name of the WiFi network. It stands for Service Set Identifier.

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

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

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

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

8.9.2 Additional Wireless Terms

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

Table 48 Additional WiFi Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>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.</p> <p>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.</p> <p>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.</p>
Preamble	A preamble affects the timing in your WiFi network. There are two preamble modes: long and short. If a device uses a different preamble mode than the Zyxel Device does, it cannot communicate with the Zyxel Device.
Authentication	The process of verifying whether a WiFi device is allowed to use the WiFi network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

8.9.3 WiFi Security Overview

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

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

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

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

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

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

8.9.3.1 SSID

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

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

8.9.3.2 MAC Address Filter

Every device that can use a WiFi network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the WiFi network, see the device's User's Guide or other documentation.

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

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

8.9.3.3 Encryption

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

-
1. Some wireless devices, such as scanners, can detect WiFi networks but cannot use WiFi networks. These kinds of wireless devices might not have MAC addresses.
 2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of authentication. (See [Section 8.9.3.3 on page 145](#) for information about this.)

Table 49 Types of Encryption for Each Type of Authentication

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

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

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

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

8.9.4 Signal Problems

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

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

8.9.5 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Zyxel Device's MBSSID (Multiple Basic Service Set Identifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

8.9.5.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

8.9.6 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.

8.9.6.1 Push Button Configuration

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

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

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

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the Zyxel Device, see [Section 8.5 on page 134](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the Zyxel Device you must press the **WiFi** button for more than 5 seconds.
- 4 Within 2 minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

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

8.9.6.2 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.

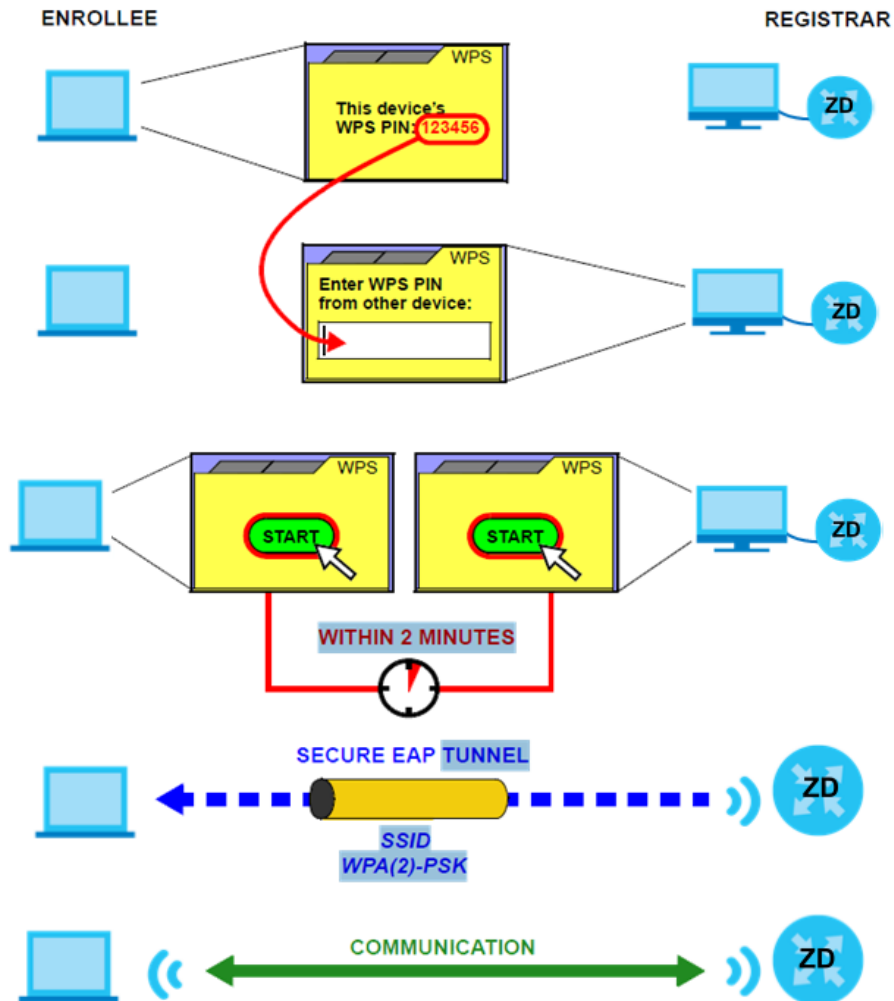
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 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 134](#)).
- 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 78 Example WPS Process: PIN Method

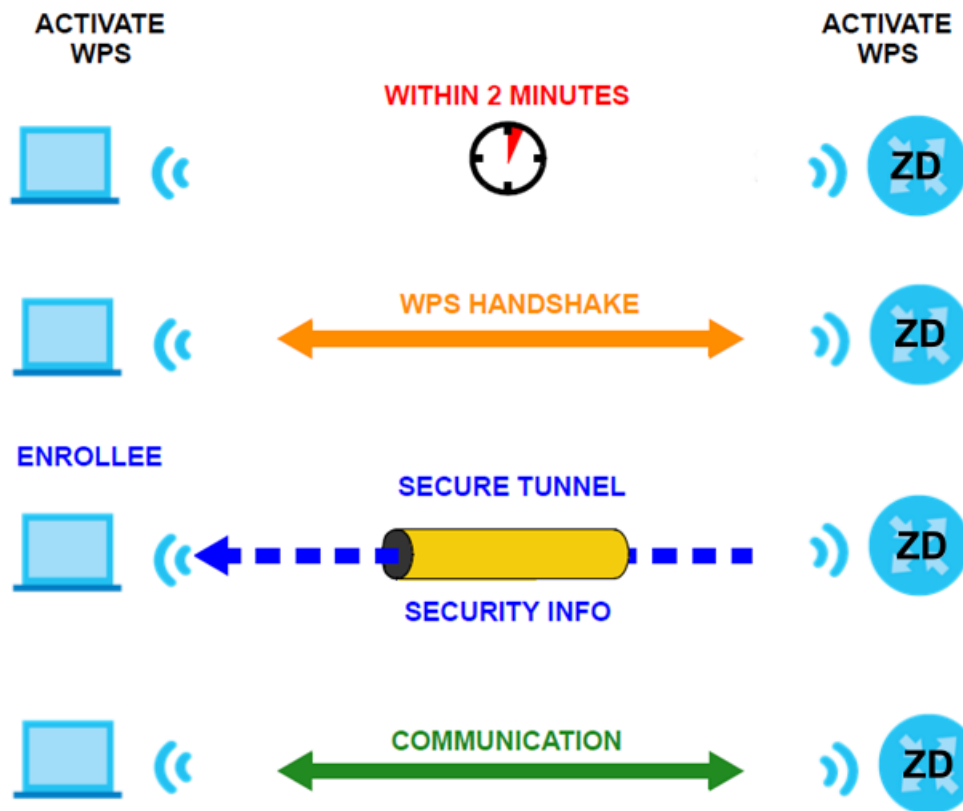


8.9.6.3 How WPS Works

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 79 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.

8.9.6.4 Example WPS Network Setup

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

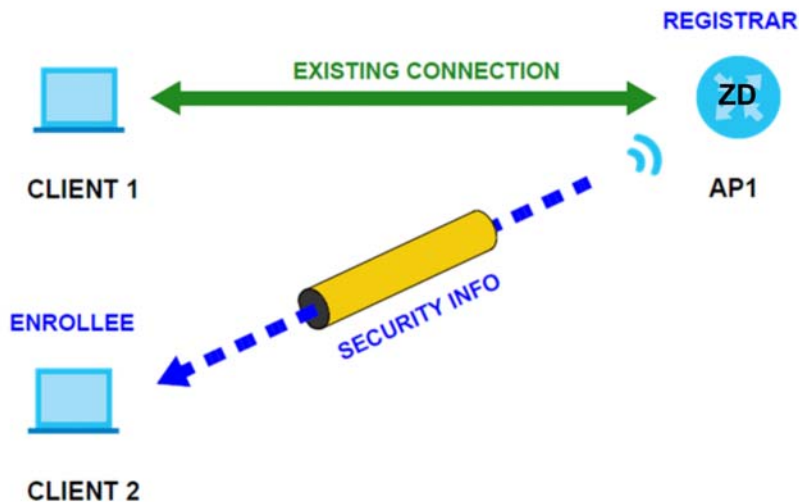
The following figure shows a sample network. In step 1, both **AP1** and **Client 1** are un-configured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 80 WPS: Example Network Step 1



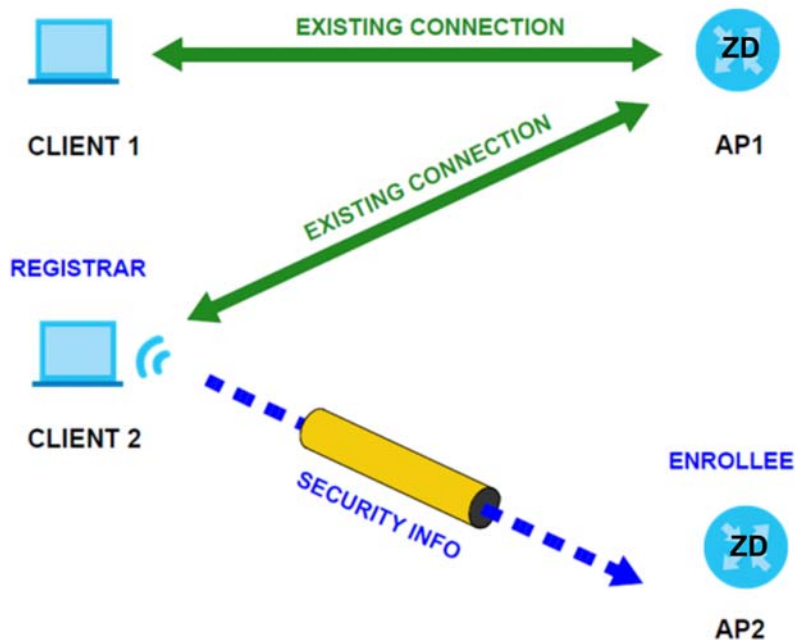
In step 2, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 81 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 82 WPS: Example Network Step 3



8.9.6.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

CHAPTER 9

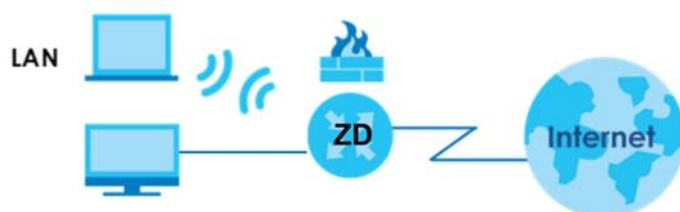
Home Networking

9.1 Overview

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

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

Figure 83 Home Networking Example



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 154](#)).
- 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 159](#)).
- Use the **UPnP** screen to enable UPnP ([Section 9.4 on page 161](#)).

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 Zykel 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 Zykel Device unless you are instructed to do otherwise.

DHCP

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

DNS

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

9.1.2.2 About UPnP

How do I know if I am using UPnP?

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

Cautions with UPnP

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

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

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

UPnP and Zyxel

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

See [Section on page 165](#) for examples on installing and using UPnP.

9.2 LAN Setup

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

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

Follow these steps to configure your LAN settings.

- 1** Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your Zyxel Device.
- 2** Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
- 3** Click **Apply** to save your settings.

Figure 84 Network Setting > Home Networking > LAN Setup

The LAN IP address is the IP address you use to log into the web configurator. The DHCP server settings define the rules on how to assign IP addresses to the LAN clients on your network.

Interface Group
 Group Name:

LAN IP Setup
 IP Address:
 Subnet Mask:

DHCP Server State
 DHCP: Enable Disable DHCP Relay

IP Addressing Values
 Beginning IP Address:
 Ending IP Address:
 Auto reserve IP for the same host:

DHCP Server Lease Time
 days hours minutes

DNS Values
 DNS: DNS Proxy Static From ISP

LAN IPv6 Mode Setup
 IPv6 Active:

Link Local Address Type
 EUI64
 Manual

LAN Global Identifier Type
 EUI64
 Manual

LAN IPv6 Prefix Setup
 Delegate prefix from WAN
 Static

LAN IPv6 Address Assign Setup

LAN IPv6 DNS Assign Setup

DHCPv6 Configuration
 DHCPv6 Active: DHCPv6 Server:

IPv6 Router Advertisement State
 RAdvD Active: Enable:

IPv6 DNS Values
 IPv6 DNS Server 1:
 IPv6 DNS Server 2:
 IPv6 DNS Server 3:

DNS Query Scenario

The following table describes the fields in this screen.

Table 50 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	This displays the name of the group that your Zyxel Device belongs to.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	<p>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.</p> <p>If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN.</p> <p>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.</p> <p>When DHCP is used, the following fields need to be set:</p>
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
Days/Hours/Minutes	DHCP server leases an address to a new device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different device.
DNS Values	
DNS	<p>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.</p> <p>Select From ISP if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).</p> <p>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.</p> <p>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.</p>
LAN IPv6 Mode Setup	
IPv6 Active	<p>Use this field to Enable or Disable IPv6 activation on the Zyxel Device.</p> <p>When IPv6 activation is used, the following fields need to be set.</p>

Table 50 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION						
Link Local Address Type	<p>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.</p> <p>Link-local Unicast Address Format</p> <table border="1" data-bbox="532 491 1062 562"> <tr> <td data-bbox="532 491 732 527">1111 1110 10</td> <td data-bbox="732 491 862 527">0</td> <td data-bbox="862 491 1062 527">Interface ID</td> </tr> <tr> <td data-bbox="532 527 732 562">10 bits</td> <td data-bbox="732 527 862 562">54 bits</td> <td data-bbox="862 527 1062 562">64 bits</td> </tr> </table>	1111 1110 10	0	Interface ID	10 bits	54 bits	64 bits
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	<p>Select how you want to obtain an IPv6 address:</p> <p>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.</p> <p>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.</p>						
LAN IPv6 DNS Assign Setup	<p>Select how the Zyxel Device provide DNS server and domain name information to the clients:</p> <p>From Router Advertisement: The Zyxel Device provides DNS information through router advertisements.</p> <p>From DHCPv6 Server: The Zyxel Device provides DNS information through DHCPv6.</p> <p>From RA & DHCPv6 Server: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.</p>						
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 DNS Values							

Table 50 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
IPv6 DNS Server 1 – 3	<p>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.</p> <p>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.</p> <p>From ISP – Select this if your ISP dynamically assigns IPv6 DNS server information.</p> <p>Proxy – Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.</p> <p>Otherwise, select None if you do not want to configure IPv6 DNS servers.</p>
DNS Query Scenario	<p>Select how the Zyxel Device handles clients' DNS information requests.</p> <p>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.</p> <p>IPv6 DNS Server Only: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives.</p> <p>IPv4 DNS Server Only: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives.</p> <p>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.</p> <p>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.</p>
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.

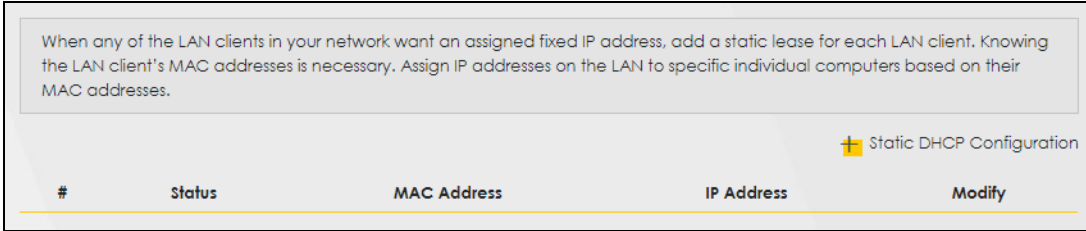
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

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 85 Network Setting > Home Networking > Static DHCP



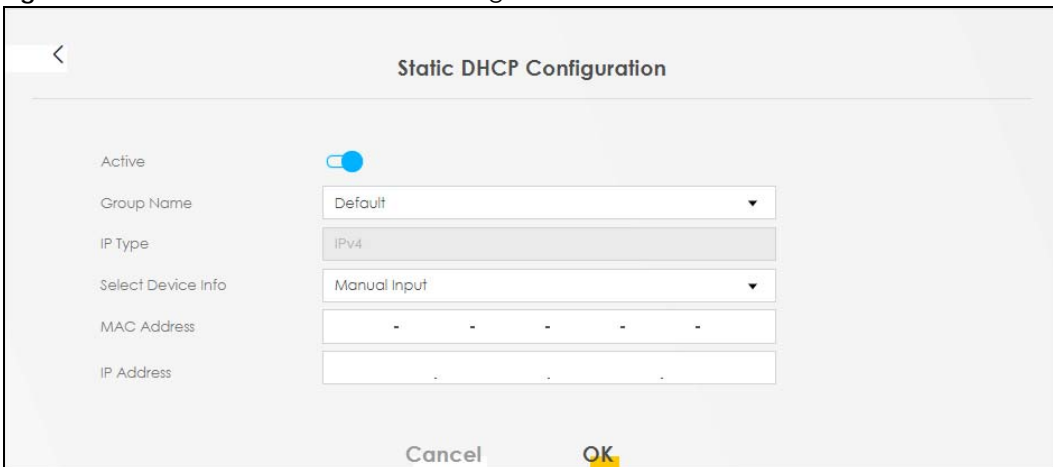
The following table describes the labels in this screen.

Table 51 Network Setting > Home Networking > Static DHCP

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

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

Figure 86 Static DHCP: Static DHCP Configuration



The following table describes the labels in this screen.

Table 52 Static DHCP: Static DHCP Configuration

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

9.4 UPnP

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

See [Section on page 165](#) 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 87 Network Setting > Home Networking > UPnP

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

UPnP State

UPnP

UPnP NAT-T State

UPnP NAT-T

Note
UPnP NAT-T only works when NAT is enable

#	Description	Destination IP Address	External Port	Internal Port	Protocol
<input type="button" value="Cancel"/> <input checked="" type="button" value="Apply"/>					

The following table describes the labels in this screen.

Table 53 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.

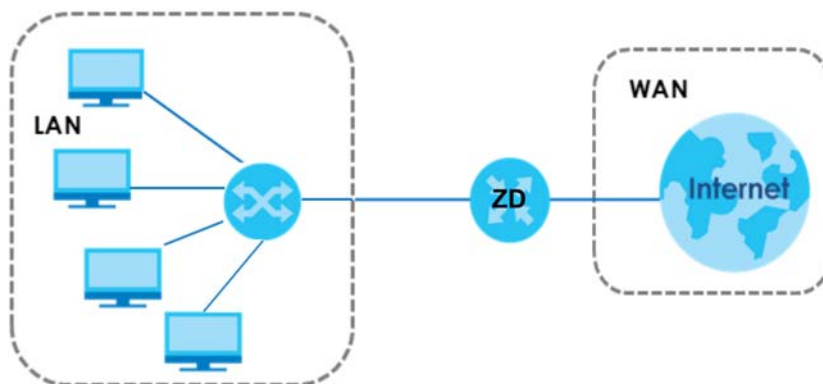
9.5 Technical Reference

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

LANs, WANs and the Zyxel Device

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

Figure 88 LAN and WAN IP Addresses



9.5.1 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.

9.5.2 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.

9.5.3 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.

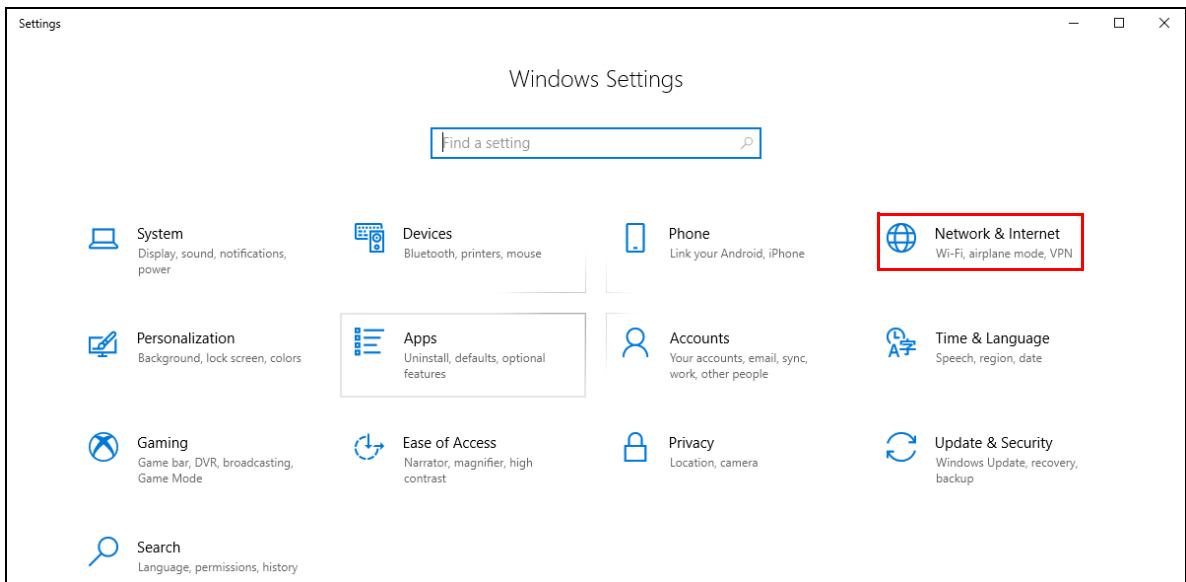
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

9.6 Turn on UPnP in Windows 10 Example

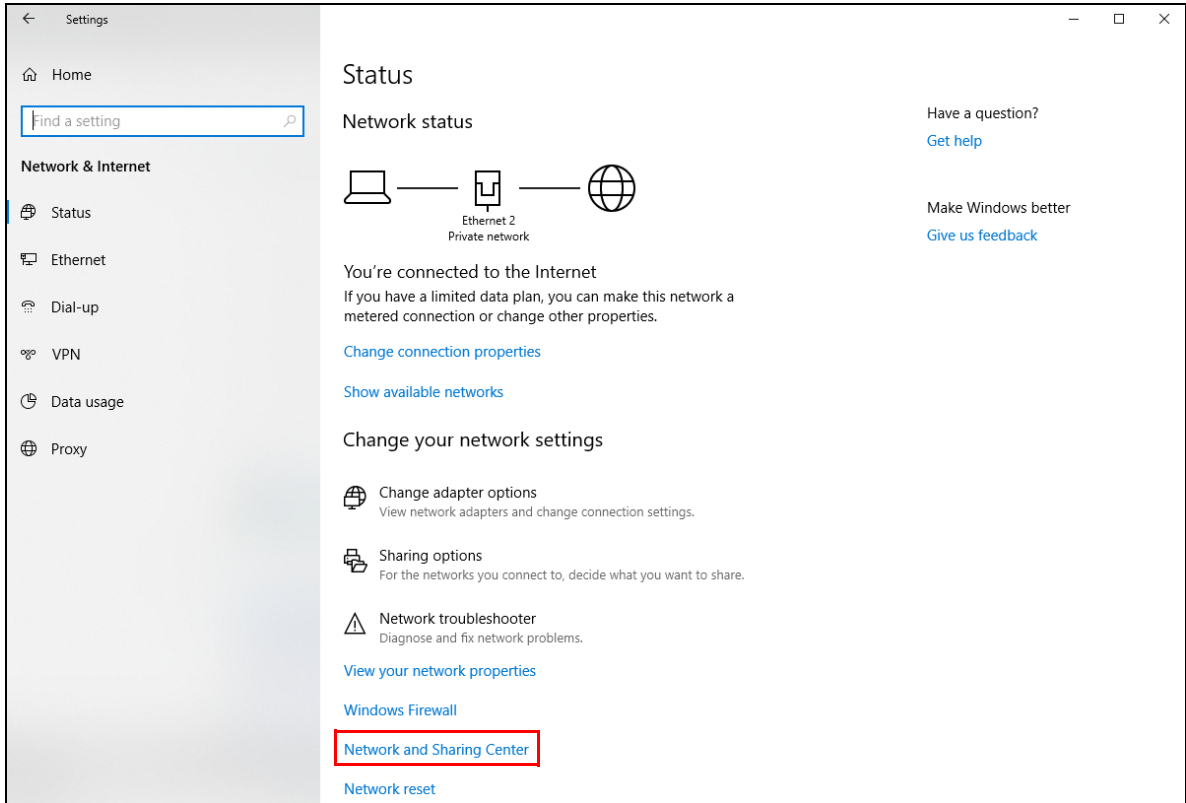
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting** > **Home Networking** > **UPnP**.

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

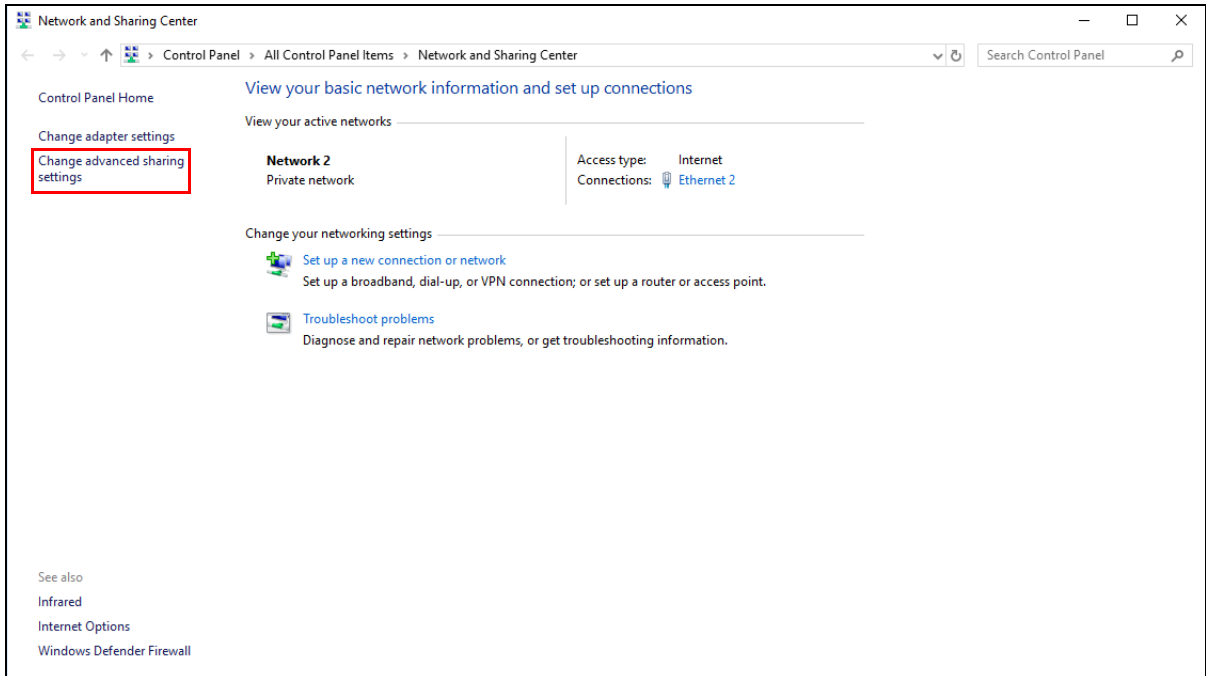
- 1 Click the start icon, **Settings** and then **Network & Internet**.



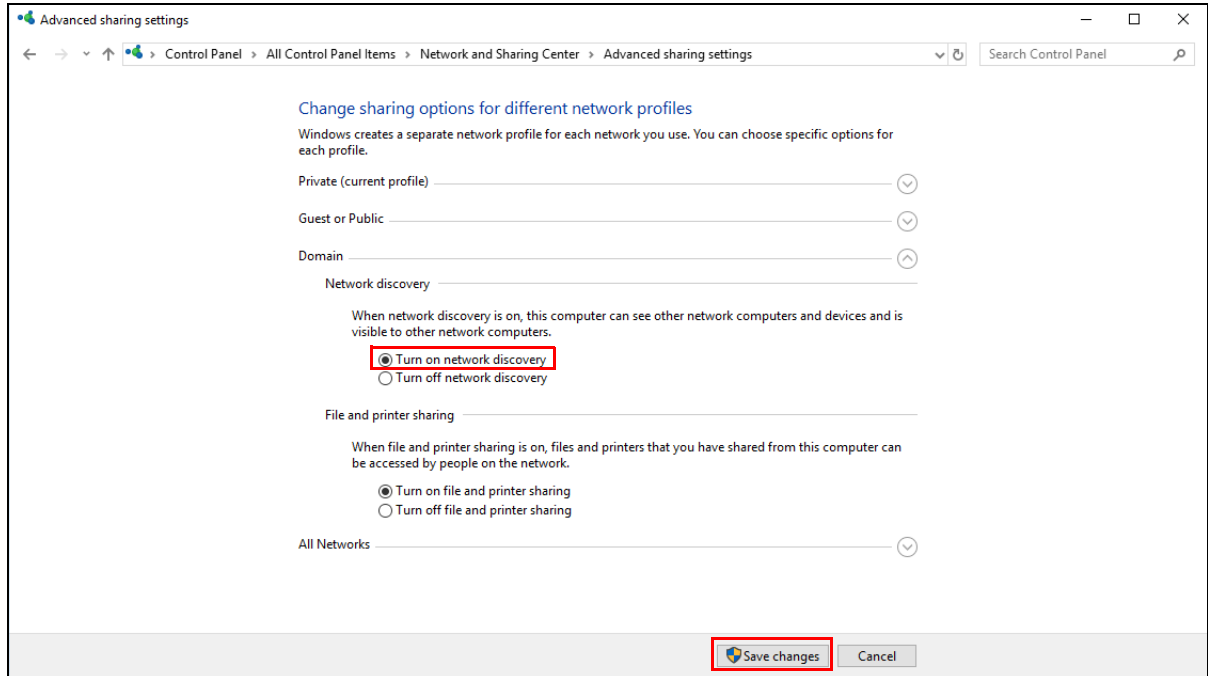
- 2 Click **Network and Sharing Center**.



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.



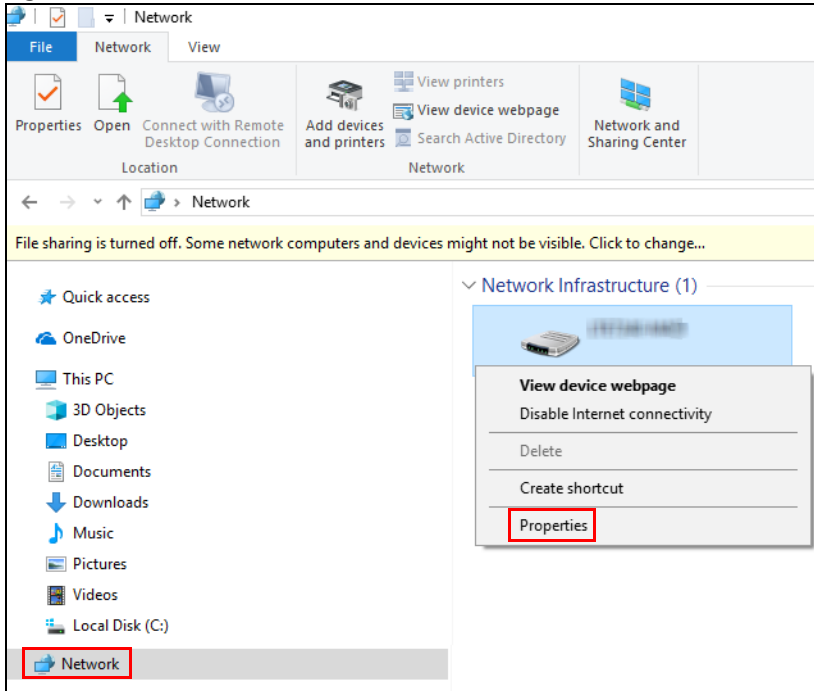
9.6.1 Auto-discover Your UPnP-enabled Network Device

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

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

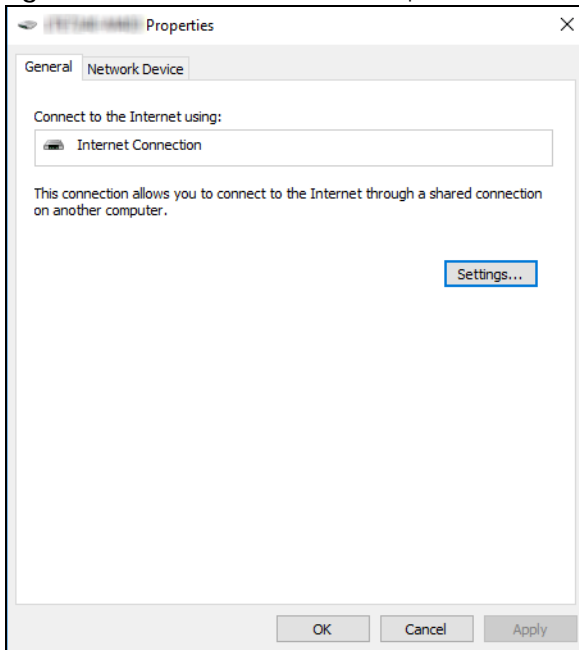
- 1 Open **File Explorer** and click **Network**.
- 2 Right-click the Zyxel Device icon and select **Properties**.

Figure 89 Network Connections

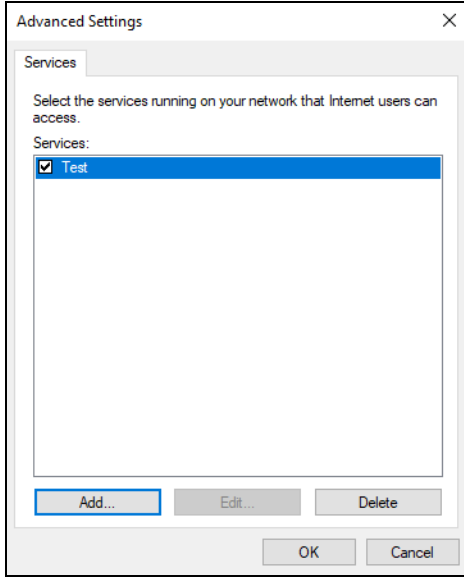
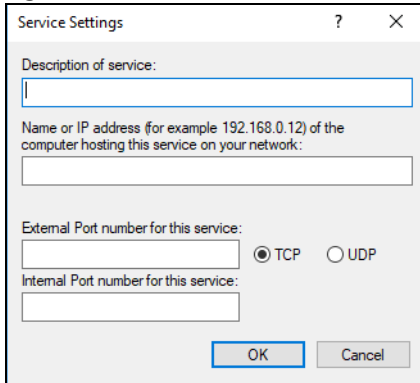


- 3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 90 Internet Connection Properties

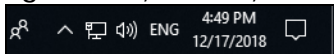


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 91 Internet Connection Properties: Advanced Settings**Figure 92** Internet Connection Properties: Advanced Settings: Add

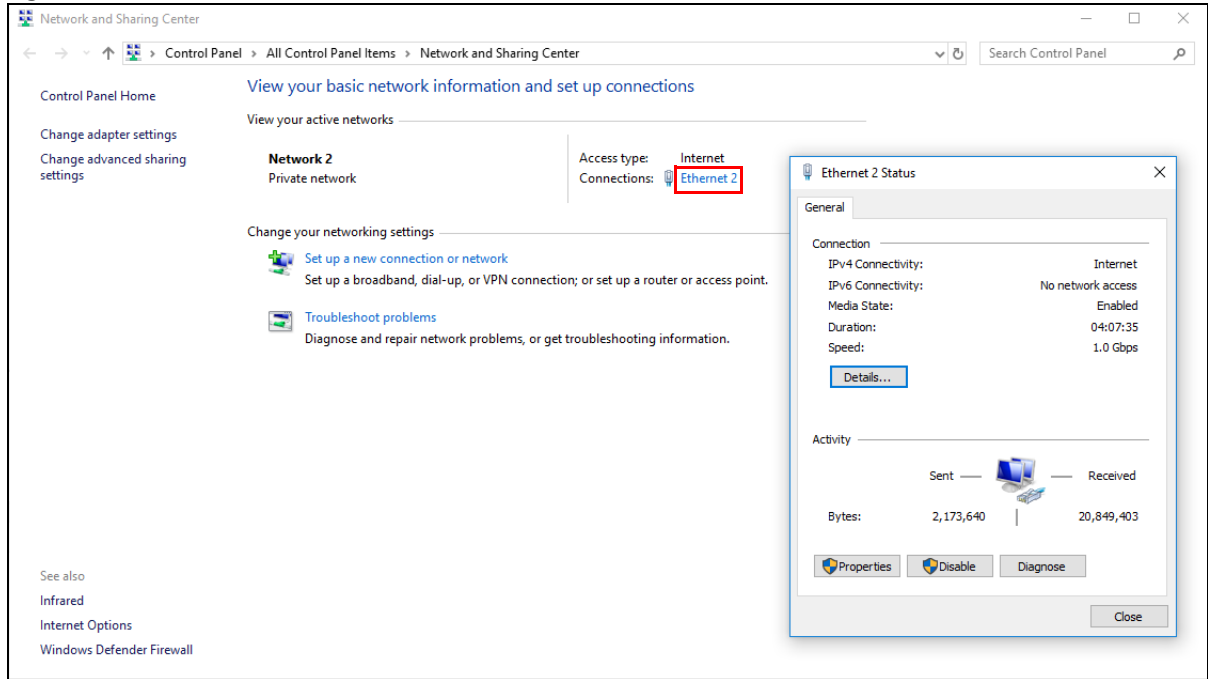
Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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

Figure 93 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 94 Internet Connection Status

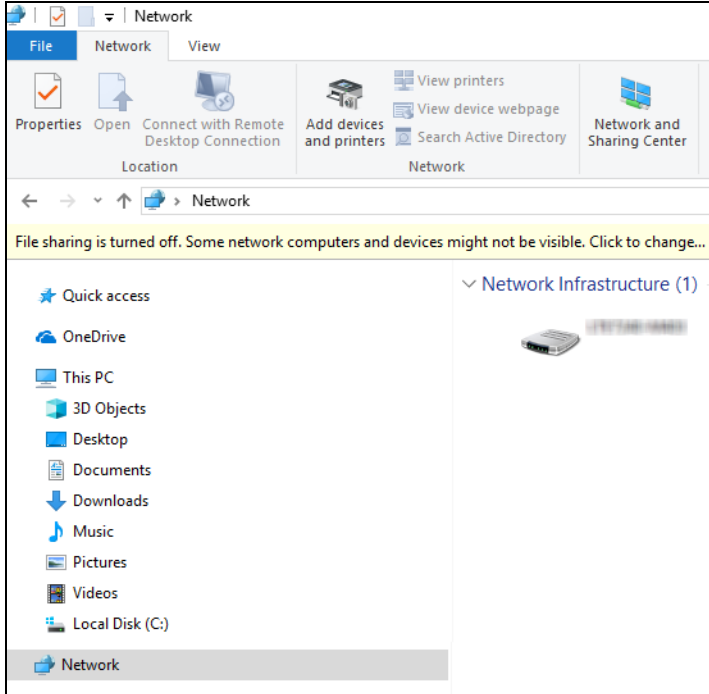


9.7 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

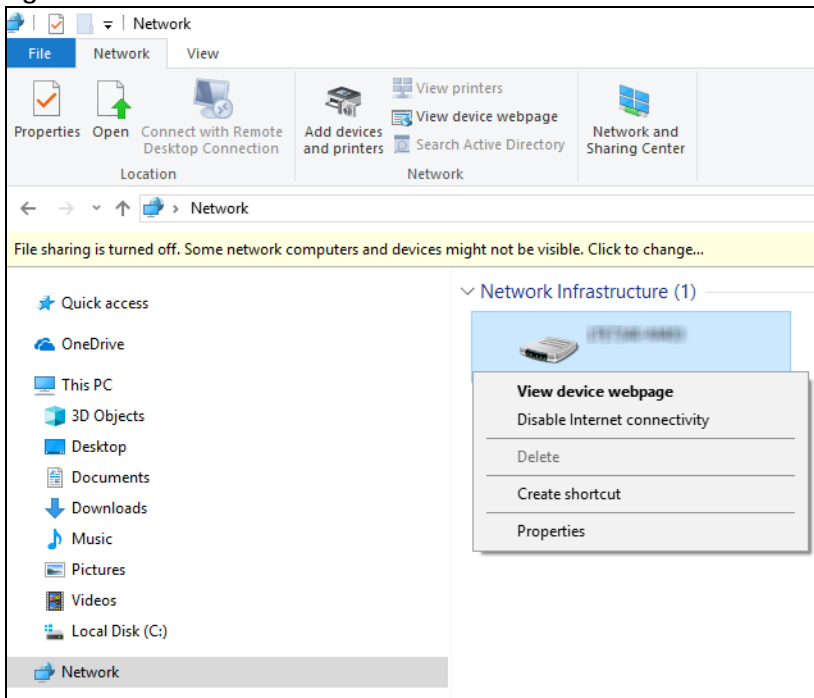
- 1 Open **File Explorer**.
- 2 Click **Network**.

Figure 95 Network Connections

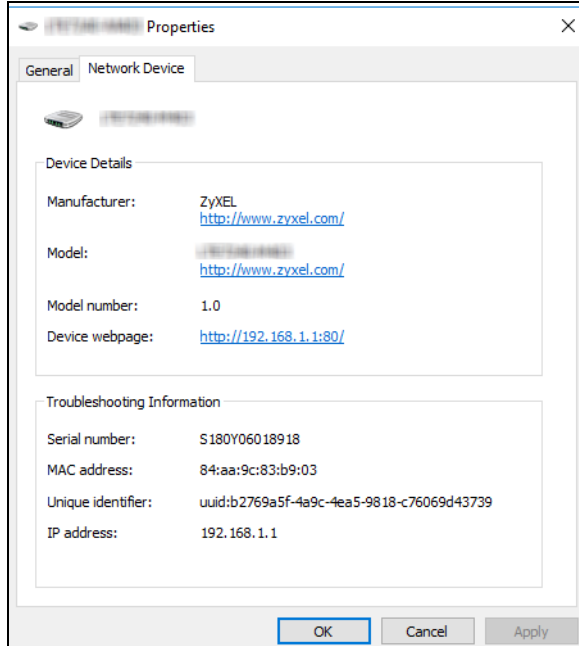


- 3 An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.
- 4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

Figure 96 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 97 Network Connections: Network Infrastructure: Properties: Example

9.7.1 DHCP Setup

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

IP Pool Setup

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

9.7.2 DNS Server Addresses

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

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

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

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

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

9.7.3 LAN TCP/IP

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

IP Address and Subnet Mask

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

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

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

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

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

Private IP Addresses

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

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

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

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

CHAPTER 10

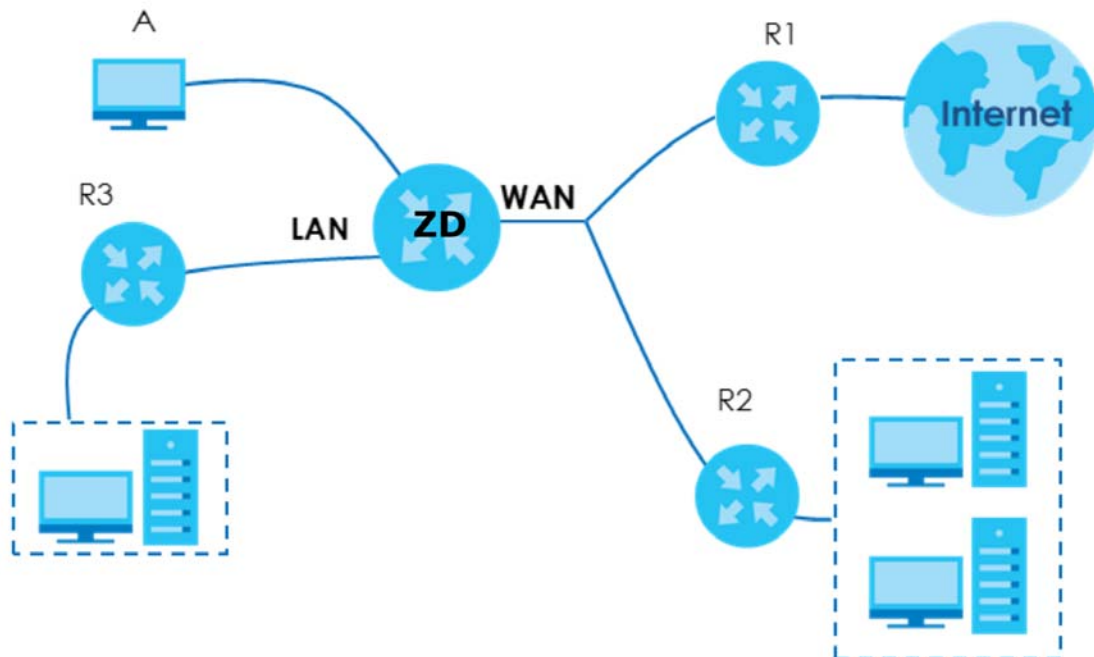
Routing

10.1 Overview

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

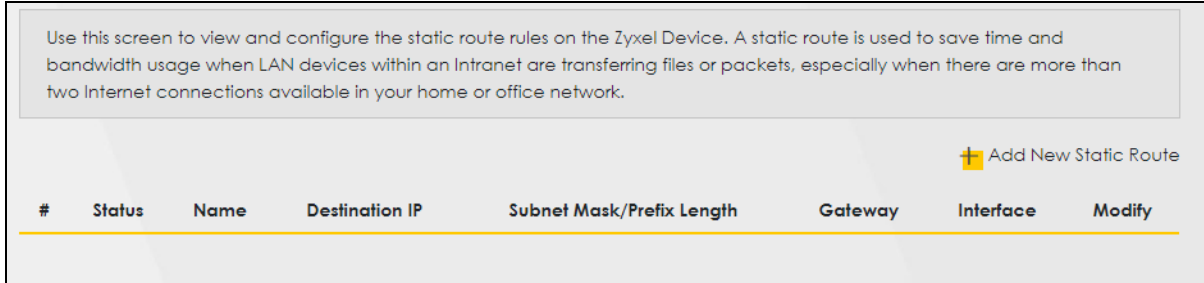
For example, the next figure shows a computer (**A**) connected to the Zyxel Device's LAN interface. The Zyxel Device routes most traffic from **A** to the Internet through the Zyxel Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router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

Figure 98 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 99 Network Setting > Routing > Static Route

The following table describes the labels in this screen.

Table 54 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 100 Network Setting > Routing > Static Route > Add New Static Route

The following table describes the labels in this screen.

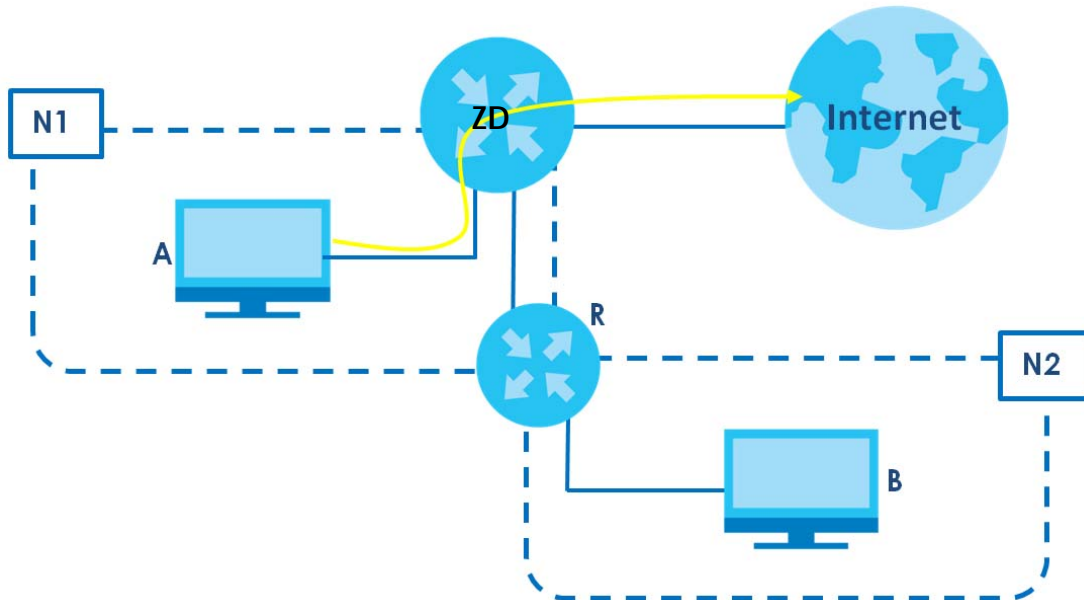
Table 55 Network Setting > Routing > Static Route > Add New Static Route

LABEL	DESCRIPTION
Active	Select Enable to activate your static route.
Route Name	Assign a name for your static route (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign (\$) vertical bar () ampersand (&) semicolon (;)
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10 ³⁸ IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.
User Interface	You can decide if you want to forward packets to a gateway IP address (Default) or a bound interface (Cellular WAN). If you want to configure bound interface, choose an interface through which the traffic is sent. You must have the WAN interfaces already configured in the Broadband screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

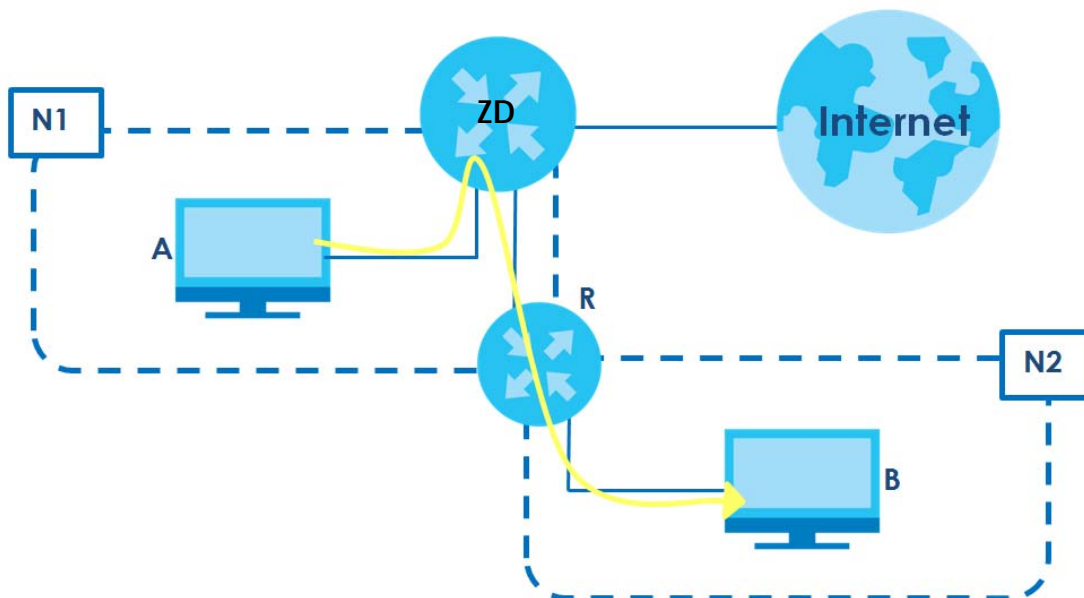
10.2.1.1 An Example of Adding a Static Route

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

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



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



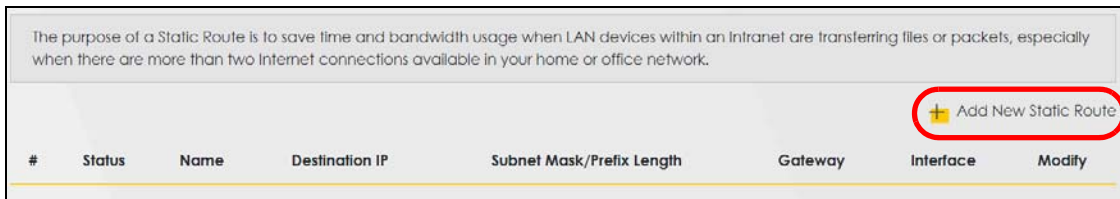
This tutorial uses the following example IP settings:

Table 56 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	192.168.1.1
IP Type	IPv4
Use Interface	VDSL
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 in advanced mode.
- 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:
 - 4a 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**.
 - 4b Set **IP Type** to **IPv4**.
 - 4c Type the **Destination IP Address 192.168.10.0** and **IP Subnet Mask 255.255.255.0** for the destination, **N2**.
 - 4d Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right () , the function is enabled. Type **192.168.1.253** (**R's N1** address) in the **Gateway IP Address** field.
 - 4e Select **VDSL** as the **Use Interface**.
 - 4f 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 101 Network Setting > Routing > DNS Route

The following table describes the labels in this screen.

Table 57 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.

Table 57 Network Setting > Routing > DNS Route (continued)

LABEL	DESCRIPTION
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 102 Network Setting > Routing > DNS Route > Add New DNS Route

The following table describes the labels in this screen.

Table 58 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 the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Zyxel Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
Subnet Mask	Type the subnet mask of the network for which to use the DNS route in dotted decimal notation, for example 255.255.255.255.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interfaces already configured in the Broadband screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

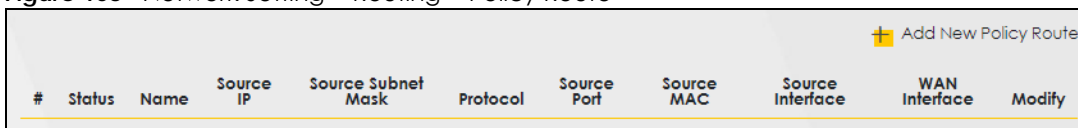
10.4 Policy Route

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 103 Network Setting > Routing > 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 59 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 104 Network Setting > Routing > Policy Route: Add or Edit

The following table describes the labels in this screen.

Table 60 Policy Route: Add or Edit

LABEL	DESCRIPTION
Active	Click this to enable (turns blue) activation of the policy route. Otherwise, click to disable (turns gray).
Route Name	Enter a descriptive name of up to eight printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (TCP , UDP , or None).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (example: br0 or LAN1 – LAN4)	Type the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interfaces already configured in the Broadband screens.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

10.5 RIP Overview

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

10.5.1 RIP

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

Figure 105 Network Setting > Routing > RIP

Static Route | DNS Route | Policy Route | **RIP**

To activate RIP for the WAN interface, select the desired RIP version and operation and place a check in the Enabled checkbox. To stop RIP on the WAN Interface, uncheck the Enabled checkbox. Click the Apply button to start/stop RIP and save the configuration.

#	Interface	Version	Operation	Enable	Disable Default Gateway
1	Cellular WAN	RIPv2	Active	<input type="checkbox"/>	<input type="checkbox"/>
2	ETHWAN	RIPv2	Active	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Apply

The following table describes the labels in this screen.

Table 61 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). RIPv1 is universally supported but RIPv2 carries more information. RIPv1 is probably adequate for most networks, unless you have an unusual network topology. When set to Both , the Zyxel Device will broadcast its routing table periodically and incorporate the RIP information that it receives
Operation	Select Passive to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select Active to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the check box to activate the settings.
Disable Default Gateway	Select the check box to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes back to the Zyxel Device.

CHAPTER 11

Network Address Translation (NAT)

11.1 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 186](#)).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings ([Section 11.3 on page 189](#)).
- Use the **DMZ** screen to configure a default server ([Section 11.4 on page 192](#)).
- Use the **ALG** screen to enable or disable the SIP ALG ([Section 11.5 on page 193](#)).

11.1.2 What You Need To Know

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

Inside/Outside and Global/Local

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

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

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

11.2 Port Forwarding

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

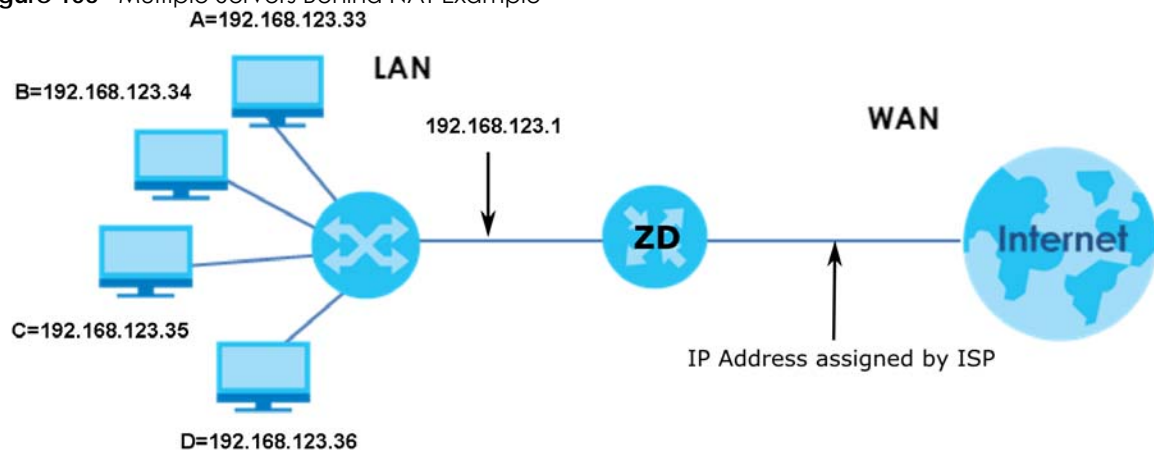
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more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

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

Configure Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example), a default server IP address of 192.168.1.35 to a third (**C** in the example), and a default server IP address of 192.168.1.36 to a fourth (**D** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 106 Multiple Servers Behind NAT Example

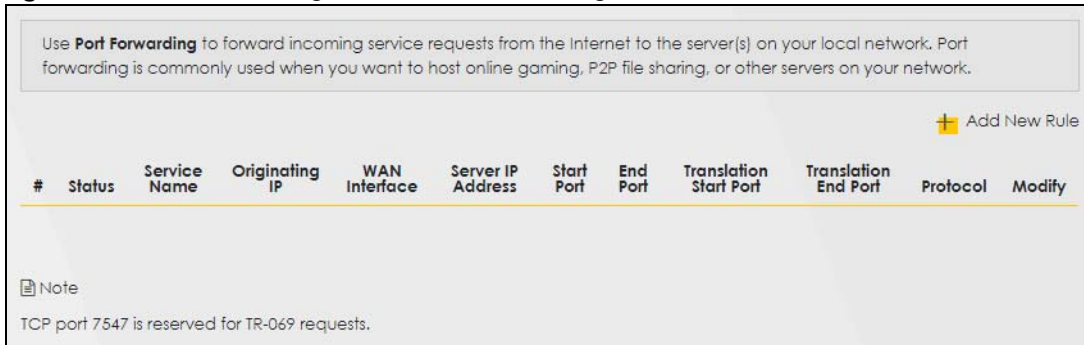


11.2.1 Port Forwarding

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

Note: TCP port 7547 is reserved for system use.

Figure 107 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
<p>Note</p> <p>TCP port 7547 is reserved for TR-069 requests.</p>											

The following table describes the fields in this screen.

Table 62 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 108 Network Setting > NAT > Port Forwarding: Add or Edit

Add New Rule

Active

Service Name

WAN Interface

Start Port

End Port

Translation Start Port

Translation End Port

Server IP Address

Configure Originating IP Enable

Originating IP

Protocol

Note

(1) Create or edit a port forwarding rule. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule.

(2) To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

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

Cancel OK

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 63 Network Setting > NAT > Port Forwarding: Add or Edit

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

Table 63 Network Setting > NAT > Port Forwarding: Add or Edit (continued)

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

11.3 Port Triggering

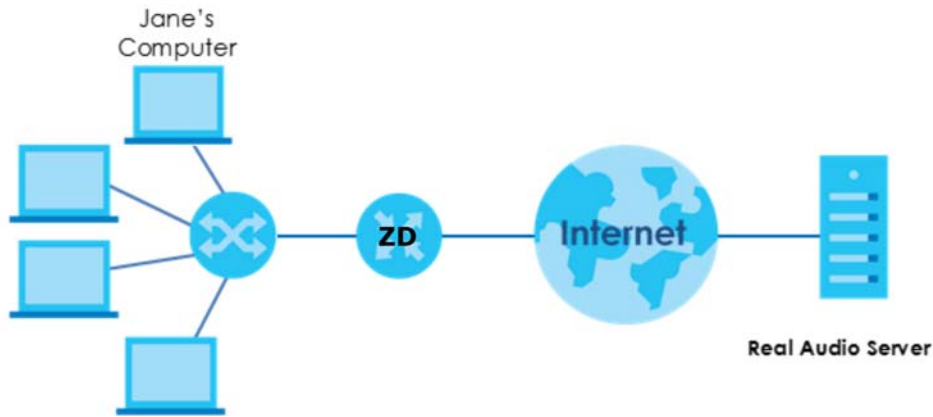
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 109 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 Zykel Device to record Jane's computer IP address. The Zykel 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 Zykel 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 Zykel 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 Zykel 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 110 Network Setting > NAT > Port Triggering

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Protocol	Modify
+ Add New Rule										

The following table describes the labels in this screen.

Table 64 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.

Table 64 Network Setting > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Protocol	This is the open transport layer protocol.
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

11.3.1 Add or Edit Port Triggering Rule

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

Figure 111 Network Setting > NAT > Port Triggering: Add or Edit

The screenshot displays the 'Add New Rule' configuration interface. It features a list of settings on the left and corresponding input fields on the right. The 'Active' setting is a toggle switch that is currently turned on. The 'Service Name' is a text input field. The 'WAN Interface' is a dropdown menu with 'Default' selected. The 'Trigger Start Port' and 'Trigger End Port' are text input fields. The 'Trigger Protocol' is a dropdown menu with 'TCP' selected. The 'Open Start Port' and 'Open End Port' are text input fields. The 'Open Protocol' is a dropdown menu with 'TCP' selected. At the bottom of the screen, there are two buttons: 'Cancel' and 'OK'.

The following table describes the labels in this screen.

Table 65 Network Setting > NAT > Port Triggering: Add or Edit

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

11.4 DMZ

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

You can put public servers, such as email, web, and FTP servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host. Click **Network Setting > NAT > DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address of the default server in the **Default Server Address** field, and click **Apply** to activate the DMZ host. Otherwise, clear the IP address in the **Default Server Address** field, and click **Apply** to deactivate the DMZ host.

Figure 112 Network Setting > NAT > DMZ

NAT

Port Forwarding | Port Triggering | **DMZ** | ALG | Address Mapping | Sessions

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

You can put public servers, such as email, web, and FTP servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host.

Default Server Address 0 . 0 . 0 . 0

Note

Enter the IP address of the default server in the **Default Server Address** field, and click **Apply** to activate the DMZ host. Otherwise, clear the IP address in the **Default Server Address** field, and click **Apply** to deactivate the DMZ host.

Cancel **Apply**

The following table describes the fields in this screen.

Table 66 Network Setting > NAT > DMZ

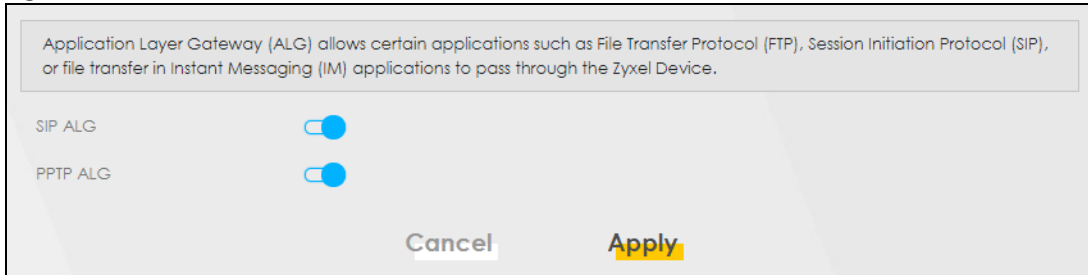
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the Port Forwarding screen. Note: If you do not assign a default server, the Zyxel Device discards all packets received for ports not specified in the virtual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

11.5 ALG

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

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

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

Figure 113 Network Setting > NAT > ALG

The following table describes the fields in this screen.

Table 67 Network Setting > NAT > ALG

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

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 68 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

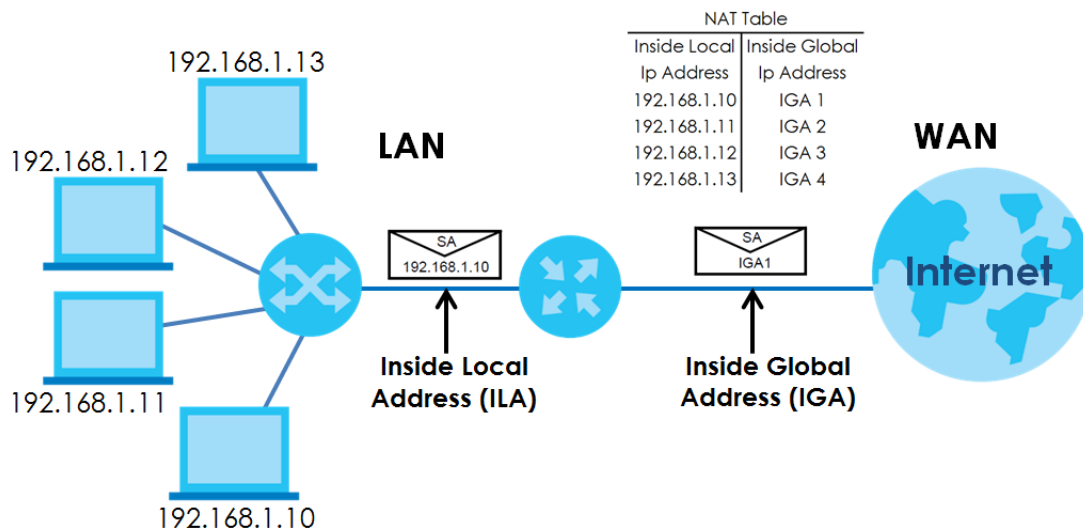
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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.

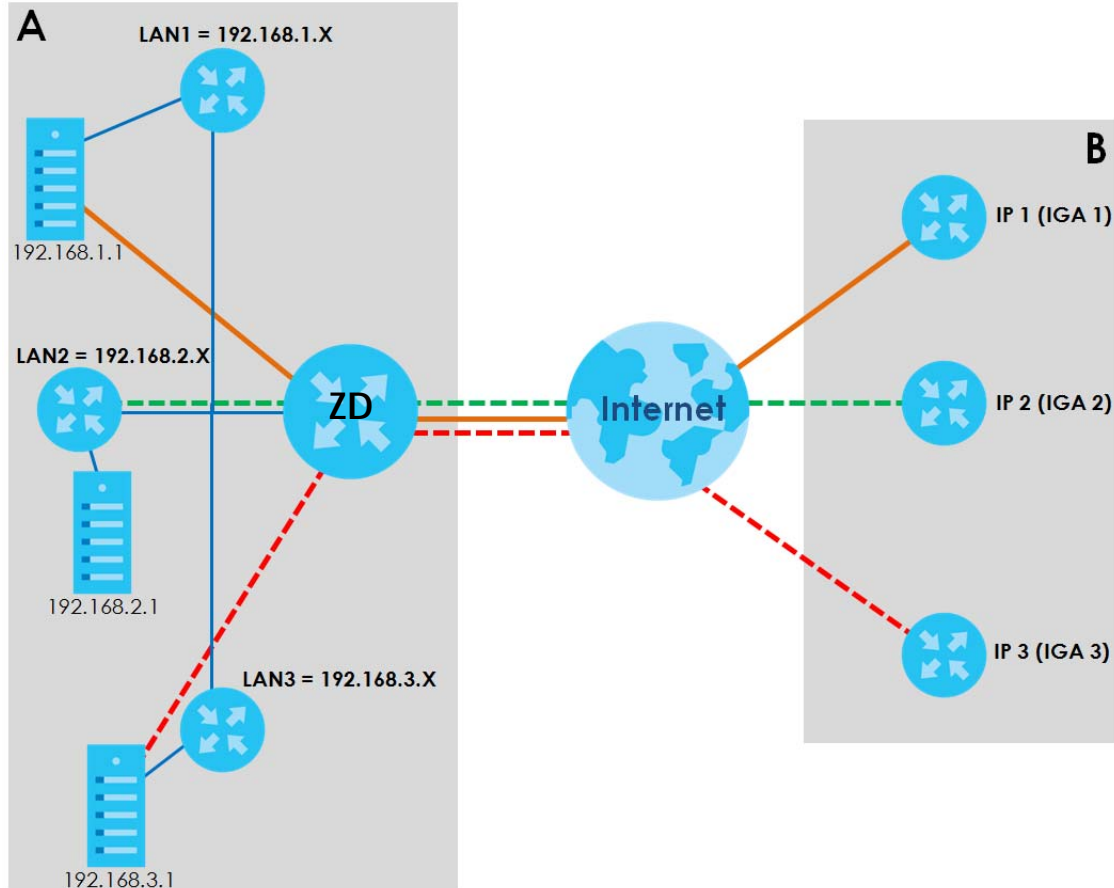
Figure 114 How NAT Works



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 115 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 69 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119

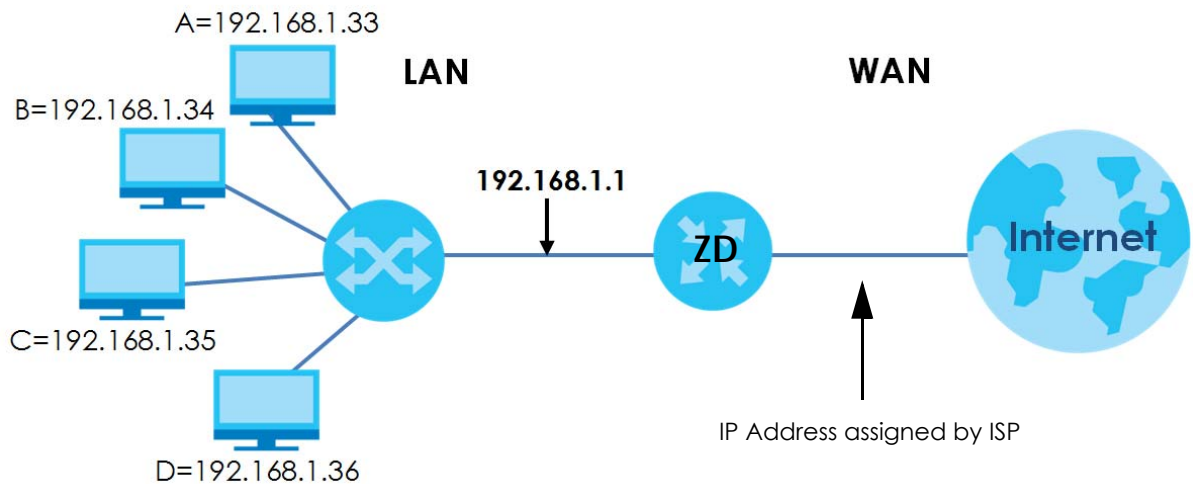
Table 69 Services and Port Numbers

SERVICES	PORT NUMBER
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

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

Figure 116 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.

Note: For information on configuring DNS route, see [Chapter 10 on page 175](#).

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they do not know your IP address.

You first need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ([Section 12.2 on page 199](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device ([Section 12.3 on page 200](#)).

12.1.2 What You Need To Know

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

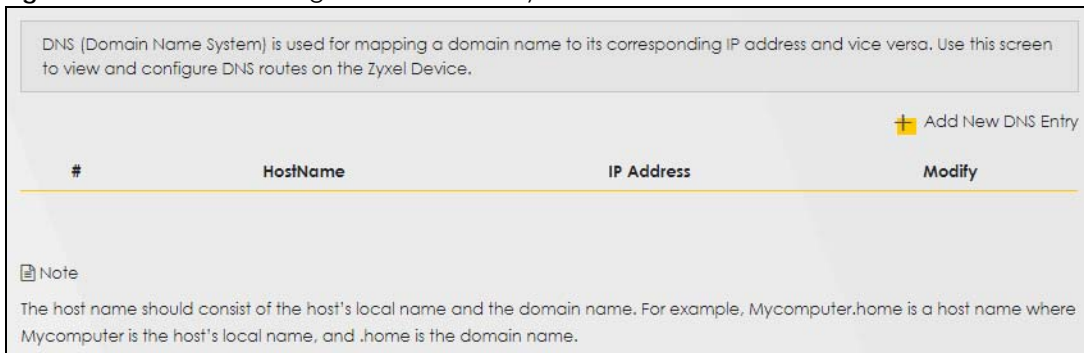
If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 DNS Entry

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure manual DNS entries 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 117 Network Setting > DNS > DNS Entry



The following table describes the fields in this screen.

Table 70 Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
HostName	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule.

12.2.1 Add or Edit DNS Entry

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

Figure 118 Network Setting > DNS > DNS Entry: Add or Edit

The following table describes the labels in this screen.

Table 71 Network Setting > DNS > DNS Entry: Add or Edit

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

12.3 Dynamic DNS

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Configure a DDNS service provider on your Zyxel Device. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 119 Network Setting > DNS > Dynamic DNS

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

Dynamic DNS Setup

Dynamic DNS Enable Disable (Settings are invalid when disable)

Service Provider

Host Name

Username

Password

Enable Wildcard Option

Enable Off Line Option (Only applies to custom DNS)

Dynamic DNS Status

User Authentication Result

Last Updated Time

Current Dynamic IP

The following table describes the fields in this screen.

Table 72 Network Setting > DNS > Dynamic DNS

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

CHAPTER 13

VLAN Group

13.1 Overview

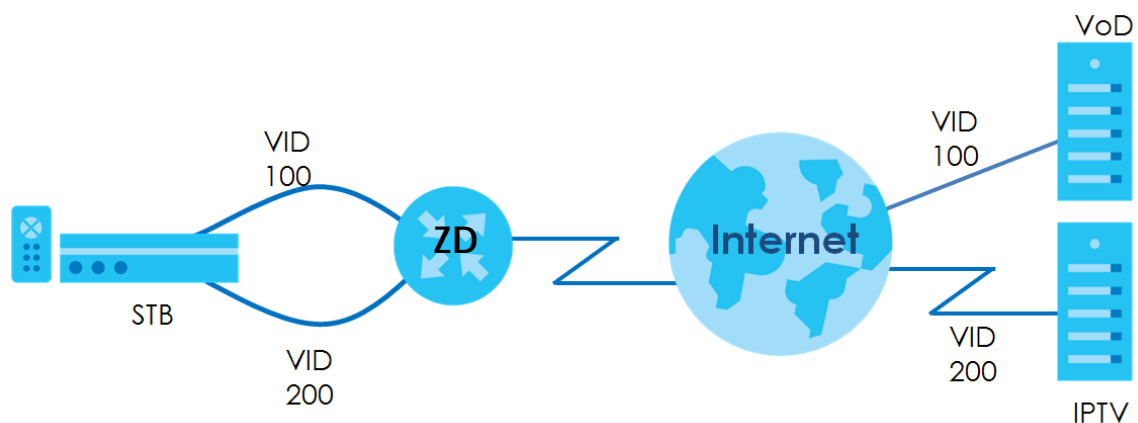
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same groups;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

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

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

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

Figure 120 VLAN Group Example



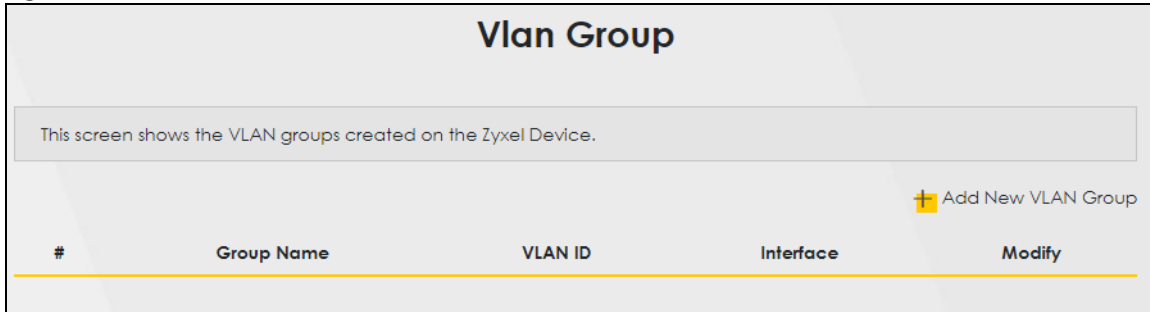
13.1.1 What You Can Do in this Chapter

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 121 Network Setting > VLAN Group



The following table describes the fields in this screen.

Table 73 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 122 Add or Edit VLAN Group

The screenshot shows a configuration screen titled "Add New VLAN Group". It features a back arrow in the top left corner. The main content area contains two input fields: "VLAN Group Name" and "VLAN ID". Below these are four rows, each corresponding to a LAN interface (LAN1, LAN2, LAN3, LAN4). Each row has two checkboxes: "Include" and "TX Tagging". At the bottom of the screen, there are two buttons: "Cancel" and "OK".

The following table describes the fields in this screen.

Table 74 Add or Edit VLAN Group

LABEL	DESCRIPTION
VLAN Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
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.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

CHAPTER 14

Interface Grouping

14.1 Interface Grouping Overview

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

14.1.1 What You Can Do in this Chapter

The **Interface Grouping** screen lets you create multiple networks on the Zyxel Device ([Section 14.2 on page 205](#)).

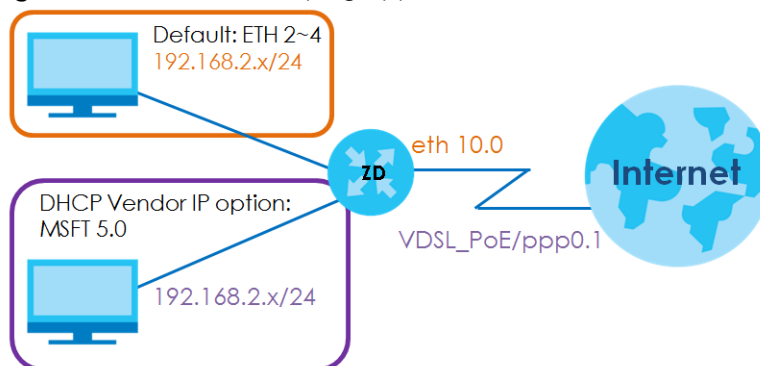
14.2 Interface Grouping

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 153](#) 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 123 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 124 Network Setting > Interface Grouping

Interface Grouping				
<p>Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.</p>				
				+ Add New Interface Group
Group Name	WAN Interface	LAN Interface	Criteria	Modify
Default	Any WAN	LAN1,ZyxeI_0CF3(*2.4G)		
APN2_VLAN123	Cellular WAN 2		VlanGroup: VLAN_123	 

The following table describes the fields in this screen.

Table 75 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.
Add	Click this button to create a new 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 125 Interface Group Configuration

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

Group Name

WAN Interfaces used in the grouping

Available LAN Interfaces **# Selected LAN Interfaces**

LAN1

Zyxel_B787(*2.4G)

Automatically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Modify

Note

(1) If a Vendor ID is configured for a specific client device, please REBOOT the client device attached to the router, to allow the client device to obtain an appropriate IP address.
(2) Total criteria rules can not add over than 15.

The following table describes the fields in this screen.

Table 76 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface. Select None to not add a WAN interface to this group.
Selected LAN Interfaces	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.
Available LAN Interfaces	To remove a LAN or wireless LAN interface from the Selected LAN Interfaces , use the right-facing arrow.

Table 76 Interface Group Configuration (continued)

LABEL	DESCRIPTION
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 208 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 126 Interface Grouping Criteria

The screenshot shows the 'Add new criteria' screen. It features a back arrow in the top left corner. The title is 'Add new criteria'. Under the 'Criteria' section, there are five radio button options: 'Source MAC address', 'DHCP option 60', 'DHCP option 61', 'DHCP option 125' (which is selected with a blue dot), and 'VLAN Group'. The 'DHCP option 125' option is expanded to show four input fields: 'Enterprise Number', 'Manufacture OUI', 'Serial Number', and 'Product Class'. At the bottom of the screen, there are two buttons: 'Cancel' and 'OK'.

Figure 127 Interface Grouping Criteria

The following table describes the fields in this screen.

Table 77 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first 3 bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

CHAPTER 15

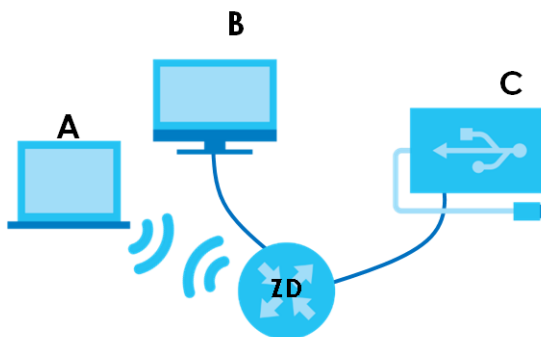
USB Service

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 128 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.

Note: This feature is only available on certain models. For details, see the features comparison table at [Section 1.1 on page 17](#).

15.1.1 What You Need To Know

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

15.1.1.1 About 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).

15.1.2 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 129 Network Setting > USB Service

USB Service

The modem 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
usb2_sda1	30111 MB	2705 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](#)

Note: The **Share Directory List** is only visible when you connect a USB device.

Each field is described in the following table.

Table 78 Network Setting > USB Service > File Sharing

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 or disable file sharing through the Zyxel Device. When the switch goes to the right , the function is enabled.
Share Directory List	
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.
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.

Table 78 Network Setting > USB Service > File Sharing (continued)

LABEL	DESCRIPTION
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. Also, spaces and the following special characters listed in the brackets [" < > ^ \$ | & ; \ / : * ?] are not allowed for the USB share name.

Figure 130 Network Setting > USB Service > File Sharing

The screenshot shows the 'Add New Share' configuration screen. It includes the following elements:

- Volume:** A dropdown menu showing 'usb1_sda1'.
- Share Path:** A text input field with a yellow 'Browse' button to its right.
- Description:** A text input field.
- Access Level:** A dropdown menu showing 'Security'.
- Allowed:** A checkbox that is currently unchecked.
- User Name:** A text input field containing 'admin'.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom.

The following table describes the labels in this menu.

Table 79 Network Setting > USB Service > File Sharing

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.
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 check box 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'll 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 27 on page 264](#), 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 1.1.2 on page 17](#) 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 131 Network Setting > Nebula

The screenshot shows the 'Nebula' configuration page. At the top, there is a title 'Nebula' and a grey box with the text: 'You can check nebula connectivity here and keep discovery protocol enabled if you want to monitor the status from nebula.' Below this is the 'Nebula Control Center Status' section, which contains two yellow status bars: 'Internet' with the message 'Can't get an IP from your DHCP server !' and 'Nebula Connectivity' with the message 'DNS queries failed'. The 'Nebula Control Center device Setting' section includes several options: 'Nebula Discovery' (checked), 'Use Proxy to Access NCC' (checked), 'Proxy Server' (empty text box with '(IP Address/FQDN)' hint), 'Proxy Port' (text box containing '3128' with '(1~65535)' hint), 'Authentication' (checked), 'User Name' (empty text box), and 'Password' (empty text box). At the bottom, there are 'Cancel' and 'Apply' buttons.

Each field is described in the following table.

Table 80 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.
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 Overview

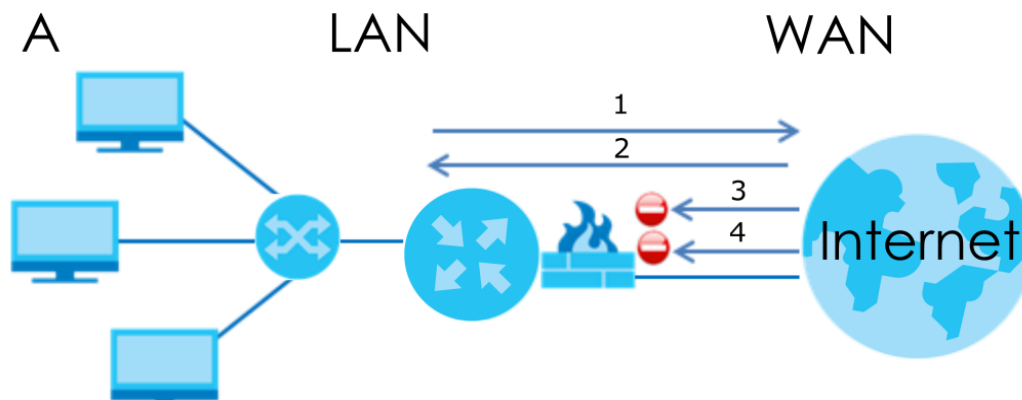
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- 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 132 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

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

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 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

17.2.1 What You Can Do in this Chapter

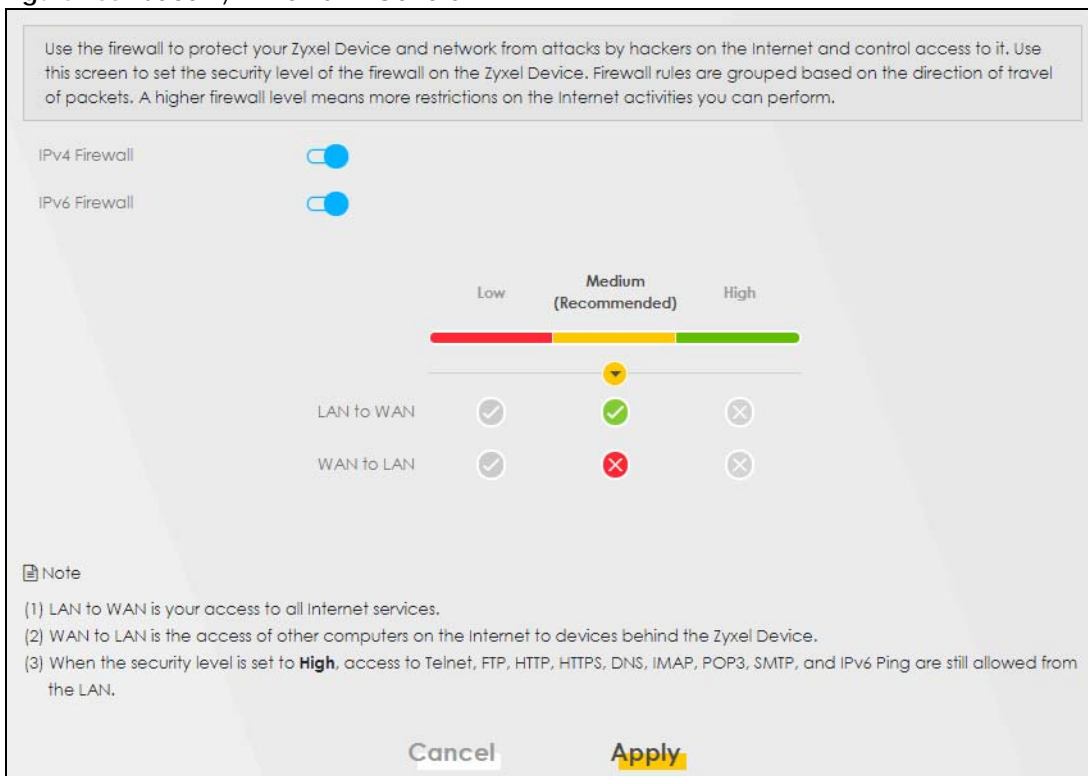
- Use the **General** screen to configure the security level of the firewall on the Zyxel Device ([Section 17.3 on page 219](#)).

- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 17.4 on page 220).
- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules (Section 17.5 on page 221).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 17.6 on page 225).

17.3 Firewall General Settings

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

Figure 133 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, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

The following table describes the labels in this screen.

Table 81 Security > Firewall > General

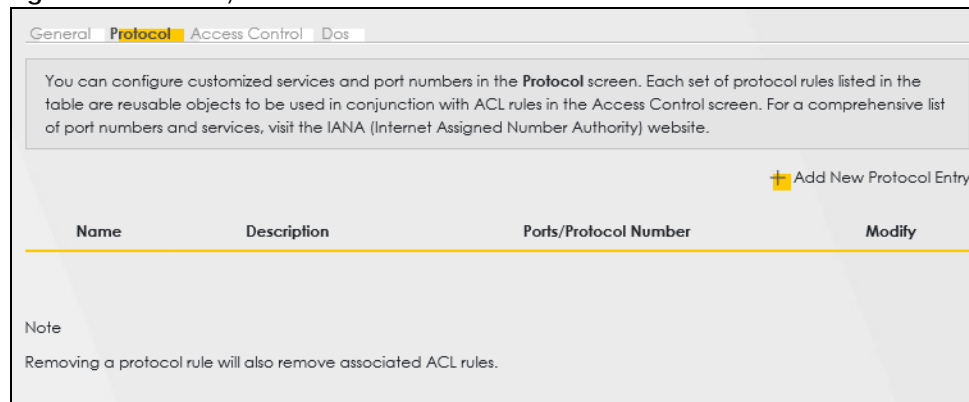
LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using IPv4 (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using IPv6 (Internet Protocol version 6).
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service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

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 134 Security > Firewall > Protocol



The following table describes the labels in this screen.

Table 82 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 82 Security > Firewall > Protocol (continued)

LABEL	DESCRIPTION
Ports/ Protocol Number	This shows the port number or range and the IP protocol 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 135 Security > Firewall > Protocol: Add New Protocol Entry

The following table describes the labels in this screen.

Table 83 Security > Firewall > Protocol: Add New Protocol Entry

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Description	Enter a description for your custom port.
Protocol	Choose the protocol (TCP , UDP , ICMP , ICMPv6 , or Other) that defines your customized port from the drop down list box.
Protocol Number	Type a single port number or the range of port numbers (0 – 255) that define your customized service.
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 136 Security > Firewall > Access Control



The following table describes the labels in this screen.

Table 84 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.

Figure 137 Security > Firewall > Access Control > Add New ACL Rule

The screenshot shows the 'Add New ACL Rule' configuration page. The page has a back arrow in the top left and a title 'Add New ACL Rule' at the top center. The configuration fields are as follows:

- Filter Name: [Empty text box]
- Order: [1]
- Select Source IP Address: [Specific IP Address]
- Source IP Address: [Empty text box] [/prefix length]
- Select Destination Device: [Specific IP Address]
- Destination IP Address: [Empty text box] [/prefix length]
- IP Type: [IPv4]
- Select Service: [Specific Service]
- Protocol: [ALL]
- Custom Source Port: [Range] [1] - [1]
- Custom Destination Port: [Range] [1] - [1]
- Policy: [ACCEPT]
- Direction: [WAN to LAN]
- Enable Rate Limit: [Toggle switch is off]
- [Empty text box] packet(s) per [Minute] (1-512)
- Scheduler Rules: [Dropdown menu] [Add New Rule]

At the bottom of the page, there are 'Cancel' and 'OK' buttons.

Figure 138 Security > Firewall > Access Control > Add New ACL Rule

The following table describes the labels in this screen.

Table 85 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Filter Name	Type a unique name for your filter rule.
Order	Assign the order of your rules as rules are applied in turn.
Select Source IP Address	If you want the source to come from a particular (single) IP, select Specific IP Address . If not, select from a detected device.
Source IP Address	If you selected Specific IP Address in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select Specific IP Address . If not, select a detected device.
Destination IP Address	If you selected Specific IP Address in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Select Service	Select a service from the Select Service box.
Protocol	Select the protocol (ALL , TCP/UDP , TCP , UDP , ICMP , or ICMPv6) used to transport the packets for which you want to apply the rule.

Table 85 Security > Firewall > Access Control > Add New ACL Rule (continued)

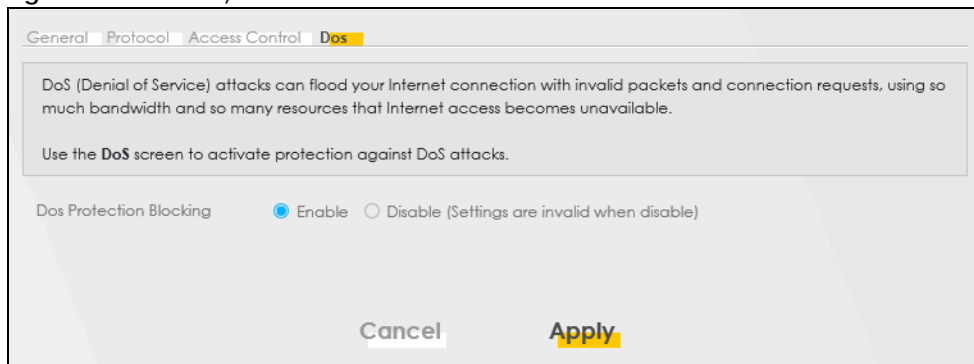
LABEL	DESCRIPTION
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN).
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 to enable (switch turns blue) 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 click Add New ACL 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 139 Security > Firewall > DoS



The following table describes the labels in this screen.

Table 86 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
- LAN to WAN
- WAN to LAN
- WAN to Router

By default, the Zyxel Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to Router
 - These rules specify which computers on the LAN can manage the Zyxel Device (remote management).

Note: You can also configure the remote management settings to allow only a specific computer to manage the Zyxel Device.

- LAN to WAN
 - These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the Zyxel Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN
 - These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to Router

By default the Zyxel Device stops computers on the WAN from managing the Zyxel Device. You could configure one of these rules to allow a WAN computer to manage the Zyxel Device.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the Zyxel Device.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the Zyxel Device's default rules.

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

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 a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4** Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the Web Configurator screens.

CHAPTER 18

MAC Filter

18.1 MAC Filter Overview

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

18.2 MAC Filter

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

Figure 140 Security > MAC Filter

Enable MAC filters and add the MAC addresses of LAN client in your home or office network to the following table, if you wish to allow or deny them to access your network. Sometimes, MAC Filter is considered a method to increase the security of your network.

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
Only devices listed here are granted access to the network.

[Cancel](#) [Apply](#)

The following table describes the labels in this screen.

Table 87 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select Enable to activate the MAC filter function.
MAC Restrict Mode	Select Allow to only permit the listed MAC addresses access to the Zyxel Device. Select Deny to permit anyone access to the Zyxel Device except the listed MAC addresses.

Table 87 Security > MAC Filter (continued)

LABEL	DESCRIPTION
Add New Rule	Click the Add button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

18.2.1 Add New Rule

You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter, as shown in the example below. Select **Security > MAC Filter > Add New Rule**. The screen appears as shown.

Figure 141 Security > MAC Filter > Add New Rule

Set	Active	Host Name	MAC Address	Delete
1	<input checked="" type="checkbox"/>	test	BC - 22 - 33 - 11 - 66 - AA	
2	<input checked="" type="checkbox"/>	Test	BC - 88 - 99 - 00 - 11 - 24	

The following table describes the labels in this screen.

Table 88 Security > MAC Filter > Add New Rule

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 19

Parental Control

19.1 Parental Control Overview

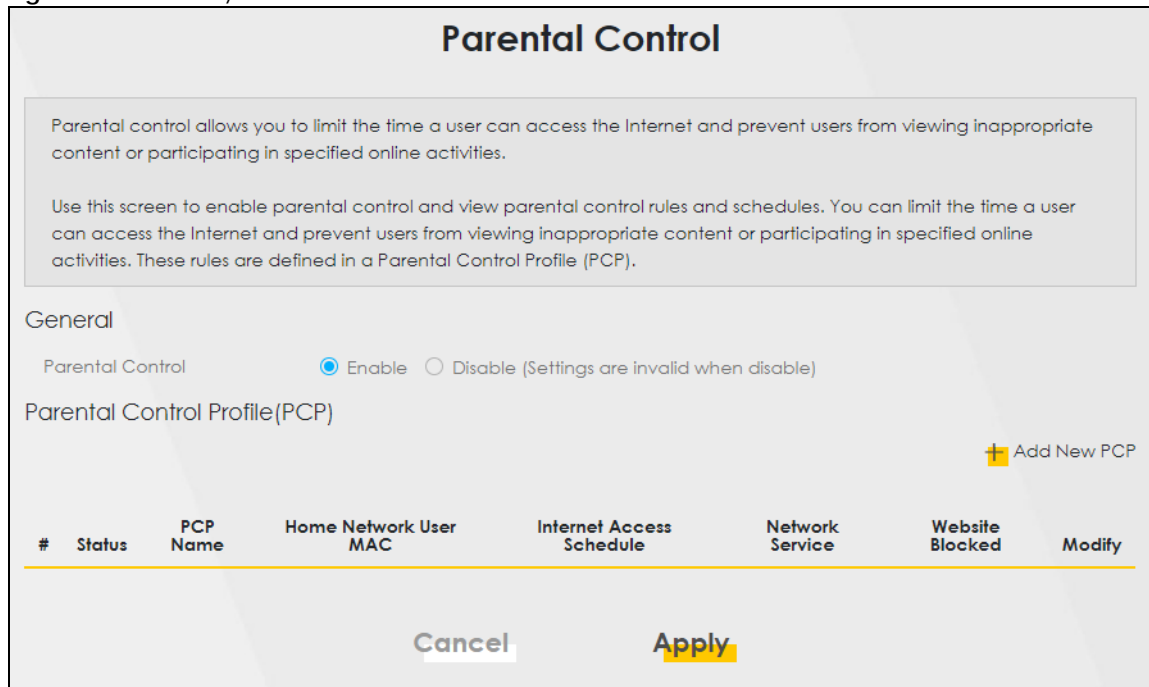
Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

19.2 Parental Control Schedule and URL Filter

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities. These rules are defined in a Parental Control Profile (PCP).

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

Figure 142 Security > Parental Control



The following table describes the fields in this screen.

Table 89 Security > Parental Control

LABEL	DESCRIPTION
General	
Parental Control	Select Enable to activate parental control on the Zyxel Device.
Parental Control Profile (PCP)	
Add new PCP	Click this if you want to configure a new Parental Control Profile (PCP).
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active
PCP Name	This shows the name of the rule.
Home Network User MAC	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the days and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, None will be shown.
Website Block	This shows whether the website block is configured. If not, None will be shown.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

19.2.1 Add or Edit a Parental Control Profile

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 143 Security > Parental Control > Add or Edit PCP (General, Rule List & Internet Access Schedule)

Add New PCP

General

Active Enable Disable (Settings are invalid when disable)

Parental Control Profile Name

Home Network User

Rule List

User MAC Address	Delete
------------------	--------

Internet Access Schedule

Day Mon Tue Wed Thu Fri Sat Sun

Add New Time

Time (Start-End)

Figure 144 Security > Parental Control > Add or Edit PCP (Network Service & Site/URL Keyword)

The screenshot shows the configuration interface for adding or editing a Parental Control Profile (PCP). It is split into two sections: 'Network Service' and 'Site/URL Keyword'. In the 'Network Service' section, there is a dropdown menu currently set to 'Block' and an 'Add New Service' button. Below this is a table with columns for '#', 'Service Name', 'Protocol:Port', and 'Modify'. The 'Site/URL Keyword' section has a dropdown menu set to 'Block the web URLs' and an 'Add' button. Below this is a table with columns for '#', 'Website', and 'Modify'. At the bottom of the screen are 'Cancel' and 'OK' buttons.

The following table describes the fields in this screen.

Table 90 Security > Parental Control > Add or Edit PCP

LABEL	DESCRIPTION
General	
Active	Select Enable or Disable to activate or deactivate the parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select Custom , enter the LAN user's MAC address. If you select All , the rule applies to all LAN users.
Rule List	In Home Network User , select Custom , enter the LAN user's MAC address, then click the Add icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the Delete icon to remove one.
Internet Access Schedule	
Day	Select check boxes for the days that you want the Zyxel Device to perform parental control.
Time (Start-End)	Drag the time bar to define the time that the LAN user is allowed access (Authorized access) or denied access (No access).
Add New Time	Click this to add a new time bar. Up to three are allowed.
Network Service	
Network Service Setting	If you select Block , the Zyxel Device prohibits the users from viewing the web sites with the URLs listed below. If you select Allow , the Zyxel Device blocks access to all URLs except ones listed below.
Add New Service	Click this to show a screen in which you can add a new service rule. You can configure the Service Name , Protocol , and Port of the new rule, as shown in Figure 145 .
#	This shows the index number of the rule.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.

Table 90 Security > Parental Control > Add or Edit PCP (continued)

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

Add New Service

Use this screen to add a new service rule.

Figure 145 Security > Parental Control > Add or Edit PCP > Add New Service

The following table describes the fields in this screen.

Table 91 Security > Parental Control > Add or Edit PCP > Add New Service

LABEL	DESCRIPTION
Add New Service	Select the name of the service from the drop-down list. Otherwise, select User Define and specify the name, protocol, and port of the service. If you have chosen a pre-defined service in the Service Name field, this field will not be configurable.
Protocol	Select the transport layer protocol used for the service. Choices are TCP , UDP , or TCP & UDP .
Port	Enter the port of the service. If you have chosen a pre-defined service in the Service Name field, this field will not be configurable.

Table 91 Security > Parental Control > Add or Edit PCP > Add New Service (continued)

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

Add Site/URL Keyword

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

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

Figure 146 Security > Parental Control > Add or Edit PCP > Add Keyword

The following table describes the fields in this screen.

Table 92 Security > Parental Control > Add or Edit PCP > Add Keyword

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

CHAPTER 20

Certificates

20.1 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.

20.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Zyxel Device's CA-signed (Certification Authority) certificates ([Section 20.3 on page 237](#)).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer ([Section 20.4 on page 241](#)).

20.2 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.

20.3 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 147 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

Table 93 Security > Certificates > Local Certificates

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

20.3.1 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 148 Create Certificate Request

The following table describes the labels in this screen.

Table 94 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select Auto to have the Zyxel Device configure this field automatically. Or select Customize to enter it manually. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address can be up to 63 ASCII characters. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

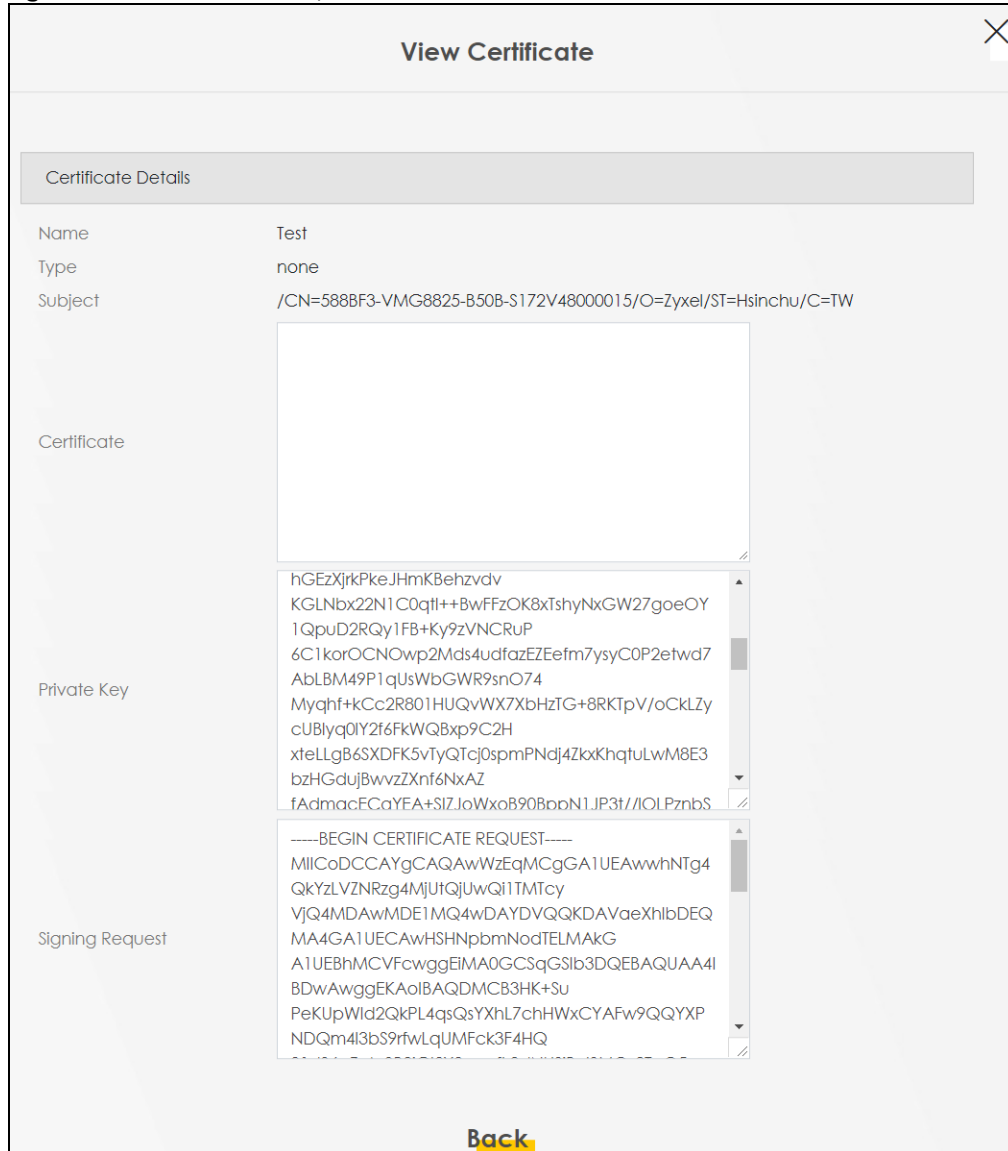
20.3.2 View Certificate Request

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 149 Certificate Request: View



The following table describes the fields in this screen.

Table 95 Certificate Request: View

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

Table 95 Certificate Request: View (continued)

LABEL	DESCRIPTION
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click Back to return to the previous screen.

20.4 Trusted CA

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

Note: A maximum of ten certificates can be added.

Figure 150 Security > Certificates > Trusted CA

Certificates

Local Certificates | **Trusted CA**

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

+ Import Certificate

#	Name	Subject	Type	Modify
Note Maximum of 10 certificates				

The following table describes the labels in this screen.

Table 96 Security > Certificates > Trusted CA

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

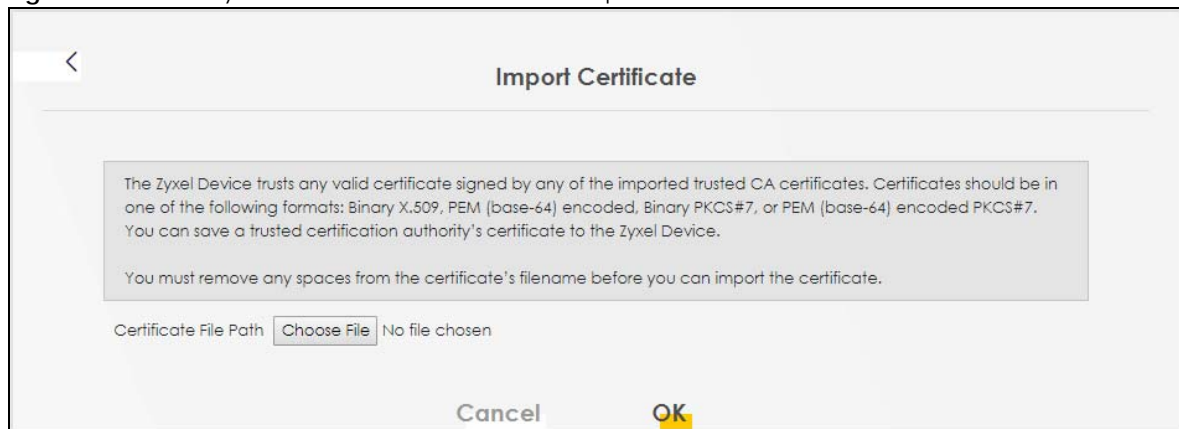
LABEL	DESCRIPTION
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the Remove icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

20.5 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 151 Security > Certificates > Trusted CA > Import



The following table describes the labels in this screen.

Table 97 Security > Certificates > Trusted CA > Import

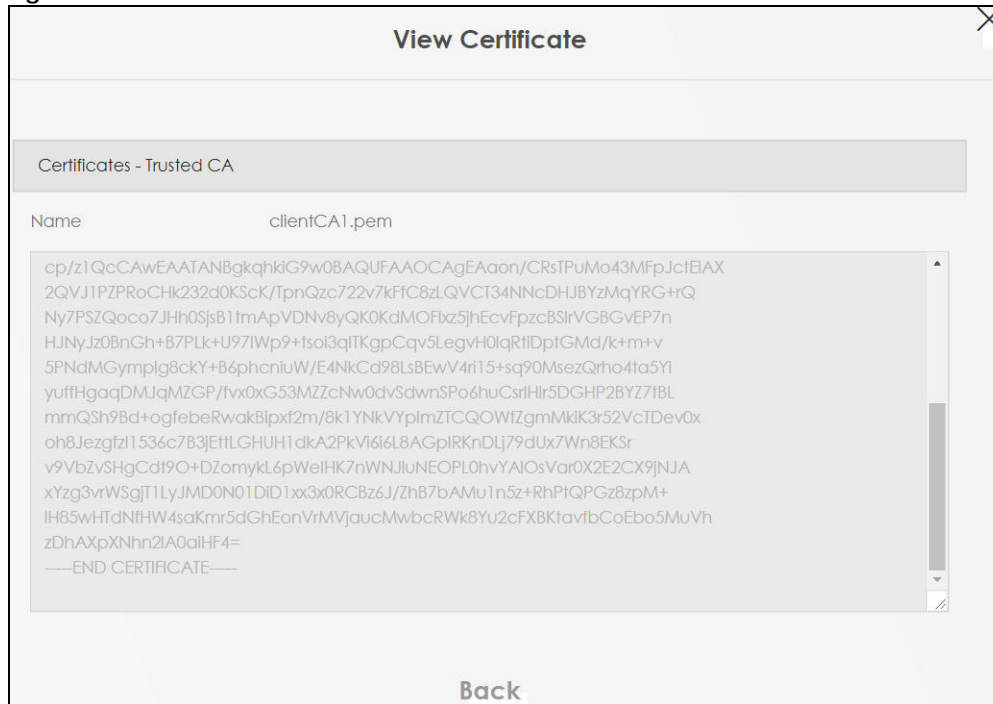
LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click Choose File/Browse to find it.
Choose File/Browse	Click this button to find the certificate file you want to upload.
OK	Click this to save the certificate on the Zyxel Device.
Cancel	Click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

20.6 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 152 Trusted CA: View



The following table describes the labels in this screen.

Table 98 Trusted CA: View

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

20.7 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.

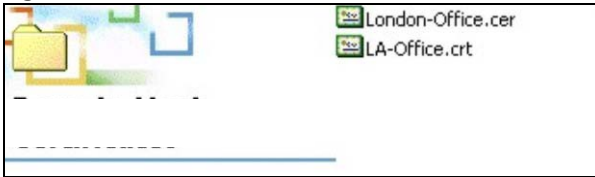
20.7.1 Verify a Certificate

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.

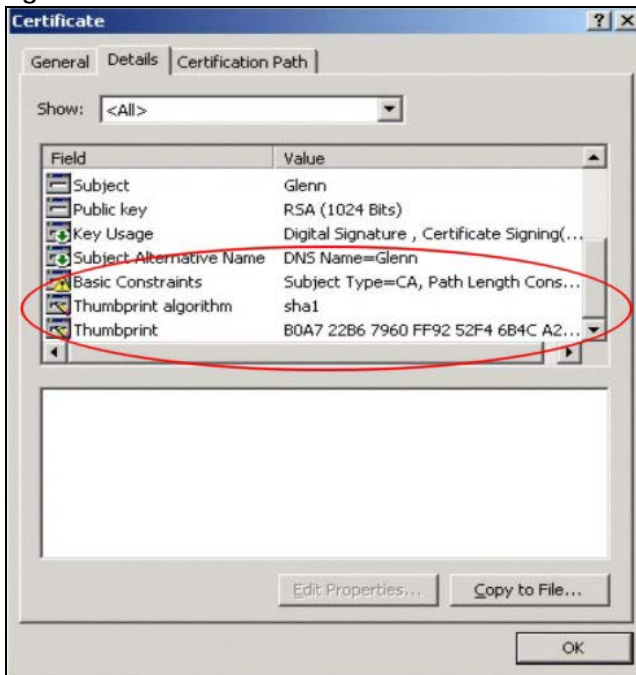
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 153 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 154 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 21

Log

21.1 Log Overview

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

21.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 21.2 on page 247](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 21.3 on page 248](#)).

21.1.2 What You Need To Know

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

Alerts and Logs

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

Syslog Overview

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

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

Table 99 Syslog Severity Levels

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

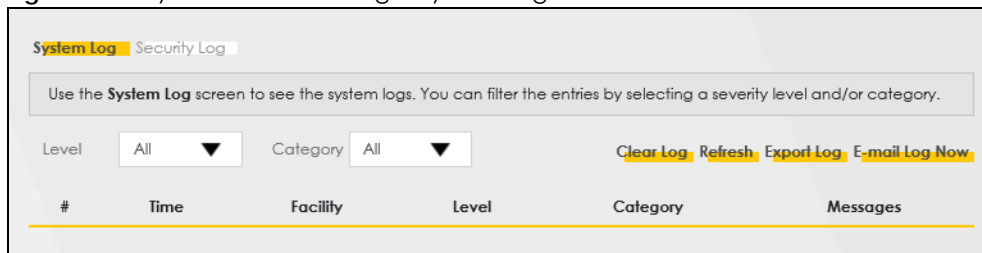
Table 99 Syslog Severity Levels (continued)

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

21.2 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 155 System Monitor > Log > System Log



The following table describes the fields in this screen.

Table 100 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.
Email 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 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.

21.3 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 156 System Monitor > Log > Security Log

The following table describes the fields in this screen.

Table 101 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.
Email 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 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 22

Traffic Status

22.1 Traffic Status Overview

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

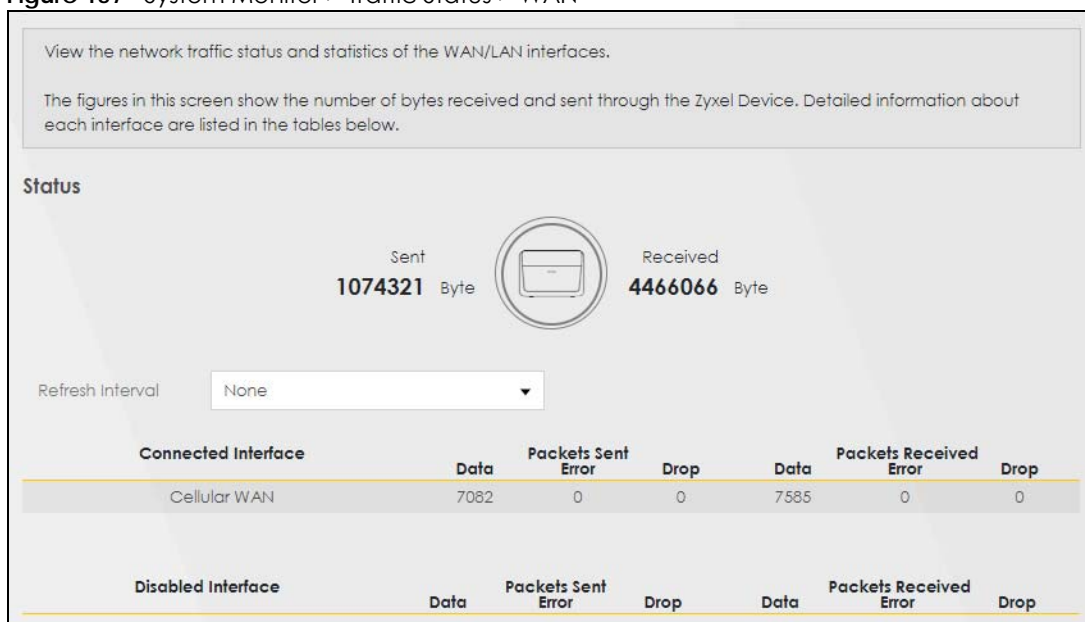
22.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 22.2 on page 249](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 22.3 on page 250](#)).

22.2 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 157 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 102 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disabled.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
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.

22.3 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 158 System Monitor > Traffic Status > LAN

Traffic Status			
WAN LAN			
Figures about data that have been sent to and received from each LAN port (including wireless) are displayed in the following table.			
Refresh Interval	30 seconds		
Interface	LAN	2.4G WLAN	5G WLAN
Bytes Sent	589466	1060	0
Bytes Received	480594	2664	0
Interface	LAN	2.4G WLAN	5G WLAN
Sent (Packet)	Data	2836	5
	Error	0	0
	Drop	0	0
Received (Packet)	Data	5096	28
	Error	0	8
	Drop	6	0

The following table describes the fields in this screen.

Table 103 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interfaces.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
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 23

ARP Table

23.1 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.

23.1.1 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.

23.2 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 159 System Monitor > ARP Table

ARP Table

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

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

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

IPv4 ARP Table

#	IPv4 Address	MAC Address	Device
1	192.168.1.100	08:00:27:00:00:01	br0
2	192.168.1.101	08:00:27:00:00:02	br0

IPv6 Neighbour Table

#	IPv6 Address	MAC Address	Device
1	fe80::200:0:0:0:0:0:0:0	08:00:27:00:00:01	br0
2	fe80::200:0:0:0:0:0:0:0	08:00:27:00:00:02	br0

The following table describes the labels in this screen.

Table 104 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 a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click the device type to go to its configuration screen.

CHAPTER 24

Routing Table

24.1 Routing Table Overview

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

24.2 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 160 System Monitor > Routing Table

Routing Table

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

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

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

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
0.0.0.0	0.0.0.0	255.255.0.0	U	0	lo
192.168.1.0/24	0.0.0.0	255.255.255.0	U	0	br0
192.168.1.1	0.0.0.0	255.0.0.0	U	0	br0

IPv6 Routing Table

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

The following table describes the labels in this screen.

Table 105 System Monitor > Routing Table

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

Table 105 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	<p>This indicates the route status.</p> <p>U-Up: The route is up.</p> <p>!-Reject: The route is blocked and will force a route lookup to fail.</p> <p>G-Gateway: The route uses a gateway to forward traffic.</p> <p>H-Host: The target of the route is a host.</p> <p>R-Reinstate: The route is reinstated for dynamic routing.</p> <p>D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.</p> <p>M-Modified (redirect): The route is modified from a routing daemon or redirect.</p>
Metric	<p>The metric represents the "cost of transmission." A router determines the best route for transmission by choosing a path with the lowest "cost." The smaller the number, the lower the "cost."</p>
Interface	<p>This indicates the name of the interface through which the route is forwarded.</p> <p>brx indicates a LAN interface where x can be 0 – 3 to represent LAN1 to LAN4 respectively.</p> <p>ethx indicates an Ethernet WAN interface using IPoE or in bridge mode.</p> <p>ppp0 indicates a WAN interface using PPPoE.</p> <p>wlx indicates a wireless interface where x can be 0 – 1.</p>

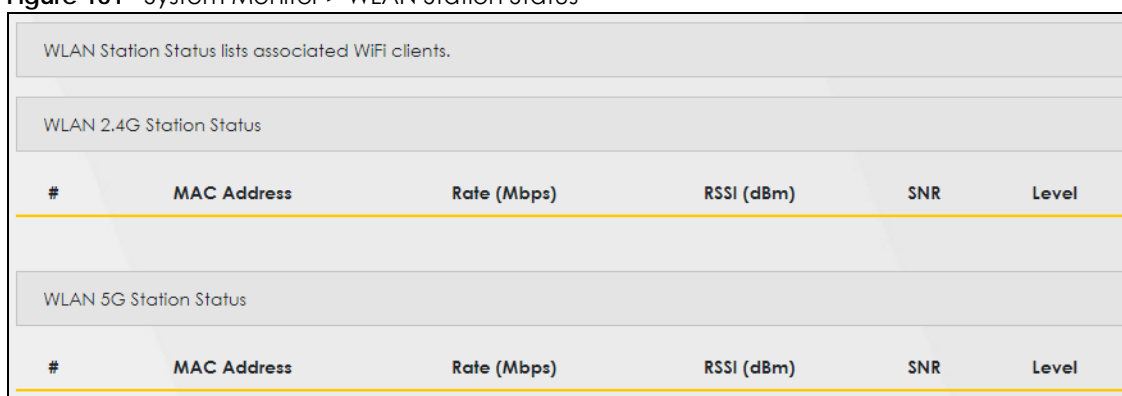
CHAPTER 25

WLAN Station Status

25.1 WLAN Station Status Overview

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

Figure 161 System Monitor > WLAN Station Status



The screenshot shows a web interface for 'WLAN Station Status'. It contains two tables. The first table is titled 'WLAN 2.4G Station Status' and the second is 'WLAN 5G Station Status'. Both tables have the same columns: '#', 'MAC Address', 'Rate (Mbps)', 'RSSI (dBm)', 'SNR', and 'Level'. The tables are currently empty.

The following table describes the labels in this screen.

Table 106 System Monitor > WLAN Station Status

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

Table 106 System Monitor > WLAN Station Status (continued)

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

CHAPTER 27

System

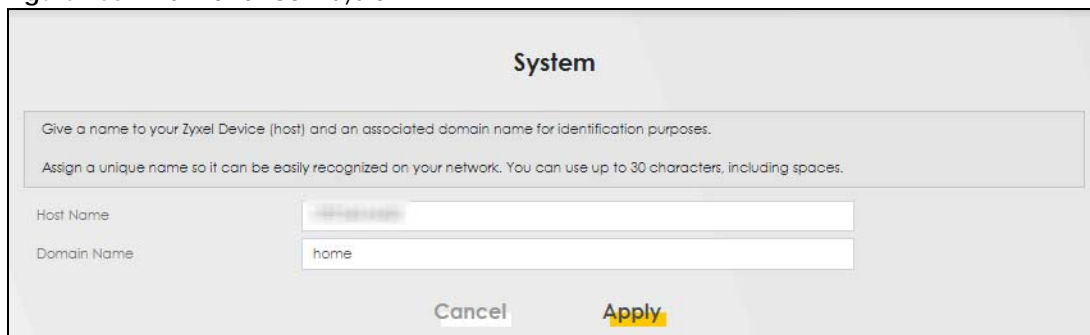
27.1 System Overview

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

27.2 System

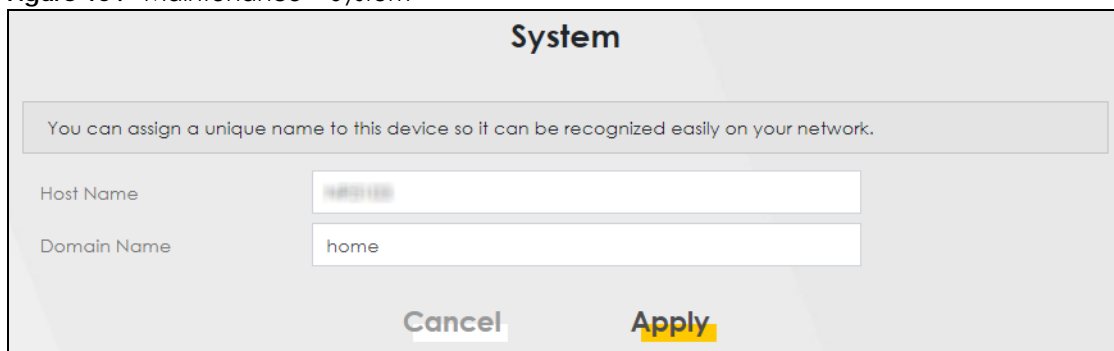
Click **Maintenance > System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 163 Maintenance > System



The screenshot shows a web interface titled "System". Below the title is a grey box containing two lines of instructional text: "Give a name to your Zyxel Device (host) and an associated domain name for identification purposes." and "Assign a unique name so it can be easily recognized on your network. You can use up to 30 characters, including spaces." Below this box are two input fields: "Host Name" with a text box containing "mydevice" and "Domain Name" with a text box containing "home". At the bottom are "Cancel" and "Apply" buttons.

Figure 164 Maintenance > System



This screenshot is identical to Figure 163, showing the "System" configuration screen with the same instructional text, input fields for "Host Name" (containing "mydevice") and "Domain Name" (containing "home"), and "Cancel" and "Apply" buttons.

The following table describes the labels in this screen.

Table 108 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a domain name for your host Zyxel Device.

Table 108 Maintenance > System (continued)

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

CHAPTER 28

User Account

28.1 User Account Overview

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

28.2 User Account

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

Figure 165 Maintenance > User Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Remote Privilege	Modify
1	<input checked="" type="checkbox"/>	admin	3	5	5	Administrator	LAN,WAN	

The following table describes the labels in this screen.

Table 109 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account (up to four Administrator accounts and four User accounts).
#	This is the index number.
Active	This indicates whether the user account is active or not. The check box is selected when the user account is enabled. It is cleared when it is disabled.
User Name	This displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in Retry Times .

Table 109 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Group	This field displays whether this user has Administrator or User privileges.
Remote Privilege	This field displays whether this user can access the Zyxel Device with HTTP, Telnet or SSH through the WAN , LAN or LAN/WAN .
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.

28.2.1 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 166 Maintenance > User Account > Add or Edit

The following table describes the labels in this screen.

Table 110 Maintenance > User Account > Add or Edit

LABEL	DESCRIPTION
Active	Click to enable (switch turns blue) or disable (switch turns gray) to activate or deactivate the user account.
User Name	Enter a new name for the account (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign (\$) vertical bar () ampersand (&) semicolon (;)
Password	Type your new system password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device.
Verify Password	Type the new password again for confirmation.

Table 110 Maintenance > User Account > Add or Edit (continued)

LABEL	DESCRIPTION
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	<p>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.</p> <p>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.</p> <p>The Administrator privileges are the following:</p> <ul style="list-style-type: none"> • 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. <p>The User privileges are the following:</p> <ul style="list-style-type: none"> • 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.
Cancel	Click Cancel to restore your previously saved settings.
OK	Click OK to save your changes.

CHAPTER 29

Remote Management

29.1 Overview

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

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

29.1.1 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 29.2 on page 269](#)).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses ([Section 29.4 on page 271](#)).
- Use **MGMT Services for IP Passthrough** to configure which interfaces you can use to access the Zyxel Device for a given service ([Section 29.3 on page 270](#)).
- 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 29.6 on page 273](#)).

29.2 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 167 Maintenance > Remote Management > MGMT Services

Configure which interface(s) you can use to access the Zyxel Device for a given service. You can also specify the service port numbers computers must use to connect to the Zyxel Device.

Service Control

WAN Interface used for services: Any_WAN Multi_WAN

Cellular WAN

Service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	443
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
PING	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	

The following table describes the fields in this screen.

Table 111 Maintenance > Remote Management > MGMT Services> MGMT Services

LABEL	DESCRIPTION
WAN Interface used for services	Select Any_WAN to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select Multi_WAN and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
Cellular WAN	Enable the cellular WAN connection configured in Network Setting > Broadband > Cellular WAN to access the service on the Zyxel Device. If there are multiple cellular WANs configured on the Zyxel Device, you can select which to use for device management.
ETHWAN	Enable the Ethernet WAN connection configured in Network Setting > Broadband > Ethernet WAN to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN/WLAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN or WLAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

29.3 MGMT Services for IP Passthrough

Configure which interfaces you can use to access the Zyxel Device in **IP Passthrough** 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**.

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

Figure 168 Maintenance > Remote Management > MGMT Services for IP Passthrough

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

Service Control

Service	WAN	Trust Domain	Port
PT_HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	20080
PT_HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	20443
PT_FTP	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	20021
PT_TELNET	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	20023
PT_SSH	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	20022

The following table describes the fields in this screen.

Table 112 Maintenance > Remote Management > MGMT Services for IP Passthrough

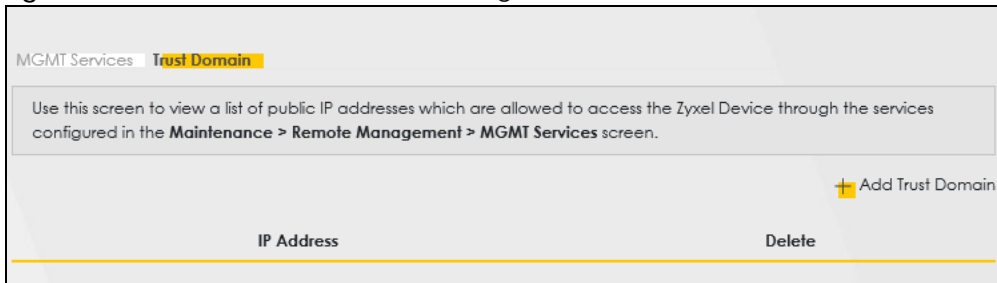
LABEL	DESCRIPTION
Service	This is the service you may use to access the Zyxel Device.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from 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.

29.4 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 169 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

Table 113 Maintenance > Remote Management > Trust Domain

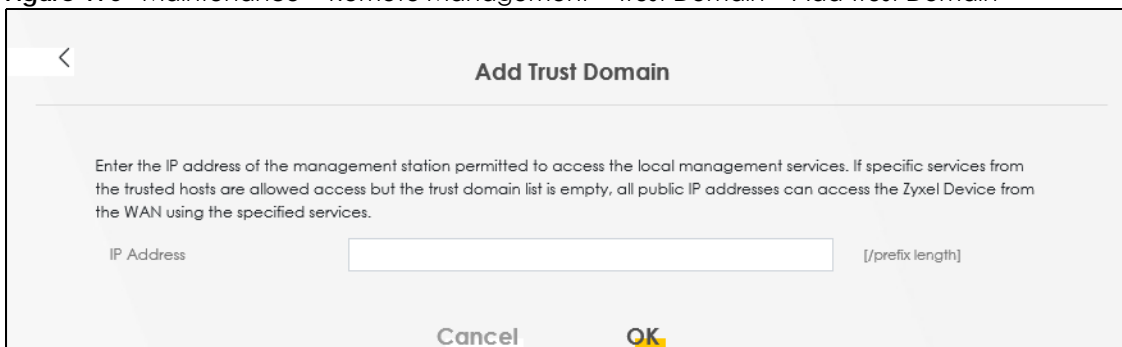
LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the Delete icon to remove the trusted host IP address.

29.5 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 170 Maintenance > Remote Management > Trust Domain > Add Trust Domain



The following table describes the fields in this screen.

Table 114 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.

Table 114 Maintenance > Remote Management > Trust Domain > Add Trust Domain (continued)

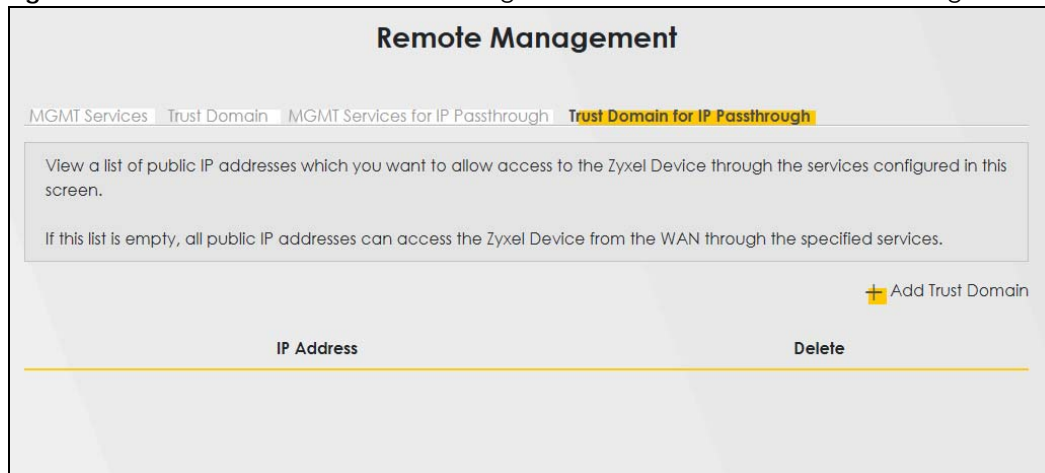
LABEL	DESCRIPTION
OK	Click OK to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

29.6 Trust Domain for IP Passthrough

Use this screen to view a list of public IP addresses/complete domain names which are allowed to access the Zyxel Device in **IP Passthrough** mode. 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 171 Maintenance > Remote Management > Trust Domain for IP Passthrough



The following table describes the fields in this screen.

Table 115 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.

29.7 Add Trust Domain

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

Figure 172 Maintenance > Remote Management > Trust Domain for IP Passthrough > Add Trust Domain

The following table describes the fields in this screen.

Table 116 Maintenance > Remote Management > Trust Domain for IP Passthrough > Add Trust Domain

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

CHAPTER 30

TR-069 Client

30.1 Overview

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

30.2 TR-069 Client

TR-069 is a protocol that defines how your Zyxel Device can be managed through a management server. You can use a management server to remotely set up the Zyxel Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Zyxel Device.

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

Figure 173 Maintenance > TR-069 Client

The screenshot shows the 'TR-069 Client' configuration page. At the top, it says 'Allow your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.' Below this, there are several settings:

- CWMP Active:** A toggle switch that is turned on (blue).
- Inform:** A toggle switch that is turned on (blue).
- Inform Interval:** A text input field containing the value '86400'.
- IP Protocol:** Three radio buttons: 'TR069 on IPv4 Only' (unselected), 'TR069 on IPv6 Only' (unselected), and 'Auto Select' (selected).
- ACS URL:** A text input field. To its right, there is a note: '[URL or IPv4 Address / Global IPv6 Address]'. Below this are two more text input fields for 'ACS User Name' and 'ACS Password'.
- WAN Interface Used by TR-069 Client:** Two radio buttons: 'Any_WAN' (unselected) and 'Multi_WAN' (selected).
- Cellular WAN:** A checked checkbox.
- Display SOAP Messages on Serial Console:** A toggle switch that is turned on (blue).
- Connection Request Authentication:** A toggle switch that is turned on (blue).
- Connection Request User Name:** A text input field.
- Connection Request Password:** A text input field.
- Connection Request URL:** A text input field.
- Validate ACS certificate:** A toggle switch that is turned on (blue).
- Local Certificate Used by TR-069 Client:** A dropdown menu.

At the bottom of the page, there are two buttons: 'Cancel' and 'Apply'.

Figure 174 Maintenance > TR-069 Client

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

CWMP Active

Inform

Inform Interval

IP Protocol TR069 on IPv4 Only TR069 on IPv6 Only Auto Select

ACS URL (URL or IPv4 Address / Global IPv6 Address)

ACS User Name

ACS Password

WAN Interface Used by TR-069 Client Any_WAN Multi_WAN

Cellular WAN 1 Cellular WAN 2

Display SOAP Messages on Serial Console

Connection Request Authentication

Connection Request User Name

Connection Request Password

Connection Request URL

Supplementary Client

Supplementary ACS URL (URL or IPv4 Address / Global IPv6 Address)

Supplementary ACS User Name

Supplementary ACS Password

Validate ACS certificate

Local Certificate Used by TR-069 Client

[Cancel](#) [Apply](#)

The following table describes the fields in this screen.

Table 117 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP Active	CPE WAN Management Protocol (CWMP) enables the Zyxel Device to be remotely configured through a WAN link. Communication between the Zyxel Device and the management server is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC). Click to enable (switch turns blue) to allow the Zyxel Device to be managed by a management server. Otherwise, click to disable (switch turns gray) to disallow the Zyxel Device to be managed by a management server.
Inform	Click to enable (switch turns blue) the Zyxel Device to send periodic inform through TR-069 on the WAN. Otherwise, click to disable (switch turns gray).
Inform Interval	Enter the time interval (in seconds) at which the Zyxel Device sends information to the auto-configuration server.
IP Protocol	Select the type of IP protocol to allow TR-069 to operate on.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.

Table 117 Maintenance > TR-069 Client (continued)

LABEL	DESCRIPTION
WAN Interface used by TR-069 client	<p>Select a WAN interface through which the TR-069 traffic passes.</p> <p>If you select Any_WAN, the Zyxel Device automatically passes the TR-069 traffic when any WAN connection is up.</p> <p>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.</p>
Cellular WAN	The Zyxel Device automatically passes the TR-069 traffic when cellular WAN connection is up.
Display SOAP messages on serial console	Click to enable (switch turns blue) the dumping of all SOAP messages during the ACS server communication with the CPE.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	<p>Enter the connection request user name.</p> <p>When the ACS makes a connection request to the Zyxel Device, this user name is used to authenticate the ACS.</p>
Connection Request Password	<p>Enter the connection request password.</p> <p>When the ACS makes a connection request to the Zyxel Device, this password is used to authenticate the ACS.</p>
Connection Request URL	<p>This shows the connection request URL.</p> <p>The ACS can use this URL to make a connection request to the Zyxel Device.</p>
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.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore the screen's last saved settings.

CHAPTER 31

Time Settings

31.1 Time Settings Overview

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

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

31.2 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 175 Maintenance > Time

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

Current Date/Time

Current Time 14:21:53
Current Date 2019-02-27

Time and Date Setup

Time Protocol SNTP (RFC-1769)

First Time Server Address pool.ntp.org
Second Time Server Address clock.nyc.he.net
Third Time Server Address clock.sjc.he.net
Fourth Time Server Address None
Fifth Time Server Address None

Time Zone

Time Zone (GMT+08:00) Taipei

Daylight Savings

Active

Start Rule

Day 1 in
 Last Sunday in

Month March
Hour 2 0

End Rule

Day 1 in
 Last Sunday in

Month October
Hour 3 0


Cancel **Apply**

The following table describes the fields in this screen.

Table 118 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 118 Maintenance > Time (continued)

LABEL	DESCRIPTION
First – Fifth Time Server Address	<p>Select an NTP time server from the drop-down list box.</p> <p>Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.</p> <p>Select None if you do not want to configure the time server.</p> <p>Check with your ISP/network administrator if you are unsure of this information.</p>
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	<p>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:</p> <p>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.</p> <p>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).</p>
End Rule	<p>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:</p> <p>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.</p> <p>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).</p>
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 32

Email Notification

32.1 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.

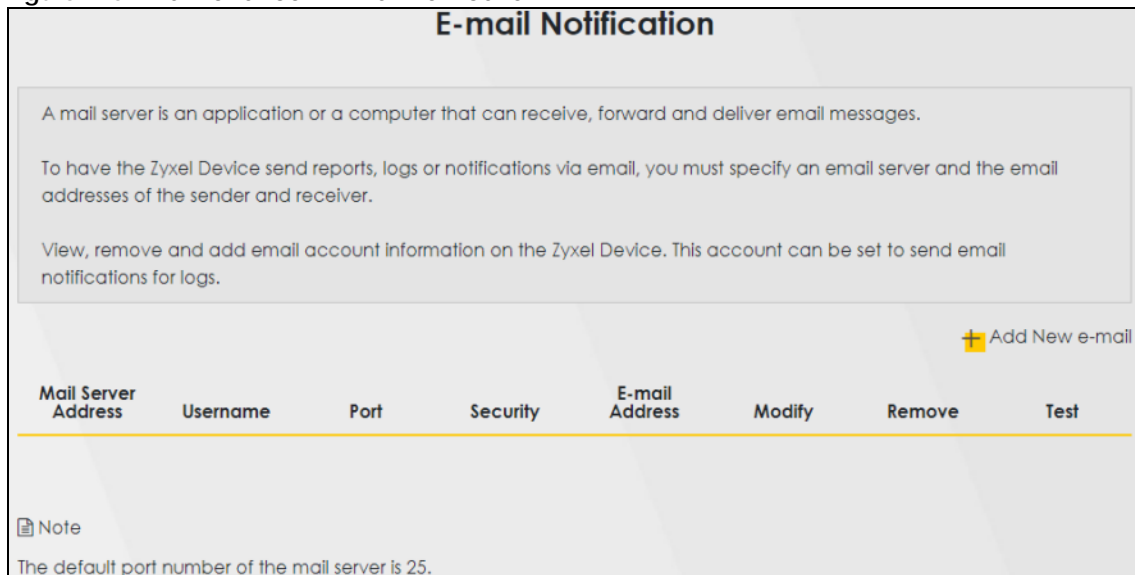
32.2 Email Notification

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 176 Maintenance > E-mail Notification



E-mail Notification

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

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

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

+ Add New e-mail

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

Note

The default port number of the mail server is 25.

The following table describes the labels in this screen.

Table 119 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.
User name	This displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the 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.

32.2.1 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 177 Maintenance > E-mail Notification > Add

The following table describes the labels in this screen.

Table 120 Maintenance > Email 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.

Table 120 Maintenance > Email Notification > Add (continued)

LABEL	DESCRIPTION
Authentication Username	Enter the user name (up to 32 characters). 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.
Cancel	Click this button to begin configuring this screen afresh.
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 33

Log Setting

33.1 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.

33.2 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 178 Maintenance > Log Setting

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

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

Syslog Setting

Syslog Logging

Mode

Syslog Server (Server NAME or IPv4/IPv6 Address)

UDP Port (Server Port)

E-mail Log Settings

E-mail Log Settings

Mail Account

System Log Mail Subject

Security Log Mail Subject

Send Log to (E-Mail Address)

Send Alarm to (E-Mail Address)

Alarm Interval (seconds)

Active Log

System Log

- WAN-DHCP
- DHCP Server
- TR-069
- HTTP
- UPNP
- System
- ACL
- Wireless
- Cellular WAN
- SAS CBSD

Security Log

- Account
- Attack
- Firewall
- MAC Filter

Cancel **Apply**

The following table describes the fields in this screen.

Table 121 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Click the switch (it will turn blue) to enable syslog logging.
Mode	<p>Select Remote to have the Zyxel Device send it to an external syslog server.</p> <p>Select Local File to have the Zyxel Device save the log file on the Zyxel Device itself.</p> <p>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.</p> <p>Note: A warning appears upon selecting Remote or Local File and Remote. Just click OK to continue.</p>

Table 121 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
E-mail Log Setting	Click the switch (it will turn blue) to allow the sending 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 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 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 Logs that you want to record.
Security Log	Select the categories of Security Logs that you want to record.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

33.2.1 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 179 Email Log Example

```

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

End of Firewall Log

```

CHAPTER 34

Firmware Upgrade

34.1 Overview

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

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

34.2 Firmware Upgrade

This screen lets you upload new firmware to your Zyxel Device by using any of the following methods.

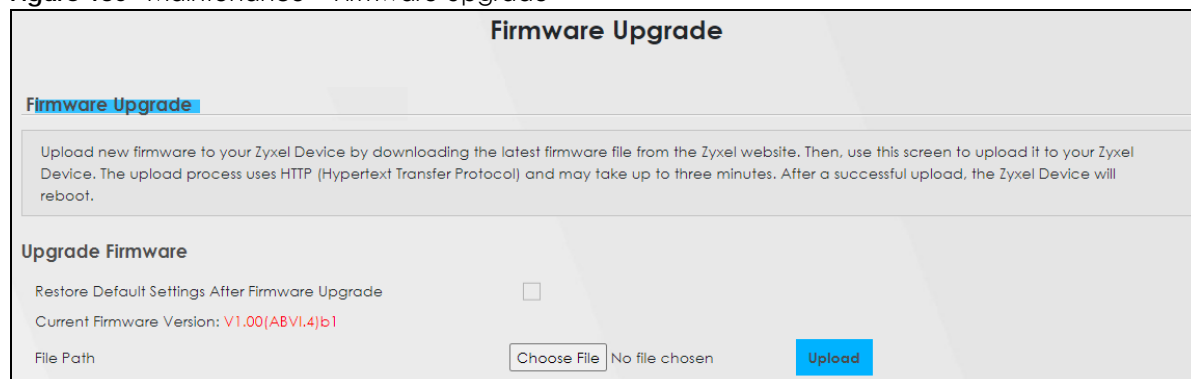
- Download the latest firmware file from the Zyxel website. Or,
- Make sure your Zyxel Device is connected to the Internet. Check for new firmware online from the Zyxel server and download the firmware file to the Zyxel Device.

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

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

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

Figure 180 Maintenance > Firmware Upgrade



The screenshot shows a web interface titled "Firmware Upgrade". At the top, there is a blue header with the text "Firmware Upgrade". Below the header, there is a section titled "Firmware Upgrade" with a blue background. This section contains a paragraph of text: "Upload new firmware to your Zyxel Device by downloading the latest firmware file from the Zyxel website. Then, use this screen to upload it to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the Zyxel Device will reboot." Below this text, there is a section titled "Upgrade Firmware". This section contains a checkbox labeled "Restore Default Settings After Firmware Upgrade" which is currently unchecked. Below the checkbox, it says "Current Firmware Version: V1.00(ABVI.4)b1". At the bottom of this section, there is a "File Path" label, a "Choose File" button, and the text "No file chosen". To the right of the "Choose File" button is a blue "Upload" button.

Figure 181 Maintenance > Firmware Upgrade

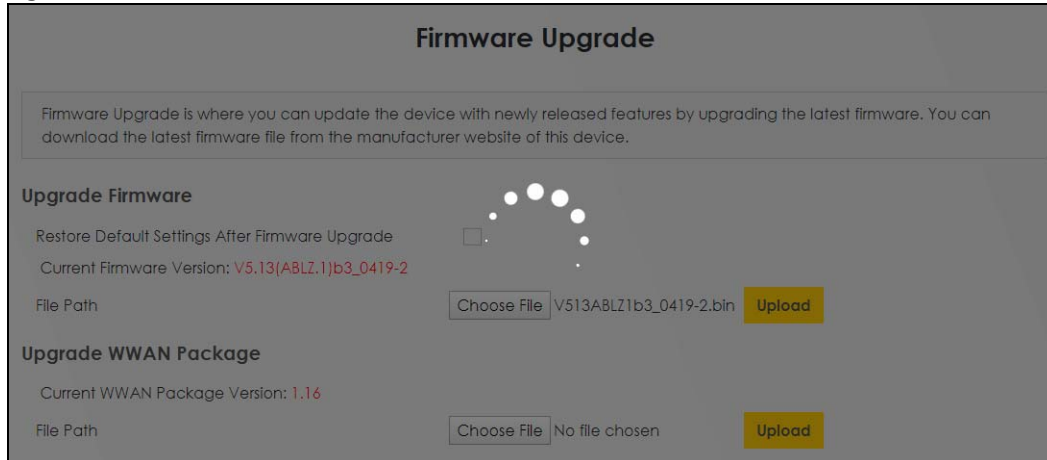
The following table describes the labels in this screen.

Table 122 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select this to enable this option that restores the factory-default to the Zyxel Device after upgrading the firmware. Otherwise, make sure this is clear if you do not want the Zyxel Device to lose all its current configurations and return to the factory defaults. Note: Make sure to backup the Zyxel Device's configuration settings first in case the restore to factory-default process is not successful. Refer to Section 35.2 on page 292 .
Current Firmware Version	This is the current firmware version.
File Path	Type 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 .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.
Do Online Firmware Upgrade	
Check for Latest Firmware Now	With the Zyxel Device connected to the Internet, click this to check for new firmware online from the Zyxel server. If a newer firmware is available, follow the online prompt to upload the new firmware to your Zyxel Device.

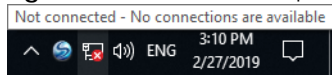
After you see the firmware updating screen, wait a few minutes before logging into the Zyxel Device again.

Figure 182 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.

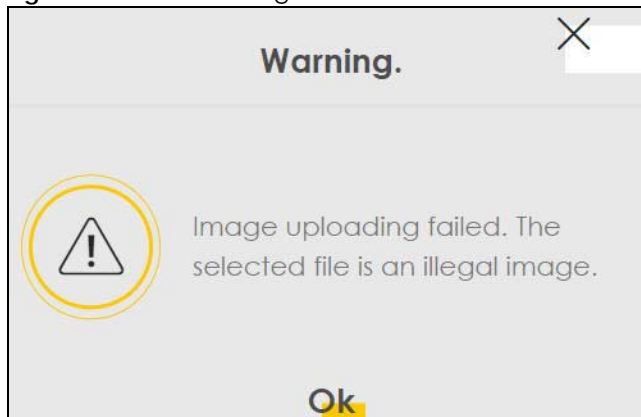
Figure 183 Network Temporarily Disconnected



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 184 Error Message



34.3 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.

Note: Use this screen to upload LTE module firmware only when you are instructed by Zyxel technical support team and provided with new LTE firmware release.

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

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

Figure 185 Maintenance > Firmware Upgrade > Module Upgrade

The following table describes the labels in this screen.

Table 123 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.

CHAPTER 35

Backup/Restore

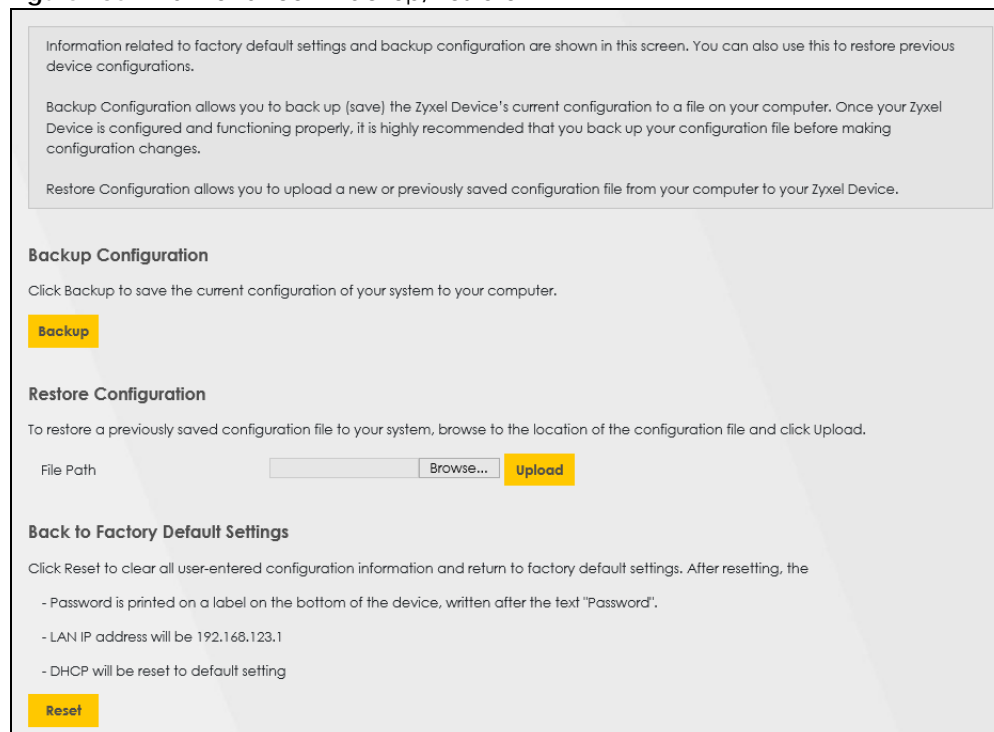
35.1 Backup/Restore Overview

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

35.2 Backup/Restore

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 186 Maintenance > Backup/Restore



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 124 Restore Configuration

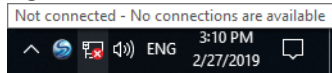
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Choose File / Browse to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click 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.

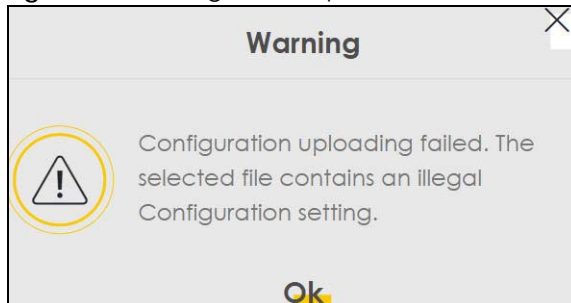
Figure 187 Network Temporarily Disconnected



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 (192.168.1.1/192.168.123.1).

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

Figure 188 Configuration Upload Error



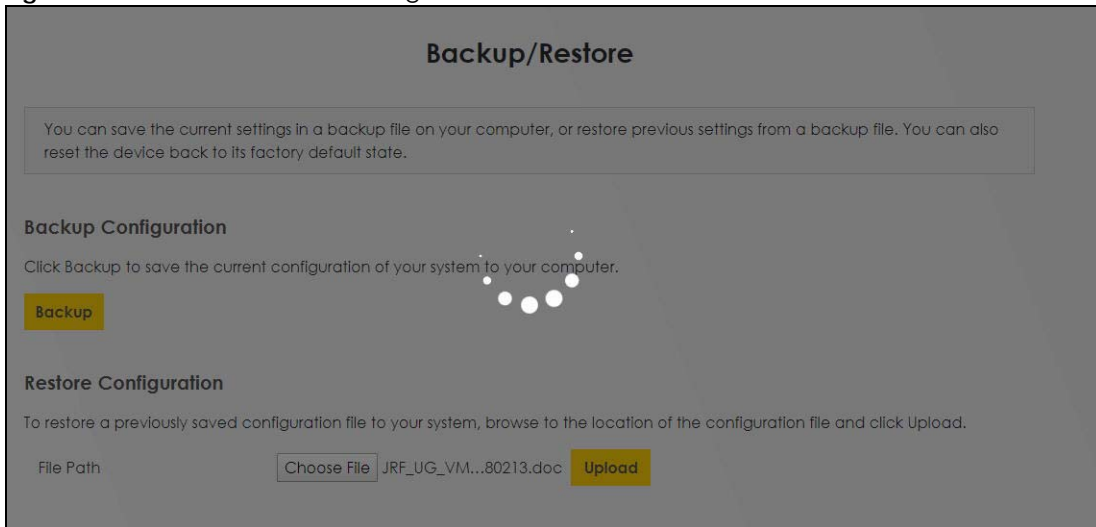
Reset to Factory Defaults

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

Figure 189 Reset Warning Message



Figure 190 Reset In Process Message



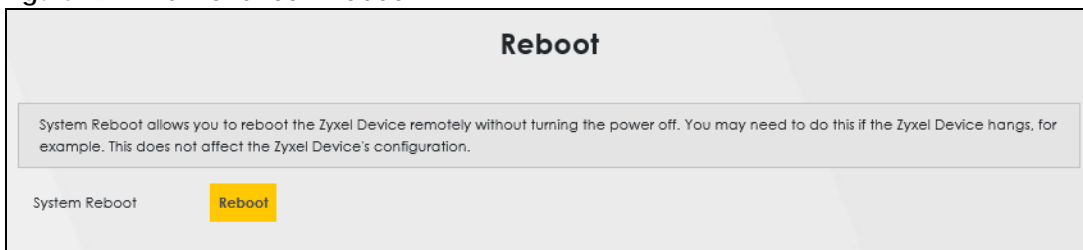
You can also press the **RESET** button on the panel to reset the factory defaults of your Zyxel Device.

35.3 Reboot

System **Reboot** allows you to reboot the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example. This does not affect the Zyxel Device's configuration.

Click **Maintenance > Reboot**. Click **Reboot** to have the Zyxel Device reboot.

Figure 191 Maintenance > Reboot



35.4 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 192 Maintenance > Reboot > Schedule Reboot

The following table describes the labels in this screen.

Table 125 Schedule Reboot

LABEL	DESCRIPTION
Periodically	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 36

Diagnostic

36.1 Diagnostic Overview

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

36.1.1 What You Can Do in this Chapter

- The **Diagnostic** screen lets you ping an IP address or trace the route packets take to a host ([Section 36.2 on page 296](#)).

36.2 Ping/TraceRoute/Nslookup Test/ Speed Test

Use this screen to ping, traceroute, nslookup, or speed test for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Use speed test to determine the download and upload speed.

Note: Not all Zyxel Devices support speed test; see [Chapter 1 on page 16](#) for more information.

Click **Maintenance > Diagnostic** to open the **Ping/TraceRoute/Nslookup/Speed Test** screen shown next.

Figure 193 Maintenance > Diagnostic > Ping/Trace Route/Nslookup

Diagnostic

You can use different diagnostic methods to test a connection and see its detailed information. The **Diagnostic** screens display information to help you identify problems with the Zyxel Device.

Perform ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa.

Ping/TraceRoute Test

TCP/IP

Address

Ping Ping 6 Trace Route Trace Route 6 Nslookup Speed Test

The following table describes the fields in this screen.

Table 126 Maintenance > Diagnostic

LABEL	DESCRIPTION
Ping/TraceRoute Test	The result of tests is shown here in the info area.
TCP/IP	
Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this button to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area.
Ping 6	Click this button to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area.
Trace Route	Click this button to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Click this button to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Click this button to perform a DNS lookup on the IP address or host name.
Speed Test	Click this button to perform an upload and download throughput test.

PART III

Troubleshooting and Appendices

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

CHAPTER 37

Troubleshooting

37.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power and Hardware Problems](#)
- [Device Access Problems](#)
- [Cellular Problems](#)
- [Internet Problems](#)
- [WiFi Problems](#)
- [USB Problems](#)
- [UPnP Problems](#)

37.2 Power and Hardware Problems

[The Zyxel Device does not turn on.](#)

To check whether your model uses Power over Ethernet (PoE) for power, see more information at [Section 2.3 on page 27](#).

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 the PoE is connected to the Zyxel Device and plugged in to an appropriate power source.

- 2 Make sure the power source is turned on.
- 3 Turn the Zyxel Device off and on.
- 4 If the problem continues, contact the vendor.

The LED does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 2.2 on page 24](#).
- 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.

37.3 Device Access Problems

I do not know the IP address of the Zyxel Device.

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address, you might be able to find the IP address of the Zyxel Device by looking up the IP address of your computer's default gateway. To do this in Microsoft Windows, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device, depending on your network environment.
- 3 If this does not work, reset the Zyxel Device to its factory defaults. Refer to [Section 35.2 on page 292](#).

I forgot the admin password.

- 1 See the Zyxel Device label or this document's cover page for the default admin password.
- 2 If you changed the password from default and cannot remember the new one, you have to reset the Zyxel Device to its factory default settings. Refer to [Section 35.2 on page 292](#).

I cannot access the Web Configurator login screen.

- 1 Make sure you are using the correct IP address.
 - The default IP address is 192.168.1.1.
 - If you changed the IP address ([Section 9.2 on page 154](#)), use the new IP address.
 - If you changed the IP address and have forgotten the new address, see the troubleshooting suggestions for [I do not know the IP address of the Zyxel Device](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 2.2 on page 24](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
- 4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote Management**).
- 5 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

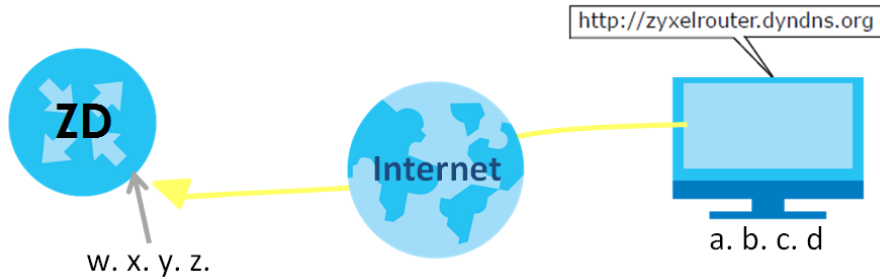
- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

[I cannot log into the Zyxel Device.](#)

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These both user name and password are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the Zyxel Device off and on.
- 4 If this does not work, you have to reset the Zyxel Device to its factory default.

[I cannot log into the Zyxel Device using DDNS.](#)

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the 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 type <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.
- Type **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 Type <http://zyxelrouter.dyndns.org> and press [Enter].
- 3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

I cannot connect to the Zyxel Device using FTP, Telnet, SSH, or Ping.

- 1 See the Remote Management section for details on allowing web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) to access the Zyxel Device.
- 2 Check the server **Port** number field for the web service in the **Maintenance > Remote Management** screen. You must use the same port number in order to use that web service for remote management.
- 3 Try the troubleshooting suggestions for [I cannot access the Web Configurator login screen](#). Ignore the suggestions about your browser.

37.4 Cellular Problems

The SIM card cannot be detected.

- 1 Disconnect the Zyxel Device from the power supply.
- 2 Remove the SIM card from its slot.
- 3 Clean the SIM card slot of any loose debris using compressed air.
- 4 Clean the gold connectors on the SIM card with a clean lint-free cloth.
- 5 Insert the SIM card into its slot and connect the Zyxel Device to the power supply to restart it.

I get an **Invalid** SIM card alert.

- 1 Make sure you have an active plan with your ISP.
- 2 Make sure that the Zyxel Device is in the coverage area of a cellular network.

I get a weak cellular signal.

- 1 Find the location of your nearest cellular base stations, then install the Zyxel Device towards the direction of those sites. The nearest site or site with a direct line-of-sight is usually preferred.

Note: It is best to test towards more than one cellular site, as the nearest site / line-of-sight is not always the best due to the terrain, interference, density of usage, and so on. All of these factors influence the stability, availability and throughput of the link to the Zyxel Device.

- 2 Position the Zyxel Device towards a direction where coverage is expected (example the nearest town).
- 3 Conduct test measurements using the Web Configurator's **System Monitor > Cellular WAN Status** screen to obtain a report of the cellular network signal strength and quality at various test positions.

Note: It is best to reboot the Zyxel Device before each test measurement is taken to ensure that it is not camping on the previous cellular site. This is because the Zyxel Device can 'lock' onto the previous cellular site even when the new cellular site is at a much better signal level and quality.

Although installing the Zyxel Device as high as possible is the usual rule of thumb, it is sometimes possible that the Zyxel Device is in a weak coverage spot at that specific height. Adjust the height to achieve the best service possible.

Note: Cellular network signals and quality can fluctuate. A measurement taken now and a few moments later can differ substantially even if nothing apparent has changed – this can be due to many aspects, such as fading, reflections, interference, capacity due to high network traffic, and so on.

It is possible that the network topology and usage changes over time, even from one minute to the next as network utilization increases. If poor performance is experienced at a later stage, re-test different installation locations again. It is possible that the current serving cellular site has become over utilized or is out-of-service. As the network design and topology changes, so will the experience change, either for the better or for the worse.

37.5 Internet Problems

I cannot access the Internet.

- 1 Check the hardware connections and make sure the LEDs are behaving as expected. See the **Quick Start Guide**.
- 2 Check the SIM card. Maybe it has wrong settings, the account has expired, it needs to be removed and reinserted (refer to the Quick Start Guide), or it is missing. See [Section 37.7 on page 306](#) for possible SIM card problems.
- 3 Make sure you entered your ISP account information correctly on the **Network Setting > Broadband** screen. Fields on this screen are case-sensitive, so make sure [Caps Lock] is not on.
- 4 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.

- 5 If you are trying to access the Internet wirelessly, make sure that you enabled the WiFi in the Zyxel Device and your wireless client and that the WiFi settings in the wireless client are the same as the settings in the Zyxel Device.
- 6 Disconnect all the cables from your device and reconnect them.
- 7 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.

I cannot connect to the Internet using a cellular connection.

- 1 The DSL and Ethernet connections have priority in that order. If the DSL or Ethernet connection is up, then the cellular connection will be down.
- 2 Make sure you have connected a compatible cellular dongle to the USB port, if required.
- 3 Check that the Zyxel Device is within range of a cellular base station.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. Look at the LEDs, and check the LED section for more information. If the signal strength is low, try moving the Zyxel Device closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 For models that support external antennas, connect two external antennas to improve the cellular WAN signal strength. Point the antennas to the base stations directions if you know where they are, or try pointing the antennas in different directions and check which provides the strongest signal to the Zyxel Device. See the Introduction chapter for more information.

- 4 Turn the Zyxel Device off and on.
- 5 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions in [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.

37.6 WiFi Problems

[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 WiFi devices.

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

- Move your WiFi device closer to the AP if the signal strength is low.
- Reduce WiFi 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.

37.7 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.

37.8 UPnP Problems

[My computer cannot detect UPnP settings from the Zyxel Device.](#)

- 1 Make sure that UPnP is enabled in your computer. For Windows 10, see [Section 9.6 on page 165](#).
- 2 On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings > Home Networking > UPnP** screen. See [Section 9.4 on page 161](#) for details.
- 3 Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.
- 4 Reconnect the Ethernet cable.
- 5 Restart your computer.

APPENDIX A

Customer Support

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

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

For Zyxel Networks offices, see <https://www.zyxel.com/index.shtml> for the latest information.

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- <https://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <https://www.zyxel.com/cn/zh/>

India

- Zyxel Technology India Pvt Ltd.
- <https://www.zyxel.com/in/en/>

Kazakhstan

- Zyxel Kazakhstan
- <https://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <https://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd.
- <https://www.zyxel.com/th/th/>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <https://www.zyxel.com/vn/vi>

Europe

Belarus

- Zyxel BY
- <https://www.zyxel.by>

Bulgaria

- Zyxel България
- <https://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <https://www.zyxel.com/cz/cs/>

Denmark

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da/>

Finland

- Zyxel Communications
- <https://www.zyxel.com/fi/fi/>

France

- Zyxel France
- <https://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <https://www.zyxel.com/de/de/>

Hungary

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu/>

Italy

- Zyxel Communications Italy
- <https://www.zyxel.com/it/it/>

Netherlands

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

Norway

- Zyxel Communications
- <https://www.zyxel.com/no/no/>

Poland

- Zyxel Communications Poland
- <https://www.zyxel.com/pl/pl/>

Romania

- Zyxel Romania

- <https://www.zyxel.com/ro/ro>

Russia

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <https://www.zyxel.com/sk/sk/>

Spain

- Zyxel Communications ES Ltd.
- <https://www.zyxel.com/es/es/>

Sweden

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

Switzerland

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

Turkey

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr/>

UK

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

Ukraine

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

South America

Argentina

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Colombia

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Ecuador

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

South America

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Middle East

Israel

- Zyxel Communications Corporation
- <http://il.zyxel.com/>

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- <https://www.zyxel.com/us/en/>

APPENDIX B

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{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 127 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 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 (0:0:0:0:0:1 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 128 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and cannot be assigned to a multicast group.

Table 129 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 130

MAC	00	:	13	:	49	:	12	:	34	:	56
-----	----	---	----	---	----	---	----	---	----	---	----

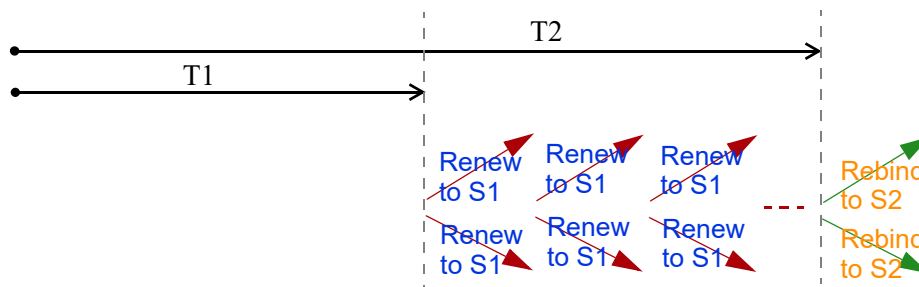
Table 131

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 unreach, 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.

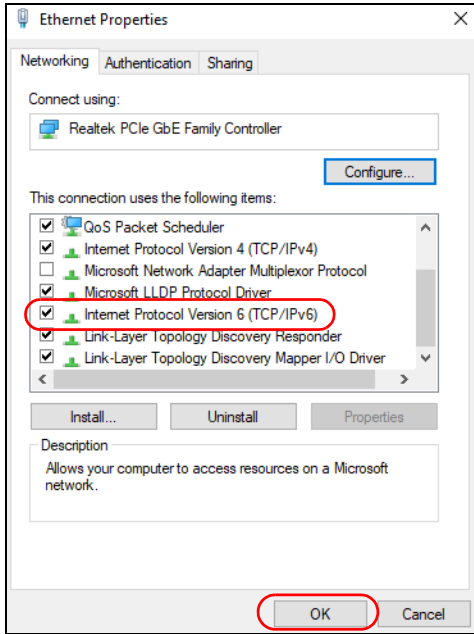
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected 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 type "cmd" in the search box..
- 5 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:f

```

APPENDIX C

Legal Information

Copyright

Copyright © 2022 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 (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 (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.

EUROPEAN UNION and 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 LTE7240-M403, the minimum distance between radio equipment and body is 25 cm.
- The maximum RF power operating for each band as follows:

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 dBm
 - 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 123.88 mW
 - The band 5470 – 5725 MHz is 612.35 mW

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 95.16 mW
 - The band 5150 – 5350 MHz is 177.42 mW
 - The band 5470 – 5725 MHz is 451.86 mW
- 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

Български (Bulgarian)	<p>C настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/EC.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	<p>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..</p>
Čeština (Czech)	<p>Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.</p>
Dansk (Danish)	<p>Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	<p>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.</p>
Eesti keel (Estonian)	<p>Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.</p>
Ελληνικά (Greek)	<p>ΜΕ ΤΗΝ ΠΑΡΟΥΣΙΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΤΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.</p>
English	<p>Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.</p>
Français (French)	<p>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.</p>
Hrvatski (Croatian)	<p>Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.</p>
Íslenska (Icelandic)	<p>Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.</p>

Italiano (Italian)	<p>Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details. Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	<p>Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. 2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozik, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your Zyxel Device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the Zyxel Device ventilation slots as insufficient airflow may harm your Zyxel Device. For example, do not place the Zyxel Device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this Zyxel Device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the Zyxel Device.
- Do not open the Zyxel Device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this Zyxel Device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this Zyxel Device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adapter first before connecting it to a power outlet.
- Do not allow anything to rest on the power adapter or cord and do NOT place the product where anyone can walk on the power adapter or cord.
- Please use the provided or designated connection cables/power cables/adapters. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adapter or cord is damaged, it might cause electrocution. Remove it from the Zyxel Device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- The following warning statements apply, where the disconnect device is not incorporated in the Zyxel Device or where the plug on the power supply cord is intended to serve as the disconnect device.
 - For permanently connected Zyxel Device, a readily accessible disconnect device shall be incorporated external to the Zyxel Device;
 - For pluggable devices, the socket-outlet shall be installed near the Zyxel Device and shall be easily accessible.

Environment Statement

ErP (LTE3301-PLUS, NR5101)

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.



About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the Zyxel Device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses please go to: https://www.zyxel.com/form/gpl_oss_software_notice.shtml

A

- access
 - troubleshooting [300](#)
- Access Control (Rules) screen [221](#)
- ACS [275](#)
- activation
 - firewalls [219](#)
 - SSID [130](#)
- Address Resolution Protocol [252](#)
- Any_WAN
 - Remote Management [270](#)
 - TR-069 traffic [277](#)
- APN information
 - obtain [107](#)
- APN Settings [110](#)
- Application Layer Gateway (ALG) [193](#)
- applications
 - Internet access [21](#)
 - wireless WAN [21](#)
- applications, NAT [196](#)
- ARP Table [215](#), [252](#), [254](#)
- authentication [144](#)
- Authentication Type
 - APN [109](#), [110](#), [112](#)
- Auto Configuration Server, see ACS [275](#)

B

- backup
 - configuration [292](#)
- backup configuration [292](#)
- Backup/Restore screen [292](#)
- Band Configuration screen [116](#)
- blinking LEDs [25](#)
- Broadband [101](#)

C

- CA [244](#)
- Cellular Band screen [116](#)
- Cellular SIM screen [115](#)
- Cellular WAN [270](#)
 - TR-069 traffic [277](#)
- Cellular WAN screen [107](#), [109](#)
- certificate
 - details [245](#)
 - factory default [238](#)
 - file format [244](#)
 - file path [242](#)
 - import [238](#), [241](#)
 - public and private keys [244](#)
 - verification [244](#)
- certificate request
 - create [238](#)
 - view [240](#)
- certificates [237](#)
 - advantages [244](#)
 - authentication [237](#)
 - CA [237](#), [244](#)
 - creating [239](#)
 - public key [237](#)
 - replacing [238](#)
 - storage space [238](#)
 - thumbprint algorithms [245](#)
 - trusted CAs [242](#)
 - verifying fingerprints [245](#)
- Certification Authority [237](#)
- Certification Authority, see CA
- certifications [324](#), [331](#)
 - viewing [325](#), [334](#)
- client list [159](#)
- configuration
 - backup [292](#)
 - firewalls [219](#)
 - restoring [293](#)
 - static route [200](#)
- contact information [308](#)
- copyright [319](#), [327](#)

Create Certificate Request screen [239](#)
creating certificates [239](#)
CTS threshold [138](#), [144](#)
customer support [308](#)
customized service [220](#)
 add [221](#)
customized services [221](#)

D

data fragment threshold [138](#), [144](#)
Data Roaming
 enable [108](#)
DDoS [218](#)
Denials of Service, see DoS
DHCP [154](#), [163](#), [172](#)
DHCP Server State [157](#)
diagnostic [296](#)
diagnostic screens [296](#)
digital IDs [237](#)
disclaimer [319](#), [327](#)
DMZ screen [192](#)
DNS [154](#), [163](#), [172](#)
DNS Values [157](#)
Domain Name [196](#)
domain name system, see DNS
DoS [218](#)
 thresholds [218](#)
DoS protection blocking
 enable [226](#)
dynamic DNS [198](#)
 wildcard [199](#)
Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard [199](#)

E

ECHO [196](#)
email
 log example [286](#)
 log setting [286](#)
Extended Service Set IDentification [126](#), [131](#)

F

factory defaults
 reset [293](#)
filters
 MAC address [133](#), [145](#)
Finger services [196](#)
firewall
 enhancing security [227](#)
 LAND attack [218](#)
 security considerations [227](#)
 traffic rule direction [225](#)
Firewall DoS screen [225](#)
Firewall General screen [219](#)
firewall rules
 direction of travel [226](#)
firewalls [217](#), [219](#)
 actions [225](#)
 configuration [219](#)
 customized service [220](#)
 customized services [221](#)
 DDoS [218](#)
 DoS [218](#)
 thresholds [218](#)
 ICMP [218](#)
 Ping of Death [218](#)
 rules [226](#)
 security [227](#)
 SYN attack [217](#)
firmware [288](#)
 version [89](#)
Firmware Upgrade screen [288](#), [291](#)
firmware upload [288](#), [291](#)
firmware version
 check [289](#), [291](#)
fragmentation threshold [138](#), [144](#)
FTP [186](#), [196](#)
 unusable [303](#)

G

General wireless LAN screen [124](#)
Guide
 Quick Start [2](#)

HHTTP [196](#)**I**ICMP [218](#)IEEE 802.11ax [124](#)IGA [194](#)ILA [194](#)Import Certificate screen [242](#)importing trusted CAs [242](#)

Inside Global Address, see IGA

Inside Local Address, see ILA

interface group [205](#)

Internet

no access [304](#)wizard setup [45](#)Internet access [21](#)wizard setup [45](#)

Internet connection

slow or erratic [305](#)

Internet Control Message Protocol, see ICMP

Internet Protocol version 6, see IPv6

IP address [164, 173](#)private [164, 173](#)WAN [102](#)IP address access control [273](#)

IP alias

NAT applications [196](#)IP Passthrough mode [120](#)IP Passthrough screen [40, 119, 120, 121, 122](#)IPv4 firewall [220](#)IPv6 [313](#)addressing [313](#)EUI-64 [315](#)global address [313](#)interface ID [315](#)link-local address [313](#)Neighbor Discovery Protocol [313](#)ping [313](#)prefix [313](#)prefix length [313](#)unspecified address [314](#)IPv6 firewall [220](#)**L**LAN [153](#)client list [159](#)DHCP [163, 172](#)DNS [163, 172](#)IP address [164, 173](#)MAC address [141, 160](#)status [90, 99](#)subnet mask [155, 164, 173](#)LAN IP address [157](#)LAN IPv6 Mode Setup [157](#)LAN Setup screen [154](#)LAN subnet mask [157](#)LAND attack [218](#)

limitations

wireless LAN [146](#)WPS [152](#)

Local Area Network, see LAN

local certificate

TR-069 client [277](#)Local Certificates screen [237](#)Log Setting screen [284](#)login [35](#)password [35](#)

Login screen

no access [300](#)logs [246, 249, 259, 284](#)**M**MAC address [134, 141, 160](#)filter [133, 145](#)LAN [160](#)MAC Authentication screen [133](#)MAC Filter [229](#)

managing the device

good habits [23](#)

using FTP. See FTP.

MBSSID [146](#)MGMT Services screen [269, 270](#)

models
 XS1930 [16](#)

module firmware [290](#)

Multi_WAN
 Remote Management [270](#)
 TR-069 traffic [277](#)

Multiple BSS, see MBSSID

N

NAT [194, 195](#)
 applications [196](#)
 IP alias [196](#)
 default server [192](#)
 DMZ host [192](#)
 example [195](#)
 global [194](#)
 IGA [194](#)
 ILA [194](#)
 inside [194](#)
 local [194](#)
 multiple server example [186](#)
 outside [194](#)
 port number [196](#)
 services [196](#)

NAT ALG screen [193](#)

NAT example [197](#)

NCC [17](#)

NCC Management [17](#)

NCC web portal [17](#)

Nebula Mobile App [23](#)

Nebula Web Portal [18](#)

Network Address Translation, see NAT

network disconnect
 temporary [290](#)

network map [40, 87](#)

network type
 select [116](#)

NNTP [196](#)

Nslookup test [297](#)

O

Others screen [137](#)

P

password [35](#)
 admin [300](#)
 good habit [23](#)
 lost [300](#)
 user [300](#)

PBC [147](#)

PIN Protection [115](#)

PIN, WPS [147](#)
 example [149](#)

Ping of Death [218](#)

Ping test [297](#)

Ping/TraceRoute/Nslookup screen [296](#)

PLMN Configuration screen [117](#)

Point-to-Point Tunneling Protocol, see PPTP

POP3 [196](#)

port forwarding rule
 add/edit [187](#)

Port Forwarding screen [186, 187](#)

Port Triggering
 add new rule [191](#)

Port Triggering screen [189](#)

ports [25](#)

PPTP [197](#)

preamble [140, 144](#)

private IP address [164, 173](#)

problem
 troubleshooting [299](#)

Protocol (Customized Services) screen [220](#)

Protocol Entry
 add [221](#)

Push Button Configuration, see PBC

push button, WPS [147](#)

Q

Quick Start Guide [2](#)

R

Reboot screen [294](#)

- remote management
 - TR-069 [275](#)
 - Remote Procedure Calls, see RPCs [275](#)
 - RESET Button [33](#)
 - reset to factory defaults [293](#)
 - restart system [294](#)
 - restore default settings
 - after firmware upgrade [289](#)
 - restoring configuration [293](#)
 - RFC 1058, see RIP
 - RFC 1389, see RIP
 - RFC 1631 [185](#)
 - RFC 3164 [246](#)
 - RIP [184](#)
 - router features [21](#)
 - Routing Information Protocol, see RIP
 - Routing Table screen [254](#)
 - RPPCs [275](#)
 - RTS threshold [138, 144](#)
- ## S
- security
 - network [227](#)
 - wireless LAN [144](#)
 - Security Log [248](#)
 - Security Parameter Index, see SPI
 - service access control [270, 272](#)
 - Service Set [126, 131](#)
 - services
 - port forwarding [196](#)
 - setup
 - firewalls [219](#)
 - static route [200](#)
 - SIM card
 - status [92, 260](#)
 - SIM configuration [114](#)
 - SMTP [196](#)
 - SNMP [197](#)
 - SNMP trap [197](#)
 - SPI [218](#)
 - SSH
 - unusable [303](#)
 - SSID [145](#)
 - activation [130](#)
 - MBSSID [146](#)
 - static DHCP [159](#)
 - configuration [161](#)
 - Static DHCP screen [159](#)
 - static route [175, 184](#)
 - configuration [200](#)
 - status [87](#)
 - firmware version [89](#)
 - LAN [90, 99](#)
 - WAN [89](#)
 - wireless LAN [90](#)
 - status indicators [25](#)
 - subnet mask [164, 173](#)
 - SYN attack [217](#)
 - syslog
 - protocol [246](#)
 - severity levels [246](#)
 - syslog logging
 - enable [285](#)
 - syslog server
 - name or IP address [286](#)
 - system
 - firmware [288](#)
 - version [89](#)
 - module firmware [290](#)
 - password [35](#)
 - status [87](#)
 - LAN [90, 99](#)
 - WAN [89](#)
 - wireless LAN [90](#)
 - time [278](#)
- ## T
- Telnet
 - unusable [303](#)
 - thresholds
 - data fragment [138, 144](#)
 - DoS [218](#)
 - RTS/CTS [138, 144](#)
 - time [278](#)
 - TR-069 [275](#)
 - authentication [277](#)
 - TR-069 Client screen [275](#)

Trace Route test [297](#)
troubleshooting [299](#)
Trust Domain
 add [272](#)
Trust Domain screen [271](#)
Trusted CA certificate
 view [243](#)
Trusted CA screen [241](#)
Turning on UPnP
 Windows 7 example [165](#)
TWT (Target Wakeup Time) [124](#)

U

Universal Plug and Play, see UPnP
upgrading firmware [288](#)
upgrading module firmware [290](#)
UPnP [161](#)
 forum [154](#)
 security issues [154](#)
 state [162](#)
 usage confirmation [154](#)
UPnP screen [161](#)
UPnP-enabled Network Device
 auto-discover [167](#)

W

WAN
 status [89](#)
 Wide Area Network, see WAN [101](#)
warranty [325, 334](#)
 note [326, 334](#)
Web Configurator
 login [35](#)
 password [35](#)
WEP [127](#)
WEP Encryption [128, 129](#)
WiFi
 MBSSID [146](#)
WiFi standards
 comparison table [124](#)
WiFi6 introduction [124](#)

Wireless General screen [124](#)
wireless LAN [123](#)
 authentication [144](#)
 example [143](#)
 fragmentation threshold [138, 144](#)
 limitations [146](#)
 MAC address filter [133, 145](#)
 preamble [140, 144](#)
 RTS/CTS threshold [138, 144](#)
 security [144](#)
 SSID [145](#)
 activation [130](#)
 status [90](#)
 WPS [147, 149](#)
 example [150](#)
 limitations [152](#)
 PIN [147](#)
 push button [147](#)
Wireless tutorial [53](#)
wizard setup
 Internet [45](#)
WMM screen [136](#)
WPA [127](#)
WPA2 [127](#)
WPA2-PSK [127](#)
WPA3-SAE (Simultaneous Authentication of Equals handshake) [127](#)
WPA-PSK (WiFi Protected Access-Pre-Shared Key) [127](#)
WPS [147, 149](#)
 example [150](#)
 limitations [152](#)
 PIN [147](#)
 example [149](#)
 push button [147](#)
WPS screen [134](#)

Z

Zyxel Air [17](#)
Zyxel Air app [17](#)
Zyxel Nebula Cloud Center [17](#)