



Questo manuale d'istruzione è fornito da [trovaprezzi.it](#). Scopri tutte le offerte per [ZyXEL LTE5398-M904](#) o cerca il tuo prodotto tra le [migliori offerte di Modem e Router](#)



Questo manuale d'istruzione è fornito da [trovaprezzi.it](#). Scopri tutte le offerte per [ZyXEL LTE5398-M904](#) o cerca il tuo prodotto tra le [migliori offerte di Modem e Router](#)

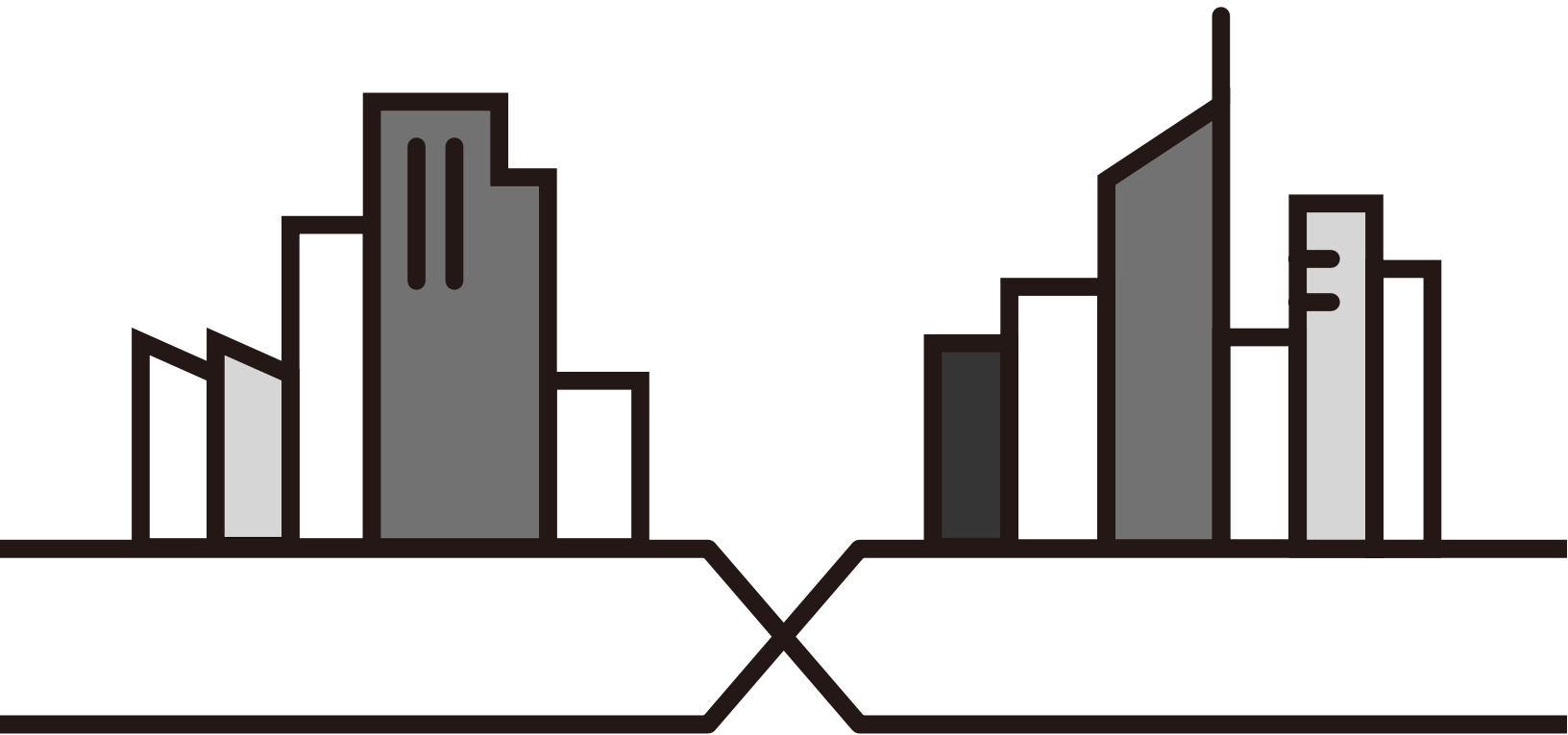
ZYXEL

User's Guide

LTE Series

Default Login Details	
LAN IP Address	http://192.168.1.1
Login	admin
Password	See the Zyxel Device label

Version 1.0-4.0 Ed 2, 12/2021



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

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

- More Information

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



Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

- The LTE 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 		

Contents Overview

User's Guide	15
Introduction	16
Hardware	21
Web Configurator	37
Quick Start	47
Tutorials	50
Technical Reference	81
Connection Status	82
Broadband	94
Wireless	114
Home Networking	142
Routing	159
Network Address Translation (NAT)	169
DNS	185
USB Service	189
Firewall	194
MAC Filter	205
Parental Control	207
Certificates	213
Voice	222
Log	237
Traffic Status	240
VoIP Status	243
ARP Table	246
Routing Table	248
WLAN Station Status	251
Cellular WAN Status	253
System	259
User Account	260
Remote Management	263
TR-069 Client	269
Time Settings	271
Email Notification	274
Log Setting	276
Firmware Upgrade	280
Backup/Restore	282
Diagnostic	285

Troubleshooting	287
Appendices	296

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	6
 Part I: User's Guide.....	 15
Chapter 1	
Introduction	16
1.1 Overview	16
1.1.1 Web-based Configurator	17
1.2 Applications for the Zyxel Device	17
1.3 Manage the Zyxel Device	19
1.4 Good Habits for Managing the Zyxel Device	20
 Chapter 2	
Hardware	21
2.1 Device Panels	21
2.2 LEDs (Lights)	25
2.3 Panel Ports and Buttons	29
2.3.1 Turning On or Off WiFi	30
2.3.2 RESET Button	33
2.4 Wall Mounting	35
 Chapter 3	
Web Configurator.....	37
3.1 Overview	37
3.1.1 Access the Web Configurator	37
3.2 Web Configurator Layout	39
3.2.1 Settings Icon	39
3.2.2 Widget and Check Icons	44
 Chapter 4	
Quick Start	47
4.1 Overview	47
4.2 Quick Start Setup	47
4.3 Quick Start Setup – Time Zone	47

4.4 Quick Start Setup – Internet Connection	48
4.4.1 Successful Internet Connection	48
4.4.2 Unsuccessful Internet Connection	49
4.5 Quick Start Setup – WiFi	49
4.6 Quick Start Setup – Finish	49

Chapter 5

Tutorials50

5.1 Overview	50
5.2 Wired Network Setup	50
5.2.1 Setting Up an Ethernet Connection	50
5.3 WiFi Network Setup	52
5.3.1 Changing Security on a WiFi Network	53
5.3.2 Connecting to the Zyxel Device's WiFi Network Using WPS	55
5.4 Cellular Network Setup	59
5.4.1 Setting up a Cellular Network Connection	59
5.5 USB Applications	60
5.5.1 File Sharing	60
5.5.2 Using FTP	64
5.6 Network Security	64
5.6.1 Configuring a Firewall Rule	64
5.6.2 Parental Control	67
5.6.3 Configuring a MAC Address Filter	72
5.7 Internet Calls	73
5.7.1 Configuring VoIP	73
5.7.2 Adding a SIP Service Provider	73
5.7.3 Adding a SIP Account	74
5.7.4 Configuring a Phone	75
5.7.5 Making a VoIP Call	76
5.7.6 Making a VoLTE Phone Call	77
5.8 Device Maintenance	77
5.8.1 Upgrading the Firmware	77
5.8.2 Backing up the Device Configuration	78
5.8.3 Restoring the Device Configuration	79

Part II: Technical Reference 81

Chapter 6

Connection Status82

6.1 Connection Status Overview	82
6.1.1 Connectivity	82

6.1.2 Icon and Device Name	83
6.1.3 System Info	83
6.1.4 Cellular Info	85
6.1.5 WiFi Settings	90
6.1.6 Guest WiFi Settings	91
6.1.7 LAN	92

Chapter 7

Broadband.....94

7.1 Overview	94
7.1.1 What You Can Do in this Chapter	94
7.1.2 What You Need to Know	95
7.1.3 Before You Begin	95
7.2 Broadband	95
7.2.1 Add or Edit Internet Connection	96
7.3 WAN Backup	100
7.4 Ethernet WAN	101
7.5 Cellular WAN	101
7.6 Cellular APN	102
7.6.1 Edit Cellular APN1/APN2	103
7.7 Cellular SIM Configuration	105
7.8 Cellular Band Configuration	106
7.9 Cellular PLMN Configuration	107
7.10 Cellular IP Passthrough	110
7.11 Cellular Lock	111
7.12 Cellular SMS	112
7.12.1 Send New Message Screen	112

Chapter 8

Wireless.....114

8.1 Overview	114
8.1.1 What You Can Do in this Chapter	114
8.1.2 What You Need to Know	114
8.2 Wireless General Settings	115
8.2.1 No Security	117
8.2.2 More Secure (Recommended)	118
8.3 Guest/More AP	119
8.4 More AP Edit	120
8.5 MAC Authentication	123
8.6 WPS	124
8.7 WMM	126
8.8 Others Screen	127
8.9 WLAN Scheduler	129

8.9.1 Add or Edit Rules	130
8.10 Channel Status	131
8.11 Technical Reference	132
8.11.1 WiFi Network Overview	132
8.11.2 Additional Wireless Terms	134
8.11.3 WiFi Security Overview	134
8.11.4 Signal Problems	136
8.11.5 WiFi Protected Setup (WPS)	136

Chapter 9

Home Networking142

9.1 Overview	142
9.1.1 What You Can Do in this Chapter	142
9.1.2 What You Need To Know	142
9.2 LAN Setup	143
9.3 Static DHCP	147
9.3.1 Before You Begin	147
9.4 UPnP	149
9.5 Technical Reference	150
9.6 Turn on UPnP in Windows 10 Example	151
9.6.1 Auto-discover Your UPnP-enabled Network Device	153
9.7 Web Configurator Easy Access in Windows 10	156

Chapter 10

Routing159

10.1 Overview	159
10.2 Configure Static Route	159
10.2.1 Add or Edit Static Route	160
10.3 DNS Route	164
10.3.1 Add or Edit DNS Route	165
10.4 Policy Route	165
10.4.1 Add or Edit Policy Route	166
10.5 RIP Overview	168
10.5.1 RIP	168

Chapter 11

Network Address Translation (NAT)169

11.1 Overview	169
11.1.1 What You Can Do in this Chapter	169
11.1.2 What You Need To Know	169
11.2 Port Forwarding	170
11.2.1 Port Forwarding	170
11.2.2 Add or Edit Port Forwarding	171

11.3 Port Triggering	173
11.3.1 Add or Edit Port Triggering Rule	175
11.4 DMZ	176
11.5 ALG	177
11.6 Address Mapping	178
11.6.1 Address Mapping Screen	178
11.6.2 Add New Rule Screen	179
11.7 Sessions	180
11.8 Technical Reference	181
11.8.1 NAT Definitions	181
11.8.2 What NAT Does	181
11.8.3 How NAT Works	182
11.8.4 NAT Application	182
Chapter 12	
DNS.....	185
12.1 DNS Overview	185
12.1.1 What You Can Do in this Chapter	185
12.1.2 What You Need To Know	186
12.2 DNS Entry	186
12.2.1 Add or Edit DNS Entry	187
12.3 Dynamic DNS	187
Chapter 13	
USB Service	189
13.1 USB Service Overview	189
13.1.1 What You Need To Know	189
13.1.2 Before You Begin	190
13.2 USB Service	190
13.2.1 Add New Share	192
13.2.2 Add New User Screen	193
Chapter 14	
Firewall.....	194
14.1 Overview	194
14.1.1 What You Need to Know About Firewall	194
14.2 Firewall	195
14.2.1 What You Can Do in this Chapter	195
14.3 Firewall General Settings	195
14.4 Protocol (Customized Services)	197
14.4.1 Add Customized Service	197
14.5 Access Control (Rules)	198
14.5.1 Add New ACL Rule	199

14.6 DoS	201
14.7 Firewall Technical Reference	202
14.7.1 Firewall Rules Overview	202
14.7.2 Guidelines For Security Enhancement With Your Firewall	203
14.7.3 Security Considerations	204
Chapter 15	
MAC Filter	205
15.1 MAC Filter Overview	205
15.2 MAC Filter	205
15.2.1 Add New Rule	206
Chapter 16	
Parental Control	207
16.1 Parental Control Overview	207
16.2 Parental Control Settings	207
16.2.1 Add or Edit a Parental Control Profile	208
Chapter 17	
Certificates	213
17.1 Certificates Overview	213
17.1.1 What You Can Do in this Chapter	213
17.2 What You Need to Know	213
17.3 Local Certificates	213
17.3.1 Create Certificate Request	214
17.3.2 View Certificate Request	215
17.4 Trusted CA	217
17.5 Import Trusted CA Certificate	218
17.6 View Trusted CA Certificate	218
17.7 Certificates Technical Reference	219
17.7.1 Verify a Certificate	220
Chapter 18	
Voice	222
18.1 Overview	222
18.1.1 What You Can Do in this Chapter	222
18.2 Voice Mode	222
18.2.1 What You Need to Know About VoIP	223
18.3 Before You Begin	224
18.3.1 SIP Account	224
18.3.2 SIP Account Entry Edit	225
18.3.3 SIP Service Provider	227
18.3.4 Provider Entry Edit	227

18.4 Phone	231
18.4.1 Phone Device	231
18.4.2 Phone Device Edit	231
18.5 Phone Region	233
18.6 Call Rule	233
18.7 Call History	234
18.7.1 Call Summary	235
Chapter 19	
Log	237
19.1 Log Overview	237
19.1.1 What You Can Do in this Chapter	237
19.1.2 What You Need To Know	237
19.2 System Log	238
19.3 Security Log	238
Chapter 20	
Traffic Status	240
20.1 Traffic Status Overview	240
20.1.1 What You Can Do in this Chapter	240
20.2 WAN Status	240
20.3 LAN Status	241
Chapter 21	
VoIP Status	243
21.1 VoIP Status Screen	243
Chapter 22	
ARP Table	246
22.1 ARP Table Overview	246
22.1.1 How ARP Works	246
22.2 ARP Table	246
Chapter 23	
Routing Table	248
23.1 Routing Table Overview	248
23.2 Routing Table	248
Chapter 24	
WLAN Station Status	251
24.1 WLAN Station Status Overview	251
Chapter 25	
Cellular WAN Status	253

25.1 Cellular WAN Status Overview	253
25.2 Cellular WAN Status	253
Chapter 26	
System.....	259
26.1 System Overview	259
26.2 System	259
Chapter 27	
User Account.....	260
27.1 User Account Overview	260
27.2 User Account	260
27.2.1 User Account Add or Edit	261
Chapter 28	
Remote Management.....	263
28.1 Overview	263
28.2 MGMT Services	263
28.3 MGMT Services for IP Passthrough	264
28.4 Trust Domain	265
28.5 Add Trust Domain	266
28.6 Trust Domain for IP Passthrough	266
28.7 Add Trust Domain	267
Chapter 29	
TR-069 Client.....	269
29.1 Overview	269
29.2 TR-069 Client	269
Chapter 30	
Time Settings.....	271
30.1 Time Settings Overview	271
30.2 Time	271
Chapter 31	
Email Notification.....	274
31.1 Email Notification Overview	274
31.2 Email Notification	274
31.2.1 E-mail Notification Edit	275
Chapter 32	
Log Setting	276
32.1 Log Setting Overview	276

32.2 Log Settings	276
32.2.1 Example Email Log	278
Chapter 33	
Firmware Upgrade	280
33.1 Overview	280
33.2 Firmware Upgrade	280
Chapter 34	
Backup/Restore	282
34.1 Backup/Restore Overview	282
34.2 Backup/Restore	282
34.3 Reboot	284
Chapter 35	
Diagnostic.....	285
35.1 Diagnostic Overview	285
35.2 What You Need to Know	285
35.3 Ping/TraceRoute/Nslookup Test	285
Chapter 36	
Troubleshooting.....	287
36.1 Overview	287
36.2 Power and Hardware Problems	287
36.3 Device Access Problems	288
36.4 Cellular Problems	291
36.5 Internet Problems	292
36.6 WiFi Problems	294
36.7 USB Problems	294
36.8 UPnP Problems	295
Part III: Appendices	296
Appendix A Customer Support	297
Appendix B IPv6.....	302
Appendix C Legal Information	308
Index	315

PART I

User's Guide

CHAPTER 1

Introduction

1.1 Overview

Zyxel Device refers to these models as outlined below.

OUTDOOR

- LTE7240-M403
- LTE7480-M804
- LTE7490-M904

INDOOR

- LTE3301-PLUS
- LTE5388-M804
- LTE5398-M904
- LTE3316-M604
- LTE3202-M437

The Zyxel Device is an LTE (Long Term Evolution) router. The following table describes the feature differences of the Zyxel Device by model.

Table 1 Zyxel Device Comparison Table

FEATURE	LTE7240-M403	LTE7480-M804	LTE7490-M904	LTE3301-PLUS
2.4 GHz WLAN	Yes	Yes	Yes	Yes
5 GHz WLAN	No	No	No	Yes
LTE Speed	150/50 Mbps (FDD-LTE)	600/100 Mbps	1200/150 Mbps	300/50 Mbps
Ethernet Port	x1 GbE port (PoE)	x1 GbE port (PoE)	x1 GbE port (PoE)	x4 GbE ports
Ethernet WAN	No	No	No	LAN4 can be a WAN backup
WAN Priority	No	No	No	Yes
Carrier Aggregation	No	Yes	Yes	No
IP Passthrough	Yes	Yes	Yes	Available when LAN4 does not act as a WAN backup
USB for File Sharing	Yes	No	No	Yes
External Antennas	No	No	No	Yes
PoE Injector	Yes	Yes	Yes	No
Wall Mount	Yes	Yes	Yes	No
Pole Mount	No	Yes	Yes	No
Firmware Version	2.00	1.00	1.00	1.00

Table 1 Zyxel Device Comparison Table (continued)

FEATURE	LTE7240-M403	LTE7480-M804	LTE7490-M904	LTE3301-PLUS
Parental Control	No	Yes	No	Yes
Voice	No	Yes	No	No
TR069	Yes	Yes	Yes	Yes

Table 2 Zyxel Device Comparison Table

FEATURE	LTE5388-M804	LTE5398-M904	LTE3316-M604	LTE3202-M437
2.4 GHz WLAN	Yes	Yes	Yes	Yes
5 GHz WLAN	Yes	Yes	Yes	No
LTE Speed	600/100 Mbps	1200/150 Mbps	300/50 Mbps	150/50 Mbps
Ethernet Port	x2 GbE ports	x2 GbE ports	x4 GbE ports	x4 FE ports
Ethernet WAN	LAN1 can be a WAN backup	LAN1 can be a WAN backup	LAN1 can be a WAN backup	No
WAN Priority	Yes	Yes	Yes	No
Carrier Aggregation	Yes	Yes	Yes	No
IP Passthrough	Available when LAN1 does not act as a WAN backup	Available when LAN1 does not act as a WAN backup	Available when LAN1 does not act as a WAN backup	Yes
USB for File Sharing	Yes	Yes	No	No
External Antennas	No	No	No	Supports the SMA type
PoE Injector	No	No	No	No
Wall Mount	No	No	Yes	No
Pole Mount	No	No	No	No
Firmware Version	1.00	1.00	2.00	1.00
Parental Control	Yes	Yes	No	Yes
Voice	Yes	Yes	Yes	No
TR069	Yes	Yes	Yes	Yes

Note: The features listed in the comparison table are valid at the time of writing and are subject to change without prior notice.

1.1.1 Web-based Configurator

The embedded Web-based Configurator enables straightforward management and maintenance. Just insert the SIM card (with an active data plan) and make the hardware connections. See the Quick Start Guide for how to do the hardware installation, wall or pole mounting, and Internet setup.

1.2 Applications for the Zyxel Device

Wireless WAN

The Zyxel Device can connect to the Internet through a 2G/3G/4G LTE SIM card to access a wireless WAN connection. Just insert a SIM card into the SIM card slot at the bottom of the Zyxel Device.

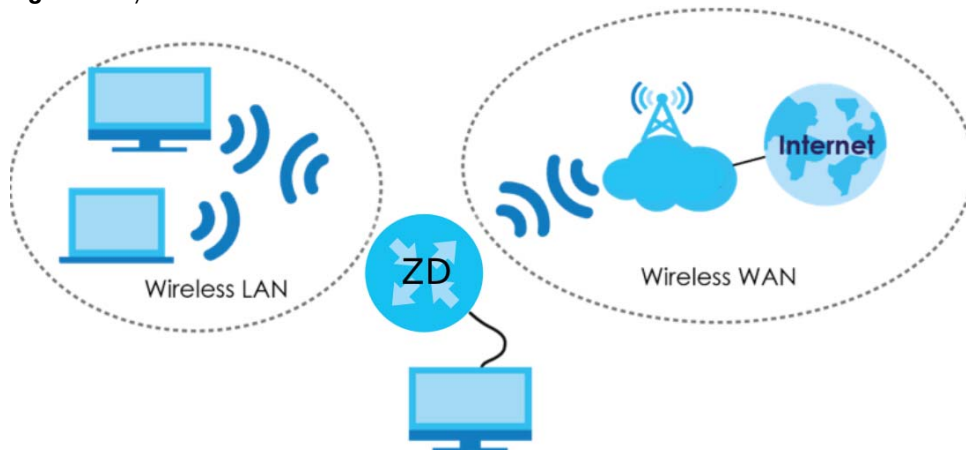
Note: You must insert the SIM card into the card slot before turning on the Zyxel Device.

You can install two external antennas to improve your wireless WAN signal strength. See [Table 1 on page 16](#) and [Table 2 on page 17](#) for the feature differences.

Wireless LAN (WiFi)

Wireless 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 wireless network with strong security.

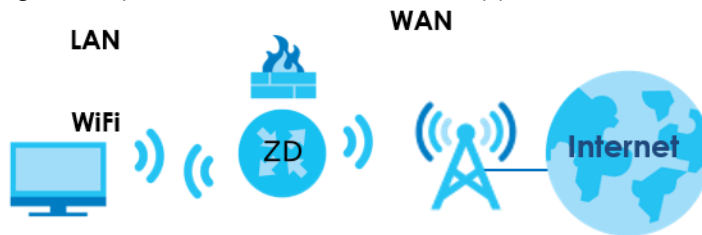
Figure 1 Zyxel Device's Wireless LAN



Internet Access

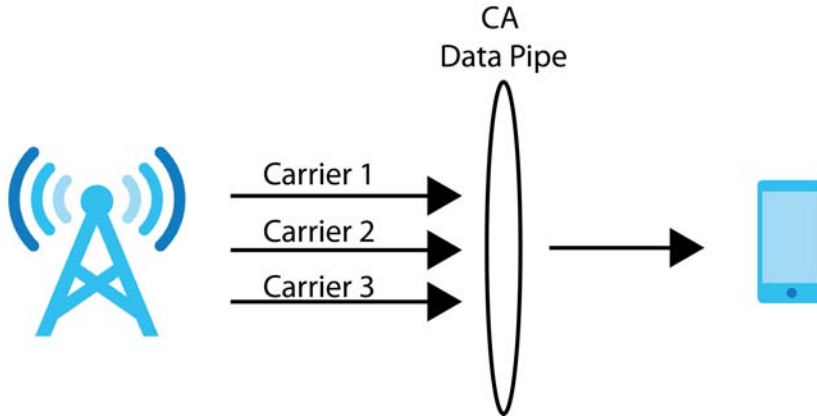
Your Zyxel Device provides shared Internet access by connecting to a cellular network. A computer can connect to the Zyxel Device's PoE injector or a **LAN** port for configuration through the Web Configurator.

Figure 2 Zyxel Device's Internet Access Application



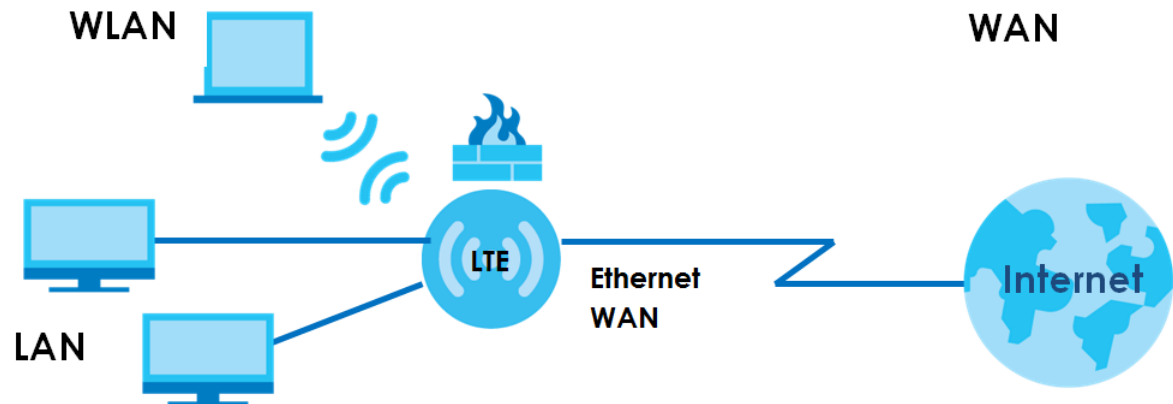
Carrier Aggregation

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

Figure 3 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 via an Ethernet connection and still use the Firewall function on the Zyxel Device.

Figure 4 Zyxel Device's Internet Access Application: Ethernet WAN

WAN Priority

The WAN connection priority is as follows:

- 1 Ethernet WAN
- 2 Cellular WAN (3G/4G)

1.3 Manage the Zyxel Device

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

- Web Configurator. This is recommended for everyday management of the Zyxel Device using a (supported) web browser. See [Chapter 3 on page 25](#).

- LTE Ally is available in Google Play and the App Store. Use the LTE Ally app on your mobile device to do the following:
 - Show how to adjust the Zyxel Device mounting angle to find the optimal LTE signal strength to/from the LTE base station
 - Check your LTE speed and LTE data usage

1.4 Good Habits for Managing the Zyxel Device

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

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

CHAPTER 2

Hardware

2.1 Device Panels

Front / Top Panels

Figure 5 Front Panel (LTE3301-PLUS)

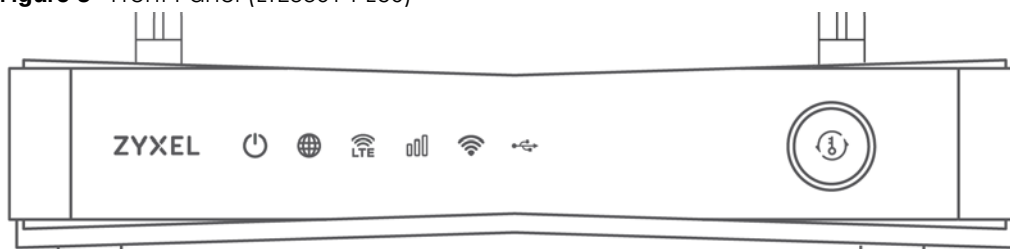


Figure 6 Front Panel (LTE7240-M403)



Figure 7 Front Panel (LTE5388-M804 / LTE5398-M904)



Figure 8 Top Panel (LTE5388-M804 / LTE5398-M904)



Figure 9 Front Panel (LTE3316-M604)

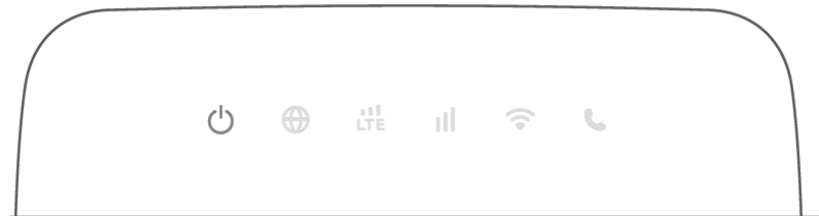


Figure 10 Top Panel (LTE3316-M604)

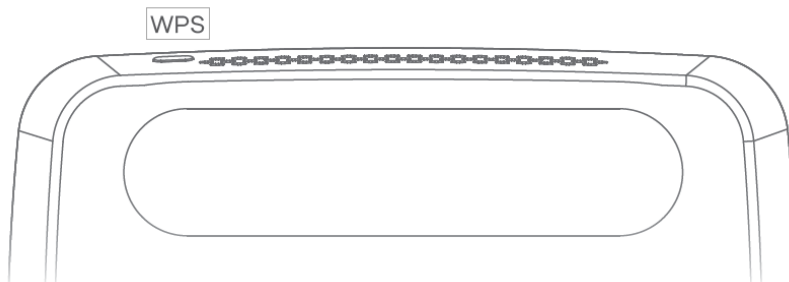


Figure 11 Front Panel (LTE3202-M437)



Bottom / Rear / Side Panels

Figure 12 Rear Panel (LTE3301-PLUS)

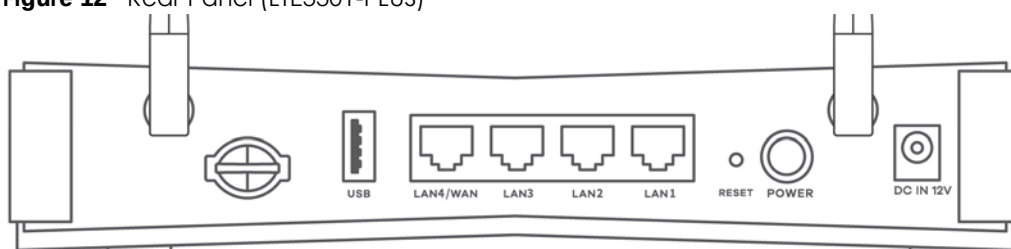


Figure 13 Bottom Panel (LTE7240-M403)



Figure 14 Bottom Panel (LTE7490-M904 /LTE7480-M804)



Figure 15 Rear Panel (LTE5388-M804 / LTE5398-M904)

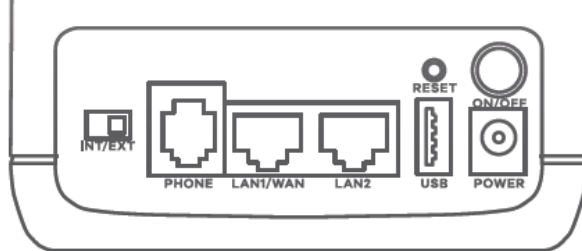


Figure 16 Bottom Panel (LTE5388-M804 / LTE5398-M904)

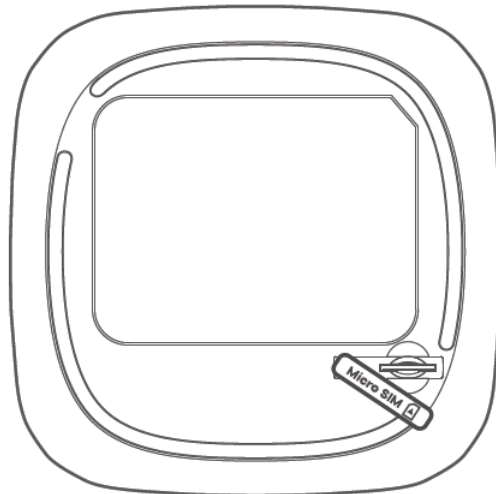


Figure 17 Rear Panel (LTE3316-M604)

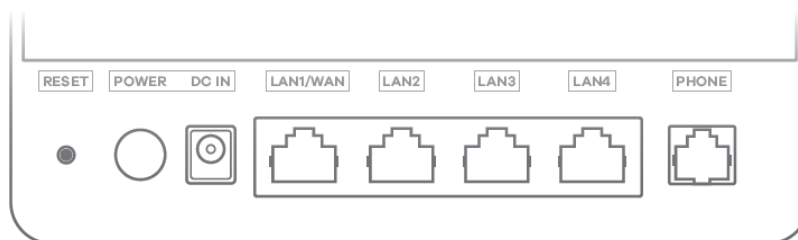


Figure 18 Side Panel (LTE3316-M604)

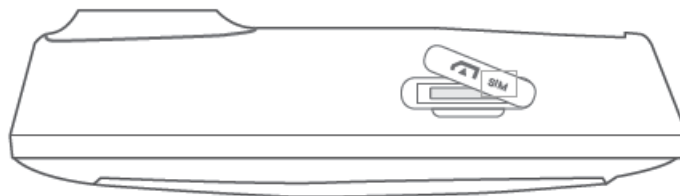
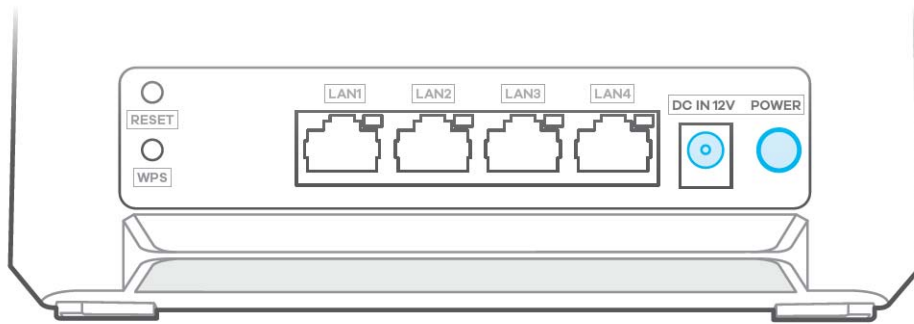


Figure 19 Rear Panel (LTE3202-M437)

2.2 LEDs (Lights)

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

Table 3 LTE3301-PLUS LED Descriptions

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.

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 LTE7240-M403 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	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.
ETHERNET	Green	On	The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Off	The Zyxel Device does not have an Ethernet connection with the LAN.
LTE/3G/2G	Green	On	The Zyxel Device is registered and successfully connected to a 4G network.
		Blinking (slow)	The Zyxel Device is connected to a 3G/2G network.
		Blinking (fast)	The Zyxel Device is trying to connect to a 4G/3G/2G network.
		Off	There is no service.
WLAN	Green	On	The wireless network is activated.
		Off	The wireless network is not activated.
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 SIM card inserted, the SIM card is invalid, the PIN code is not correct.
		Off	There is no signal or the signal strength is below the poor level.

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

Table 5 LTE7480-M804 / LTE7490-M904 LED Descriptions

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.

Table 6 LTE5388-M804 / LTE5398-M904 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
Power/System or 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	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.
Internet/SMS	Green	On	There is Internet connection.
		Blinking	There is a new SMS message.
		Off	There is no Internet connection.
LTE/3G 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 LTE/3G signal or the signal strength is below the poor level.
WiFi/WPS	Green	On	The WiFi AP is activated.
		Blinking (fast)	Data is being transmitted and received.
		Blinking (slow)	The WPS is activated.
Voice	Green	On	A telephone connected to the PHONE port has its receiver off the hook.
		Blinking	The Zyxel Device is receiving an incoming call.
		Off	A telephone connected to the PHONE port has its receiver on the hook.
LAN	Green	On	The Zyxel Device recognizes an Ethernet cable through the LAN port.
		Blinking	The Zyxel Device is sending/receiving data through the LAN.
		Off	The wireless network is not activated.

Table 7 LTE3316-M604 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
Power	White	On	The Zyxel Device is receiving power and functioning properly.
		Blinking	The Zyxel Device is in the process of starting up or default restoring.
		Off	The Zyxel Device is not receiving power.
Internet	White	On	The Zyxel Device's WAN connection is ready, but there is no traffic.
		Blinking	The Zyxel Device is transmitting and receiving data through the WAN.
		Off	The WAN connection is not ready, or has failed.
LTE/3G/Ethernet	White	On	The Zyxel Device is successfully connected to a 4G network.
		Blinking	The Zyxel Device is successfully connected to a 3G network.
	Green	On	The Zyxel Device is successfully connected to an Ethernet WAN network.
LTE/3G Signal Strength	Green	On	The signal strength is good.
	Orange	On	The signal strength is fair.
	Red	On	The signal strength is poor.
		Blinking	A valid SIM card is inserted, but no signal is detected.
WiFi/WPS	White	On	This indicates either 5G and 2.4G wireless LAN are both on or the 5G wireless LAN is on.
		Blinking	This indicates either 5G and 2.4G WPS are both on or the 5G WPS is on.
	Green	On	The 2.4G wireless LAN is on, but the Zyxel Device is not sending/receiving data through the wireless LAN.
		Blinking	The Zyxel Device is ready and the 2.4G WPS is on.
Voice	White	On	A telephone connected to the PHONE port has its receiver on the hook.
		Blinking	The Zyxel Device is receiving an incoming call.
		Off	A telephone connected to the PHONE port has its receiver off the hook.
LAN	Green	On	A 10/100 Mbps LAN connection is ready.
		Blinking	The Zyxel Device is sending/receiving data at 10/100 Mbps through a LAN port.
		Off	The wireless network is not activated.
	Orange	On	A 1000 Mbps LAN connection is ready.
		Blinking	The Zyxel Device is sending/receiving data at 1000 Mbps through a LAN port.
		Off	The wireless network is not activated.

Table 8 LTE3202-M437 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
Network	Blue	Blinking	The Zyxel Device is booting.
		On	The Zyxel Device is successfully connected to a 4G network.
	Green	On	The Zyxel Device is successfully connected to a 3G network.
	Yellow	On	The Zyxel Device is successfully connected to a 2G network.
	Red	On	There is a system failure during POST.
		Blinking	There is no service.
Signal Strength (Using for 4G/3G/2G)	Blue	On	The signal strength is excellent.
	Green	On	The signal strength is fair.
	Red	Blinking	The signal strength is poor.
LAN	Blue	On	The Ethernet LAN connection is ready.
		Blinking	The Zyxel Device is sending/receiving data on the LAN.
		Off	The Zyxel Device does not have an Ethernet connection on the LAN.
WiFi/WPS	Blue	On	The WiFi is activated.
		Blinking	The WPS process is in progress.
		Off	The WiFi is not activated.
SMS	Blue	Blinking	There is a new SMS message.
		Off	There is no unread SMS message.

2.3 Panel Ports and Buttons

The connection ports are located on the bottom or rear panels.

The following table describes the items on the bottom or rear panels.

Table 9 Panel Ports and Buttons

LABELS	DESCRIPTION
ANT1-ANT2	Install the external antennas to strengthen the cellular signal.
USB	The USB port of the Zyxel Device is used for file sharing.
LAN/Ethernet	Connect a computer through the PoE injector for configuration. Connect the PoE injector to a power outlet to start the device.
LAN/WAN	For LTE5388-M804 / LTE5398-M904 / LTE3316-M604, connect an RJ45 cable to a modem to connect to the Internet when using a LAN port as a WAN port.
LAN	For LTE5388-M804 / LTE5398-M904 / LTE3316-M604 / LTE3202-M437, connect an RJ45 cable to a computer to connect to the internal network In using a LAN port.
WiFi	Press the WLAN (WiFi) button for more than 5 seconds to enable the wireless function. To set up a WiFi connection between the Zyxel Device and a wireless client, press the WPS button for longer than 5 seconds for LTE5388-M804 / LTE5398-M904, and press the WPS button for 2 seconds for LTE3316-M604.

LABELS	DESCRIPTION
WPS	After the wireless function 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. To enable WPS, press the WPS button for less than 5 seconds for LTE5388-M804 / LTE5398-M904, and press the WPS button for more than 5 seconds for LTE3316-M604. Press the WPS button for 5 seconds to enable WiFi and then press the WPS button for one second to enable WPS for the LTE3202-M437.
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.
PHONE	For LTE5388-M804 / LTE5398-M904 / LTE3316-M604, the phone port is used for VoIP and VoLTE.
INT/EXT	For LTE5388-M804 / LTE5398-M904, the internal/external switch is used for selecting between the internal or external LTE antenna.

2.3.1 Turning On or Off WiFi

Use the **WPS** or **WiFi/WPS** button on the Zyxel Device to turn on or turn off the wireless network.

Note: Use the WiFi function of the / LTE7480-M804 / LTE7490-M904 / LTE3202-M437 for configuration (for example, connect to the LTE Ally app of your mobile device to find the optimal LTE signal strength and manage your / LTE7480-M804 / LTE7490-M904).

Note: WiFi is for the local management use only.

Figure 20 LTE3301-PLUS WiFi/WPS Button

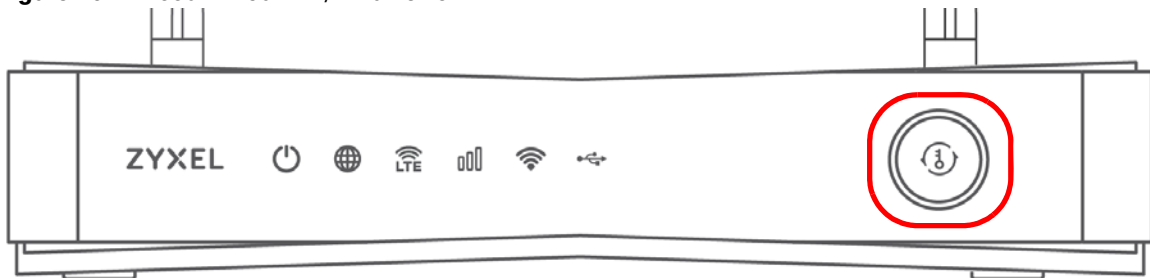


Figure 21 LTE7240-M403 WiFi Button

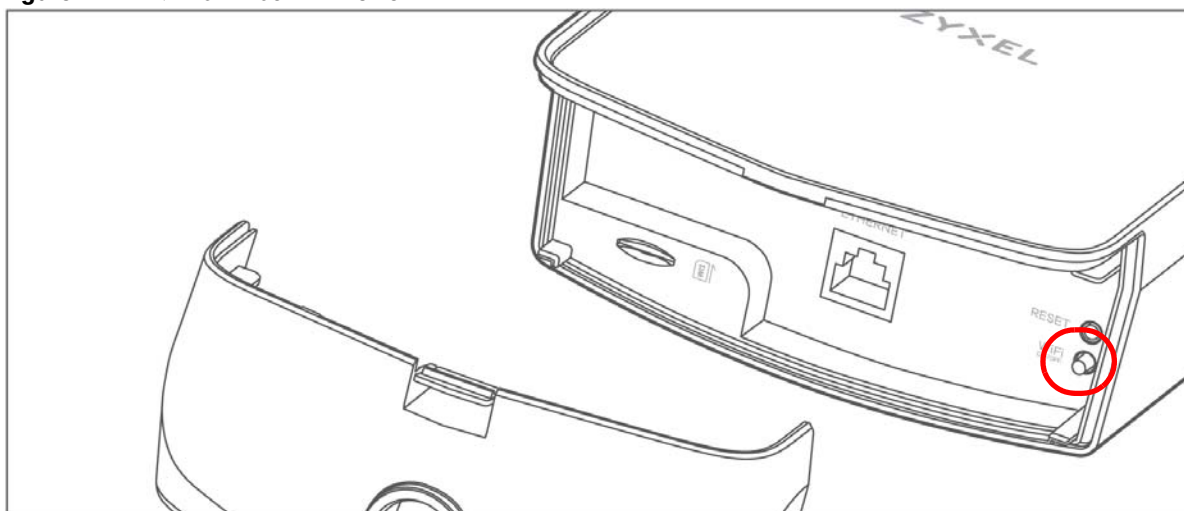


Figure 22 LTE7480-M804 / LTE7490-M904 WiFi Button



Figure 23 LTE5388-M804 / LTE5398-M904 WPS Button

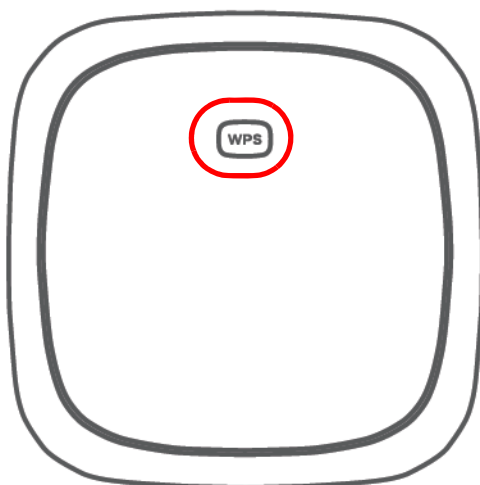


Figure 24 LTE3316-M604 WPS Button

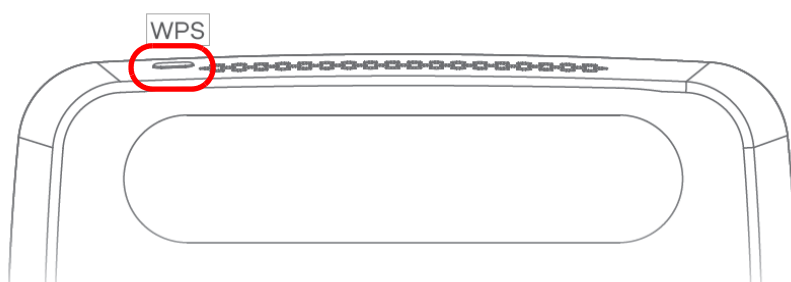
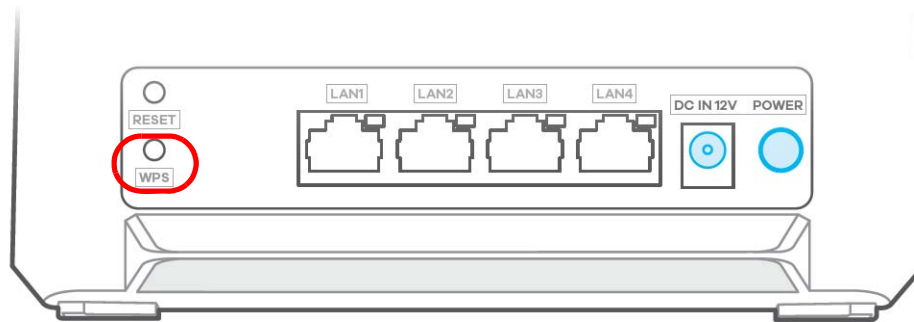


Figure 25 LTE3202-M437 WPS Button**To turn on WiFi:**

- Make sure the power is on. Press the **WiFi** or **WiFi/WPS** button for more than 5 seconds and release it.

Table 10 The LED Behavior for WiFi On

MODEL	LED BEHAVIOR
LTE3301-PLUS	The WLAN LED turns green/white
LTE7240-M403	The WLAN LED turns green
LTE7480-M804	The LED blinks amber
LTE7490-M904	The LED blinks amber
LTE5388-M804	The WiFi/WPS LED turns green
LTE5398-M904	The WiFi/WPS LED turns green
LTE3202-M437	The WiFi LED turns blue

- Make sure the **POWER** LED is on and not blinking. Press the **WiFi** or **WiFi/WPS** button for 2 seconds.

Table 11 The LED Behavior for WiFi On

MODEL	LED BEHAVIOR
LTE3316-M604	The WLAN LED turns green/white

To activate WPS (WiFi must be already on):

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

- Press the **WiFi** or **WiFi/WPS** button for more than 1 second but less than 5 seconds and release it (pressing more than 5 seconds will turn off WiFi). Press the WPS button on another WPS-enabled device within range of the Zyxel Device.

Table 12 The LED Behavior for WPS On

MODEL	LED BEHAVIOR
LTE3301-PLUS	The WLAN LED turns green/white
LTE7240-M403	The WLAN LED turns green
LTE7480-M804	The LED blinks amber
LTE7490-M904	The LED blinks amber
LTE5388-M804	The WPS LED blinks green

Table 12 The LED Behavior for WPS On

MODEL	LED BEHAVIOR
LTE5398-M904	The WPS LED blinks green
LTE3202-M437	The WPS LED blinks blue

- Press the **WiFi** or **WiFi/WPS** button for more than 5 seconds of the Zyxel Device and release it. Press the WPS button on another WPS-enabled device within range of the Zyxel Device.

Table 13 The LED Behavior for WPS On

MODEL	LED BEHAVIOR
LTE3316-M604	The WPS LED blinks green/white

- Press the **WPS** button for more than 1 – 4 seconds of the Zyxel Device and release it. Press the WPS button on another WPS-enabled device within range of the Zyxel Device.

To turn off WiFi:

- Press the **WiFi** or **WiFi/WPS** button for more than 5 seconds.

Table 14 The LED Behavior for WiFi Off

MODEL	LED BEHAVIOR
LTE3301-PLUS	The WLAN LED turns off
LTE7240-M403	The WLAN LED turns off
LTE7480-M804	The amber LED turns off
LTE7490-M904	The amber LED turns off
LTE5388-M804	The WLAN LED turns off
LTE5398-M904	The WLAN LED turns off
LTE3316-M604	The WLAN LED turns off
LTE3202-M437	The WiFi LED turns off

- Press the **WiFi** or **WiFi/WPS** button for 2 seconds.

Table 15 The LED Behavior for WiFi Off

MODEL	LED BEHAVIOR
LTE3316-M604	The WLAN LED turns off

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 is reset to the default (see the Zyxel Device label) and the IP address is reset to **192.168.1.1**.

Figure 26 Reset Button (LTE3301-PLUS)

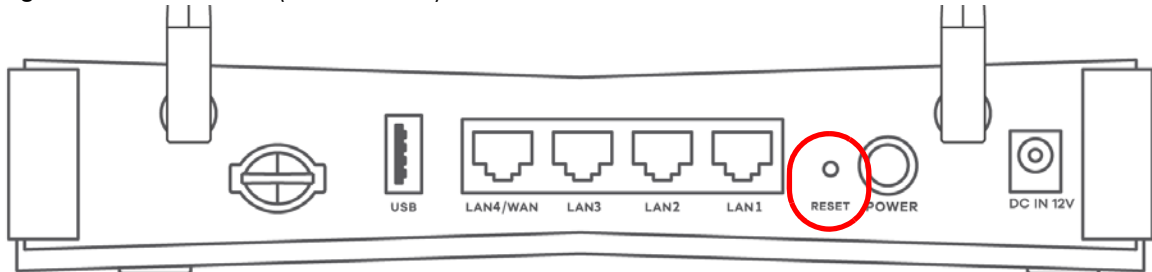


Figure 27 Reset Button (LTE7240-M403)

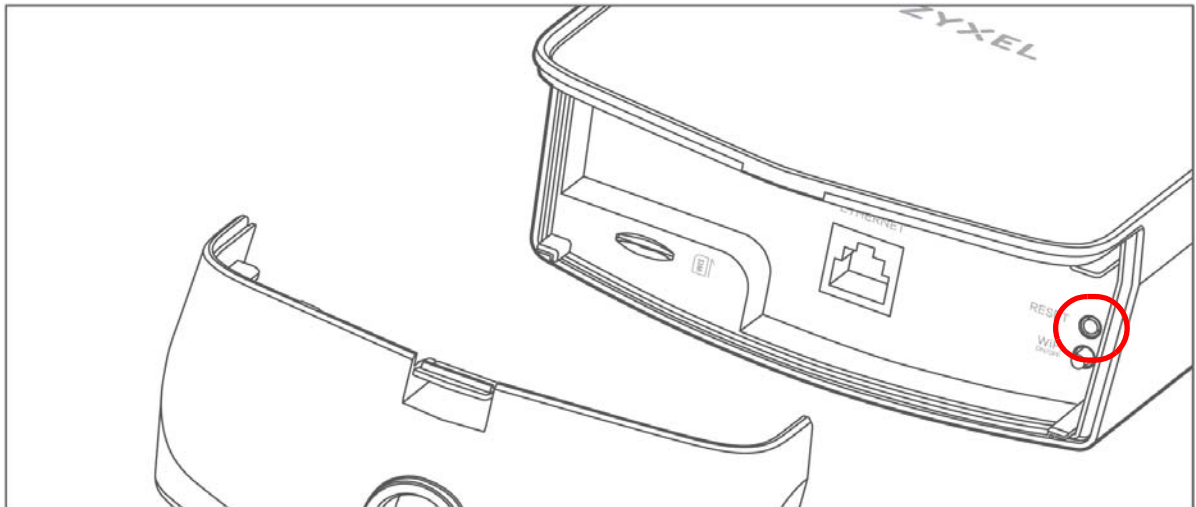


Figure 28 Reset Button (LTE7480-M804 / LTE7490-M904)



Figure 29 Reset Button (LTE5388-M804 / LTE5398-M904)

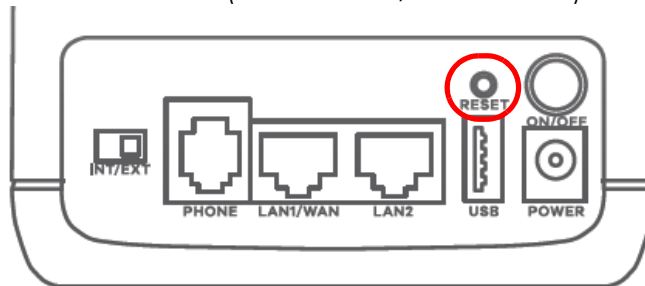
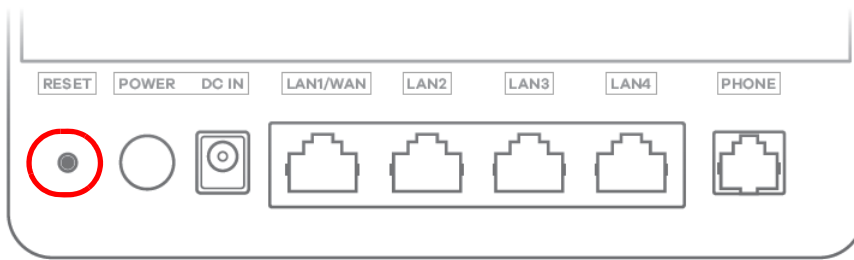
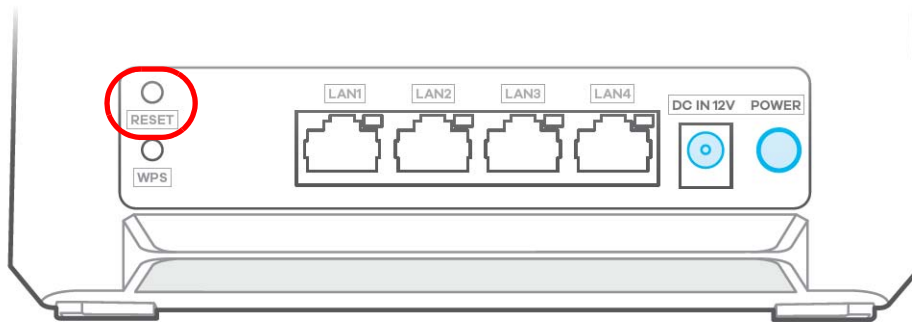


Figure 30 Reset Button (LTE3316-M604)**Figure 31** Reset Button (LTE3202-M437)

- 1 Make sure the Zyxel Device is connected to power and **POWER** LED is on.
- 2 Using a thin object, press the **RESET** button for 5 seconds.

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

2.4 Wall Mounting

Please refer to the installation guide below for the wall mounting procedures of the LTE3316-M604. You may need screw anchors if mounting on a concrete or brick wall.

Table 16 Wall Mounting Information

Distance between holes	100 mm
M4 Screws	Two
Screw anchors (optional)	Two

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

- 1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.
- 2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

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

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

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

- 4 Make sure the screws are fastened well enough to hold the weight of the Zyxel Device with the connection cables.
- 5 Align the holes on the back of the Zyxel Device with the screws on the wall. Hang the Zyxel Device on the screws.

Figure 32 Wall Mounting Example

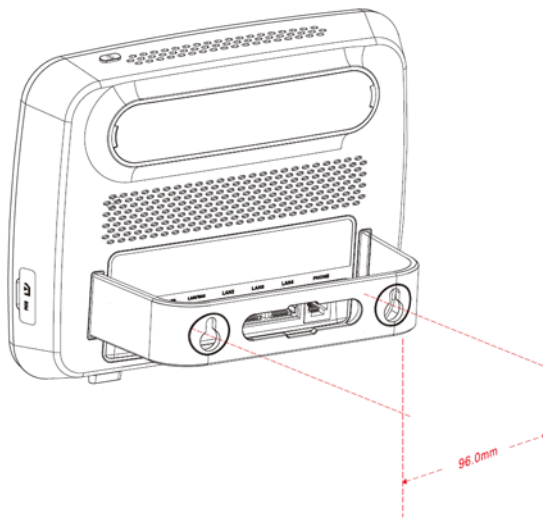
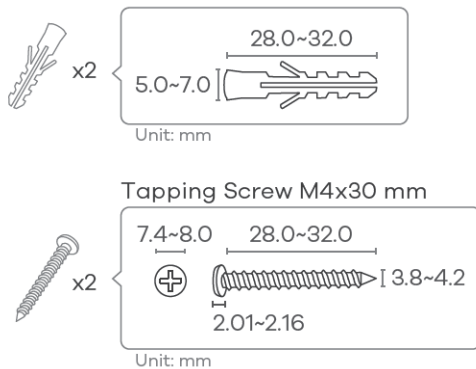


Figure 33 Wall Mounting Screw Specifications



CHAPTER 3

Web Configurator

3.1 Overview

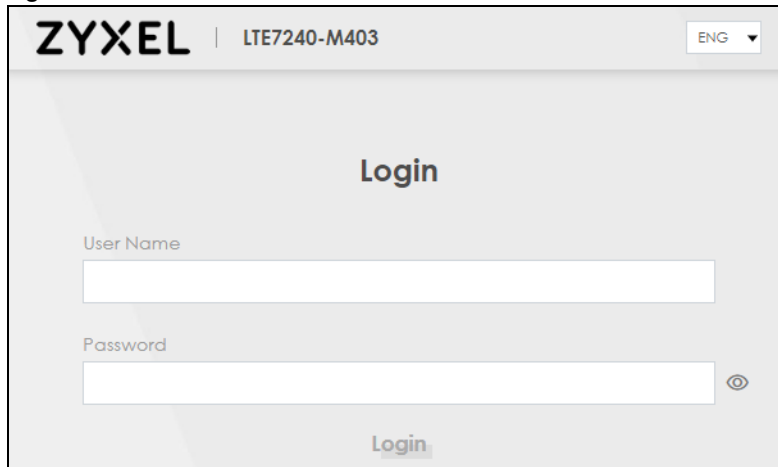
The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768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

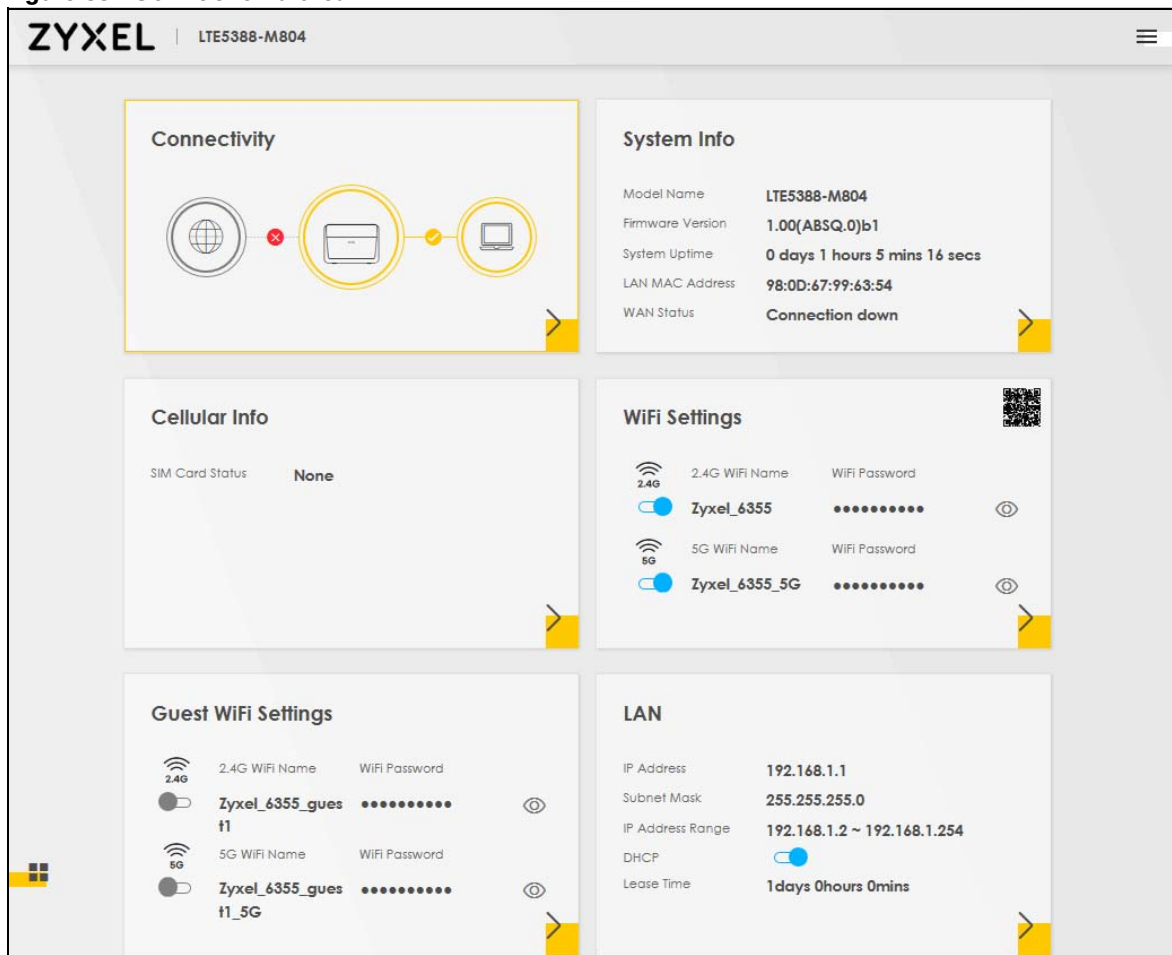
- 1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Make sure your computer has an IP address in the same subnet as the Zyxel Device. Your computer should have an IP address from 192.168.1.2 to 192.168.1.254.
- 3 Launch your web browser. If the Zyxel Device 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 34 Password Screen


The screenshot shows the ZyXEL web configurator login screen for the LTE7240-M403 model. At the top, the ZyXEL logo and model number are displayed, along with a language dropdown set to 'ENG'. The main heading is 'Login'. Below it, there are two input fields: 'User Name' and 'Password'. The 'Password' field has a toggle icon to the right. At the bottom, there is a 'Login' button.

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 35 Connection Status


The screenshot shows the ZyXEL web configurator 'Connection Status' screen for the LTE5388-M804 model. The screen is divided into several sections:

- Connectivity:** A diagram showing the connection path from the Internet (globe icon) to the router (server icon) and then to a laptop. The connection to the router is highlighted with a yellow circle and a checkmark, while the connection to the laptop is also highlighted with a yellow circle and a checkmark.
- System Info:**
 - Model Name: LTE5388-M804
 - Firmware Version: 1.00(ABSQ.0)b1
 - System Uptime: 0 days 1 hours 5 mins 16 secs
 - LAN MAC Address: 98:0D:67:99:63:54
 - WAN Status: Connection down
- Cellular Info:**
 - SIM Card Status: None
- WiFi Settings:**
 - 2.4G WiFi Name: Zyxel_6355, WiFi Password:
 - 5G WiFi Name: Zyxel_6355_5G, WiFi Password:
- Guest WiFi Settings:**
 - 2.4G WiFi Name: Zyxel_6355_gues t1, WiFi Password:
 - 5G WiFi Name: Zyxel_6355_gues t1_5G, WiFi Password:
- LAN:**
 - IP Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
 - IP Address Range: 192.168.1.2 ~ 192.168.1.254
 - DHCP: Enabled (toggle on)
 - Lease Time: 1 days 0 hours 0 mins

3.2 Web Configurator Layout

Figure 36 Screen Layout



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

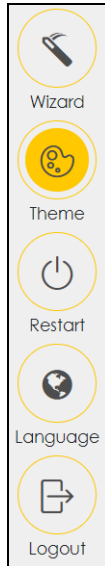
- **A** – Settings Icon (Navigation Panel and Side Bar)
- **B** – Widget Icon
- **C** – Main Window

3.2.1 Settings Icon

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

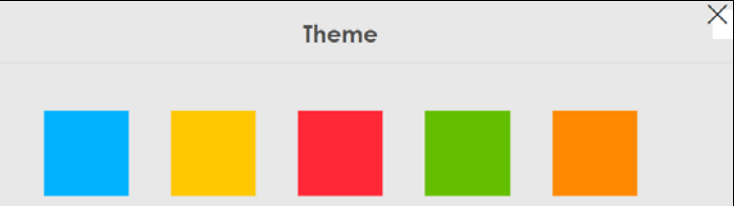
3.2.1.1 Side Bar

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

Figure 37 Side Bar

The icons provide the following functions.

Table 17 Web Configurator Icons in the Title Bar

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

3.2.1.2 Navigation Panel

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

Table 18 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.
	WAN Backup	Use this screen to configure your Zyxel Device's Internet settings if the cellular connection is down.
	Ethernet WAN	Use this screen to convert the LAN port as WAN port, or restore the WAN port to LAN port.
	Cellular WAN	Use this screen to configure a cellular WAN connection.
	Cellular APN	Use this screen to configure the Access Point Name (APN) provided by your service provider.
	Cellular SIM	Use this screen to enter a PIN for your SIM card to prevent others from using it.
	Cellular Band	Use this screen to configure the cellular frequency bands that can be used for Internet access as provided by your service provider.
	Cellular PLMN	Use this screen to view available PLMNs and select your preferred network.
	Cellular IP Passthrough	Use this screen to enable IP Passthrough 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.
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.
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
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.

Table 18 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
	ALG	Use this screen to enable or disable SIP ALG.
	Address Mapping	Use this screen to change your Zyxel Device's IP address mapping settings.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the Zyxel Device.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
USB	USB Service	Use this screen to enable file sharing through the Zyxel Device.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Parental Control	Parental Control	Use this screen to define time periods and days during which the Zyxel Device performs parental control and/or block web sites with the specific URL.
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.
Voice	Voice Mode	Use this screen to enable the Voice Mode on the Zyxel Device.
	SIP	Use this screen to set up information about your SIP account.
	Phone	Use this screen to change settings that depend on the country you are in.
	Call Rule	Use this screen to add, edit, or remove speed-dial numbers for outgoing calls.
	Call History	Use this screen to view a call history list.
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.

Table 18 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
	Security Log	Use this screen to view all security related events. You can select the level and category of the security events in their proper drop-down list window. Levels include: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: • Account • Attack • Firewall • MAC Filter
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
VoIP Status	VoIP Status	Use this screen to view VoIP registration, current call status and phone numbers for the phone ports.
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 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.
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.

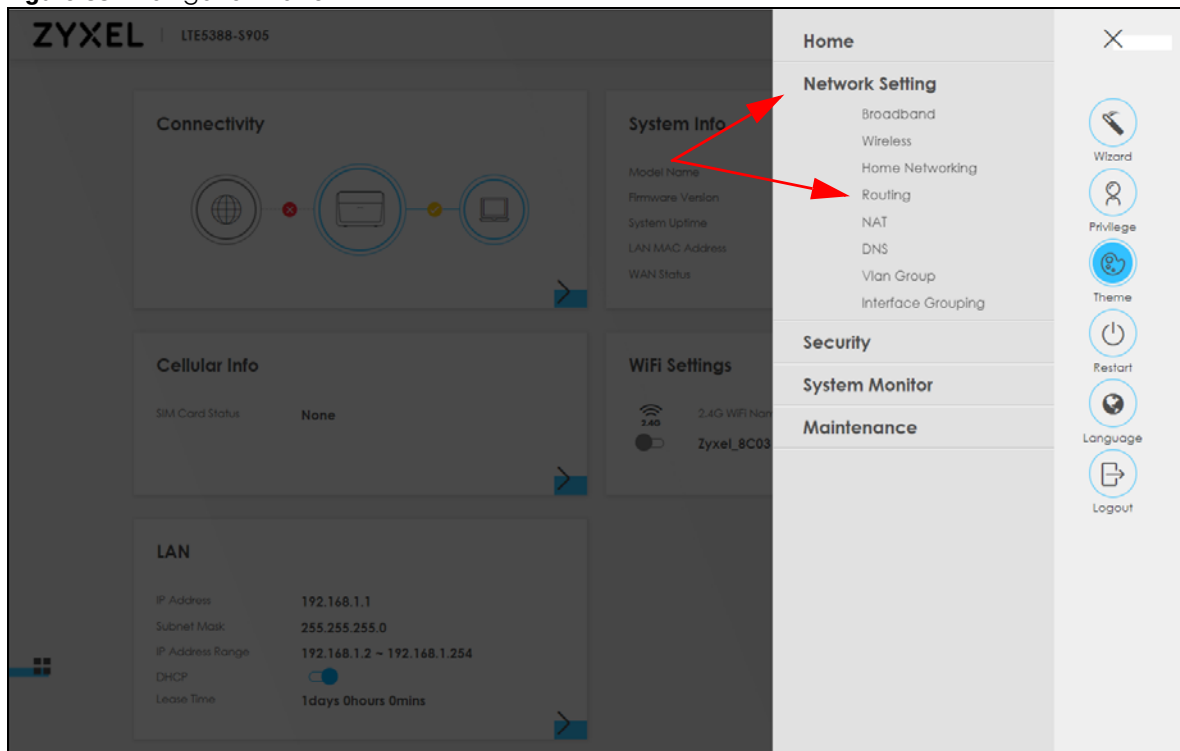
Table 18 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Zyxel Device . You can use Ping, TraceRoute, or Nslookup to help you identify problems.

3.2.1.3 Dashboard

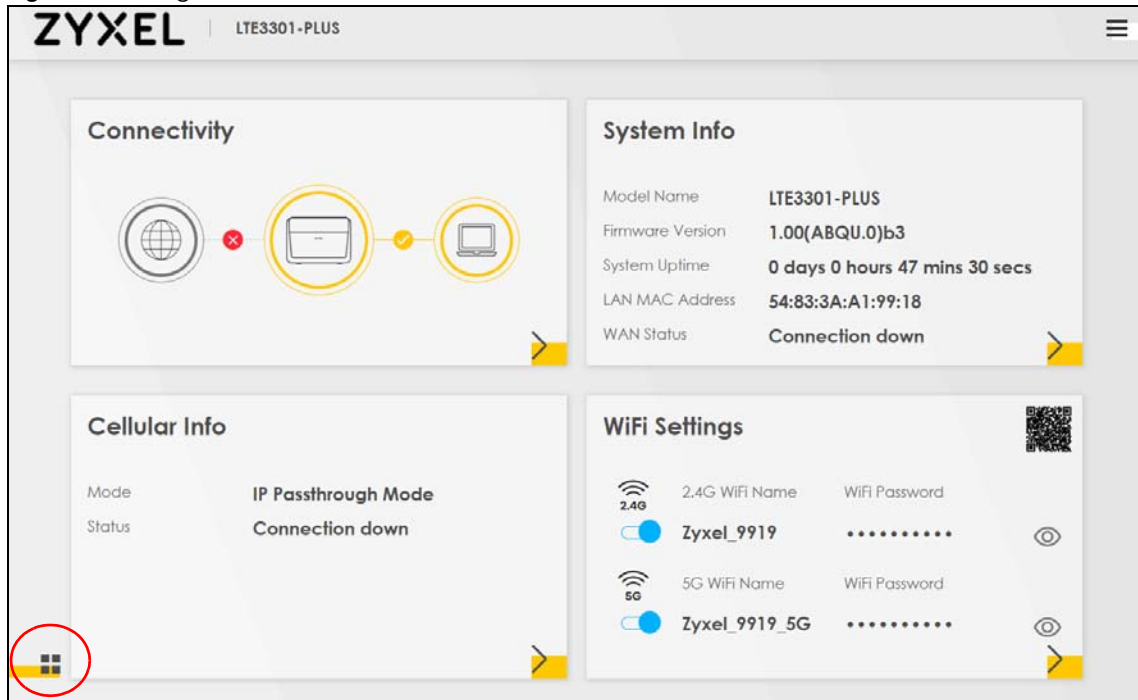
Use the menu items in the navigation panel on the right to open screens to configure the Zyxel Device's features

Figure 38 Navigation Panel

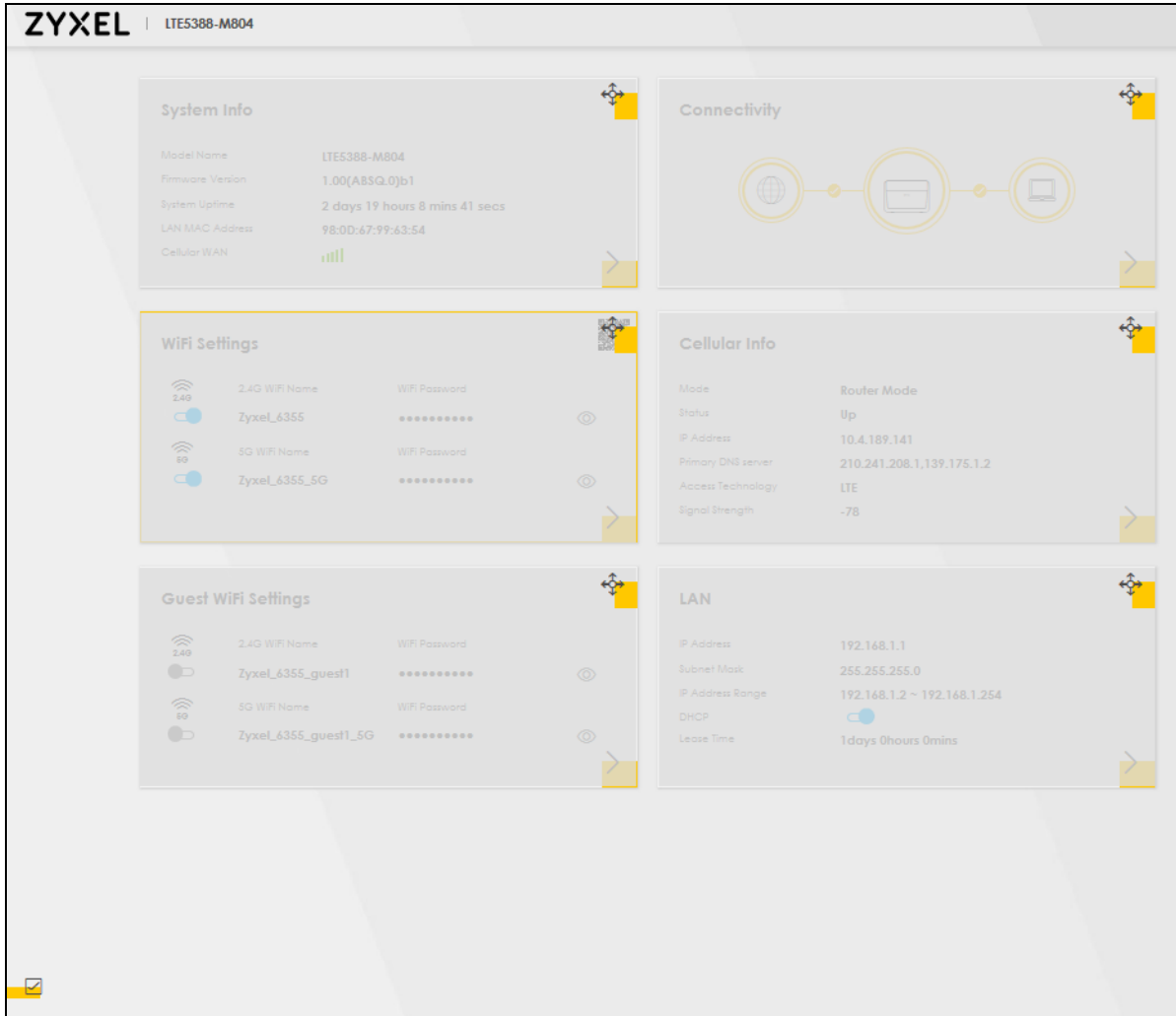


3.2.2 Widget and Check Icons

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

Figure 39 Widget Icon

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 40 Screen Order

CHAPTER 4

Quick Start

4.1 Overview

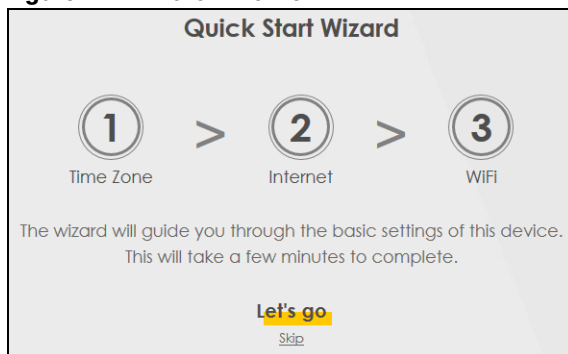
Use the **Wizard** screens to configure the Zyxel Device's time zone and wireless settings.

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

4.2 Quick Start Setup

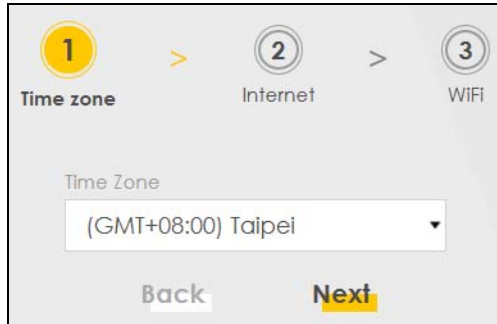
You can click the **Wizard** icon in the side bar to open the **Wizard** screens. After you click the **Wizard** icon, the following screen appears. Click **Let's go** to proceed with settings on time zone and wireless networks. It will take you a few minutes to complete the settings on the **Wizard**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

Figure 41 Wizard – Home



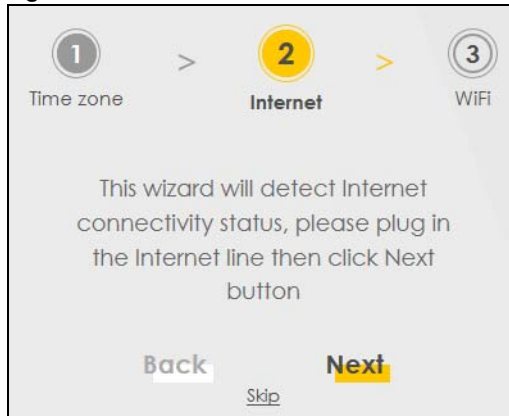
4.3 Quick Start Setup – Time Zone

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

Figure 42 Wizard – Time Zone

4.4 Quick Start Setup – Internet Connection

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

Figure 43 Wizard – Internet

4.4.1 Successful Internet Connection

The Zyxel Device has Internet access.

Figure 44 Wizard – Successful Internet Connection

4.4.2 Unsuccessful Internet Connection

The Zyxel Device did not detect a WAN connection.

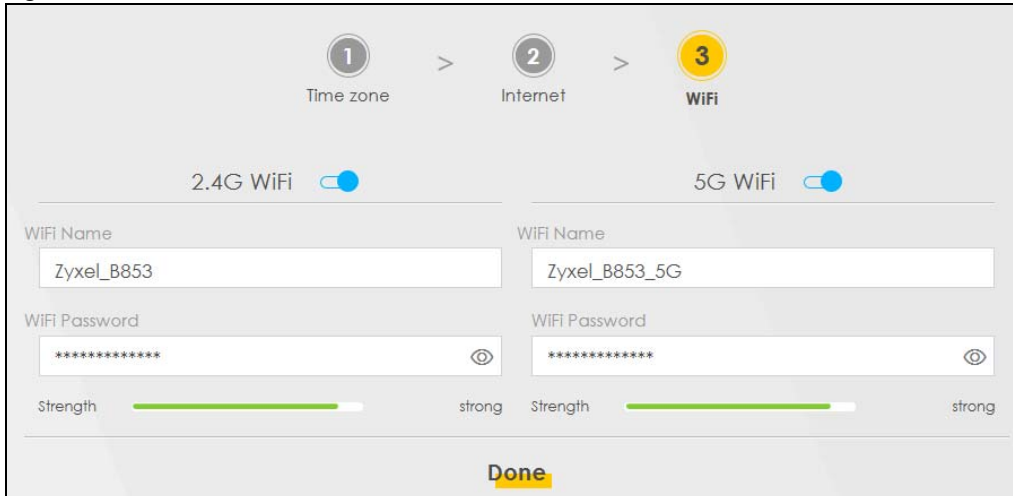
Figure 45 Wizard – Internet Connection is Down



4.5 Quick Start Setup – WiFi

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

Figure 46 Wizard – Wireless



4.6 Quick Start Setup – Finish

Your Zyxel Device saves your 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.

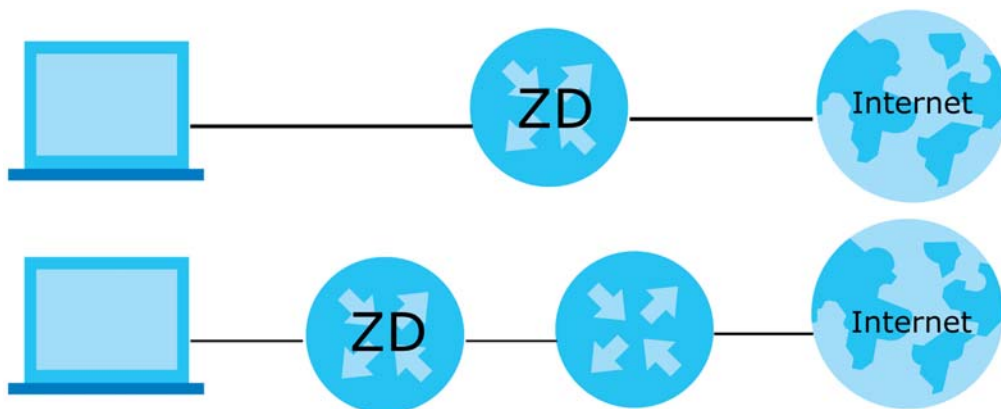
- [Wired Network Setup](#)
- [WiFi Network Setup](#)
- [Cellular Network Setup](#)
- [USB Applications](#)
- [Network Security](#)
- [Internet Calls](#)
- [Device Maintenance](#)

5.2 Wired Network Setup

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

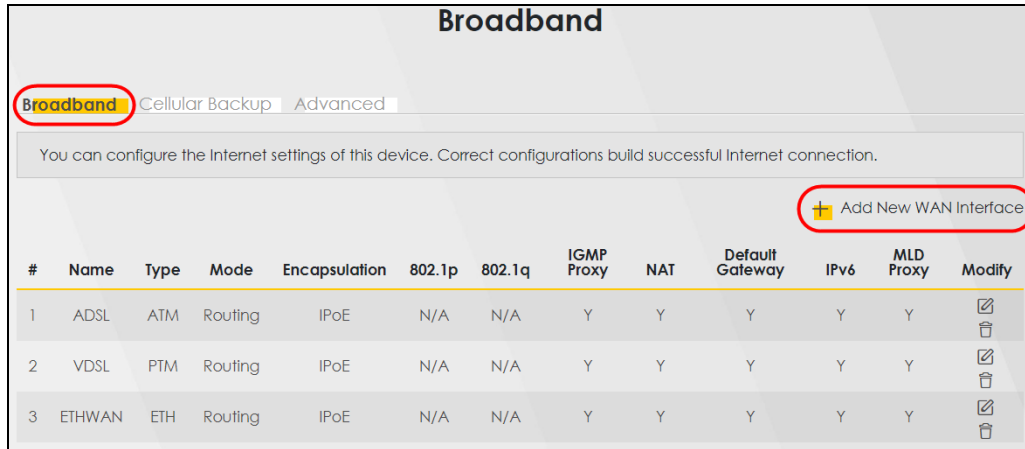
5.2.1 Setting Up an Ethernet Connection

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.



- 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.

Edit WAN Interface

General

Name

My ETH Connecti

Type

Ethernet

Mode

Routing

Encapsulation

IPoE

IPv4/IPv6 Mode

IPv4 Only

VLAN

802.1p

0

802.1q

(1~4094)

MTU

1500

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

DNS Server

☒ Obtain DNS Info Automatically

☐ Use Following Static DNS Address

Routing Feature

NAT

☒ NAT

Apply as Default Gateway

☒ Apply as Default Gateway

IGMP Proxy

☐ IGMP Proxy

Fullcone NAT

☐ Fullcone NAT

6RD

☐ 6RD

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

Add New WAN Interface

#	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 47 WiFi Network Setup

The diagram illustrates a WiFi network setup. On the left, a blue laptop icon represents the WiFi client. To its right are two blue curved arrows indicating a wireless connection to a blue circle labeled 'ZD' (Zyxel Device), which acts as the access point. A solid blue line connects the 'ZD' circle to another blue circle on the right labeled 'Internet', representing the connection to the external network.

LTE Series User's Guide

52

See the label on the Zyxel Device for the WiFi network settings and then connect manually to the Zyxel Device. See [Section 5.3.2 on page 55](#). Alternatively, you can set up a WiFi network using WPS.

5.3.1 Changing Security on a WiFi Network

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

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

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

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

Cancel Apply

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

Wireless

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

The configurations below are the advanced wireless settings.

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

Cancel Apply

You can now use the WPS feature to establish a WiFi connection between your notebook and the Zyxel Device (see [Section 5.3.2 on page 55](#)). 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 55](#). 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 5.3.2.2 on page 58](#). 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**.

Wireless

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

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 ☒ **1**

Step1. Click WPS button **WPS** **3**

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

Method 2 PIN ☐

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

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

1. Please release configuration if you want to configure the wireless settings

Release Configuration

2. Enter current PIN number on your wireless client

Generate New PIN

Note

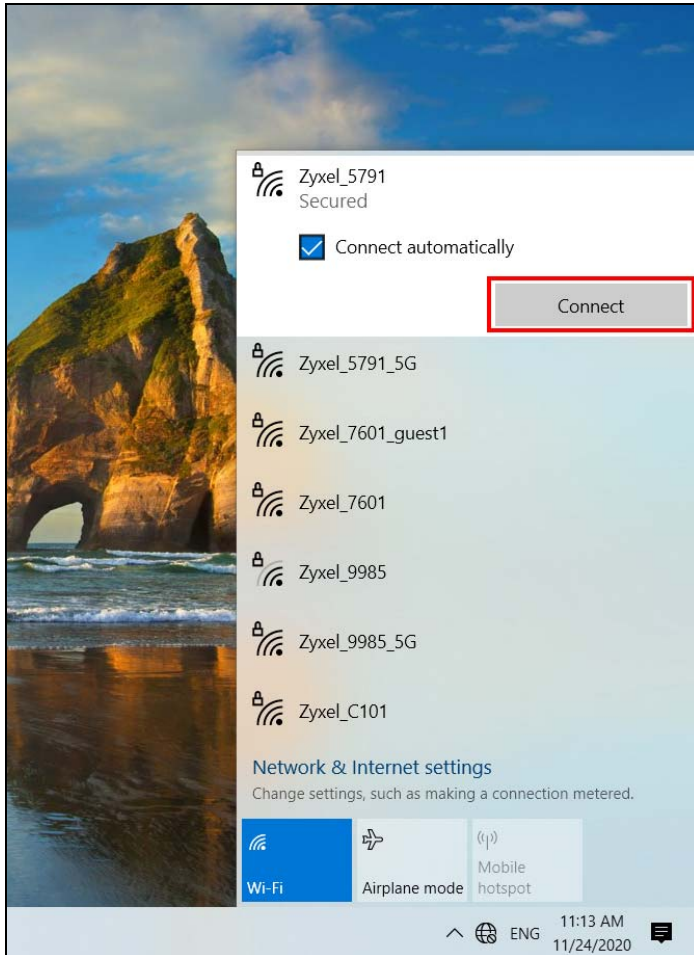
(1) If WPS is Enabled, UPnP will automatically be turned on.
 (2) The Zyxel Device applies the security settings of the main SSID (SSID1) profile.
 (3) The WPS switch is grayed out when wireless LAN is disabled.

Cancel **Apply** **2**

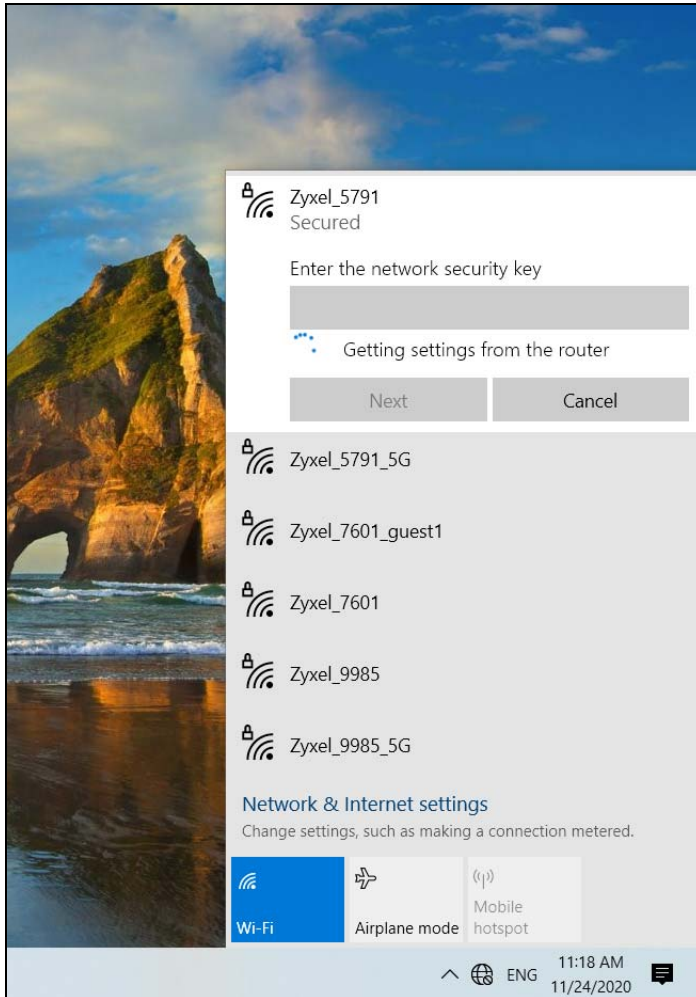
- 3 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.



- 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 **WPS**

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 **3**

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

Enter AP's PIN Number in wireless Client

Current state Configured

Please release configuration if you want to configure the wireless settings

Release Configuration

2 Enter current PIN number on your wireless client

Generate New PIN

Method 3 ☐

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.

5.4 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

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

Cancel
Apply

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:

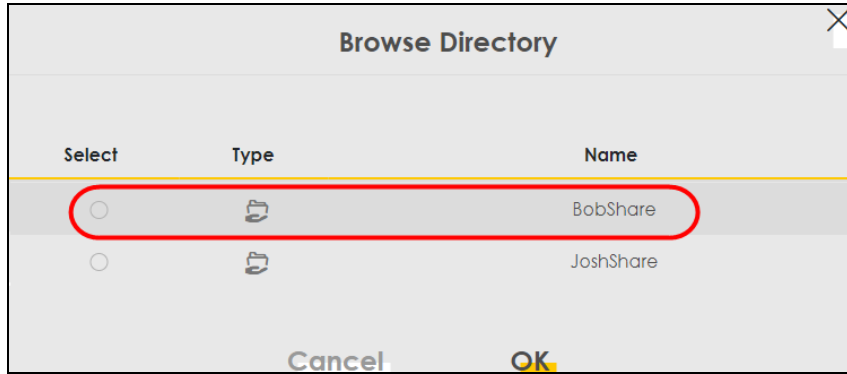
Share Path: Browse

Description:

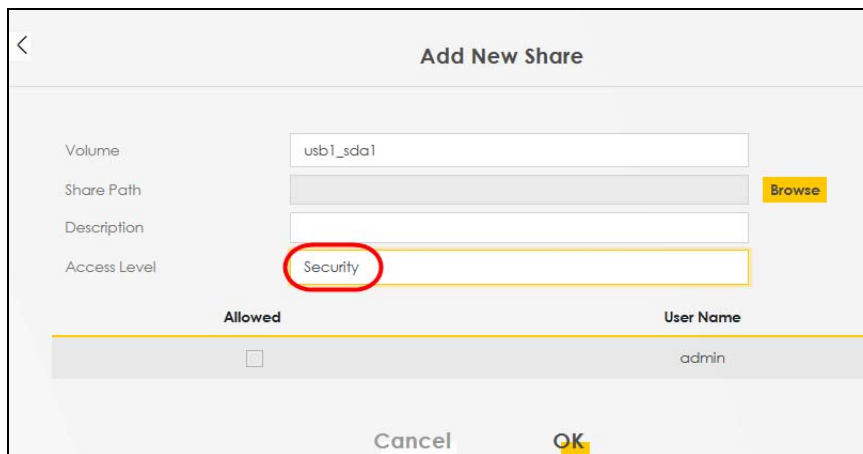
Access Level:

Cancel
OK

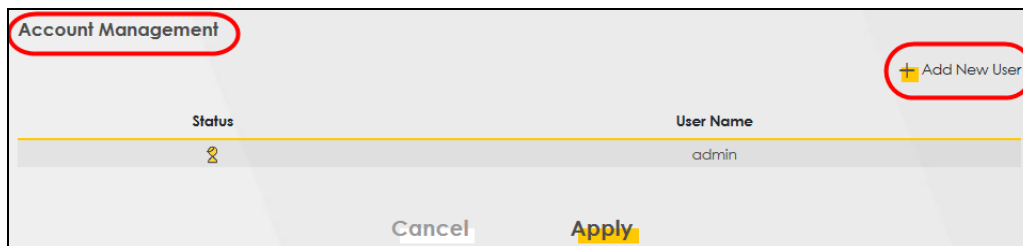
5d On the **Browse Directory** screen, select the folder that you want to add as a share. In this example, select **BobShare** and then click **OK**.



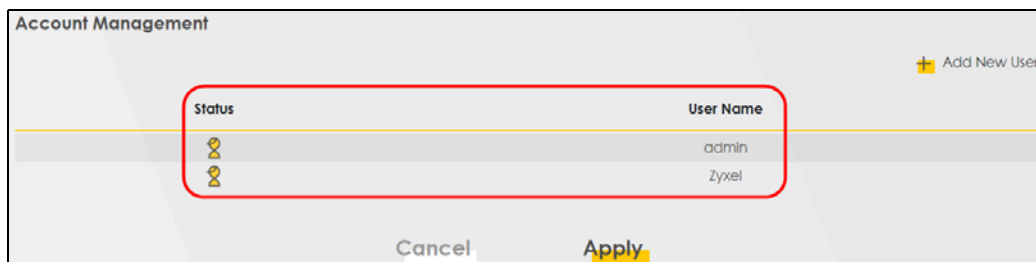
- 5e In **Access Level**, select **Public** to let the share to be accessed by all users connected to the Zyxel Device. Otherwise, select **Security** to let the share to be accessed by specific users to access only. Click **OK** to save the settings.



- 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.

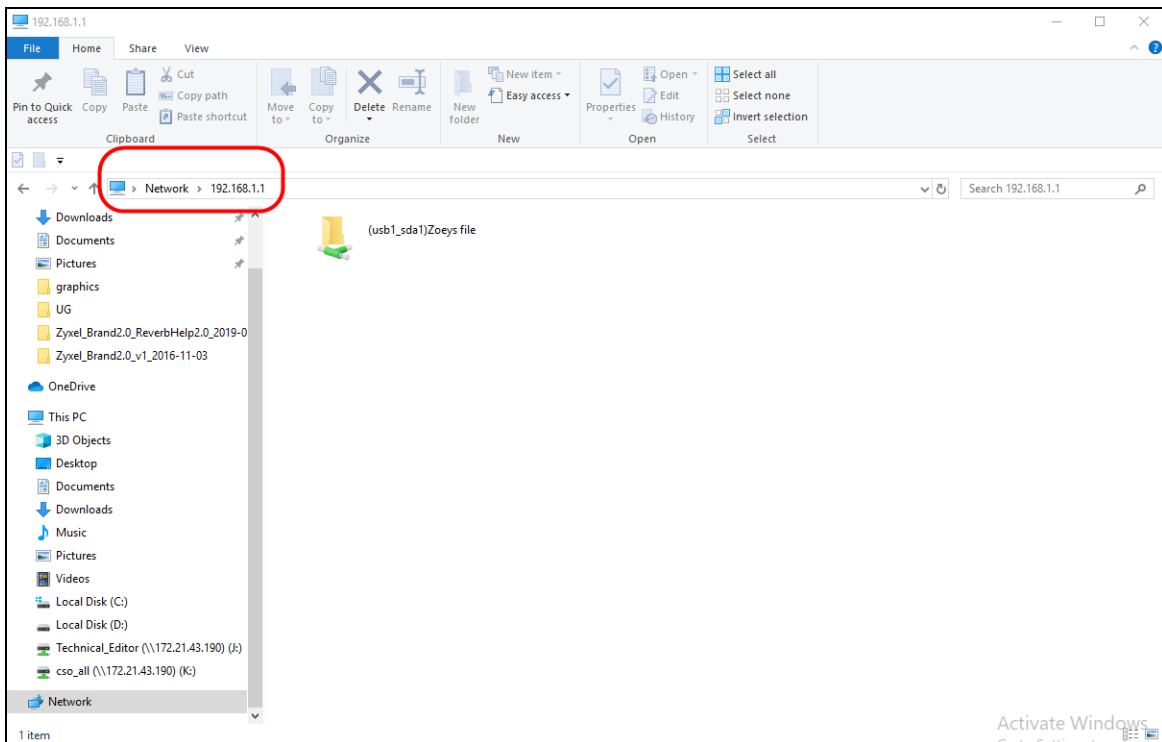
Share Directory List						Add New Share	
Active	Status	Share Name	Share Path	Share Description	Modify		
☒		BobShare	/mnt/usb1_sda1/BobShare	Bob			
☒		JoshShare	/mnt/usb1_sda1/JoshShare	Josh			

5.5.1.2 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)Zoeys file. Refer to your operating system's documentation for how to browse your file structure.

- 1 Open Windows Explorer.
- 2 In the Windows Explorer's address bar, enter a double backslash "\\" followed by the IP address of the Zyxel Device (the default IP address of the Zyxel Device is 192.168.1.1)



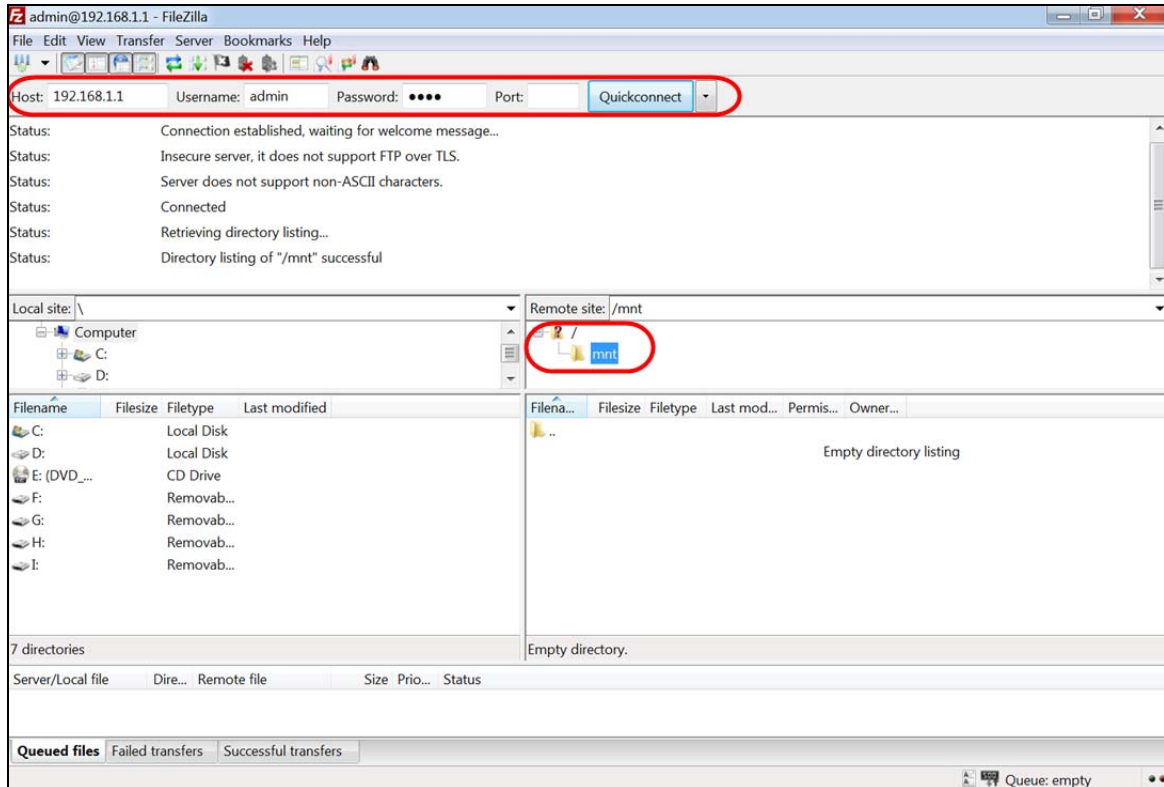
- 3 Double-click on **(usb1_sda)Zoeys file**, and then enter the share's username and password if prompted.
- 4 After you access **(usb1_sda)Zoeys file** through your Zyxel Device, you do not have to log in again unless you restart your computer.

5.5.2 Using FTP

This section shows how to use an FTP program to access files on an USB storage device connected to the Zyxel Device.

Note: This example uses the FileZilla FTP program to browse your shared files.

- 1 In FileZilla, enter the IP address of the Zyxel Device (The default IP is **192.168.1.1**), your account's **Username**, **Password** and **Port** number, and then click **Quickconnect**. A screen asking for password authentication appears.



- 2 After you log in, the **mnt** folder is displayed as shown.

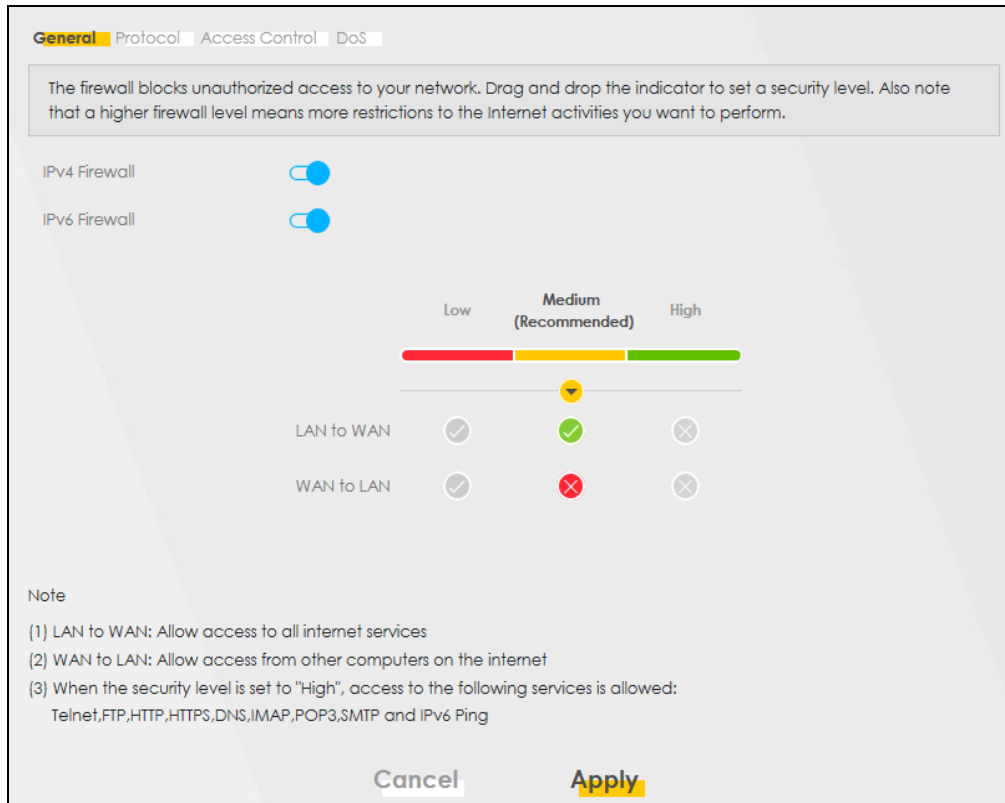
5.6 Network Security

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.

<

Add New ACL Rule

Active

☒

Filter Name

Order

Select Source IP Address

Source IP Address

[/prefix length]

Select Destination Device

Destination IP Address

[/prefix length]

MAC Address

IP Type

Select Service

Protocol

Custom Source Port

Range

-

Custom Destination Port

Range

-

Policy

Direction

Enable Rate Limit

☐

packet(s) per

(1-512)

Scheduler Rules

▼

Add New Rule

Cancel

OK

Add New ACL Rule

Filter Name:

Order:

Select Source IP Address:

Source IP Address: [/prefix length]

Select Destination Device:

Destination IP Address: [/prefix length]

IP Type:

Select Service:

Protocol:

Custom Source Port: -

Custom Destination Port: -

Policy:

Direction:

Enable Rate Limit: ☐

packet(s) per (1-512)

Scheduler Rules:

- 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.

The style and features of your parental control vary depending on the Zyxel Device you are using, see [Section 5.6.2.1 on page 68](#) and [Section 5.3.2.2 on page 58](#) for more information.

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

TWPCNT03116-01 (dc-4a-3e-40-ec-67)
▼

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.

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.

#	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.

#	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.

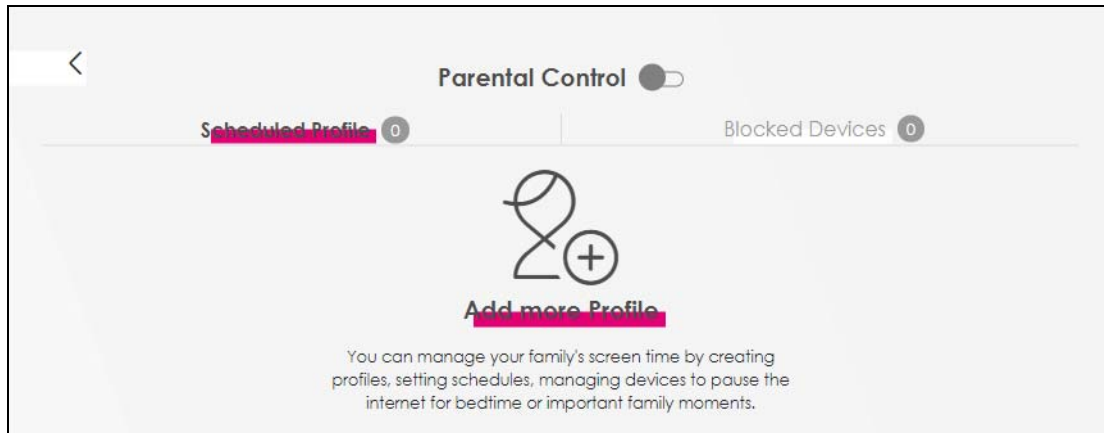
5.6.2.2 Configuring a Parental Control Schedule

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.

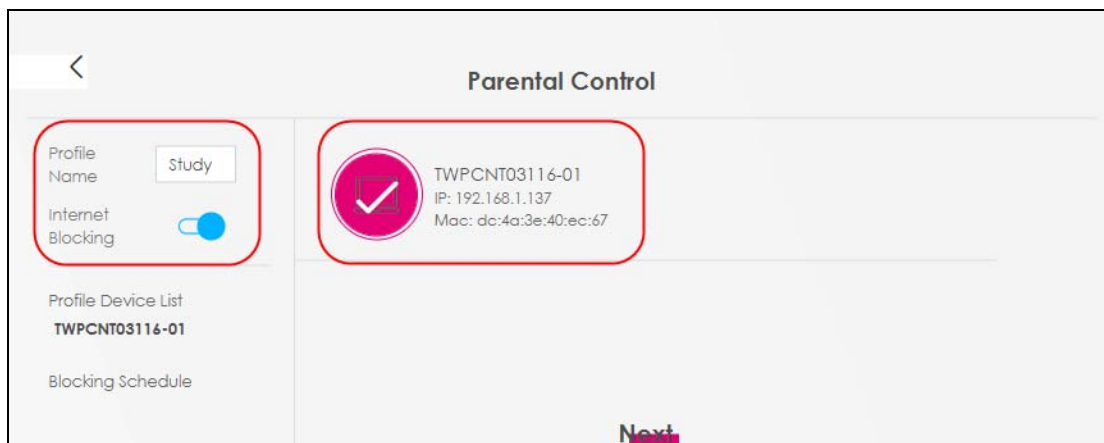


- 2 Use this screen to add a Parental Control rule.

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

2b Click on the switch to enable **Internet Blocking**.

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.

Parental Control

Profile Name: Study

Internet Blocking: ☒

Profile Device List: TWPCNT03116-01

Blocking Schedule

Mon, Tue, Wed, Thu, Fri
From 8:00 am to 11:00 pm

Mon, Tue, Wed, Thu, Fri
From 1:00 am to 5:00 pm

Schedule Add New Schedule

Start blocking: 8 0 am End blocking: 11 0 pm ☐ All Day

Repeat On: Mon Tue Wed Thu Fri Sat Sun

Start blocking: 1 0 am End blocking: 5 0 pm ☐ All Day

Repeat On: Mon Tue Wed Thu Fri Sat Sun

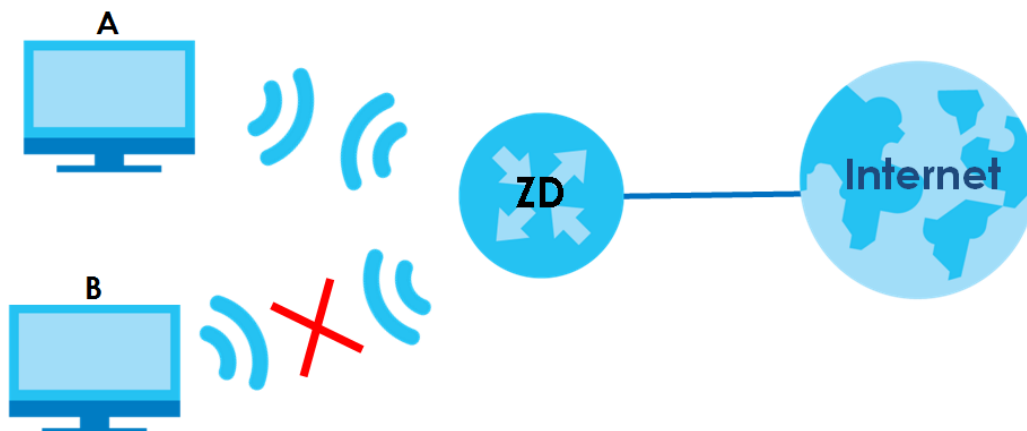
Back Save

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 48 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	☒	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 **VoIP > 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 Verizon

SIP Local Port 5060 (1025~65535)

SIP Proxy Server Address sip.infostrada.it

SIP Proxy Server Port 5060 (1025~65535)

SIP REGISTRAR Server Address sip.infostrada.it

SIP REGISTRAR Server Port 5060 (1025~65535)

SIP Service Domain sip.infostrada.it

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 **VoIP > 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 **VoIP > 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).

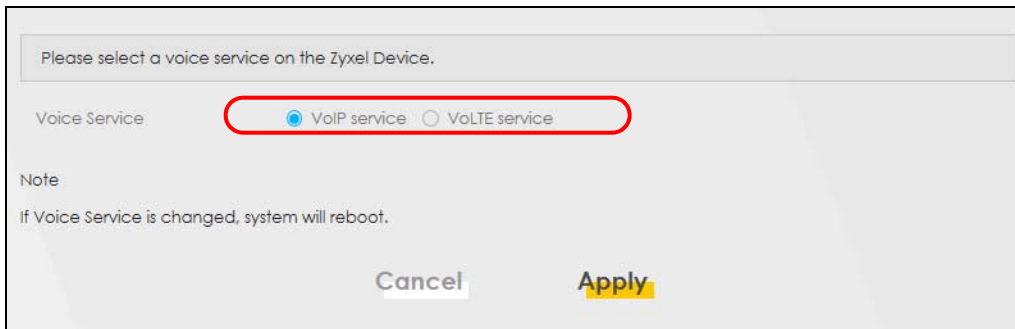
- Make sure you connect a telephone to phone port 1 on the Zyxel Device.
- Make sure the Zyxel Device is turned on and connected to the Internet.

- 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.

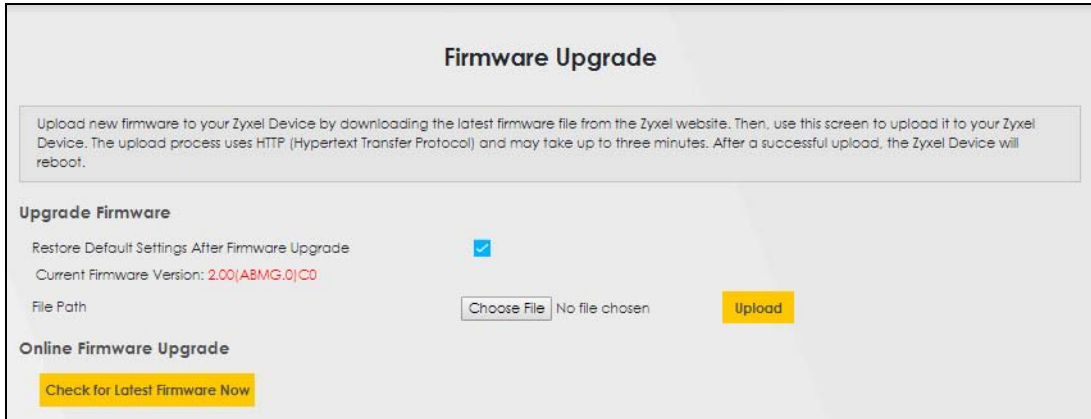
5.8 Device Maintenance

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 ABLZ. 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**.



The image shows a web interface titled "Firmware Upgrade". At the top, there is a text box explaining the process: "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, the "Upgrade Firmware" section contains a checkbox for "Restore Default Settings After Firmware Upgrade" which is checked, and a text label "Current Firmware Version: 2.00(ABMG.0)C0". There is a "File Path" label, a "Choose File" button, and a "No file chosen" text. To the right of these is a yellow "Upload" button. Below the "Upgrade Firmware" section is the "Online Firmware Upgrade" section, which contains a yellow button labeled "Check for Latest Firmware Now".

- 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.

Backup/Restore

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

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

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

Backup Configuration

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

Backup

Restore Configuration

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

File Path

Browse...
Upload

Back to Factory Default Settings

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

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

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

Save
Cancel
✕

5.8.3 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 **Browse...** **Upload**

Back to Factory Default Settings

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

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

Reset

- 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

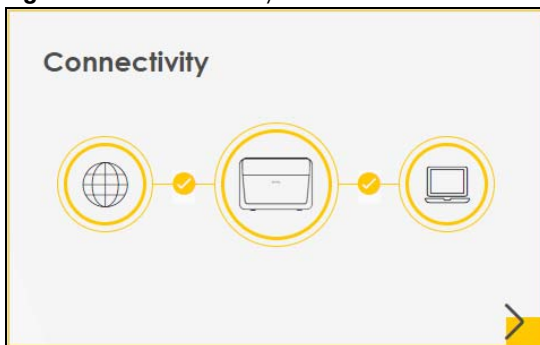
6.1 Connection Status Overview

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

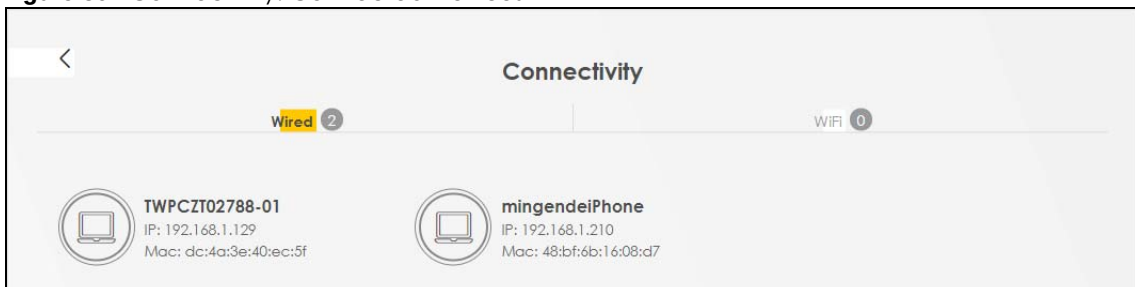
Use this screen to view the network connection status of the Zyxel Device and its clients.

Figure 49 Connectivity



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

Figure 50 Connectivity: Connected Devices

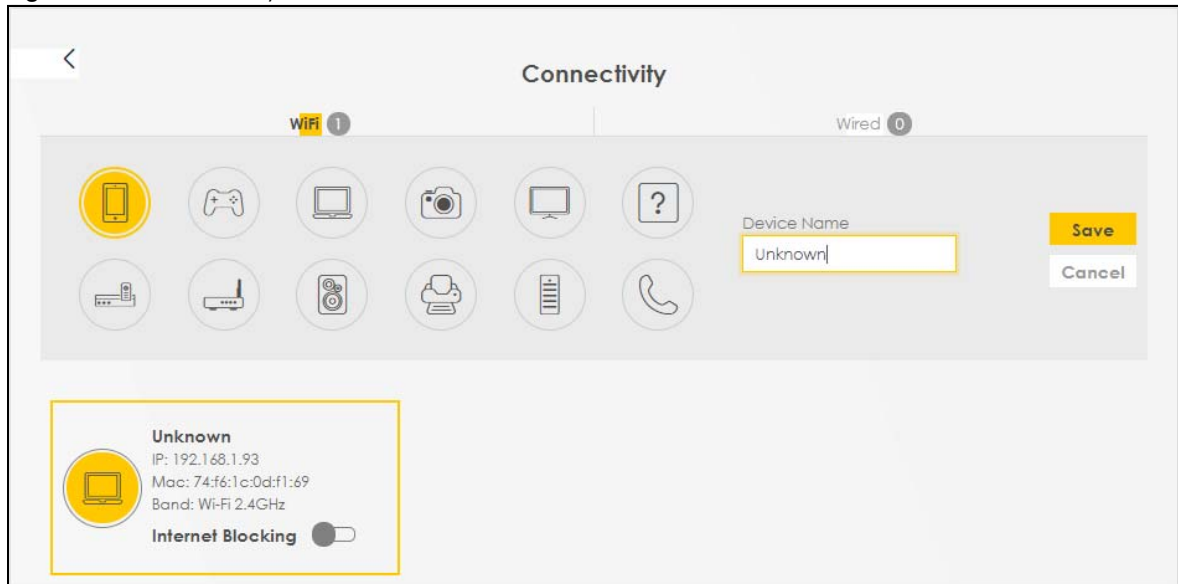


You can change the icon and name of a connected device. Place your mouse within the device block, and an Edit icon () will appear. Click the Edit icon, and you'll see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Click to enable ()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

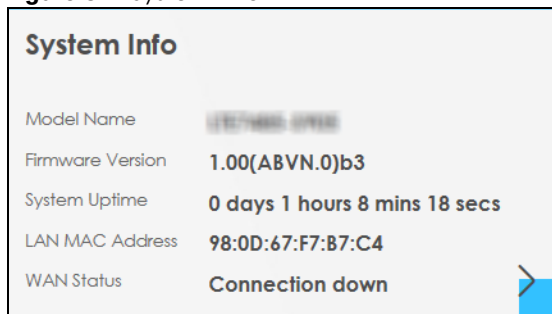
Figure 51 Connectivity: Edit



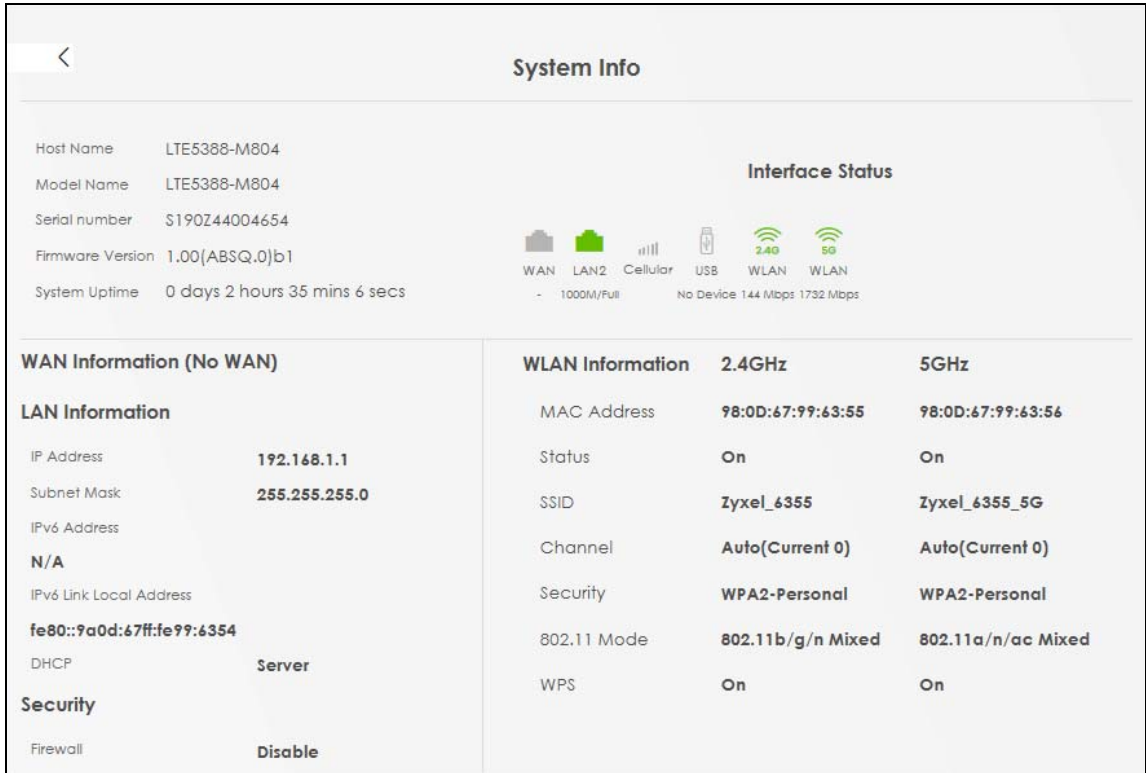
6.1.3 System Info

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

Figure 52 System Info



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

Figure 53 System Info: Detailed Information

Each field is described in the following table.

Table 19 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 19 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 54 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 55 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 20 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 20 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.
Service Information	Note: If the cellular service provider supports carrier aggregation (CA), then this section displays statistics for the connection's primary component carrier (PCC).
Access Technology	This displays the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.
Band	This displays the current cellular band of your Zyxel Device (WCDMA2100).
RSSI	This displays the strength of the cellular signal between an associated cellular station and the Zyxel Device.

Table 20 Cellular Info: Detailed Information (continued)

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

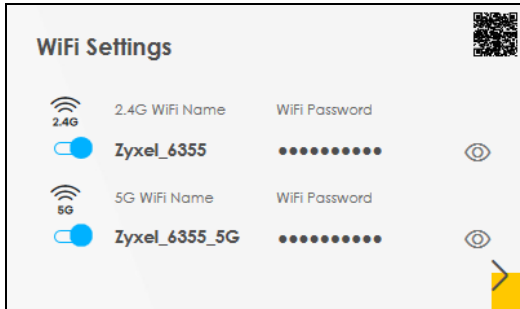
Table 20 Cellular Info: Detailed Information (continued)

LABEL	DESCRIPTION
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level. The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example -240 dB. This parameter is for UMTS only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not UMTS or there is no network connection.
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber. The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101. This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN. The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
RAC	This displays the RAC (Routing Area Code), which is used in mobile network "packet domain service" (PS) to identify a routing area within a location area. In a mobile network, the Zyxel Device uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and uses RAC to identify the location of data service like HSDPA or LTE. The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station. This parameter is for GPRS only. The value is '0' (zero) if the Current Access Technology is not GPRS. The value is 'N/A' if there is no network connection.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good or bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI). PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer). PMI determines how cellular data are encoded for the antennas to improve downlink rate.

6.1.5 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 (👁️).

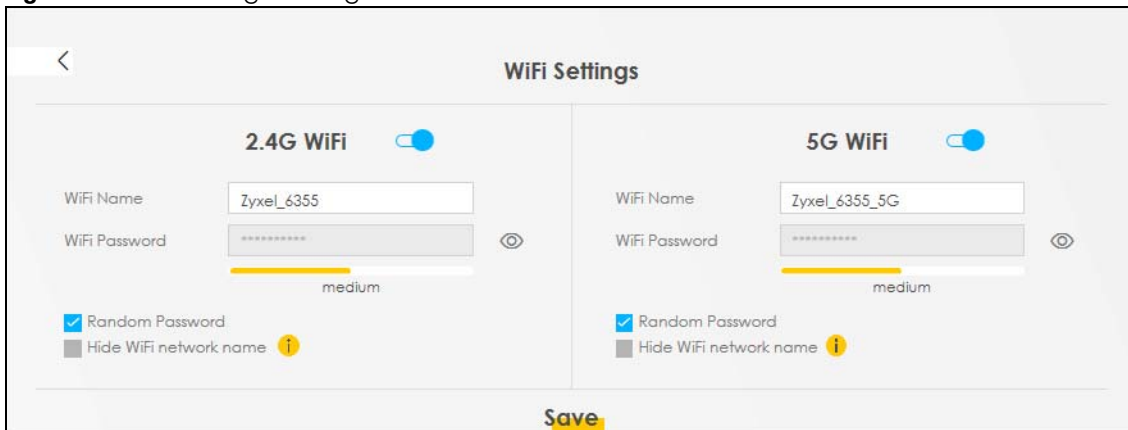
Figure 56 WiFi Settings



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.

Figure 57 WiFi Settings: Configuration



Each field is described in the following table.

Table 21 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.

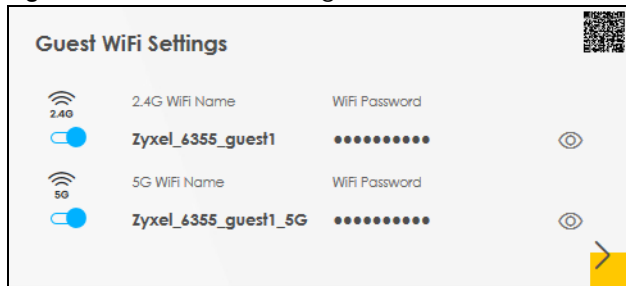
Table 21 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
	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.

6.1.6 Guest WiFi Settings

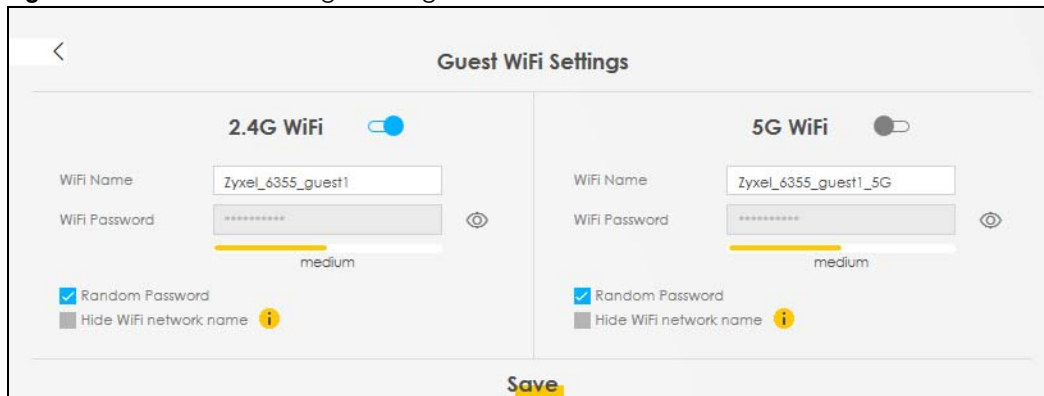
Use this screen to enable or disable the guest wireless network. When the switch turns blue () the function is enabled. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the guest wireless networks. If you want to show or hide your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

Figure 58 Guest WiFi Settings



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

Figure 59 Guest WiFi Settings: Configuration



Each field is described in the following table.

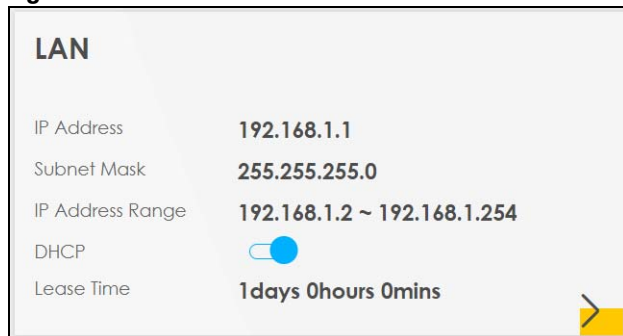
Table 22 Guest WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4 GHz / 5 GHz WiFi	Click this switch to enable or disable the 2.4G / 5G wireless 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 option to have the Zyxel Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.
Hide WiFi network name	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID.
Save	Click Save to save your changes.

6.1.7 LAN

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

Figure 60 LAN



LAN

IP Address **192.168.1.1**

Subnet Mask **255.255.255.0**

IP Address Range **192.168.1.2 ~ 192.168.1.254**

DHCP 

Lease Time **1days 0hours 0mins**



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

Figure 61 LAN Setup

The screenshot shows the LAN Setup interface. At the top, there's a back arrow and the title 'LAN'. Below this, the interface is divided into three main sections. The first section, 'LAN IP Setup', contains two input fields: 'IP Address' with the value '192 , 168 , 1 , 1' and 'Subnet Mask' with the value '255 , 255 , 255 , 0'. The second section, 'IP Addressing Values', contains two input fields: 'Beginning IP Address' with the value '192 , 168 , 1 , 2' and 'Ending IP Address' with the value '192 , 168 , 1 , 254'. The third section, 'DHCP Server State', contains a 'DHCP Server Lease Time' field with a value of '1' days, '0' hours, and '0' minutes. At the bottom of the page, there is a yellow 'Save' button.

Each field is described in the following table.

Table 23 Status Screen

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
DHCP Server State	
DHCP Server Lease Time	This is the period of time 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

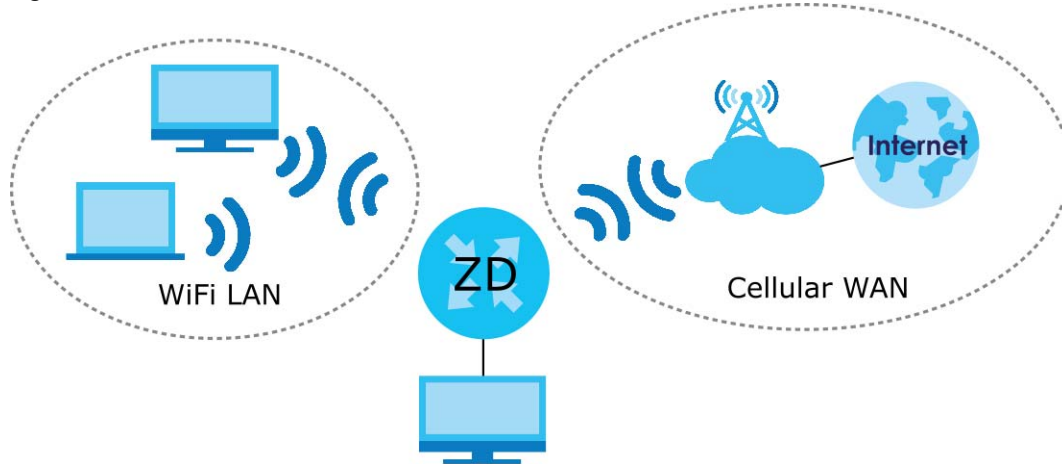
Broadband

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 62 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 95](#)).
- Use the **WAN Backup** screen to configure your Zyxel Device's WAN backup settings ([Section 7.4 on page 101](#)).
- 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 7.4 on page 101](#)).
- Use the **Cellular WAN** screen to configure a cellular WAN connection ([Section 7.5 on page 101](#)).
- Use the **Cellular APN** screen to configure the APN setting ([Section 7.6 on page 102](#)).
- Use the **Cellular SIM** screen to enter the PIN of your SIM card ([Section 7.7 on page 105](#)).
- 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 7.8 on page 106](#)).
- Use the **Cellular PLMN** screen to display available Public Land Mobile Networks ([Section 7.9 on page 107](#)).
- Use the **Cellular IP Passthrough** screen to configure a cellular WAN connection ([Section 7.10 on page 110](#)).

- Use the **Cellular Lock** screen to configure the base station you choose to connect to ([Section 7.11 on page 111](#)).
- Use the **Cellular SMS** screen to send and receive SMS messages from the Zyxel Device ([Section 7.12 on page 112](#)).

Table 24 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 63 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/A	Y	Y	Y	N/A	
2	Cellular WAN 2	CELL	Routing	IPoE	N/A	N/A	N/A	Y	N	Y	N/A	

The following table describes the labels in this screen.

Table 25 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 64 Network Setting > Broadband > Add or Edit New WAN Interface

Edit WAN Interface

General ☒

Name: Cellular WAN

Type:

Mode: Routing

Encapsulation: IPoE

IPv4/IPv6 Mode: IPv4 IPv6 DualStack

VLAN ☒

802.1p: 0

802.1q: [1~4094]

MTU

MTU: 1500

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

DNS Server

☒ Obtain DNS Info Automatically

☐ Use Following Static DNS Address

DHCP Options

Request Options

☐ option 43 ☐ option 120 ☐ option 121

Sent Options

☐ option 60

Vendor ID:

☐ option 61

IAID:

DUID:

☐ option 125

Routing Feature

NAT ☒ IGMP Proxy ☒

Apply as Default Gateway ☒ Fullcone NAT ☒

IPv6 Address

☒ Obtain an IPv6 Address Automatically

☐ Static IPv6 Address

IPv6 DNS Server

☒ Obtain IPv6 DNS Info Automatically

☐ Use Following Static IPv6 DNS Address

IPv6 Routing Feature

MLD Proxy ☒ Apply as Default Gateway ☒

Cancel Apply

The following table describes the labels in this screen.

Table 26 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 26 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 26 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 WAN Backup

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

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

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

Figure 65 Network Setting > Broadband > WAN Backup

The screenshot shows the 'Broadband' settings page with 'WAN Backup' selected. A message states: 'Whenever the WAN connection is down, WAN Backup takes over the job and keeps you online.' The 'WAN Backup Enable' toggle is turned on. The 'Primary WAN' is set to 'Ethernet'. The 'The Destination for Connection Check' is set to 'Google DNS' with an IP address of '8.8.8.8'. The 'Connection Check Interval' is set to '60' seconds (range 30-600). The 'Check Fail Limit' is set to '3' (range 1-10). At the bottom are 'Cancel' and 'Apply' buttons.

The following table describes the fields in this screen.

Table 27 Network Setting > Broadband > WAN Backup

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

Table 27 Network Setting > Broadband > WAN Backup (continued)

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

7.4 Ethernet WAN

Use this screen to have a LAN port act as an Ethernet WAN port. When the switch goes to the right, the LAN port acts as an Ethernet WAN port. Otherwise, the LAN port remains as a LAN port. Click **Apply** to save your changes back to the Zyxel Device.

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

Figure 66 Network Setting > Broadband > Ethernet WAN

Broadband

Broadband WAN Backup **Ethernet WAN** Cellular WAN Cellular SIM Cellular Band Cellular PLMN

You can convert Ethernet LAN port 4 to Ethernet WAN port or restore the WAN port to LAN port.

State: ☒

Note

(1) Active Enable, the Ethernet Port is WAN Ethernet.
 (2) Active Disable, the Ethernet Port is LAN Ethernet.
 (3) If Ethernet WAN cable and Cellular interface is connected at the same time, only Ethernet WAN will link up.

Cancel **Apply**

7.5 Cellular WAN

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

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

Figure 67 Network Setting > Broadband > Cellular WAN

The following table describes the fields in this screen.

Table 28 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 () 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.
Apply	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

7.6 Cellular APN

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

Note: This feature is only available on certain models. For details, see the features comparison table at [Section 1.1 on page 16](#).

Figure 68 Network Setting > Broadband > Cellular APN

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

The following table describes the labels in this screen.

Table 29 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.
Modify	Click the Edit icon to change the APN settings.

7.6.1 Edit Cellular APN1/APN2

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

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

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

Figure 69 Network Setting > Broadband > Cellular APN > Edit APN 1**Figure 70** Network Setting > Broadband > Cellular APN > Edit APN 2

The following table describes the fields in this screen.

Table 30 Network Setting > Broadband > Cellular APN > Edit APN

LABEL	DESCRIPTION
Enable	Click this to enable () the APN on the Zyxel Device
APN Manual Mode	Disable this to have the Zyxel Device configure the APN (Access Point Name) of a cellular network automatically. Otherwise, Click this to enable () and enter the APN manually in the field below.
APN	This field allows you to display the Access Point Name (APN) in the profile. Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method. You can enter up to 64 printable ASCII characters. Spaces are allowed.
Username	Enter the user name. You can enter up to 64 printable ASCII characters. Spaces are allowed.
Password	Enter the password associated with the user name above. You can enter up to 64 printable ASCII characters. Spaces are allowed.
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.
OK	Click OK to save your changes.
Cancel	Click Cancel to return to the previous screen without saving.

7.7 Cellular SIM Configuration

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

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

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

Figure 71 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 31 Network Setting > Broadband > Cellular SIM

LABEL	DESCRIPTION
PIN Management	
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. Click to enable (☒) if the service provider requires you to enter a PIN to use the SIM card. Click to disable if the service provider lets you use the SIM without inputting a PIN.
PIN	If you enabled PIN verification, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly too many times, the ISP may block your SIM card and not let you use the account to access the Internet.
Attempts Remaining	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card. If your ISP locks your SIM card, you will need to request a PUK code from them to unlock it.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to return to the previous screen without saving.

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

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

Figure 72 Network Setting > Broadband > Cellular Band

The following table describes the fields in this screen.

Table 32 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.
Band Management	
Band Auto Selection	Select the cellular bands to use for the Zyxel Device's cellular WAN connection. Click to enable () 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.

7.9 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 73 Network Setting > Broadband > Cellular PLMN

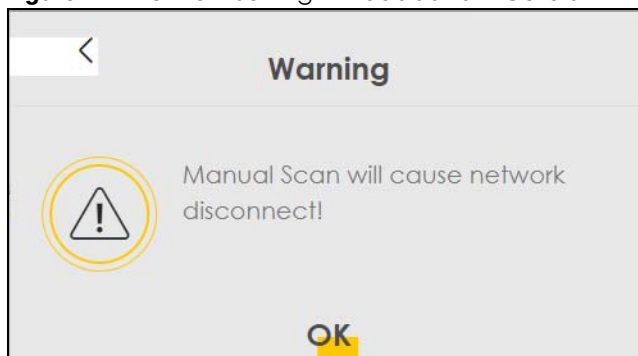
The following table describes the labels in this screen.

Table 33 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 74 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 75 Network Setting > Broadband > Cellular PLMN > Manual Scan

Cellular PLMN Configuration

PLMN Management

PLMN Auto Selection ☐

Scan

#	Status	Name	Type	PLMN
☐	Available	FET	LTE	46601
☐	Current	FET	UMTS	46601
☐	Forbidden	TWM	UMTS	46697
☐	Available	Chunghwa	UMTS	46692
☐	Available	Chunghwa	LTE	46692
☐	Forbidden	T Star	LTE	46689
☐	Forbidden	TWM	LTE	46697
☐	Forbidden	466 05	GPRS	46605
☐	Forbidden	466 05	LTE	46605
☐	Forbidden	T Star	UMTS	46689

Cancel **Apply**

The following table describes the labels in this screen.

Table 34 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.

7.10 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.

Figure 76 Network Setting > Broadband > Cellular IP Passthrough

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

Figure 77 Network Setting > Broadband > Cellular IP Passthrough > Enable Warning

The following table describes the fields in this screen.

Table 35 Network Setting > Broadband > Cellular IP Passthrough

LABEL	DESCRIPTION
IP Passthrough Management	
IP Passthrough	IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the LAN computer and will not go through NAT.
Passthrough Mode	Select Dynamic to allow traffic to be forwarded to the first LAN computer on the local network of the Zyxel Device. Select Fixed to allow traffic to be forwarded to a specific computer (for example, Client A) by entering its MAC address. Note: This field will show after enabling IP Passthrough in the previous field.

Table 35 Network Setting > Broadband > Cellular IP Passthrough (continued)

LABEL	DESCRIPTION
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.

7.11 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 78 Cellular Lock

The following table describes the fields in this screen.

Table 36 Cellular Lock

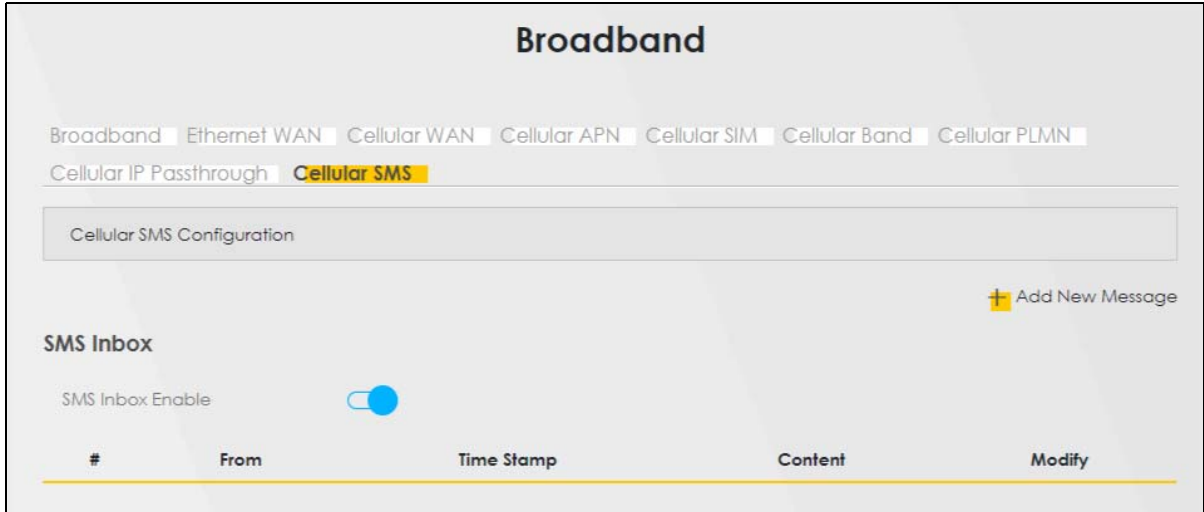
LABEL	DESCRIPTION
PCI Lock	Select this to enable or disable PCI (Physical Cell Identifier) Lock.
Add New Rule	Select this if you want to add a new rule or to configure cellular lock rules.
Physical Cell ID	Use this to enter the PCI number of the base station you choose to connect to (0 – 504).
RFCN	Use RFCN (Radio Frequency Channel Number) to enter the LTE frequency of the specified PCI number(1 – 65535).
Cancel	Click this to exit this screen without saving.
Apply	Click this to save your changes.

7.12 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 79 Cellular SMS



The following table describes the fields in this screen.

Table 37 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.

7.12.1 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 80 Send New Message

Send New Message

Character Set: GSM default alphabet

Mobile Number:

Text Message: 140

Non-GSM Character:

Note

(1) The character limit for a single SMS message is 140 by using GSM-7 encoding.
 (2) The character limit for a single SMS message is 70 by using Unicode encoding.

Cancel OK

The following table describes the fields in this screen.

Table 38 Cellular SMS

LABEL	DESCRIPTION
Character Set	Select whether you want to send the SMS message using GSM-7 encoding or unicode. GSM default alphabet: Use standard ASCII numbers, letters, and special characters. The maximum length of the message is 140 characters. Unicode alphabet: Use any non-English Unicode characters. The maximum length of the message is 70 characters.
Mobile Number	Specify the cellphone number that you want to send the message to.
Text Message	Specify the content of the message.
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 115](#)).
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device ([Section 8.3 on page 119](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device ([Section 8.5 on page 123](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 8.6 on page 124](#)).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications ([Section 8.7 on page 126](#)).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold ([Section 8.8 on page 127](#)).
- Use the **WLAN Scheduler** screen to create rules to schedule the times to permit Internet traffic from each wireless network interfaces ([Section 8.9 on page 129](#)).
- Use the **Channel Status** screen to scan the number of accessing points and view the results ([Section 8.10 on page 131](#)).

8.1.2 What You Need to Know

Wireless Basics

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

Finding Out More

See [Section 8.11 on page 132](#) 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.

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

Figure 81 Network Setting > Wireless > General

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

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 Network Setup

Band: 2.4GHz

Wireless: ☒

Channel: Auto Current : 1

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Zyxel_8853

Max Clients: 32

☐ Hide SSID ⓘ

☒ Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

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 device sets the value automatically.
 (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

SSID: 98:0D:67:5D:B8:53

Security Level

No Security More Secure (Recommended)

Security Mode: WPA2-PSK

☒ Generate password automatically

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

Password:

Strength: strong

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

Table 39 Network Setting > Wireless > General

LABEL	DESCRIPTION
WiFi Network Setup	
Band	This shows the WiFi band which this radio profile is using. • 2.4 GHz is used by IEEE 802.11b/g/n WiFi clients • 5 GHz is used by IEEE 802.11a/n/ac/ax WiFi clients
WiFi	Click Enable to enable the wireless LAN in this field.
Channel	Use Auto to have the Zyxel Device automatically determine a channel to use.

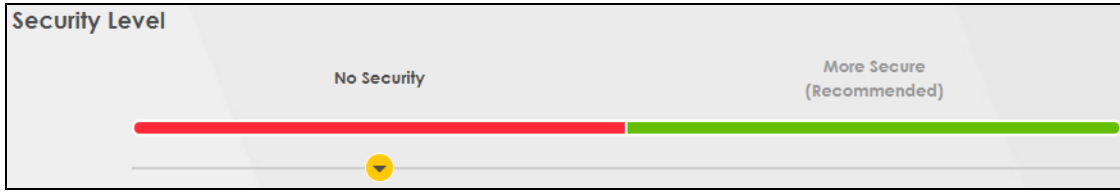
Table 39 Network Setting > Wireless > General (continued)

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

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 82 Wireless > General: No Security

The following table describes the labels in this screen.

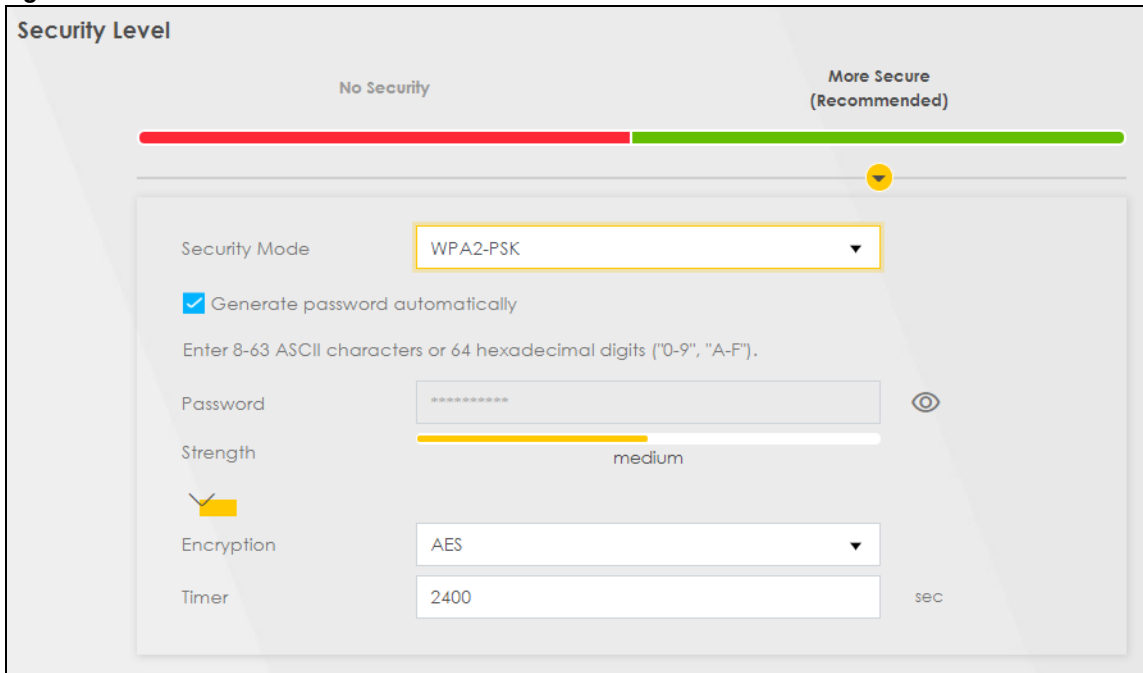
Table 40 Wireless > General: No Security

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

8.2.2 More Secure (Recommended)

The 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 83 Wireless > General: More Secure: WPA2-PSK

The following table describes the labels in this screen.

Table 41 Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select More Secure to enable WPA2-PSK data encryption.
Security Mode	WPA2-PSK is the default security mode.

Table 41 Wireless > General: More Secure: 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	Select Generate password automatically or enter a Password. The password has two uses. 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8 – 63 ASCII characters or exactly 64 hexadecimal ('0 – 9', 'a – f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: Enter 8 – 63 ASCII characters only. 64 hexadecimal characters are not accepted for WPS. Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it is hidden.
more...	Click this  to show more fields in this section. Click this  to hide them.
Encryption	AES is the default data encryption type, which uses a 128-bit key. 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	This is the rate at which the RADIUS server sends a new group key out to all clients.

8.3 Guest/More AP

Use this screen to configure a guest wireless network that allows access to the Internet through the Zyxel Device. Click **Network Setting > Wireless > Guest/More AP**. The screen appears as shown. This allows you to 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.

Figure 84 Network Setting > Wireless > Guest/More AP

WiFi

General **Guest/More AP** MAC Authentication WPS WMM Others WLAN Scheduler

This modem can enable up to 4 WiFi networks to work at the same time. Assign a name and a security level (if needed) to start the 2nd, 3rd, and 4th Wi-Fi network services.

#	1	2	3
Status			
SSID	Zyxel_6355_guest1	Zyxel_6355_guest2	Zyxel_6355_guest3
Security	WPA2-Personal	WPA2-Personal	WPA2-Personal
Guest WLAN	External Guest	External Guest	External Guest
Modify			

The following table describes the labels in this screen.

Table 42 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Status	This shows whether the SSID profile is active (a yellow bulb) or not (a gray bulb).
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. You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the Zyxel Device. 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 field shows whether the SSID profile is an external or home guest.
Modify	Click Modify to change the SSID profile.

8.4 More AP Edit

Use this screen to create a guest wireless network and configure its security settings.

Click the **Modify** icon in the **Guest/More AP** screen. The following screen displays.

Figure 85 Network Setting > Wireless > 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 Kbps

Max. Downstream Bandwidth Kbps

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 device sets the value automatically.
 (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID

SSID Subnet ☒

DHCP Start Address

DHCP End Address

SSID Subnet Mask

LAN IP Address

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 strong

Encryption

Timer sec

Cancel

The following table describes the labels in this screen.

Table 43 Network Setting > Wireless > More AP Edit

LABEL	DESCRIPTION
WiFi Network Setup	
WiFi	Click Enable to enable the wireless LAN in this field.
Security Level	
WiFi Network Name	The SSID (Service Set Identity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.

Table 43 Network Setting > Wireless > 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. This check box is grayed out if the WPS function is enabled in the Network > Wireless > WPS screen.
Guest WLAN	Select the check box to enable Guest WLAN.
Access Scenario	If you select Home Guest , clients connecting to the same SSID can communicate with 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	Select Enable to create an independent subnet for the SSID, which is separated from the LAN subnets.
DHCP Start Address	Enter the first of the contiguous addresses in the IP address pool for the SSID subnet. The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Enter the last of the contiguous addresses in the IP address pool for the SSID subnet.
SSID Subnet Mask	Enter the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Enter the IP address of the Zyxel Device for the Guest SSID.
Security Level	
Security Mode	Select More Secure or WPA2-PSK to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate with this network without any data encryption or authentication. See the following sections for more details about this field.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	Select Generate password automatically or enter a Password . The password has two uses. 1. Manual. Manually enter the same password on the Zyxel Device and the client. Enter 8 – 63 ASCII characters or exactly 64 hexadecimal ('0 – 9', 'a – f') characters. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: Enter 8 – 63 ASCII characters only. 64 hexadecimal characters are not accepted for WPS. Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed  , you will see the password in plain text. Otherwise, it is hidden.
more...	Click this  to show more fields in this section. Click this  to hide them.
Encryption	AES is the default data encryption type, which uses a 128-bit key.

Table 43 Network Setting > Wireless > More AP Edit (continued)

LABEL	DESCRIPTION
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

8.5 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.

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.

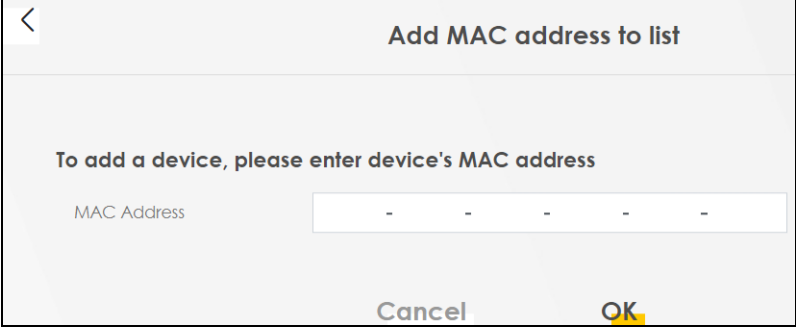
Figure 86 Network Setting> Wireless > MAC Authentication

The following table describes the labels in this screen.

Table 44 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 44 Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
Add new MAC address	This field is available when you select Deny or Allow in the MAC Restrict Mode field. Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the WiFi devices that are allowed or denied access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. 
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the WiFi devices that are allowed or denied access to the Zyxel Device.
Modify	Click the Edit icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the Delete icon to delete the entry.
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

8.6 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 8.11.5.3 on page 138](#) 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 118](#)).

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 87 Network Setting > Wireless > WPS

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

General

WPS ☐

Add a new device with WPS Method

Method 1 PBC ☒ **1**

Step1. Click WPS button

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

WPS

Method 2 PIN ☐ **3**

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

Register

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

1. Please release configuration if you want to configure the wireless settings
Release Configuration

2. Enter current PIN number on your wireless client
Generate New PIN

Note

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

Cancel **Apply** **2**

The following table describes the labels in this screen.

Table 45 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.

Table 45 Network Setting > Wireless > WPS (continued)

LABEL	DESCRIPTION
Method 3	Use this section to set up a WPS WiFi network by entering the PIN of the Zyxel Device into the client. Click this switch to make it turn blue. Click Apply to activate WPS method 3 on the Zyxel Device.
Release Configuration	The default WPS status is configured . Click this button to remove all configured WiFi and WiFi security settings for WPS connections on the Zyxel Device.
Generate New PIN	If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the 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.

8.7 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 88 Network Setting > Wireless > WMM

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

WMM and APSD have beneficial effects on delay-sensitive applications over wireless connection such as, VoIP and multimedia streaming, because WMM enhances data transmission quality and APSD improves power management on wireless clients

WMM of SSID1 ☐

WMM of SSID2 ☐

WMM of SSID3 ☐

WMM of SSID4 ☐

WMM Automatic Power Save Delivery (APSD) ☒

Note
WMM is mandatory to be enabled if 802.11 mode includes 802.11n or 802.11ac

Cancel Apply

Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

The following table describes the labels in this screen.

Table 46 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.

8.8 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 8.11.2 on page 134](#) for detailed definitions of the terms listed here.

Figure 89 Network Setting > Wireless > Others

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/ax Mixed	▼
802.11 Protection	Auto	▼
Preamble	Long	
Protected Management Frames	Capable	▼
Cancel Apply		

The following table describes the labels in this screen.

Table 47 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: 20%, 40%, 60%, 80% or 100%.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50 ms to 1000 ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	For 2.4 GHz frequency WiFi devices: • Select 802.11b Only to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select 802.11g Only to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11b/g/n Mixed to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11b/g/n/ax Mixed to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. For 5 GHz frequency WiFi devices: • Select 802.11a Only to allow only IEEE 802.11a compliant WiFi devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select 802.11ac Only to allow only IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. • Select 802.11a/n Mixed to allow either IEEE 802.11a or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11n/ac Mixed to allow either IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11a/n/ac Mixed to allow IEEE 802.11a, IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11a/n/ac/ax Mixed to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.

Table 47 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select Off to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network. This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.
Preamble	Select a preamble type from the drop-down list box. Choices are Long or Short. See Section 8.11.5 on page 136 for more information. This field is configurable only when you set 802.11 Mode to 802.11b.
Protected Management Frames	WiFi with Protected Management Frames (PMF) provides protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging. Select Capable if the WiFi client supports PMF, then the management frames will be encrypted. Select Required to force the WiFi client to support PMF; otherwise the authentication cannot be performed by the Zyxel Device. Otherwise, select Disabled.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

8.9 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 90 Network Setting > Wireless > WLAN Scheduler

WiFi

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

WLAN Scheduler allows you to permit internet traffic from each Wi-Fi network interfaces.
Out of those periods, the specified WiFi network will be automatically switched off.
Can be also created a rule to automatically switch off all the WLAN together.

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

WLAN Scheduler Access ☐

+ Add New Rule

#	Active	Rule Name	SSID	Day	Time	Description	Modify
Cancel Apply							

The following table describes the labels in this screen.

Table 48 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.

8.9.1 Add or Edit Rules

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

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

Figure 91 Network Setting > Wireless > WLAN Scheduler > Add New Rule

The following table describes the labels in this screen.

Table 49 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.

8.10 Channel Status

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

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

Figure 92 Network Setting > Wireless > Channel Status



8.11 Technical Reference

This section discusses wireless LANs in depth.

8.11.1 WiFi Network Overview

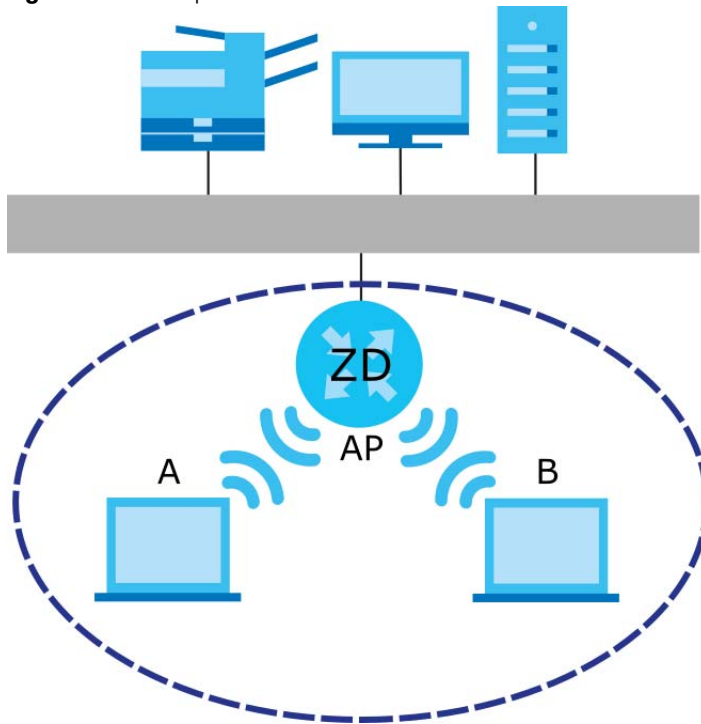
WiFi networks consist of WiFi clients, access points and bridges.

- 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 93 Example of a WiFi Network



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

Every WiFi network must follow these basic guidelines.

- Every device in the same WiFi network must use the same SSID.
The SSID is the name of the WiFi network. It stands for Service Set Identifier.
- If two WiFi networks overlap, they should use a different channel.
Like radio stations or television channels, each WiFi network uses a specific channel, or frequency, to send and receive information.
- Every device in the same WiFi network must use security compatible with the AP.
Security stops unauthorized devices from using the WiFi network. It can also protect the information that is sent in the WiFi network.

8.11.2 Additional Wireless Terms

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

Table 50 Additional WiFi Terms

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

8.11.3 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.

8.11.3.1 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.

8.11.3.2 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.

8.11.3.3 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See [Section 8.11.3.3 on page 135](#) for information about this.)

Table 51 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest ↕	No Security	WPA WPA2
	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**.

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.

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.

8.11.4 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.

8.11.5 WiFi Protected Setup (WPS)

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

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

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

8.11.5.1 Push Button Configuration

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

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

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

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the Zyxel Device, see [Section 8.6 on page 124](#)).
- 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.

8.11.5.2 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.

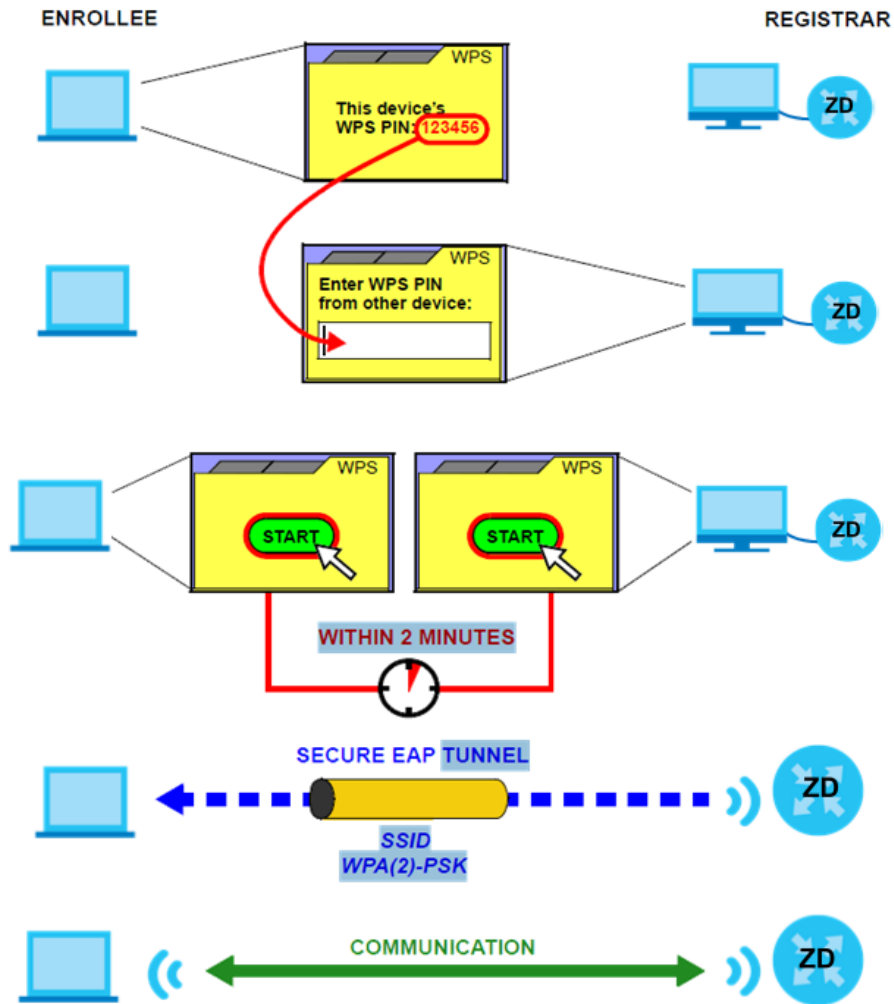
When you use the PIN method, you must enter the PIN from one device (usually the WiFi client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network 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 8.6 on page 124](#)).
- 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.

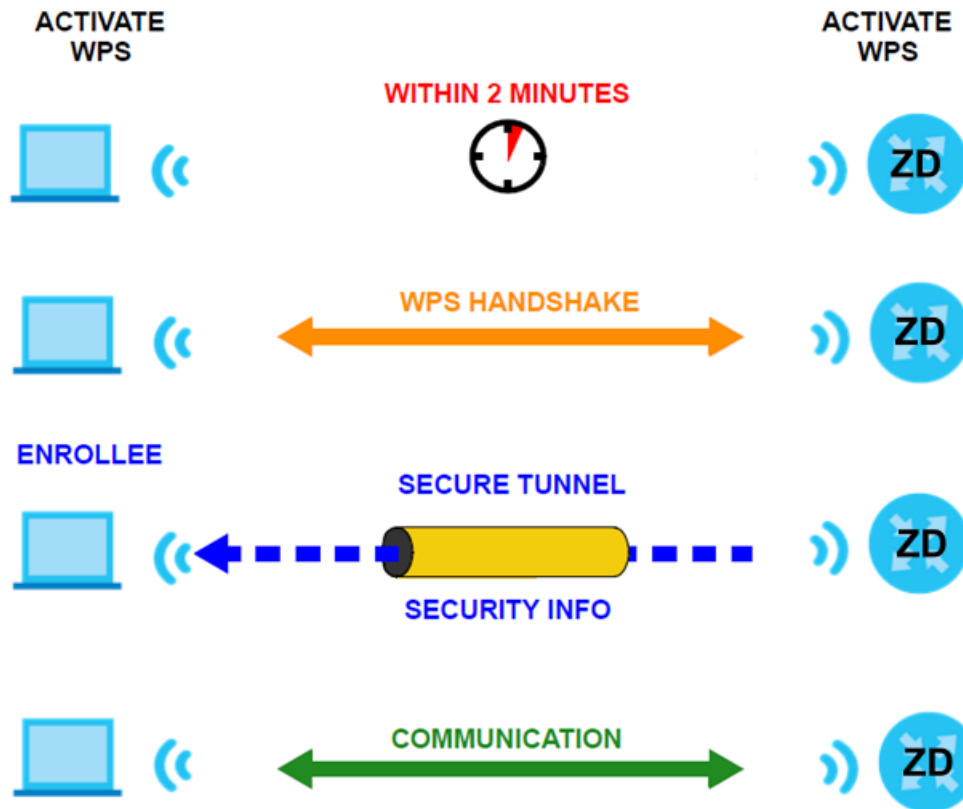
The following figure shows a WPS-enabled WiFi client (installed in a notebook computer) connecting to the WPS-enabled AP through the PIN method.

Figure 94 Example WPS Process: PIN Method

8.11.5.3 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 95 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.

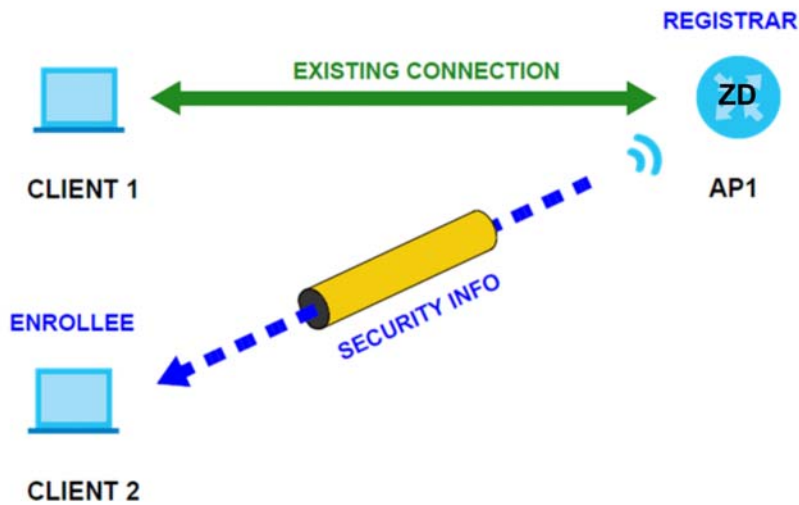
8.11.5.4 Example WPS Network Setup

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

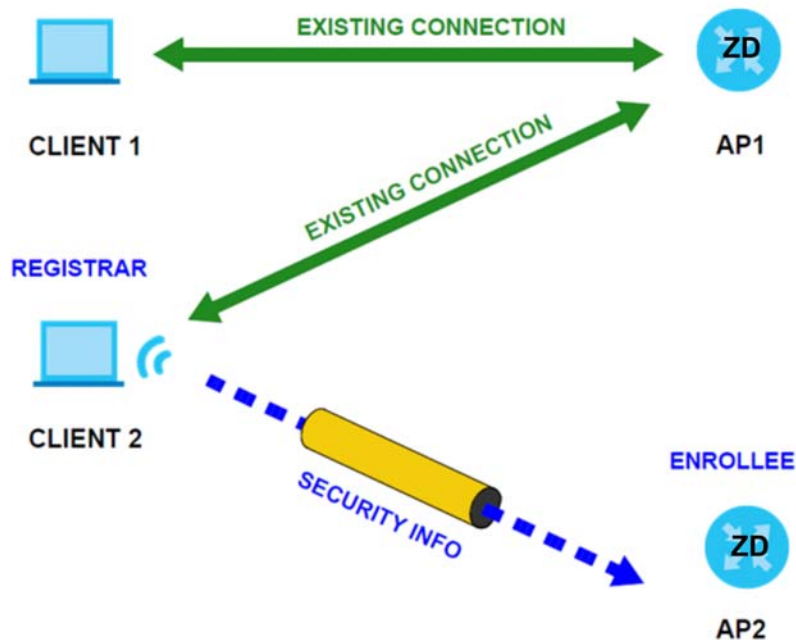
The following figure shows a sample network. In step 1, both **AP1** and **Client 1** are un-configured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 96 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 97 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 98 WPS: Example Network Step 3

8.11.5.5 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

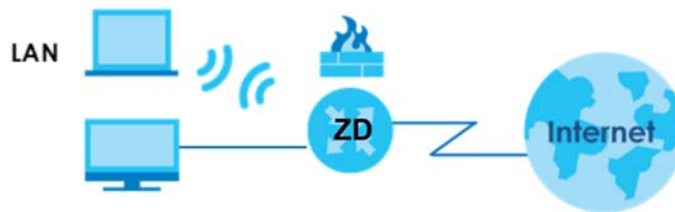
Home Networking

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 99 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 143](#)).
- 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 147](#)).
- Use the **UPnP** screen to enable UPnP ([Section 9.4 on page 149](#)).

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 150](#) 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 '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 . Configure DHCP settings to have the or a DHCP server assign IP addresses to devices. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Figure 100 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 52 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	This displays the name of the group that your Zyxel Device belongs to.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select Enable to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN. If you select DHCP Relay, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. When DHCP is used, the following fields need to be set:
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
Days/Hours/Minutes	DHCP server leases an address to a new device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different device.
DNS Values	
DNS	The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client. Select From ISP if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address). Select Static if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select DNS Proxy to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.
LAN IPv6 Mode Setup	
IPv6 Active	Use this field to Enable or Disable IPv6 activation on the Zyxel Device. When IPv6 activation is used, the following fields need to be set.

Table 52 Network Setting > Home Networking > LAN Setup (continued)

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

Table 52 Network Setting > Home Networking > LAN Setup (continued)

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

9.3 Static DHCP

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

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

9.3.1 Before You Begin

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

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

Figure 101 Network Setting > Home Networking > Static DHCP

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

+ Static DHCP Configuration

#	Status	MAC Address	IP Address	Modify
---	--------	-------------	------------	--------

The following table describes the labels in this screen.

Table 53 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 102 Static DHCP: Static DHCP Configuration

Static DHCP Configuration

Active ☒

Group Name

IP Type

Select Device Info

MAC Address

IP Address

Cancel OK

The following table describes the labels in this screen.

Table 54 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 150](#) for more information on UPnP.

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

Figure 103 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
Cancel Apply					

The following table describes the labels in this screen.

Table 55 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.

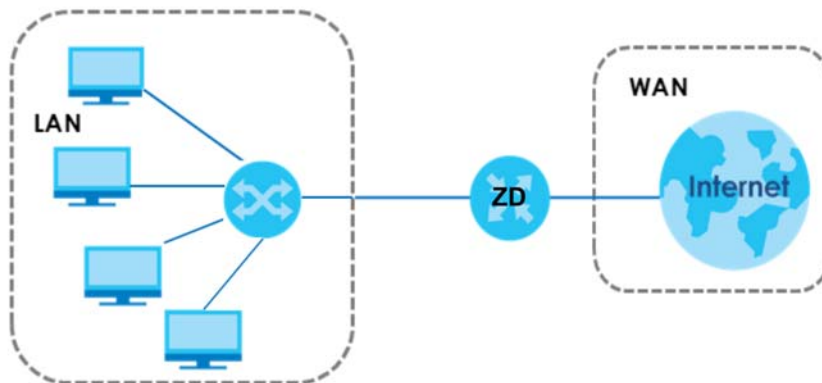
9.5 Technical Reference

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 104 LAN and WAN IP Addresses

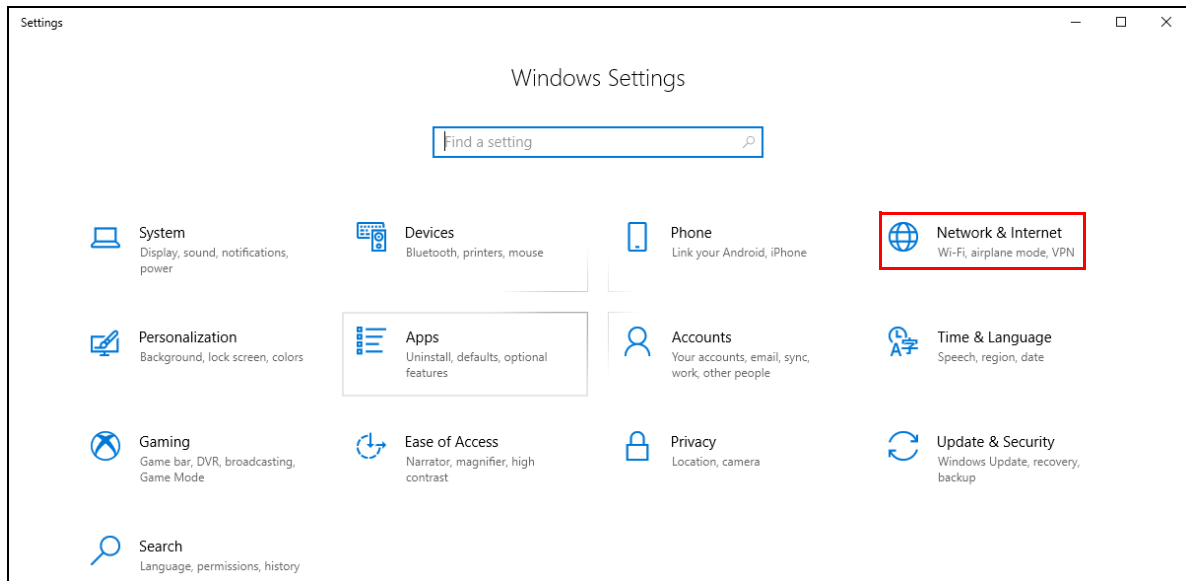


9.6 Turn on UPnP in Windows 10 Example

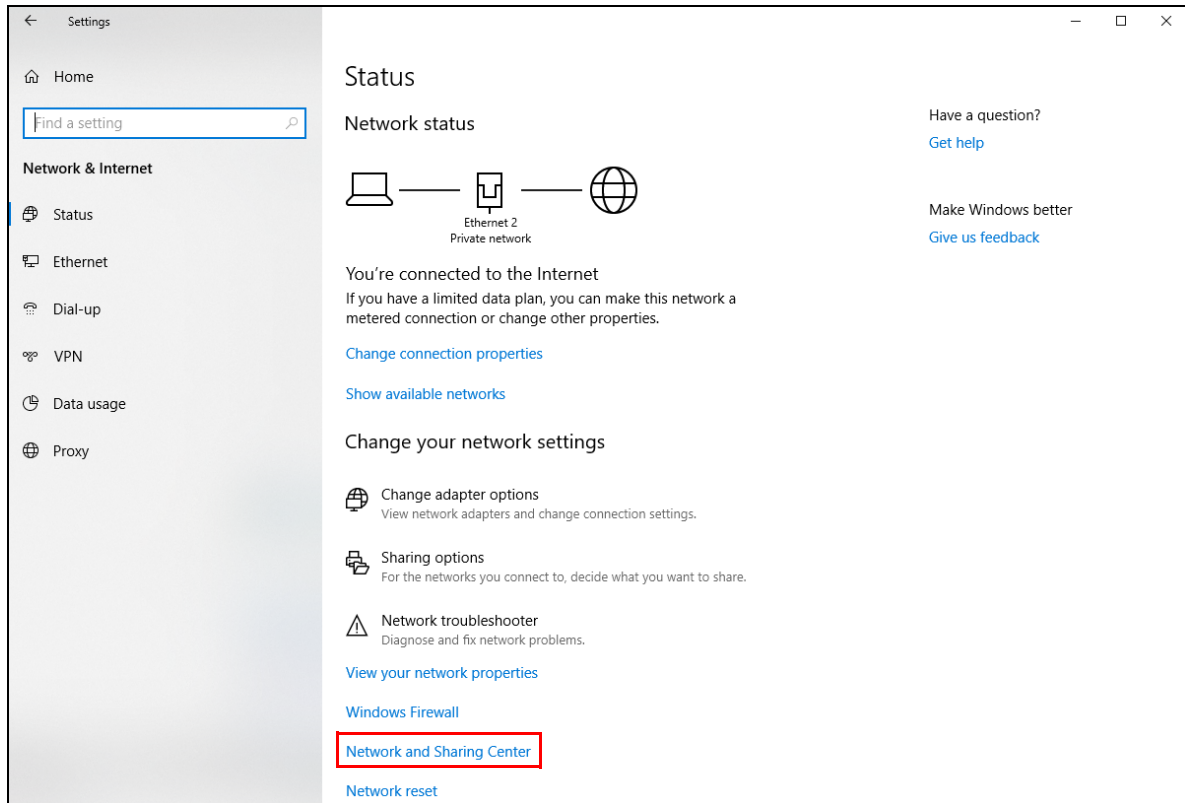
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting** > **Home Networking** > **UPnP**.

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

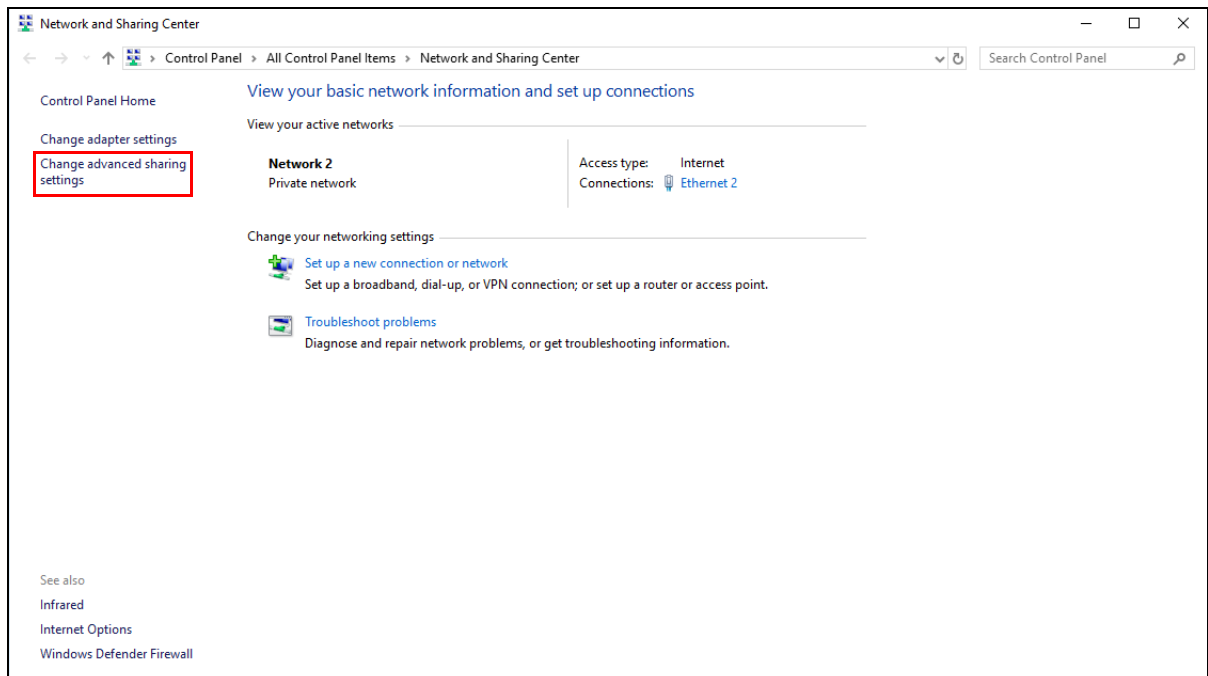
- 1 Click the start icon, **Settings** and then **Network & Internet**.



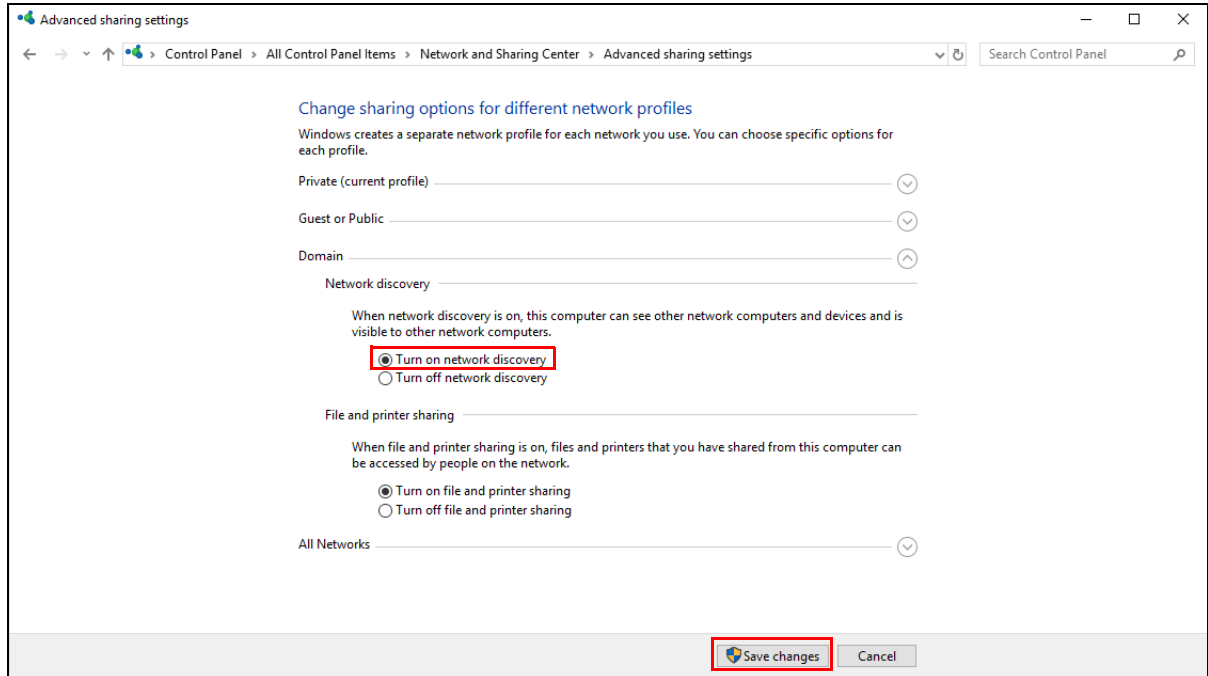
- 2 Click **Network and Sharing Center**.



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.

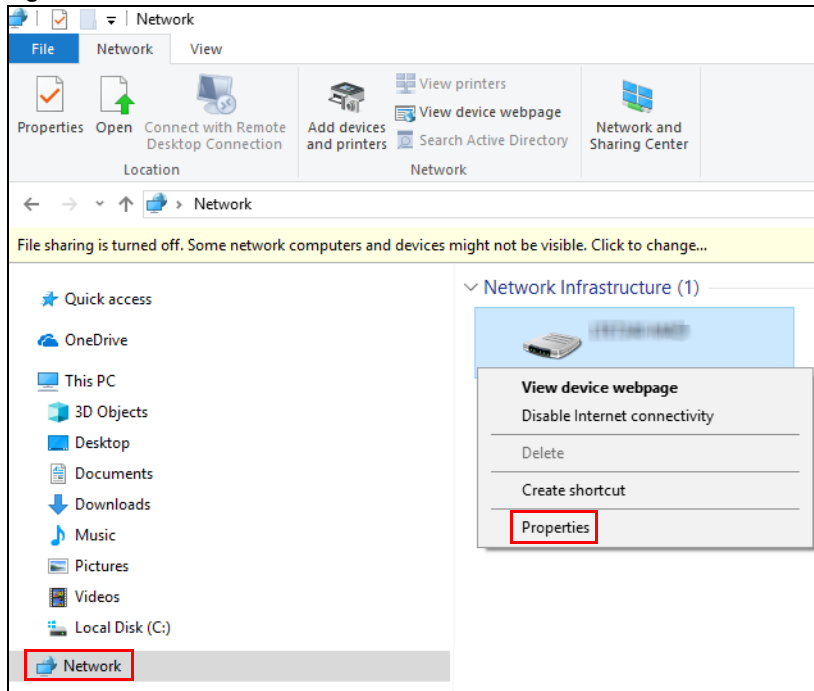


9.6.1 Auto-discover Your UPnP-enabled Network Device

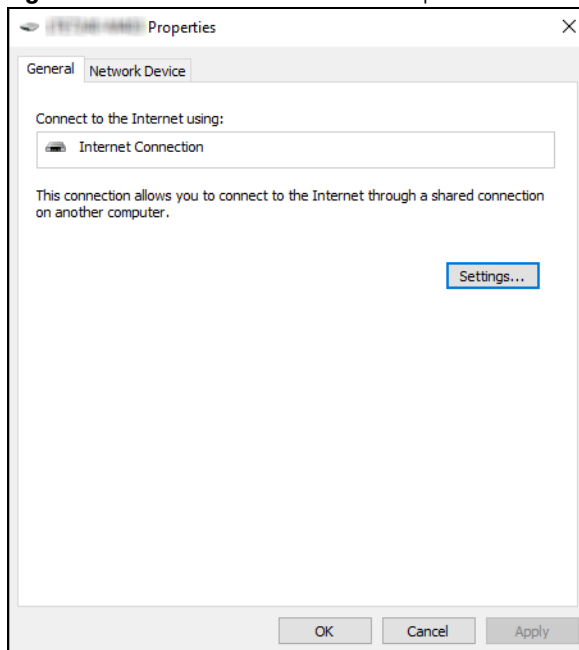
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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

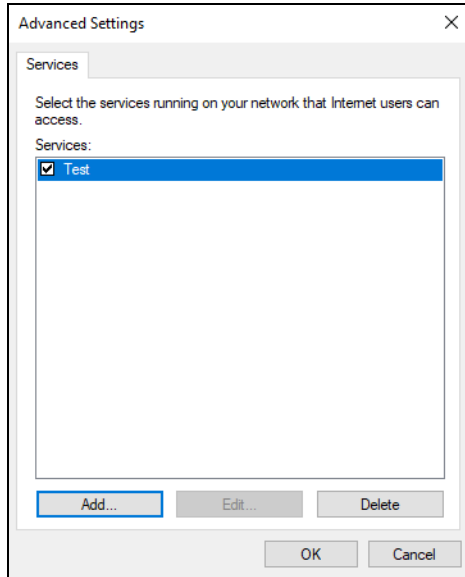
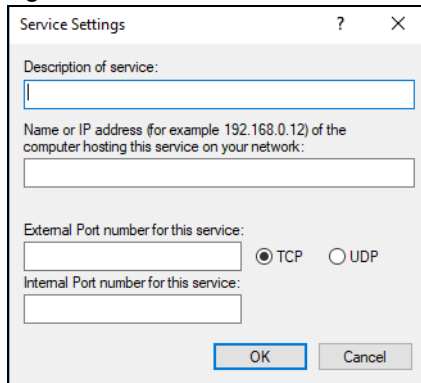
- 1 Open **File Explorer** and click **Network**.
- 2 Right-click the Zyxel Device icon and select **Properties**.

Figure 105 Network Connections

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

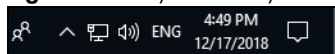
Figure 106 Internet Connection Properties

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

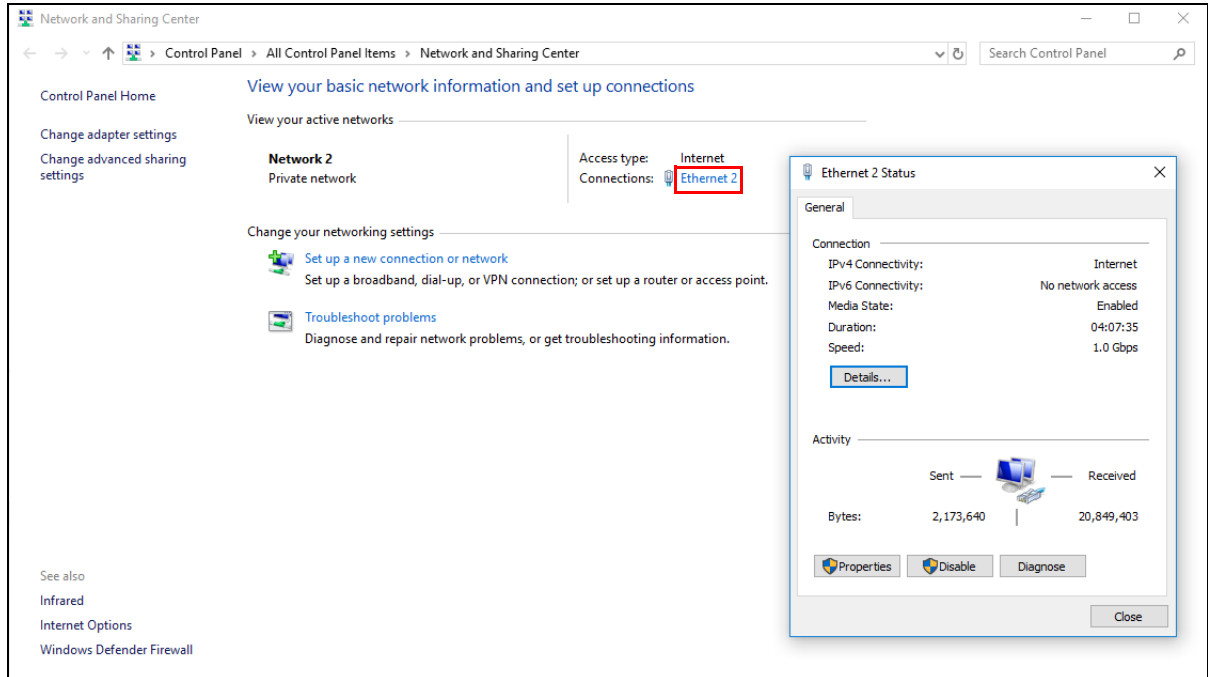
Figure 107 Internet Connection Properties: Advanced Settings**Figure 108** Internet Connection Properties: Advanced Settings: Add

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 109 System Tray Icon

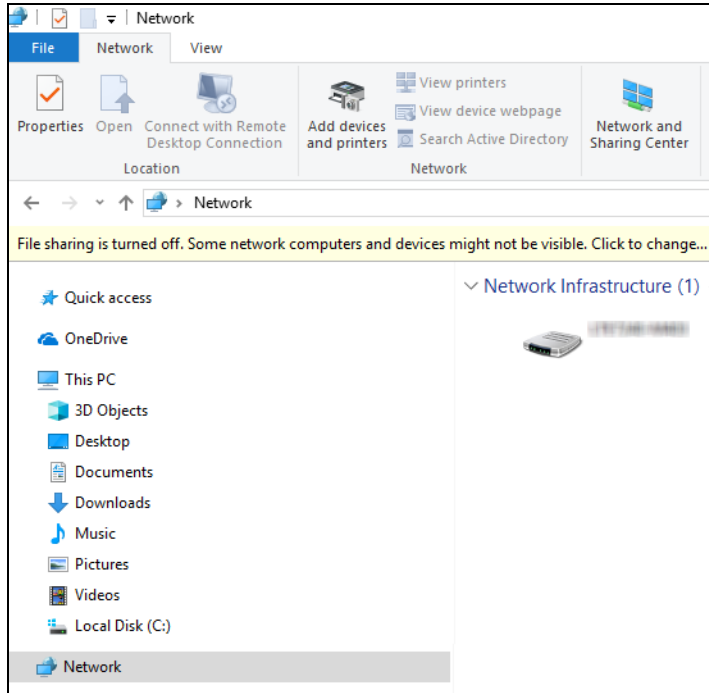
- 6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 110 Internet Connection Status

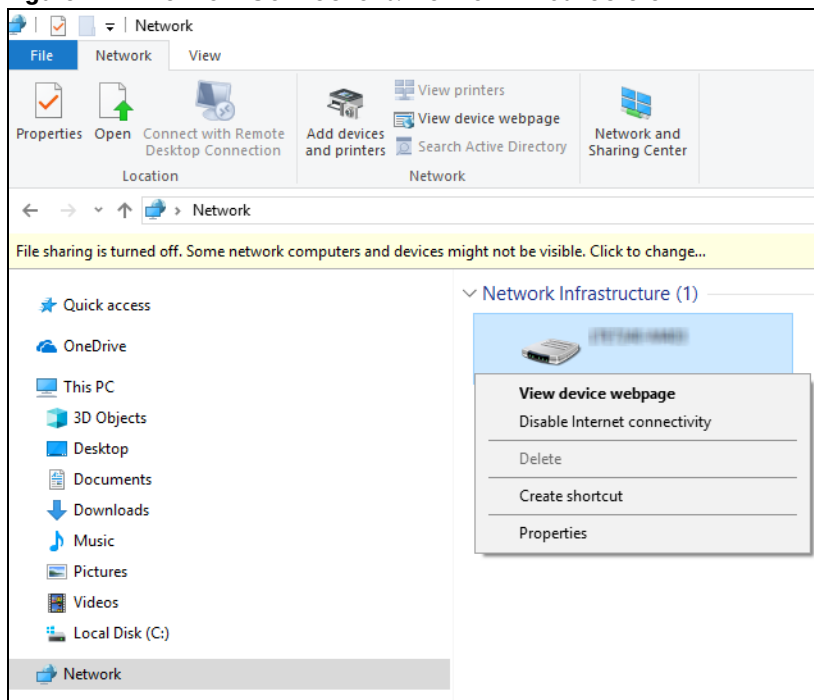
9.7 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

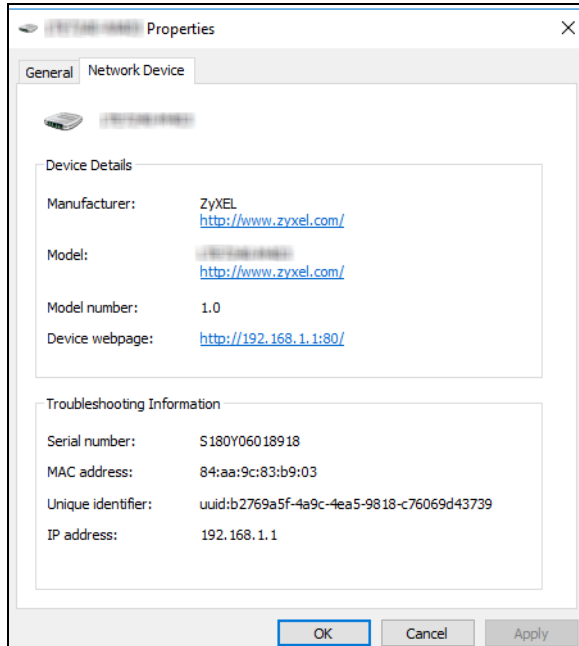
- 1 Open **File Explorer**.
- 2 Click **Network**.

Figure 111 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 112 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 113 Network Connections: Network Infrastructure: Properties: Example

CHAPTER 10

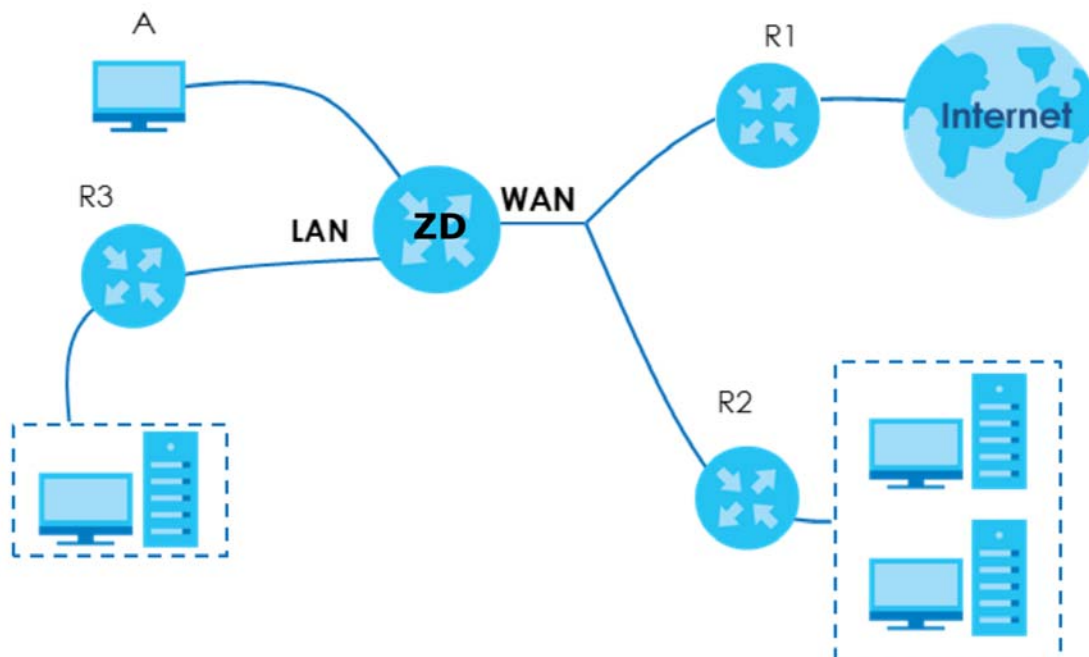
Routing

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 114 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 115 Network Setting > Routing > Static Route

Routing

Static Route | DNS Route | Policy Route | RIP

Use this screen to view and configure the static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

+ Add New Static Route

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

The following table describes the labels in this screen.

Table 56 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 116 Network Setting > Routing > Static Route > Add New Static Route

The following table describes the labels in this screen.

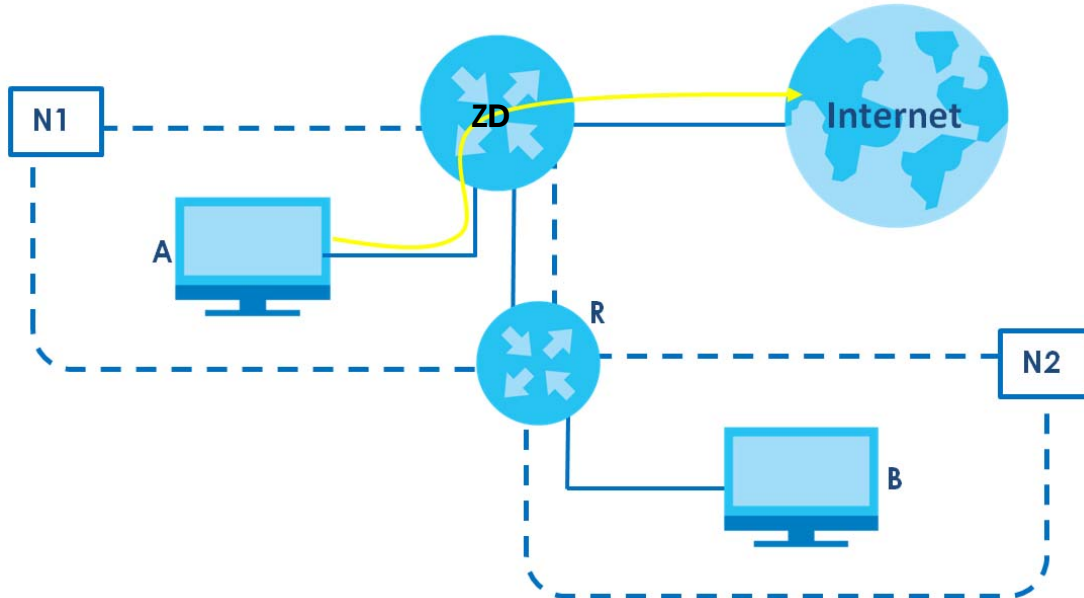
Table 57 Network Setting > Routing > Static Route > Add New Static Route

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 1038 IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.
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.

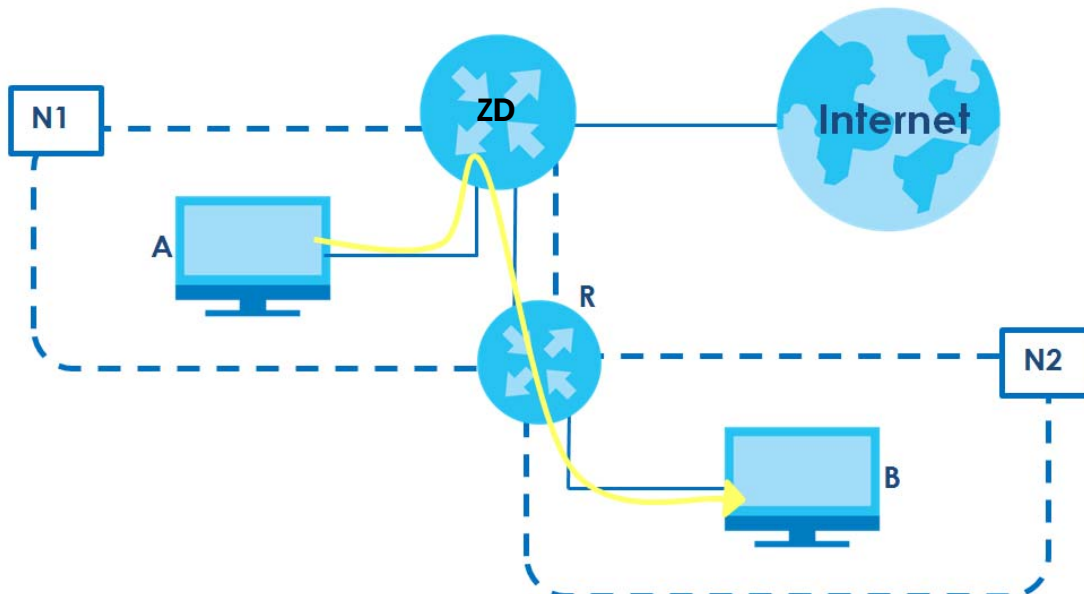
10.2.1.1 An Example of Adding a Static Route

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**.



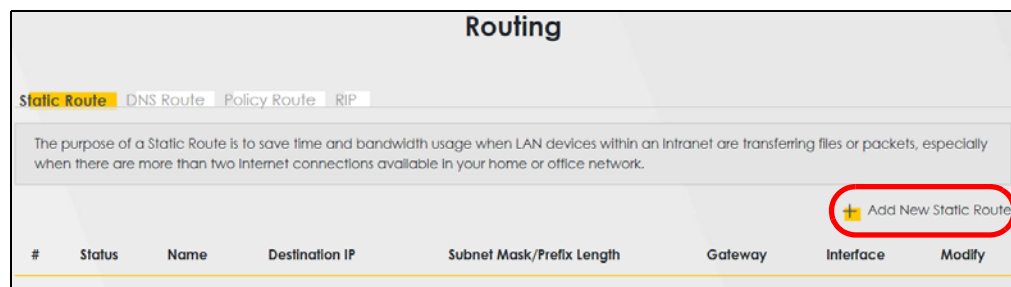
This tutorial uses the following example IP settings:

Table 58 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

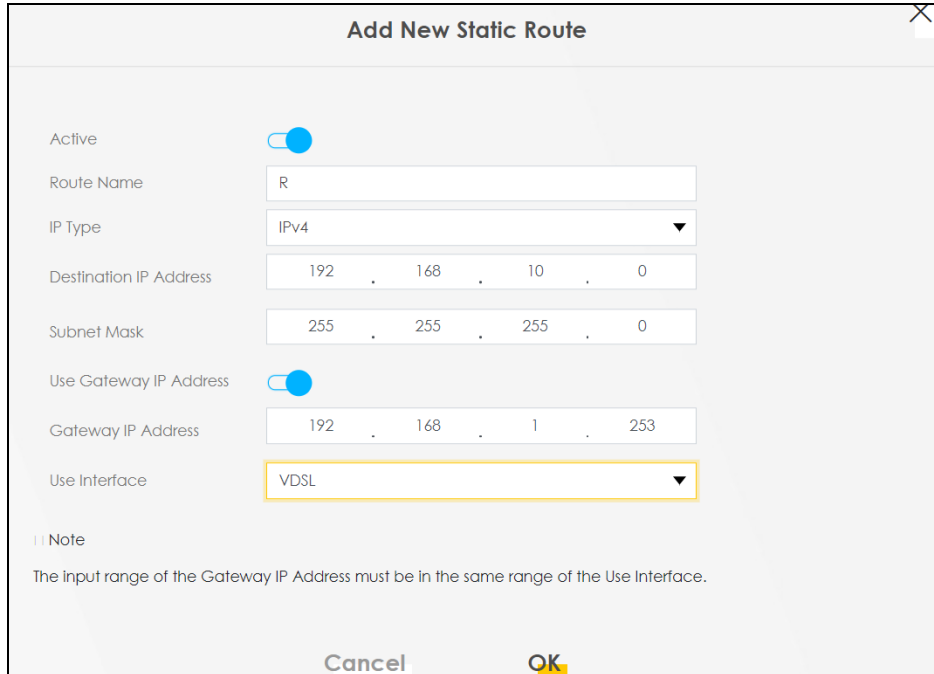
To configure a static route to route traffic from **N1** to **N2**:

- 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.



Add New Static Route

Active ☒

Route Name

IP Type

Destination IP Address

Subnet Mask

Use Gateway IP Address ☒

Gateway IP Address

Use Interface

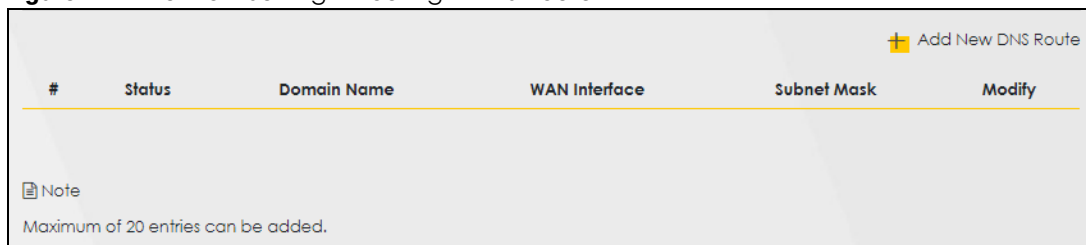
Note
The Input range of the Gateway IP Address must be in the same range of the Use Interface.

Cancel OK

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 117 Network Setting > Routing > DNS Route



+

 Add New DNS Route

#	Status	Domain Name	WAN Interface	Subnet Mask	Modify
Note Maximum of 20 entries can be added.					

The following table describes the labels in this screen.

Table 59 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 59 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 118 Network Setting > Routing > DNS Route > Add New DNS Route

The following table describes the labels in this screen.

Table 60 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 119 Network Setting > Routing > Policy Route

										+ Add New Policy Route	
#	Status	Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Source Interface	WAN Interface	Modify	

The following table describes the labels in this screen.

Table 61 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 120 Policy Route: Add or Edit

The screenshot shows the 'Add New Policy Route' configuration screen. It includes a back arrow in the top left corner. The title 'Add New Policy Route' is centered at the top. The configuration fields are as follows:

- Active:** A blue toggle switch is turned on.
- Route Name:** An empty text input field.
- Source IP Address:** An empty text input field.
- Source Subnet Mask:** An empty text input field.
- Protocol:** A dropdown menu with 'None' selected.
- Source Port:** A text input field containing the number '0'.
- Source MAC:** An empty text input field.
- Source Interface(ex: br0 or LAN1~LAN4):** An empty text input field.
- WAN Interface:** A dropdown menu with 'Cellular WAN' selected.

At the bottom of the screen, there are two buttons: 'Cancel' and 'OK'.

The following table describes the labels in this screen.

Table 62 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 121 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	☐	☐
2	ETHWAN	RIPv2	Active	☐	☐

Cancel Apply

The following table describes the labels in this screen.

Table 63 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 170](#)).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings ([Section 11.3 on page 173](#)).
- Use the **DMZ** screen to configure a default server ([Section 11.4 on page 176](#)).
- Use the **ALG** screen to enable or disable the SIP ALG ([Section 11.5 on page 177](#)).
- Use the **Address Mapping** screen to enable and disable the NAT Address Mapping in the Zyxel Device ([Section 11.6 on page 178](#)).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use ([Section 11.7 on page 180](#)).

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.

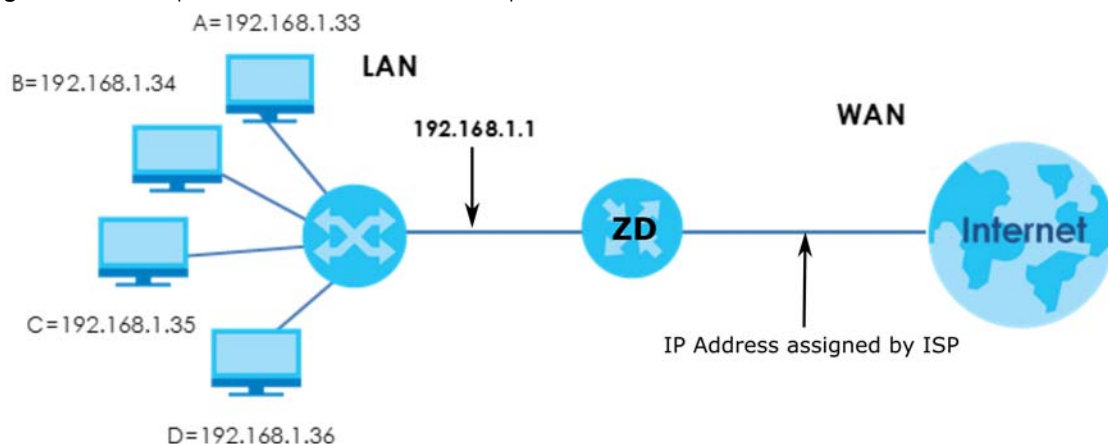
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more 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 122 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 123 Network Setting > NAT > Port Forwarding

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

+ Add New Rule

#	Status	Service Name	Originating IP	WAN Interface	Server IP Address	Start Port	End Port	Translation Start Port	Translation End Port	Protocol	Modify
Note TCP port 7547 is reserved for TR-069 requests.											

The following table describes the fields in this screen.

Table 64 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 124 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 65 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 65 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.

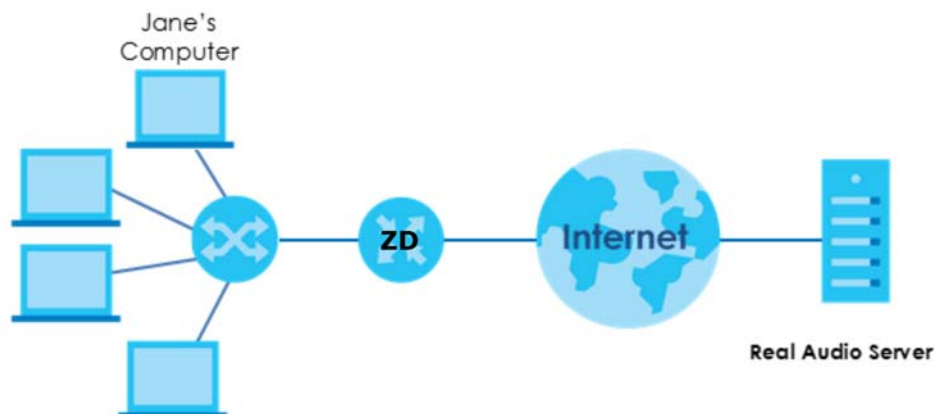
11.3 Port Triggering

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 125 Trigger Port Forwarding Process: Example

- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970 – 7170.
- 3 The Real Audio server responds using a port number ranging between 6970 – 7170.
- 4 The Zyxel Device forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in 3 minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

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

Note: TCP port 7547 is reserved for system use.

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

Figure 126 Network Setting > NAT > Port Triggering

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

The following table describes the labels in this screen.

Table 66 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 66 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 127 Port Triggering: Add or Edit

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

- Active:** A toggle switch that is currently turned on (blue).
- Service Name:** A text input field.
- WAN Interface:** A dropdown menu with 'Default' selected.
- Trigger Start Port:** A text input field.
- Trigger End Port:** A text input field.
- Trigger Protocol:** A dropdown menu with 'TCP' selected.
- Open Start Port:** A text input field.
- Open End Port:** A text input field.
- Open Protocol:** A dropdown menu with 'TCP' selected.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

The following table describes the labels in this screen.

Table 67 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 128 Network Setting > NAT > DMZ

A client in the Demilitarized Zone (DMZ) is no longer behind the Zyxel Device and can therefore run any Internet application such as video conferencing and Internet gaming without restrictions. This, however, may pose a security threat to the Zyxel Device. Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen.

Default Server Address

 **Note**

(1) Use an IPv4 address for the DMZ server.
 (2) Enter the IP address and click **Apply** to activate the DMZ host.
 Otherwise, clear the IP address field and click **Apply** to de-activate the DMZ host.

Cancel **Apply**

The following table describes the fields in this screen.

Table 68 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

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 129 Network Setting > NAT > ALG

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

SIP ALG ☒

PPTP ALG ☒

Cancel **Apply**

The following table describes the fields in this screen.

Table 69 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 Address Mapping

Use this screen to enable or disable the NAT Address Mapping in the Zyxel Device.

11.6.1 Address Mapping Screen

Click **Network Setting > NAT > Address Mapping** to open the **Address Mapping** screen.

Figure 130 Network Setting > NAT > Address Mapping

NAT

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

Address Mapping can map Local IP Addresses to Global IP Addresses.

+ Add New Rule

Rule Name	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	WAN Interface	Modify
-----------	----------------	--------------	-----------------	---------------	------	---------------	--------

The following table describes the fields in this screen.

Table 70 Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
Rule Name	This is the name of the rule.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.

Table 70 Network Setting > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Type	This is the address mapping type. One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type. Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.
WAN Interface	This is the WAN interface to which the address mapping rule applies.
Modify	Click the Edit icon to go to the screen where you can edit the address mapping rule. Click the Delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

11.6.2 Add New Rule Screen

To add or edit an address mapping rule, click **Add New Rule** or the **Modify** icon in the **Address Mapping** screen to display the screen shown next.

Figure 131 Network Setting > NAT > Address Mapping > Add New Rule

The screenshot shows the 'Add New Rule' configuration screen. It includes the following fields and options:

- Rule Name:** An empty text input field.
- Type:** A dropdown menu currently showing 'One-to-One'.
- Local Start IP:** An empty IP address input field.
- Local End IP:** A disabled IP address input field with the placeholder '.*.*.*.*'.
- Global Start IP:** An empty IP address input field.
- Global End IP:** A disabled IP address input field with the placeholder '.*.*.*.*'.
- WAN Interface:** A dropdown menu currently showing 'Default'.

At the bottom of the screen, there are two buttons: 'Cancel' and 'OK'.

The following table describes the fields in this screen.

Table 71 Network Setting > NAT > Address Mapping > Add New Rule

LABEL	DESCRIPTION
Rule Name	Type up to 20 alphanumeric characters for the name of this rule.
Type	Choose the IP or port mapping type from one of the following. One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type. Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the device's Single User Account feature that previous routers supported only. Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types.
WAN Interface	Select a WAN interface to which the address mapping rule applies.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

11.7 Sessions

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use. Click **Network Setting > NAT > Sessions** to open the **Sessions** screen.

Figure 132 Network Setting > NAT > Sessions

NAT

Port Forwarding
Port Triggering
DMZ
ALG
Address Mapping
Sessions

The figure below limits the open sessions on a per host (a LAN IP Address) basis. Some applications, especially like P2P file sharing demand a greater number of NAT sessions in order to get a better uploading and downloading rate.

MAX NAT Session Per Host (0 ~ 20480)

2048

Note

(1) Enter session number and click "Apply" to activate this feature.

(2) Clear the session number field and click "Apply" to de-activate this feature.

Cancel
Apply

The following table describes the fields in this screen.

Table 72 Network Setting > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Session Per Host (0 – 20480)	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

11.8 Technical Reference

This part contains more information regarding NAT.

11.8.1 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 73 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.

11.8.2 What NAT Does

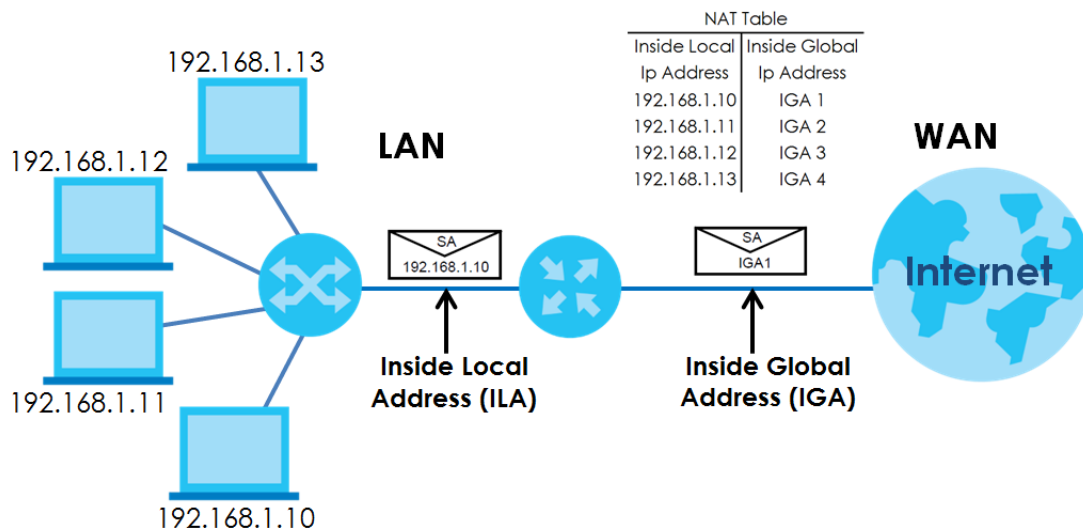
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

11.8.3 How NAT Works

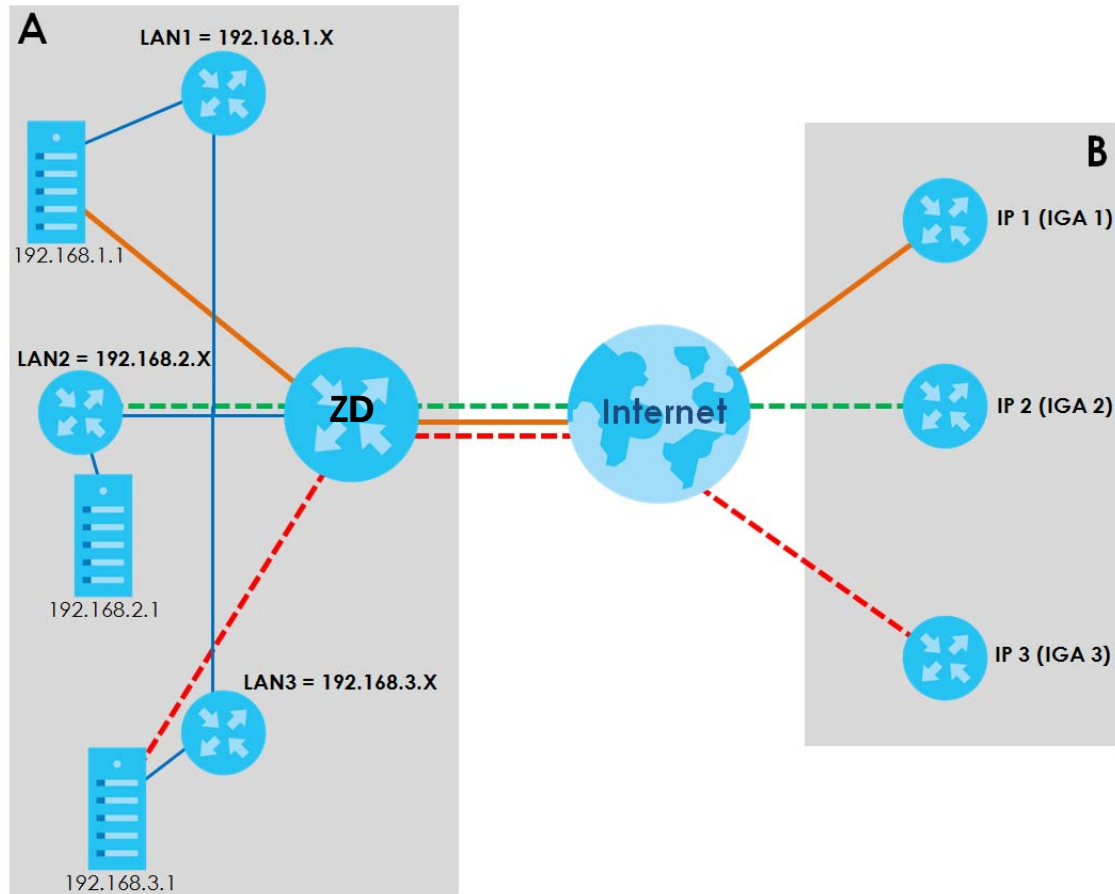
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, 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 133 How NAT Works



11.8.4 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 134 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.

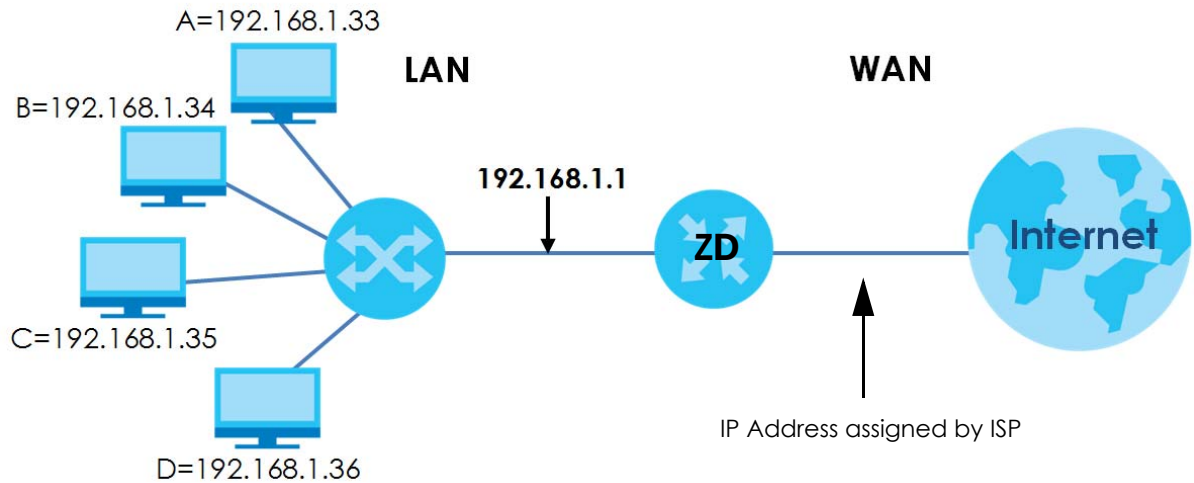
Table 74 Services and Port Numbers

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
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 135 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 159](#).

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 186](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device ([Section 12.3 on page 187](#)).

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 136 Network Setting > DNS > DNS Entry

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

+ Add New DNS Entry

#	HostName	IP Address	Modify
Note The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.			

The following table describes the fields in this screen.

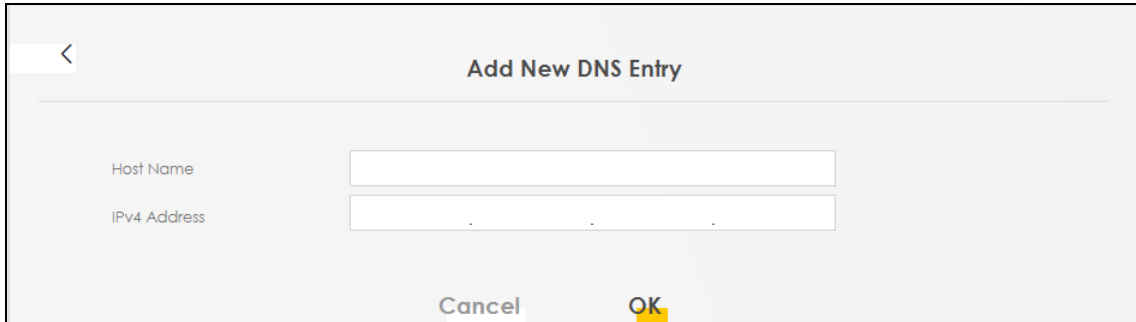
Table 75 Network Setting > DNS > DNS Entry

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 137 DNS Entry: Add or Edit



The following table describes the labels in this screen.

Table 76 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 138 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 77 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

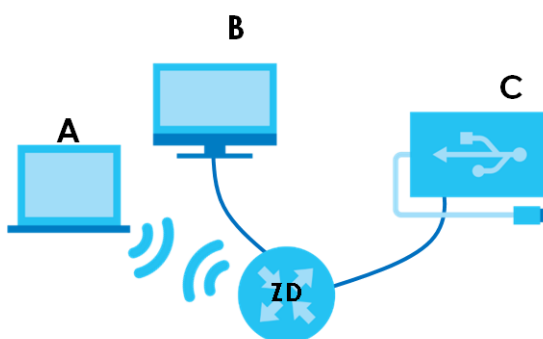
USB Service

13.1 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 139 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 16](#).

13.1.1 What You Need To Know

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

13.1.1.1 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).

13.1.2 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.

13.2 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 140 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.

13.2.1 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 141 Network Setting > USB Service > File Sharing > Add New Share

The screenshot shows the 'Add New Share' interface. It includes a back arrow in the top left corner. The title 'Add New Share' is centered at the top. Below the title, there are four labeled input fields: 'Volume' (a dropdown menu currently showing 'usb2_sda1'), 'Share Path' (a text input field with a yellow 'Browse' button to its right), 'Description' (a text input field), and 'Access Level' (a dropdown menu currently showing 'Public'). At the bottom of the screen, there are two buttons: 'Cancel' on the left and 'OK' on the right.

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.

13.2.2 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 260](#), for detailed information about **User Account** screen.

CHAPTER 14

Firewall

14.1 Overview

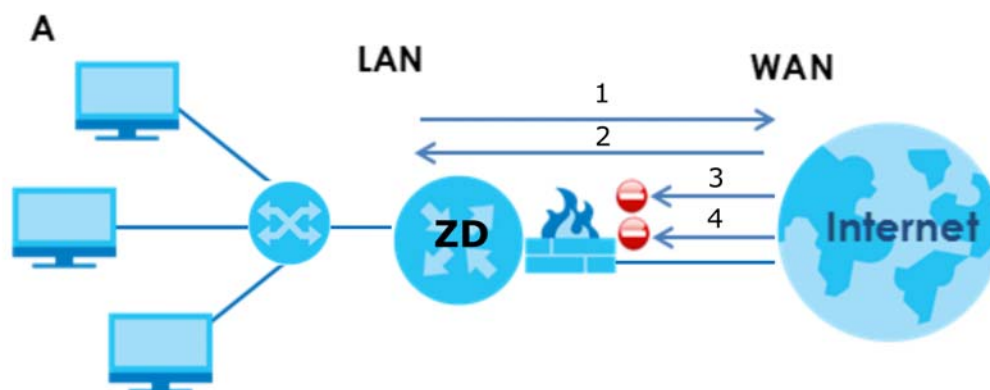
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- 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 142 Default Firewall Action



14.1.1 What You Need to Know About Firewall

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.

14.2 Firewall

14.2.1 What You Can Do in this Chapter

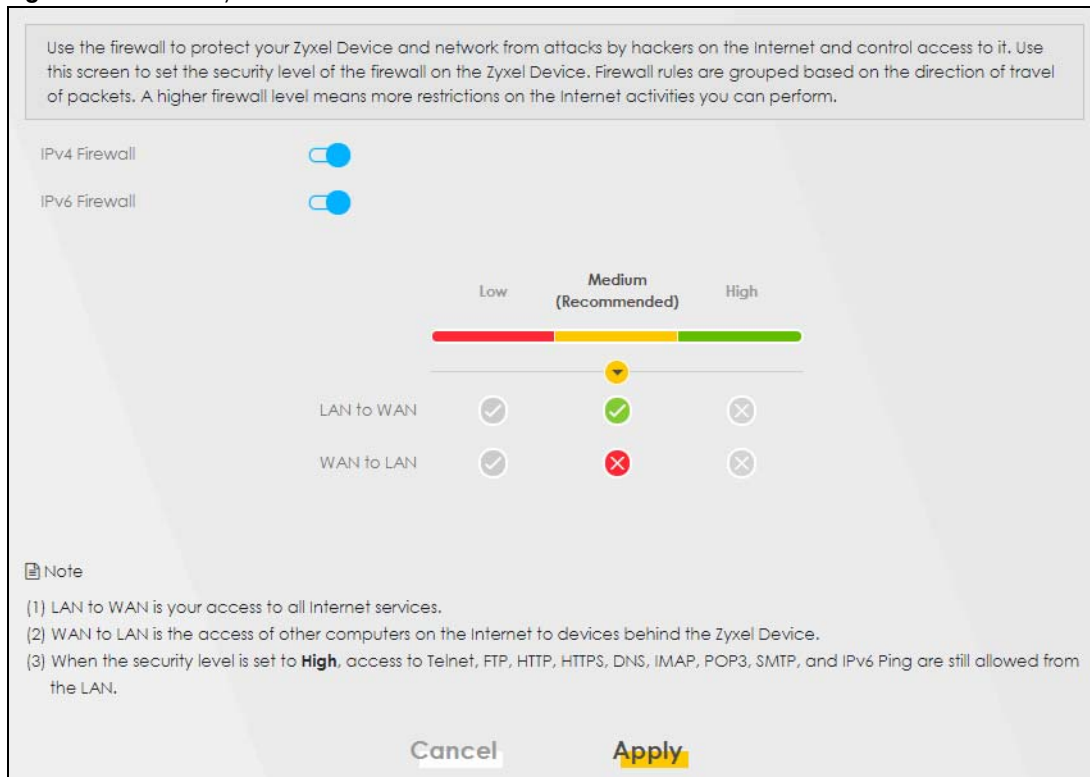
- Use the **General** screen to configure the security level of the firewall on the Zyxel Device ([Section 14.3 on page 195](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 14.4 on page 197](#)).
- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules ([Section 14.5 on page 198](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 14.6 on page 201](#)).

14.3 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 143 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 80 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.

14.4 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 144 Security > Firewall > Protocol

A protocol is a port number rule which defines a service. Services include Email, File sharing, Instant messaging, Online games, Print servers, Voice over IP and so on. Define services in this screen that you want to apply access control rules to in the **Firewall > Access Control** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website.

+ Add New Protocol Entry

Name	Description	Ports/Protocol Number	Modify
Note Removing a protocol rule will also remove associated ACL rules.			

The following table describes the labels in this screen.

Table 81 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.
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.

14.4.1 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 145 Security > Firewall > Protocol: Add New Protocol Entry

The following table describes the labels in this screen.

Table 82 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.

14.5 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 146 Security > Firewall > Access Control

The following table describes the labels in this screen.

Table 83 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.

14.5.1 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 147 Security > Firewall > Access Control > Add New ACL Rule

The following table describes the labels in this screen.

Table 84 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.

Table 84 Security > Firewall > Access Control > Add New ACL Rule (continued)

LABEL	DESCRIPTION
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).
Select Service	Select a service from the Select Service box.
Protocol	Select the protocol (ALL , TCP/UDP , TCP , UDP , ICMP , or ICMPv6) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN).
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 from 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.

14.6 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 148 Security > Firewall > DoS

The following table describes the labels in this screen.

Table 85 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.

14.7 Firewall Technical Reference

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

14.7.1 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.

14.7.2 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.

14.7.3 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 15

MAC Filter

15.1 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.

15.2 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 149 Security > MAC Filter

MAC Filter

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

MAC Address Filter ☒ Enable ☐ Disable (Settings are invalid when disable)

MAC Restrict Mode ☒ Allow ☐ Deny

Add New Rule

Set	Active	Host Name	MAC Address	Delete
-----	--------	-----------	-------------	--------

Note

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

Cancel Apply

The following table describes the labels in this screen.

Table 86 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select Enable to activate the MAC filter function.
MAC Restrict Mode	Select Allow to only permit the listed MAC addresses access to the Zyxel Device. Select Deny to permit anyone access to the Zyxel Device except the listed MAC addresses.
Add New Rule	Click the Add button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of 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.

15.2.1 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 150 Security > MAC Filter > Add New Rule

Set	Active	Host Name	MAC Address	Delete
1	☒	test	BC - 22 - 33 - 11 - 66 - AA	
2	☒	Test	BC - 88 - 99 - 00 - 11 - 24	

The following table describes the labels in this screen.

Table 87 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 16

Parental Control

16.1 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.

16.2 Parental Control Settings

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 151 Security > Parental Control

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](#)

The following table describes the fields in this screen.

Table 88 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.

16.2.1 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 152 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

Custom

▼

Add

-

-

-

-

-

Rule List

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

Internet Access Schedule

Day

Mon

Tue

Wed

Thu

Fri

Sat

Sun

+

Add New Time

Time (Start-End)

00:00

24:00

LTE Series User's Guide

209

Figure 153 Security > Parental Control > Add or Edit PCP (Network Service & Site/URL Keyword)

Network Service

Network Service Setting: Block Selected Service(s): + Add New Service

#	Service Name	Protocol:Port	Modify

Site/URL Keyword

Block or Allow the Web Site: Block the web URLs + Add

#	Website	Modify

☐ Redirect blocked site to Zyxel Family Safety page i

Cancel OK

The following table describes the fields in this screen.

Table 89 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 154 .
#	This shows the index number of the rule.
Service Name	This shows the name of the rule.

Table 89 Security > Parental Control > Add or Edit PCP (continued)

LABEL	DESCRIPTION
Protocol:Port	This shows the protocol and the port of the rule.
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 154 Security > Parental Control > Add or Edit PCP > Add New Service

The following table describes the fields in this screen.

Table 90 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 .

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

LABEL	DESCRIPTION
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.
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 155 Security > Parental Control > Add or Edit PCP > Add Keyword

The following table describes the fields in this screen.

Table 91 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 17

Certificates

17.1 Certificates Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

17.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Zyxel Device's CA-signed (Certification Authority) certificates ([Section 17.3 on page 213](#)).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer ([Section 17.4 on page 217](#)).

17.2 What You Need to Know

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

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Zyxel Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

17.3 Local Certificates

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

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

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

Figure 156 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

Table 92 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.

17.3.1 Create Certificate Request

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

Figure 157 Create Certificate Request

The following table describes the labels in this screen.

Table 93 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.

17.3.2 View Certificate Request

Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

Click the **View** icon in the **Local Certificates** screen to open the following screen.

Figure 158 Certificate Request: View

The screenshot shows a window titled "View Certificate" with a close button in the top right corner. Below the title bar is a section labeled "Certificate Details". This section contains a table with the following information:

Name	Test
Type	none
Subject	/CN=588BF3-VMG8825-B50B-S172V48000015/O=Zyxel/ST=Hsinchu/C=TW

Below the table, there are three text areas with labels on the left:

- Certificate:** A large text area containing a long string of base64-encoded text.
- Private Key:** A text area containing a long string of base64-encoded text.
- Signing Request:** A text area containing a long string of base64-encoded text.

At the bottom of the window, there is a yellow button labeled "Back".

The following table describes the fields in this screen.

Table 94 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).
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.

Table 94 Certificate Request: View (continued)

LABEL	DESCRIPTION
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click Back to return to the previous screen.

17.4 Trusted CA

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

Note: A maximum of four certificates can be added.

Figure 159 Security > Certificates > Trusted CA



The following table describes the labels in this screen.

Table 95 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.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Modify	Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the Remove icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

17.5 Import Trusted CA Certificate

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

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

Figure 160 Security > Certificates > Trusted CA > Import

The following table describes the labels in this screen.

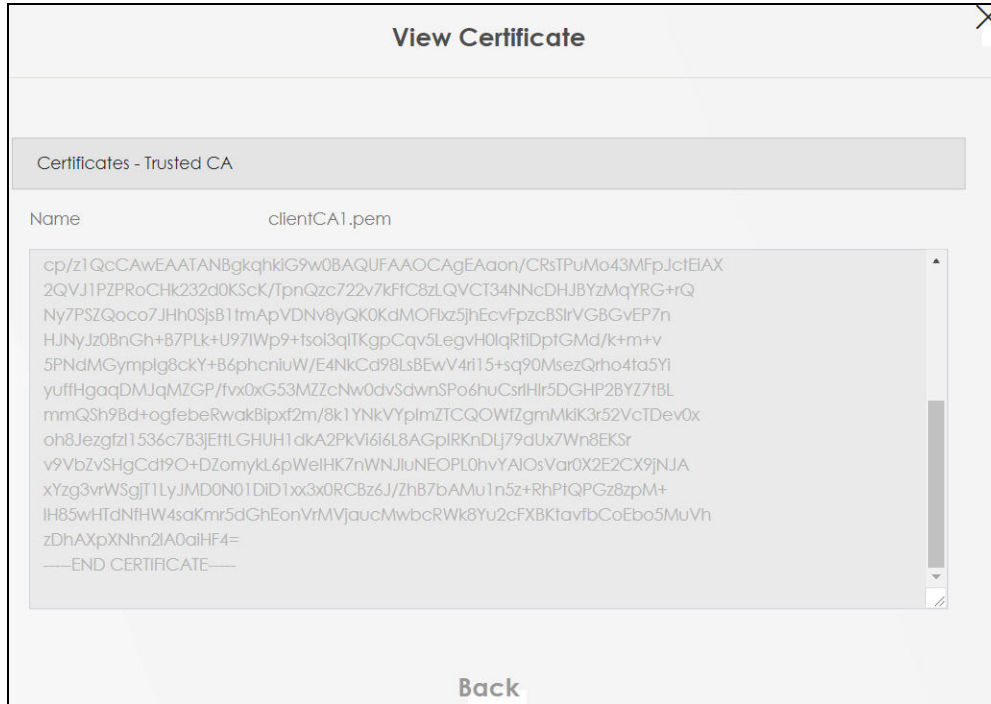
Table 96 Security > Certificates > Trusted CA > Import

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.

17.6 View Trusted CA Certificate

Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 161 Trusted CA: View

The following table describes the labels in this screen.

Table 97 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.

17.7 Certificates Technical Reference

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

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Advantages of Certificates

Certificates offer the following benefits.

- The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Format

The certification authority certificate that you want to import has to be in PEM (Base-64) encoded X.509 file format. This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

17.7.1 Verify a Certificate

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

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

- 1 Browse to where you have the certificate saved on your computer.

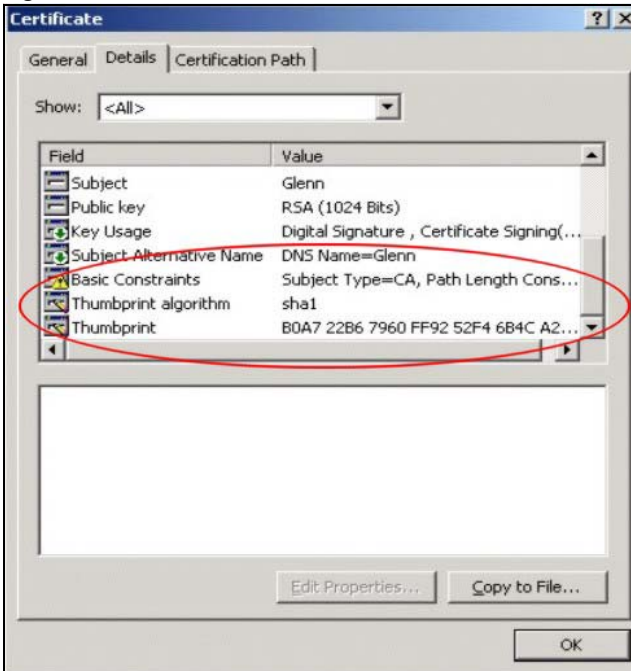
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 162 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 163 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 18

Voice

18.1 Overview

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.

Use this chapter to:

- Connect an analog phone to the Zyxel Device.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

With the voice service, users do not need a SIP account and SIP server to make phone calls over the Internet.

Note: This feature is only available on certain models. For details, see the features comparison table at [Section 1.1 on page 16](#).

18.1.1 What You Can Do in this Chapter

These screens allow you to configure your Zyxel Device to make phone calls over the Internet and your regular phone line, and to set up the phone you connect to the Zyxel Device.

- Use the **Voice Mode** screen to enable VoIP or VoLTE services on the Zyxel Device ([Section 18.2 on page 222](#)).
- Use the **SIP Account** screen to set up information about your SIP account, control which SIP accounts the phones connected to the Zyxel Device use, and configure audio settings such as volume levels for the phones connected to the Zyxel Device ([Section 18.3.1 on page 224](#)).
- Use the **SIP Service Provider** screen to configure the SIP server information, and the numbers for certain phone functions ([Section 18.3.3 on page 227](#)).
- Use the **Phone** screen to change settings that depend on which region of the world the Zyxel Device is in ([Section 18.4 on page 231](#)).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers ([Section 18.6 on page 233](#)).
- Use the **Call History** screen to view a call history list ([Section 18.7 on page 234](#)).

18.2 Voice Mode

Use this screen to enable VoIP or VoLTE services on the Zyxel Device. To access this screen, click **Voice > Voice Mode**.

Figure 164 Voice > Voice Mode

Voice Mode

Please select a voice service on the Zyxel Device.

Voice Service ☒ VoIP service ☐ VoLTE service

Note
If Voice Service is changed, system will reboot.

Cancel **Apply**

The following table describes the labels in this screen.

Table 98 Voice > Voice Mode

LABEL	DESCRIPTION
Configuration	
Voice Service	Select Enable to activate VoIP or VoLTE on the Zyxel Device.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to start configuring this screen again.

18.2.1 What You Need to Know About VoIP

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signaling standard that lets one network device (like a computer or the Zyxel Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your Zyxel Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call. To access this screen, click **Voice > SIP**.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the Zyxel Device to use your SIP account to make calls, the Zyxel Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you do not need a SIP account. It is possible for one SIP device (like the Zyxel Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup – figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

SIP Address

A SIP address is a URI (Uniform Resource Identifier) that resembles an email address, using the format: user@domain. It uniquely identifies a telephone extension over a VoIP system. A SIP address of 123-45-67@voip-provider.net tells a client to connect to voip-provider.net and request a connection to 123-45-67. While VoIP can only send voice messages over the Internet, SIP (though strictly speaking is a type of VoIP) can send voice, data, video, and other media. VoIP phones also need to be connected to a computer to function, whereas SIP phones only need to be connected to a modem.

18.3 Before You Begin

- Before you can use these screens, you need to have a VoIP account already set up. If you do not have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the Zyxel Device.

18.3.1 SIP Account

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

To access this screen, click **Voice > SIP > SIP Account**.

Figure 165 Voice > SIP > SIP Account

#	Enable	SIP Account	Service Provider	Account Number	Modify
1	Disabled	SIP1	ChangeMe	ChangeMe	

The following table describes the labels in this screen.

Table 99 Voice > SIP > SIP Account

LABEL	DESCRIPTION
#	This is the index number of the entry.
Enable	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
Service Provider	This shows the name of the SIP service provider.
Account Number	This shows the SIP number.
Modify	Click the Modify icon to configure the SIP account.

18.3.2 SIP Account Entry Edit

You can configure a SIP account. To access this screen, click the **Modify** icon.

Figure 166 Voice > SIP > SIP Account > SIP Account Entry Edit

SIP Account Entry Edit

SIP Account Selection

SIP Account Selection SIP1

SIP Service Provider Association

SIP Account Associated with ChangeMe

General

☐ Enable SIP Account

SIP Account Number ChangeMe

Authentication

Username ChangeMe

Password *****

URL Type

URL Type SIP

Voice Features

Primary Compression Type G.711u

Secondary Compression Type G.729

Third Compression Type G.711a

Speaking Volume Control Middle

Listening Volume Control Middle

☒ Enable G.168 (Echo Cancellation)

☐ Enable VAD (Voice Active Detector)

Call Features

☒ Send Caller ID

☒ Enable Call Waiting

Call Waiting Reject Timer 20 (10~60) Second

☐ Enable Do Not Disturb (DND)

Warning:

If you enable this item, you will not get indication when somebody call you.

☐ Active Incoming Anonymous Call Block

Cancel OK

The following table describes the labels in this screen.

Table 100 Voice > SIP > SIP Account > SIP Account Entry Edit

LABEL	DESCRIPTION
SIP Service Provider Association	
SIP Service Provider Associated with	Select the check box to use this account. Clear it to not use this account.

Table 100 Voice > SIP > SIP Account > SIP Account Entry Edit (continued)

LABEL	DESCRIPTION
General	
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the Zyxel Device sends the SIP number. SIP – include the SIP service domain name. TEL – do not include the SIP service domain name.
Voice Features	
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder or decoder (codec) that you want the Zyxel Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • G.729 provides good sound quality and reduces the required bandwidth to 8 kbps. • G.711a is typically used in Europe. • G.711u is typically used in North America and Japan. • G.726-32 operates at 16, 24, 32 or 40 kbps. • G.722 operates at 6.3 kbps or 5.3 kbps. When two SIP devices start a SIP session, they must agree on a codec. Select the Zyxel Device's first choice for voice coder or decoder. Select the Zyxel Device's second choice for voice coder or decoder. Select None if you only want the Zyxel Device to accept the first choice. Select the Zyxel Device's third choice for voice coder or decoder. Select None if you only want the Zyxel Device to accept the first or second choice.
Speaking Volume Control	Select the loudness that the Zyxel Device uses for speech that it sends to the peer device. Choices are Minimum, Middle, and Maximum.
Listening Volume Control	Select the loudness that the Zyxel Device uses for speech that it receives from the peer device. Choices are Minimum, Middle, and Maximum.
Enable G. 168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Enable VAD (Voice Active Detector)	Select this if the Zyxel Device should stop transmitting when you are not speaking. This reduces the bandwidth the Zyxel Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

18.3.3 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. To access this screen, click **Voice > SIP > SIP Service Provider**.

Figure 167 Voice > SIP > SIP Service Provider

#	SIP Service Provider Name	SIP Proxy Server Address	REGISTER Server Address	SIP Service Domain	Modify
1	ChangeMe	ChangeMe	ChangeMe	ChangeMe	

The following table describes the labels in this screen.

Table 101 Voice> SIP > SIP Service Provider

LABEL	DESCRIPTION
#	This is the index number of the entry.
SIP Service Provider Name	This shows the name of the SIP service provider.
SIP Proxy Server Address	This shows the IP address or domain name of the SIP server.
Register Server Address	This shows the IP address or domain name of the SIP register server.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @symbol. You can use up to 127 printable ASCII Extended set characters.
Modify	Click the Modify icon to configure the profile of SIP service provider settings.

18.3.4 Provider Entry Edit

Use this screen to configure the SIP server information, the numbers for certain phone functions and dialing plan for a SIP service provider. Click **Voice > SIP > SIP Service Provider** and then click the **Modify** icon next to a profile of SIP service provider settings to open the following screen.

Figure 168 Voice > SIP > SIP Service Provider: Edit

Provider Entry Edit

SIP Service Provider Selection
Service Provider Selection: ChangeMe

General
☒ Enable SIP Service Provider
 SIP Service Provider Name: ChangeMe
 SIP Local Port: 5040 (1025-65535)
 SIP Proxy Server Address: ChangeMe
 SIP Proxy Server Port: 5040 (1025-65535)
 SIP REGISTRAR Server Address: ChangeMe
 SIP REGISTRAR Server Port: 5040 (1025-65535)
 SIP Service Domain: ChangeMe

RFC Support
☐ PRACK (RFC 3262, Requires 100rel)

VoIP IOP Flags
☒ Replace dial digit '8' to '%23' in SIP messages
☐ Remove the 'Route' header in SIP messages

Bound Interface Name
 Bound Interface Name: ☒ AnyWAN ☐ MultiWAN

Outbound Proxy
 Outbound Proxy Address:
 Outbound Proxy Port: 5040 (1025-65535)
☐ Use DHCP Option 120 List

RTP Port Range
 Start Port: 40000 (1024-65535)
 End Port: 40010 (1044-65500)

DTMF Mode
 DTMF Mode: RFC 2833

Transport Type
 Transport Type: UDP

Ignore Direct IP
☒ Enable ☐ Disable

FAX Option
☒ G.711 Fax Passthrough ☐ T.38 Fax Relay

QoS Tag
 SIP DSCP Mark Setting: 46 (0-43)
 RTP DSCP Mark Setting: 46 (0-43)

Timer Setting
 SIP Register Expiration Duration: 3600 (60-65535) second
 SIP Register Fail Re-try Timer: 1800 (100-65535) second
 Session Expires (SE): 900 (100-3600) second
 Min-SE: 600 (90-1800) second

Dialing Interval Selection
 Dialing Interval Selection: 3 second

DNS SRV
☐ Enable DNS SRV

Cancel OK

The following table describes the labels in this screen.

Table 102 Voice > SIP > SIP Service Provider > Edit

LABEL	DESCRIPTION
General	
SIP Service Provider	Select this if you want the Zyxel Device to use this SIP provider. Clear it if you do not want the Zyxel Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the Zyxel Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Proxy Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.

Table 102 Voice > SIP > SIP Service Provider > Edit (continued)

LABEL	DESCRIPTION
SIP Proxy Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP REGISTAR Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 95 printable ASCII characters.
SIP REGISTAR Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RFC Support	
PRACK (RFC 3262)	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select Supported or Required to have the Zyxel Device include a SIP Require or Supported header field with the option tag 100rel in all INVITE requests. When the Zyxel Device receives a SIP response message indicating that the phone it called is ringing, the Zyxel Device sends a PRACK message to have both sides confirm the message is received. If you select Supported, the peer device supports the option tag 100rel to send provisional responses reliably. If you select Required, the peer device requires the option tag 100rel to send provisional responses reliably. Select Disabled to turn off this function.
VoIP IOP Flags – Select VoIP inter-operability settings.	
	Replace dial digit '#' to '%23' in SIP messages.
	Remove ':5060' and 'transport=udp' from request-uri in SIP messages.
	Remove the 'Route' header in SIP messages.
	Do not send re-Invite to the remote party when there are multiple codecs answered in the Session Description Protocol (SDP).
	Remove the 'Authentication' header in SIP ACK messages.
Bound Interface Name	
Bound Interface Name	If you select AnyWAN, the Zyxel Device automatically activates the VoIP service when any WAN connection is up. If you select MultiWAN, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Zyxel Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Zyxel Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server.
Outbound Proxy Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
Use DHCP Option 120 first	Select this to have the Zyxel Device use DHCP Option 120 first.

Table 102 Voice > SIP > SIP Service Provider > Edit (continued)

LABEL	DESCRIPTION
RTP Port Range	
Start Port End Port	Enter the listening port numbers for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the Start Port and End Port fields. To enter a range of ports, - enter the port number at the beginning of the range in the Start Port field. - enter the port number at the end of the range in the End Port field.
DTMF Mode	Control how the Zyxel Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. RFC2833 – send the DTMF tones in RTP packets. Inband – send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.726) can distort the tones. SIP Info – send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol UDP or TCP (usually UDP) used for SIP.
Ignore Direct IP	Select Enable to have the connected devices accept SIP requests only from the SIP proxy/register server specified above. SIP requests sent from other IP addresses will be ignored.
FAX Option	This field controls how the Zyxel Device handles fax messages.
QoS Tag	
SIP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
SIP Register Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Zyxel Device automatically tries to re-register your SIP account when one-half of this time has passed (The SIP register server might have a different expiration).
SIP Register Fall Re-try timer	Enter the number of seconds the Zyxel Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires [SE]	Enter the number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Zyxel Device accepts.
Dialing interval selection	
Dialing interval selection	Enter the number of seconds the Zyxel Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
Enable DNS SRV	Select this to have the Zyxel Device query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls.

Table 102 Voice > SIP > SIP Service Provider > Edit (continued)

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

18.4 Phone

Use these screen to configure SIP numbers and regions for IP phones that are connected to the Zyxel Device.

18.4.1 Phone Device

Use this screen to view detailed information on phones used for Internet phone calls (SIP). You can define which phones 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.

To access this screen, click **Voice > Phone > Phone Device**.

Figure 169 Voice > Phone > Phone Device

Phone Device configuration defines the relations between your SIP account(s) and phone(s). That is, which phone(s) will ring when a specific SIP account number receive an incoming call; and which SIP account number will be used when a specific phone is used to make an outgoing call.				
Analog Phone				
#	Phone ID	Incoming SIP Number	Outgoing SIP Number	Modify
1	PHONE1	ChangeMe	ChangeMe	

Each field is described in the following table.

Table 103 Voice > Phone > Phone Device

LABEL	DESCRIPTION
#	This displays the index number of the phone device.
Phone ID	This field displays the name of a phone port on the Zyxel Device.
Incoming SIP Number	This field displays the SIP address that you use to receive calls on this phone port.
Outgoing SIP Number	This field displays the SIP address that you use to make calls on this phone port.
Modify	Click the Edit icon to configure the SIP account.

18.4.2 Phone Device Edit

Use this screen to control which SIP account and PSTN line each phone uses. Click an **Edit** icon in **Voice > Phone > Phone Device** to open the following screen.

Figure 170 Voice > Phone > Phone Device > Edit

Phone Device Edit

SIP Account to Make Outgoing Call

SIP Account	SIP Number
☒ SIP1	ChangeMe
☐ SIP2	ChangeMe

SIP Account(s) to Receive Incoming Call

SIP Account	directoryNumber
☒ SIP1	ChangeMe
☐ SIP2	ChangeMe

Immediate Dial Enable

☒ Immediate Dial Enable

Cancel OK

Each field is described in the following table.

Table 104 Voice > Phone > Phone Device > Edit

LABEL	DESCRIPTION
SIP Account to Make Outgoing Call	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Account(s) to Receive Incoming Call	Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port. If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
Immediate Dial Enable	Select this if you want to use the pound key (#) to tell the Zyxel Device to make the phone call immediately, instead of waiting for the number of second you selected in the Dialog Interval Selection field of the VoIP > SIP > SIP Service Provider > Add New Provider or Edit screen. If you select this, dial the phone number, and then press the pound key. The Zyxel Device makes the call immediately instead of waiting. You can still wait, if you want.
Cancel	Click Cancel to exit this screen without saving
OK	Click OK to save your changes.

18.5 Phone Region

Use this screen to configure settings that depend on which region of the world the Zyxel Device is in. Selecting the region where the device is physically located improves the quality of phone calls. To access this screen, click **Voice > Phone**.

Figure 171 Voice > Phone

The following table describes the labels in this screen.

Table 105 Voice > Phone

LABEL	DESCRIPTION
Region Setting	Select the place in which the Zyxel Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. • Europe Type – use supplementary phone services in European mode. • USA Type – use supplementary phone services American mode. You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the Zyxel Device.
Cancel	Click this to set every field in this screen to its last-saved value.

Note: You need to reboot the device after changing the region settings for it to take effect.

18.6 Call Rule

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number. To access this screen, click **Voice > Call Rule**.

Figure 172 Voice > Call Rule

Call Rule

When certain phone numbers are dialed on a regular basis, Speed Dial accelerates dialing process. The following rules apply to all the phone devices connected to this device.

[Clear All Speed Dials](#)

Keys	Number	Description
#01		
#02		
#03		
#04		
#05		
#06		
#07		
#08		
#09		
#10		

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

The following table describes the labels in this screen.

Table 106 Voice > Call Rule

LABEL	DESCRIPTION
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the Zyxel Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Clear All Speed Dials	Click this button to remove all speed dials saved.
Apply	Click this to save your changes and to apply them to the Zyxel Device.
Cancel	Click this to set every field in this screen to its last-saved value.

18.7 Call History

The Zyxel Device logs calls from or to your SIP addresses. This screen allows you to view a summary of received, dialed and missed calls and a call history list. You can also view detailed information on each outgoing and incoming call.

To access this screen, click **Voice > Call History**.

Figure 173 Voice > Call History

Call History

The Zyxel Device logs calls from or to your SIP addresses. This screen allows you to view the summary of received, dialed and missed calls and a call history list. You can also see detailed information for each outgoing call you made or each incoming call from someone calling you. The Zyxel Device stores up to 300 incoming call logs and 300 outgoing call logs. If the number of entries exceed the maximum value, the earliest log of that type will be deleted.

[Clear](#) [Refresh](#)

Summary

Date	Total Calls	Outgoing Calls	Incoming Calls	Missing Calls	Total Duration(hh:mm:ss)
>					

Classify All

📞 Incoming
📞 Outgoing
📞 Missed

Type	Date/Time	Peer Number	Phone Number	Duration (hh:mm:ss)	Delete
>					

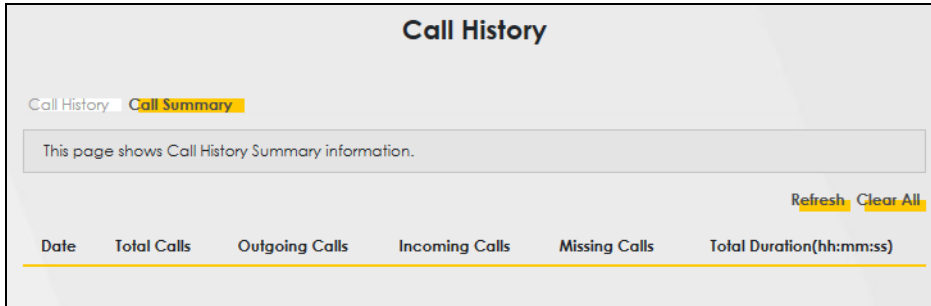
Each field is described in the following table.

Table 107 Voice> Call History

LABEL	DESCRIPTION
Clear	Click this button to remove all entries from the call history list.
Refresh	Click this button to renew the call history list.
Summary	
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP addresses that day.
Incoming Calls	This displays how many calls you received that day.
Outgoing Calls	This displays how many calls originated from you that day.
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration (hh:mm:ss)	This displays how long all calls lasted that day.
Classify	Select the type of the calls. The call types are: All , Incoming , Outgoing and Missed .
Type	This displays the type of the calls.
Date/Time	This displays the date and time when the calls were made.
Peer Number	This displays the SIP address that called you or you called.
Phone Number	This displays the phone number of the call.
Duration (hh:mm:ss)	This displays how long the call lasted.
Modify	Click the Delete icon to remove the call history.

18.7.1 Call Summary

The Zyxel Device logs calls to or from your SIP addresses. This screen allows you to view the summary of received, dialed and missed calls. To access this screen, click **Voice > Call History > Call Summary**.

Figure 174 Voice > Call History > Call Summary

The following table describes the labels in this screen.

Table 108 Voice > Call History > Call Summary

LABEL	DESCRIPTION
Refresh	Click this button to renew the call history list.
Clear All	Click this button to remove all entries from the call history list.
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP numbers that day.
Outgoing Calls	This displays how many calls originated from you that day.
Incoming Calls	This displays how many calls you received that day.
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration	This displays how long all calls lasted that day.

CHAPTER 19

Log

19.1 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.

19.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 19.2 on page 238](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 19.3 on page 238](#)).

19.1.2 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 109 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 109 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.

19.2 System Log

Use the **System Log** screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor > Log** to open the **System Log** screen.

Figure 175 System Monitor > Log > System Log

Export or email the system logs. You can filter the entries by clicking the **Level** and/or **Category** drop-down list boxes.

Level: Category:

[Clear Log](#) [Refresh](#) [Export Log](#) [E-mail Log Now](#)

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the fields in this screen.

Table 110 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.

19.3 Security Log

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

Figure 176 System Monitor > Log > Security Log

View the security-related logs for the categories that you select. You can filter the entries by clicking the **Level** and/or **Category** drop-down list boxes.

Level: Category:

[Clear Log](#) [Refresh](#) [Export Log](#) [E-mail Log Now](#)

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the fields in this screen.

Table 111 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 20

Traffic Status

20.1 Traffic Status Overview

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

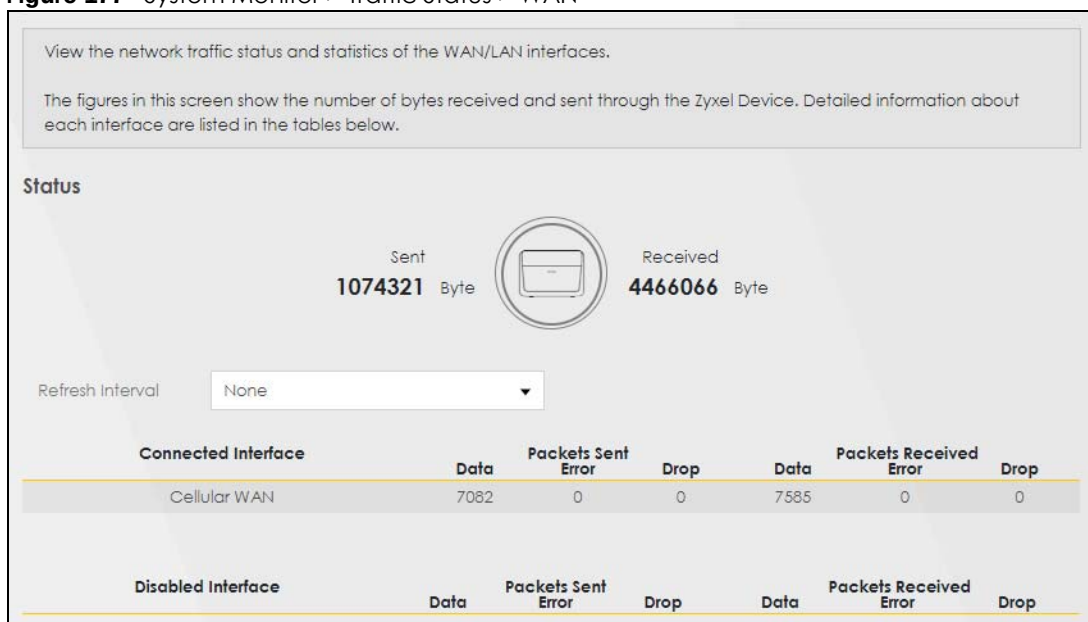
20.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 20.2 on page 240](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 20.3 on page 241](#)).

20.2 WAN Status

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

Figure 177 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 112 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.

20.3 LAN Status

Click **System Monitor > Traffic Status > LAN** to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.

Figure 178 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 113 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 21

VoIP Status

21.1 VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the Voice over IP (VoIP) registration, current call status and phone numbers in this screen.

Figure 179 System Monitor > VoIP Status

Information, such as whether a SIP account is registered and the total call volume made by a SIP account, can be viewed in the page.

Poll Interval sec
(s) Set Interval Stop

SIP Status

Account	Register Action	Registration	Registration Time	URI	Message Waiting	Last Incoming Number	Last Outgoing Number
1	☐	Disabled		ChangeMe@ChangeMe	No		

Call Status

Account	Duration	Status	Call Type	Codec	From Phone Port Type	To Phone Port Type	Peer Number
---------	----------	--------	-----------	-------	----------------------	--------------------	-------------

Phone Status

Phone	Outgoing Number	Incoming Number	Hook Status
Phone 1	ChangeMe	ChangeMe	On-hook

The following table describes the labels in this screen.

Table 114 System Monitor > VoIP Status

LABEL	DESCRIPTION
Poll Interval	Enter the number of seconds the Device needs to wait before updating this screen and then click Set Interval. Click Stop to have the Device stop updating this screen.
SIP Status	
Account	This column displays each SIP account in the Device.
Register Action	Click on this switch to register/unregister the SIP account. This switch will turn blue if a registration attempt is successful; otherwise, it will revert to its unregistered setting. Unregistering an account does not delete the SIP account itself, but removes the mapping between your SIP identity and your IP address or domain name,

Table 114 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. You can change this in the Status screen. Registered – The SIP account is registered with a SIP server. Not Registered – The last time the Device tried to register the SIP account with the SIP server, the attempt failed. The Device automatically tries to register the SIP account when you turn on the Device or when you activate it. Inactive – The SIP account is not active. You can activate it in VoIP > SIP > SIP Account .
Registration Time	This field displays the last time the Device successfully registered the SIP account. The field is blank if the Device has never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screen.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. Idle – There are no current VoIP calls, incoming calls or outgoing calls being made. Dial – The callee's phone is ringing. Ring – The phone is ringing for an incoming VoIP call. Process – There is a VoIP call in progress. DISC – The callee's line is busy, the callee hung up or your phone was left off the hook.
Call Type	This field displays the call direction type of the current VoIP call. Outgoing Call – It is a SIP VoIP call made by local phone ports, and this SIP account is able to issue a (SIP-based) call setup to the SIP account of remote peers for a VoIP call establishment. This (SIP-based) call setup signal is sent to the SIP server first, and then the SIP server would relay it to the target peer after correctly resolving and locating the target peer. During the call setup (signaling) phase, Calling state is displayed in the Status field, and it turns to InCall state once the call is successfully established. Incoming Call – It is a SIP VoIP call made or originated by remote SIP accounts to connect to this local SIP account. One or more local phone ports can be configured to receive this type of call, see the Incoming Number below, and all of them should begin to ring during the call setup (signaling phase), see the Status above. Once some remote SIP accounts start to ring one local phone, answer by off-hook to the call, and the call is successfully established. The other ringing local phone ports will stop ringing and turning to InCall state in the Status field. Internal Call – It is a local VoIP call between two different local phone ports. No SIP signaling is needed and thus no SIP server is involved to establish this type of call. This type of call is established through the Internal and Non-SIP local setup signaling procedure between the call- originating and call-terminating local phone ports. In general, one or more local phone ports can be designed to receive this type of call, and once any of the ringing phones answer the call, the other ringing ones will stop ringing. During the call setup phase (signaling phase), Calling state is displayed in Status field, and turns to InCall state once the call is successfully established.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.

Table 114 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
From Phone Port Type	This field displays the phone ports type used to originate, start, or create the current VoIP call. Two possible type values will be displayed here: SIP – For the current call which is categorized as Incoming Call in the Call Type field, this field will show the type SIP. FXS – As for the other cases: Outgoing Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device.
To Phone Port Type	This field displays the phone ports type used to receive the current VoIP call. Three possible type values will be displayed here: SIP – For the current call which is categorized as Outgoing Call in the Call Type field, this field will show the type SIP. FXS and Unknown – As for the other cases: Incoming Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device. While the call is established, this field shows Unknown during the call setup phase (signaling phase). This is because one or more local phone ports can be configured or designed to receive these two types of calls, see the Call Type above, and the local phone port will answer the call that hasn't been determined yet at that time.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays the name of a phone port on the Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Hook Status	This field displays whether the phone is in the on or off hook status. Off-Hook means a telephone connected to one of the phone port has its receiver off the hook. On-Hook means a telephone connected to one of the phone port has its receiver on the hook.

CHAPTER 22

ARP Table

22.1 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.

22.1.1 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.

22.2 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 180 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	192.168.1.129	dc:4a:3e:40:ec:5f	br0
2	192.168.1.93	74:f6:1c:0d:f1:69	br0
IPv6 Neighbour Table			
#	IPv6 Address	MAC Address	Device
1	fe80::ecad:ab45:c530:cc3f	dc:4a:3e:40:ec:5f	br0
2	fe80::2d8d:742c:122d:59ae	74:f6:1c:0d:f1:69	br0

The following table describes the labels in this screen.

Table 115 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 23

Routing Table

23.1 Routing Table Overview

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

23.2 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 181 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 destination can be a network or host. 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. Flags can be U - up, I - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), or M - modified (redirect). Metric is the distance to the target (usually counted in hops). Interface is how the packets for this route will be sent.					
IPv4 Routing Table					
Destination	Gateway	Subnet Mask	Flag	Metric	Interface
0.0.0.0	10.60.62.158	0.0.0.0	UG	0	wwan0
10.60.62.156	0.0.0.0	255.255.255.252	U	0	wwan0
127.0.0.0	0.0.0.0	255.255.0.0	U	0	lo
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	br0
IPv6 Routing Table					
Destination	Gateway	Flag	Metric	Interface	
fe80::/64	::	U	256	eth2	
fe80::/64	::	U	256	br0	
fe80::/64	::	U	256	ra0	
fe80::/64	::	U	256	wwan0	
::1/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::3065:f9ff:fe8c:186/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b903/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b903/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b904/128	::	U	0	lo	
ff02::1/128	::	UC	0	br0	
ff00::/8	::	U	256	eth2	
ff00::/8	::	U	256	br0	
ff00::/8	::	U	256	ra0	
ff00::/8	::	U	256	wwan0	

The following table describes the labels in this screen.

Table 116 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 116 System Monitor > Routing Table (continued)

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

CHAPTER 24

WLAN Station Status

24.1 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 182 System Monitor > WLAN Station Status

The screenshot shows the 'WLAN Station Status' interface. At the top, it says 'WLAN Station Status lists associated WiFi clients.' Below this, there are two sections: 'WLAN 2.4G Station Status' and 'WLAN 5G Station Status'. Each section has a table with the following columns: '#', 'MAC Address', 'Rate (Mbps)', 'RSSI (dBm)', 'SNR', and 'Level'.

The following table describes the labels in this screen.

Table 117 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen. Select None to stop refreshing.
#	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 117 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The greater the number, the better the quality of WiFi. The normal range is 15 to 40. If the value drops below 15, try moving the associated wireless station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated wireless station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. 5 means the Zyxel Device is receiving an excellent WiFi signal. 4 means the Zyxel Device is receiving a very good WiFi signal. 3 means the Zyxel Device is receiving a weak WiFi signal, 2 means the Zyxel Device is receiving a very weak WiFi signal. 1 means the Zyxel Device is not receiving a WiFi signal.

CHAPTER 25

Cellular WAN Status

25.1 Cellular WAN Status Overview

View the cellular connection details and signal strength value that you can use as reference for positioning the Zyxel Device, as well as SIM card and module information.

25.2 Cellular WAN Status

To open this screen, click **System Monitor > Cellular WAN Status**. Cellular information is available on this screen only when you insert a valid SIM card in the Zyxel Device.

Figure 183 System Monitor > Cellular WAN Status

Cellular WAN Status

View the LTE connection details and signal strength value that you can use as reference for positioning the Zyxel Device, as well as SIM card and module information.

Cellular information is available on this screen only when you insert a valid SIM card in the Zyxel Device.

Refresh Interval None

Module Information

IMEI	869257030005652
Module SW Version	EG06ALAR02A07M4G

SIM Status

SIM Card Status	Available
IMSI	001780000000148
ICCID	8912317800000001486F
PIN Protection	Disable
PIN Remaining Attempts	3

IP Passthrough Status

IP Passthrough Enable	Disable
-----------------------	---------

Cellular Status

Cellular Status	Up
Data Roaming	Disable
Operator	4G 8148
PLMN	178

Figure 184 System Monitor > Cellular WAN Status (Service Information)

Refresh Interval	178
Service Information	
Access Technology	LTE
Band	LTE_BC7
RSSI	-57
Cell ID	19088910
Physical Cell ID	103
UL Bandwidth (MHz)	10
DL Bandwidth (MHz)	10
RFCN	3400
RSRP	-80
RSRQ	-6
RSCP	N/A
EcNo	N/A
TAC	12849
LAC	N/A
RAC	N/A
BSIC	N/A
SINR	25
CQI	15
MCS	1
RI	2
PMI	0
Neighbour Cells	
# 1	
Neighbour Type	Intra-Frequency
Connection Mode	LTE
Physical Cell ID	103
RFCN	3400
RSSI	-56
RSRP	-79

The following table describes the labels in this screen.

Table 118 System Monitor > Cellular WAN Status

LABEL	DESCRIPTION
Refresh Interval	Select the time interval the Zyxel Device will check and refresh the fields shown on this screen. Select None to stop detection.
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Module SW Version	This shows the software version of the cellular module.
SIM Status	

Table 118 System Monitor > Cellular WAN Status (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 doesn't have PIN code security. Locked – the SIM card has PIN code security, but you did not enter the PIN code yet. Blocked – you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card. Error - the Zyxel Device detected that the SIM card has errors.
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (ICCID). This is the serial number of the SIM card.
PIN Protection	A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. Shows Enable if the service provider requires you to enter a PIN to use the SIM card. Shows Disable if the service provider lets you use the SIM without inputting a PIN.
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
IP Passthrough Enable	This displays if IP Passthrough is enabled on the Zyxel Device. IP Passthrough allows a LAN computer on the local network of the Zyxel Device to have access to web services using the public IP address. When IP Passthrough is configured, all traffic is forwarded to the first LAN computer on the local network and will not go through NAT.
IP Passthrough Mode	This displays the IP Passthrough mode. This displays Dynamic and the Zyxel Device will allow traffic to be forwarded to the first LAN computer requesting an IP address from the Zyxel Device. This displays Fixed and the Zyxel Device will allow traffic to be forwarded to a specific LAN computer on the local network of the Zyxel Device.
Cellular Status	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 number.
Service Information	
Access Technology	This displays the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.
Band	This displays the current cellular band of your Zyxel Device (WCDMA2100).
RSSI	This displays the strength of the WiFi signal between an associated wireless station and an AP. 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 118 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
Cell ID	This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting. The value depends on the Current Access Technology: - For GPRS, it is the Cell Identity as specified in 3GPP-TS.25.331. - For UMTS, it is the Cell Identity as defined in SIB3 3GPP-TS.25.331, 3GPP-TS.24.008. - For LTE, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331. The value is '0' (zero) or 'N/A' if there is no network connection.
Physical Cell ID	This shows the Physical Cell ID (PCI), which are queries and replies between the Zyxel Device and the mobile network it is connecting to. The normal range is 1 to 504.
UL Bandwidth (MHz)	This shows the cellular channel bandwidth from the Zyxel Device to the base station. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
DL Bandwidth (MHz)	This shows the cellular channel bandwidth from the base station to the Zyxel Device. According to 3GPP specifications, the bandwidths defined by the standard are 1.4, 3, 5, 10, 15, and 20 MHz. The wider the bandwidth the higher the throughput.
RFCN	This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting. The value depends on the Current Access Technology: - For GPRS, it is the ARFCN (Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.45.005. - For UMTS, it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. - For LTE, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. The value is '0' (zero) or 'N/A' if there is no network connection.
RSRP	This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth. The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133. An undetectable signal is indicated by the lower limit, example -140 dBm. This parameter is for LTE only. The normal range is -30 to -140. The value is -140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSRQ	This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal. The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example -240. This parameter is for LTE only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.
RSCP	This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device. The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example -120 dBm. This parameter is for UMTS only. The normal range is -30 to -120. The value is -120 if the Current Access Technology is not UMTS. The value is 'N/A' if there is no network connection.

Table 118 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
EcNo	This displays the ratio (in dB) of the received energy per chip and the interference level. The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example -240 dB. This parameter is for UMTS only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not UMTS or there is no network connection.
TAC	This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber. The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101. This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.
LAC	This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN. The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
RAC	This displays the RAC (Routing Area Code), which is used in mobile network "packet domain service" (PS) to identify a routing area within a location area. In a mobile network, it uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and use RAC to identify the location of data service like HSDPA or LTE. The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003]. This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.
BSIC	The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station. This parameter is for GPRS only. The value is '0' (zero) if the Current Access Technology is not GPRS. The value is 'N/A' if there is no network connection.
SINR	This displays the Signal to Interference plus Noise Ratio (SINR) in dB. This is also a measure of signal quality and used by the UE (User Equipment) to calculate the Channel Quality Indicator (CQI) that it reports to the network. A negative value means more noise than signal.
CQI	This displays the Channel Quality Indicator (CQI). It is an indicator carrying the information on how good/bad the communication channel quality is.
MCS	MCS stands for modulation coding scheme. The base station selects MCS based on current radio conditions. The higher the MCS the more bits can be transmitted per time unit.
RI	This displays the Rank Indication, one of the control information that a UE will report to eNodeB (Evolved Node-B) on either PUCCH (Physical Uplink Control Channel) or PUSCH (Physical Uplink Shared Channel) based on uplink scheduling.
PMI	This displays the Precoding Matrix Indicator (PMI). PMI is for transmission modes 4 (closed loop spatial multiplexing), 5 (multi-user MIMO), and 6 (closed loop spatial multiplexing using a single layer). PMI determines how cellular data are encoded for the antennas to improve the downlink rate.

Table 118 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
Neighbour Cells	This displays the type of the neighbor cell's carrier frequency detected by the Zyxel Device. Intra-Frequency – when the current cell and target cell operate on the same carrier frequency. Inter-Frequency – when the current cell and target cell operate on different carrier frequencies.
#	This is the index number of the entry.
Connection Mode	This displays the connection mode of the detected neighbor cell. The default value is LTE .
PhyCellID	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 0 to 503.
RFCN	This displays the Radio Frequency Channel Number (RFCN) of the detected base station. This is the carrier frequency designated by EARFCN. The range is 0 – 65535.
RSSI	This displays the Received Signal Strength Indicator (RSSI) level of the detected base station. RSSI is an indicator of the signal strength, including signals and noises received by the target cell. The normal range is –30dBm to –79dBm.
RSRP	This displays the Reference Symbol Received Power (RSRP) level of the detected base station. RSRP is the average signal strength of the target station and is usually measured during a handover. The normal range is –140dBm to –44dBm.
RSRQ	This displays the Reference Signal Received Quality (RSRQ) level of the detected base station. RSRQ is the indicator of the signal quality of data transmission. The normal range is –24.0dB to 0dB. RSRQ is defined as $RSRP/RSSI \times N$. N is the number of resource blocks. A resource block is the smallest unit of radio resources allocated to a user and contains twelve sub-carriers in frequency and 0.5 ms in time.

CHAPTER 26

System

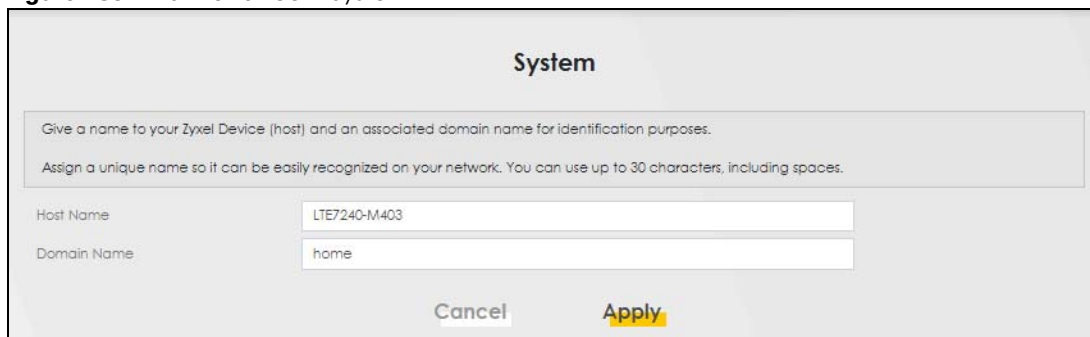
26.1 System Overview

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

26.2 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 185 Maintenance > System



The following table describes the labels in this screen.

Table 119 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.
Cancel	Click Cancel to abandon this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 27

User Account

27.1 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.

27.2 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 186 Maintenance > User Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	☒	admin	0	60	5	Administrator	
2	☒	User-S	0	60	5	User	

The following table describes the labels in this screen.

Table 120 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.

Table 120 Maintenance > User Account (continued)

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

27.2.1 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 187 Maintenance > User Account > Add or Edit

The following table describes the labels in this screen.

Table 121 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 121 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	Specify whether this user will have Administrator or User privileges. An Administrator account can access all Web Configurator menus. A User account can only access Monitor and Maintenance menus. The maximum account number of Administrator and User are both four. The total number of the users allowed to log in the Zyxel Device at the same time is eight. The Administrator privileges are the following: • Quick Start setup. • The following screens are visible for setup: Broadband, Wireless, Home Networking, Routing, NAT, DNS, Firewall, MAC Filter, Certificates, Voice, Log, Traffic Status, ARP Table, Routing Table, Cellular WAN Status, System, User Account, Remote Management, TR-069 Client, Time, Email Notification, Log Setting, Firmware Upgrade, Backup/Restore, Reboot, Diagnostic. The User privileges are the following: • The following screens are visible for setup: Log, Traffic Status, ARP Table, Routing Table, Cellular WAN Status, User Account, Remote Management, Time, Email Notification, Log Setting, Firmware Upgrade, Backup/Restore, Reboot, Diagnostic.
Cancel	Click Cancel to restore your previously saved settings.
OK	Click OK to save your changes.

CHAPTER 28

Remote Management

28.1 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.

28.2 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** to open the following screen.

Figure 188 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	☒ Enable	☐ Enable	☐ Enable	80
HTTPS	☒ Enable	☐ Enable	☐ Enable	443
FTP	☒ Enable	☐ Enable	☐ Enable	21
TELNET	☒ Enable	☐ Enable	☐ Enable	23
SSH	☒ Enable	☐ Enable	☐ Enable	22
PING	☒ Enable	☐ Enable	☐ Enable	

Cancel Apply

The following table describes the fields in this screen.

Table 122 Maintenance > Remote Management > 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.

28.3 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**. See [Section 7.10 on page 110](#) for details.

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

Figure 189 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	☒ Enable	☐ Enable	20080
PT_HTTPS	☒ Enable	☐ Enable	20443
PT_FTP	☐ Enable	☐ Enable	20021
PT_TELNET	☐ Enable	☐ Enable	20023
PT_SSH	☐ Enable	☐ Enable	20022

Cancel Apply

The following table describes the fields in this screen.

Table 123 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.

28.4 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 190 Maintenance > Remote Management > Trust Domain

View a list of public IP addresses which you want to allow access to the Zyxel Device through the services configured in this screen.

If this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

+ Add Trust Domain

IP Address	Delete
------------	--------

The following table describes the fields in this screen.

Table 124 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.

28.5 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 191 Maintenance > Remote Management > Trust Domain > Add Trust Domain

The following table describes the fields in this screen.

Table 125 Maintenance > Remote Management > Trust Domain > Add Trust Domain

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

28.6 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**. See [Section 7.10 on page 110](#) for details.

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

Figure 192 Maintenance > Remote Management > Trust Domain for IP Passthrough

Remote Management

MGMT Services Trust Domain MGMT Services for IP Passthrough **Trust Domain for IP Passthrough**

View a list of public IP addresses which you want to allow access to the Zyxel Device through the services configured in this screen.

If this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

+ Add Trust Domain

IP Address	Delete
------------	--------

The following table describes the fields in this screen.

Table 126 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.

28.7 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 193 Maintenance > Remote Management > Trust Domain for IP Passthrough > Add Trust Domain

Add Trust Domain

Configure a public IP address which you want to allow access to the Zyxel Device.

IP Address [prefix length]

Cancel **OK**

The following table describes the fields in this screen.

Table 127 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 29

TR-069 Client

29.1 Overview

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

29.2 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 194 Maintenance > TR-069 Client

TR-069 Client

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

CWMP Active ☒

Inform ☒

Inform Interval

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

Display SOAP Messages on Serial Console ☒

Connection Request Authentication ☒

Connection Request User Name

Connection Request Password

Connection Request URL

Validate ACS certificate ☒

Local Certificate Used by TR-069 Client

Cancel Apply

The following table describes the fields in this screen.

Table 128 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP Active	CPE WAN Management Protocol (CWMP) enables the Zyxel Device to be remotely configured through a WAN link. Communication between the Zyxel Device and the management server is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC). Click to enable (switch turns blue) to allow the Zyxel Device to be managed by a management server. Otherwise, click to disable (switch turns gray) to disallow the Zyxel Device to be managed by a management server.
Inform	Click to enable (switch turns blue) the Zyxel Device to send periodic inform through TR-069 on the WAN. Otherwise, click to disable (switch turns gray).
Inform Interval	Enter the time interval (in seconds) at which the Zyxel Device sends information to the auto-configuration server.
IP Protocol	Select the type of IP protocol to allow TR-069 to operate on.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select Any_WAN, the Zyxel Device automatically passes the TR-069 traffic when any WAN connection is up. If you select Multi_WAN, you also need to select two or more pre-configured WAN interfaces. The Zyxel Device automatically passes the TR-069 traffic when one of the selected WAN connections is up.
Cellular WAN	The Zyxel Device automatically passes the TR-069 traffic when cellular WAN connection is up.
Display SOAP messages on serial console	Click to enable (switch turns blue) the dumping of all SOAP messages during the ACS server communication with the CPE.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the Zyxel Device, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the Zyxel Device, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the Zyxel Device.
Validate ACS Certificate	Click to enable (switch turns blue) the validation of a local certificate used by TR-069 client.
Local certificate used by TR-069 client	You can choose a local certificate used by TR-069 client. The local certificate should be imported in the Security > Certificates > Local Certificates screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore the screen's last saved settings.

CHAPTER 30

Time Settings

30.1 Time Settings Overview

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

30.2 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 195 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 129 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 129 Maintenance > Time (continued)

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

CHAPTER 31

Email Notification

31.1 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.

31.2 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 196 Maintenance > E-mail Notification

The following table describes the labels in this screen.

Table 130 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.
Remove	Click this button to delete the selected entries.

31.2.1 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 197 E-mail Notification > Add

Add New e-mail

E-mail Notification Configuration

Mail Server Address (SMTP Server NAME or IP)

Port Default:25

Authentication Username

Authentication Password 👁

Account e-mail Address

Connection Security ☐ SSL ☒ STARTTLS

Cancel **OK**

The following table describes the labels in this screen.

Table 131 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.
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 32

Log Setting

32.1 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.

32.2 Log Settings

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 198 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 132 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Click the switch (it will turn blue) to enable syslog logging.
Mode	Select Remote to have the Zyxel Device send it to an external syslog server. Select Local File to have the Zyxel Device save the log file on the Zyxel Device itself. Select Local File and Remote to have the Zyxel Device save the log file on the Zyxel Device itself and send it to an external syslog server. Note: A warning appears upon selecting Remote or Local File and Remote. Just click OK to continue.

Table 132 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.

32.2.1 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 199 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 33

Firmware Upgrade

33.1 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.

33.2 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 200 Maintenance > Firmware Upgrade

The screenshot shows the 'Firmware Upgrade' screen. At the top, the title 'Firmware Upgrade' is centered. Below it, the text 'Firmware Upgrade' is repeated in a blue box. A large, light gray watermark 'ZyXEL' is visible in the background. The main content area contains the following 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'. It includes a checkbox for '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, there is a 'File Path' label, a 'Choose File' button, the text 'No file chosen', and a blue 'Upload' button.

The following table describes the labels in this screen.

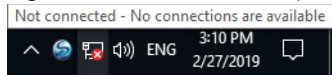
Table 133 Maintenance > Firmware Upgrade

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 34.2 on page 282 .
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.

After you see the firmware updating screen, wait a few minutes before logging into the Zyxel Device again.

The Zyxel Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 201 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.

CHAPTER 34

Backup/Restore

34.1 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.

34.2 Backup/Restore

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 202 Maintenance > Backup/Restore

Back up and restore your Zyxel Device configurations. You can also reset your Zyxel Device settings back to the factory default.

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once the Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

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

Backup Configuration

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

Backup

Restore Configuration

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

File Path **Browse...** **Upload**

Back to Factory Default Settings

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

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

Reset

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 134 Restore Configuration

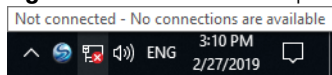
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Choose File / Browse to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click 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.

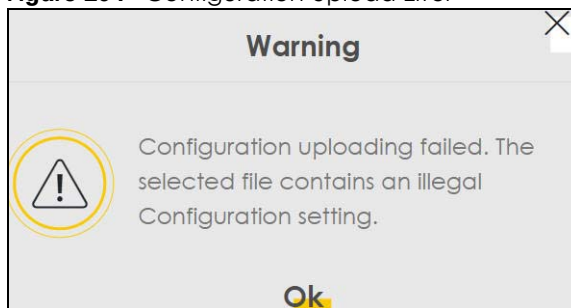
Figure 203 Network Temporarily Disconnected



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).

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

Figure 204 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 205 Reset Warning Message

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

34.3 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 206 Maintenance > Reboot

CHAPTER 35

Diagnostic

35.1 Diagnostic Overview

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

The route between an Ethernet switch and one of its Customer-Premises Equipment (CPE) may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

35.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

- Loopback test – checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test – provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

35.3 Ping/TraceRoute/Nslookup Test

Use this screen to ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Click **Maintenance > Diagnostic** to open the **Ping/TraceRoute/Nslookup** screen shown next.

Figure 207 Maintenance > Diagnostic > Ping/Trace Route/Nslookup

Diagnostic

The **Diagnostic** screens display information to help you identify problems with the Zyxel Device.

Use this screen to ping, traceroute, or nslookup for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on 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/Nslookup Test

TCP/IP

Address

The following table describes the fields in this screen.

Table 135 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.

CHAPTER 36

Troubleshooting

36.1 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](#)

36.2 Power and Hardware Problems

[The Zyxel Device does not turn on.](#)

To check whether your model uses Power over Ethernet (PoE), see the hardware tables at [Section 1.1 on page 16](#).

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.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LEDs. See [Section 2.2 on page 25](#)
- 2 Check the hardware connections.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Zyxel Device off and on.
- 5 If the problem continues, contact the vendor.

36.3 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 34.2 on page 282](#).

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 34.2 on page 282](#).

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 143](#)), 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 25](#)
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
- 4 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

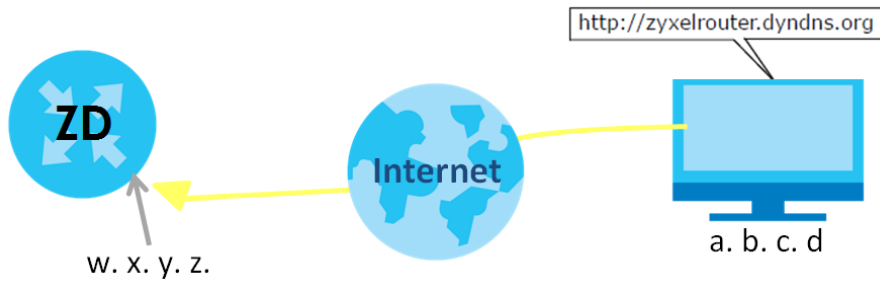
- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management 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.

36.4 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.

36.5 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 (refer to [Section 7.7 on page 105](#)), the account has expired, it needs to be removed and reinserted (refer to the Quick Start Guide), or it is missing. See [Section 36.7 on page 294](#) 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 wireless LAN in the Zyxel Device and your wireless client and that the wireless 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 [Section on page 288](#).

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

36.6 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 wireless devices.

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

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless 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 wireless client.
- Reduce the number of wireless 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 wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

36.7 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.

36.8 UPnP Problems

My computer cannot detect UPnP settings from the Zyxel Device.

- 1 Make sure that UPnP is enabled in your computer. For Windows 7, see [Section on page 150](#). For Windows 10, see [Section 9.6 on page 151](#).
- 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 149](#) 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.

PART III

Appendices

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

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 136 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 137 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and cannot be assigned to a multicast group.

Table 138 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 139

MAC	00	:	13	:	49	:	12	:	34	:	56
------------	----	---	----	---	----	---	----	---	----	---	----

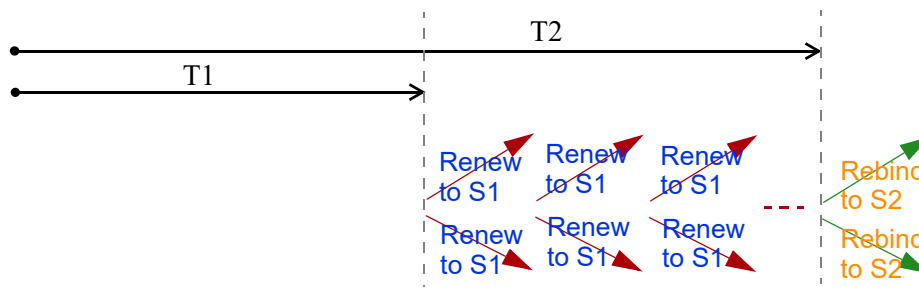
Table 140

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.

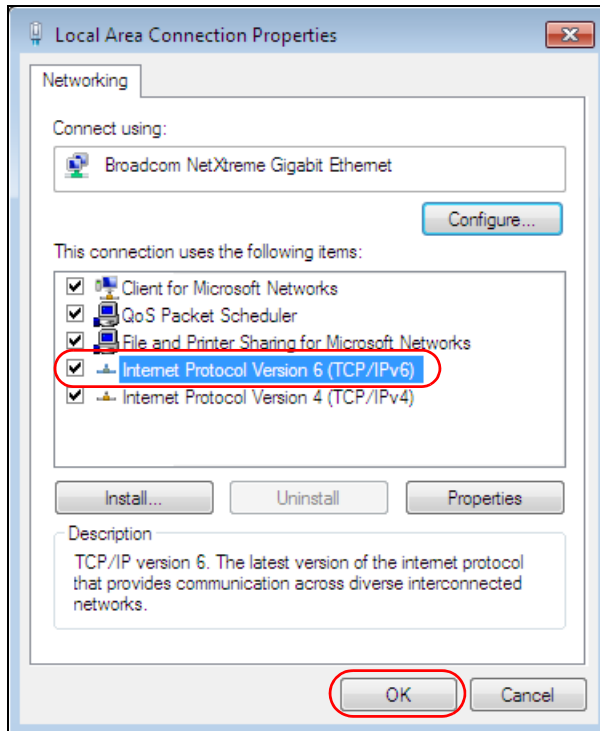
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 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:feaa:7125%11
                                172.16.100.254
```

APPENDIX C

Legal Information

Copyright

Copyright © 2021 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

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:

(LTE7240-M403)

- WiFi
 - The band 2,400 – 2,483.5 MHz is 88.51 mW
- GSM
 - The GSM 900 is 1967.89 mW
 - The DCS 1800 is 968.28 mW
- WCDMA
 - The WCDMA Band I is 213.8 mW
 - The WCDMA Band VIII is 208.93 mW
- LTE
 - The LTE Band 1 is 204.17 mW
 - The LTE Band 3 is 199.53 mW
 - The LTE Band 7 is 190.55 mW
 - The LTE Band 8 is 208.93 mW
 - The LTE Band 20 is 223.87 mW
 - The LTE Band 38 is 147.91 mW
 - The LTE Band 40 is 141.25 mW

(LTE3301-PLUS)

- WiFi
 - The band 2,400 – 2,483.5 MHz is 81.28 mW
 - The band 5,150 – 5,350 MHz is 180.3 mW
 - The band 5,470 – 5,725 MHz is 612.35 mW

- WCDMA
 - The WCDMA Band I is 193.64 mW
 - The WCDMA Band III is 228.56 mW
 - The WCDMA Band VIII is 198.15 mW
- LTE
 - The LTE Band 1 is 223.87 mW
 - The LTE Band 3 is 239.88 mW
 - The LTE Band 7 is 218.78 mW
 - The LTE Band 8 is 186.21 mW
 - The LTE Band 20 is 186.21 mW
 - The LTE Band 28 is 206.06 mW
 - The LTE Band 38 is 247.17 mW
 - The LTE Band 40 is 231.21 mW

(LTE7480-M804 & LTE7490-M904)

- The band 2,400 – 2,483.5 MHz is 88.72 mW (LTE7480-M804)
- The band 2,400 – 2,483.5 MHz is 87.1 mW (LTE7490-M904)
- WCDMA
 - The WCDMA Band I is 316.23 mW
 - The WCDMA Band III is 316.23 mW
 - The WCDMA Band VIII is 281.84 mW
- LTE
 - The LTE Band 1/3/7/8/20/28/38/40 is 281.84 mW

(LTE3316-M604)

- WCDMA
 - The WCDMA Band I is 193.64 mW
 - The WCDMA Band III is 228.56 mW
 - The WCDMA Band VIII is 198.15 mW
- LTE
 - The LTE Band 1 is 223.87 mW
 - The LTE Band 3 is 251.19 mW
 - The LTE Band 7 is 218.78 mW
 - The LTE Band 8 is 186.21 mW
 - The LTE Band 20 is 186.21 mW
 - The LTE Band 28 is 206.06 mW
 - The LTE Band 38 is 247.17 mW
 - The LTE Band 40 is 231.21 mW
- 802.11 Mode
 - 802.11b Band (2,400 – 2,483.5 MHz) is 84.3 mW
 - 802.11g Band (2,400 – 2,483.5 MHz) is 95.72 mW
 - 802.11n Band (2,400 – 2,483.5 MHz) is 96.83 mW
 - 802.11ac Band (5,150 – 5,350 MHz) is 195.88 mW
 - 802.11ac Band (5,470 – 5,725 MHz) is 392.64 mW

(LTE5388-M804 & LTE5398-M904)

- WiFi
 - The band 2,400 – 2,483.5 MHz is 87.9 mW
 - The band 5,150 – 5,350 MHz is 194.09 mW
 - The band 5,470 – 5,725 MHz is 450.82 mW
- WCDMA
 - The WCDMA band I is 316.23 mW
 - The WCDMA band III is 316.23 mW
 - The WCDMA band VIII is 281.84 Mw
- LTE
 - The LTE band 1/3/7/8/20/28/38/40 is 281.84 mW

(LTE3202-M437)

- WiFi
 - The band 2400 – 2483.5MHz is 90.78 mW
- GSM
 - The GSM 900 is 1828.1 mW
 - The GSM 1800 is 950.6 mW
- WCDMA
 - The WCDMA Band I is 251.19 mW
 - The WCDMA Band VIII is 251.19 mW
- LTE
 - The LTE Band 1/3/7/8/20/28/38/40 is 199.53 mW

Български (Bulgarian)	С настоящото ZyXel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. National Restrictions - The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. - Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. - Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	Por medio de la presente ZyXel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..
Čeština (Czech)	ZyXel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede ZyXel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. National Restrictions - In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. - I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt ZyXel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab ZyXel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΙΑ ΖΥΧΕΛ ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, ZyXel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente ZyXel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	ZyXel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, ZyXel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente ZyXel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. National Restrictions - This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check 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)	Ar šo ZyXel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. National Restrictions - 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 nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawn hekk, 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 laitteen 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 (All LTE Models)

- 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 / LTE5388-M804 / LTE5398-M904 / LTE3316-M604/ LTE3202-M437))

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless settings, please refer to the chapter about wireless settings for more detail.)

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區：

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區：

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 – 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	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:

for Zyxel Communication products, please go to: <https://service-provider.zyxel.com/global/en/gpl-oss-software-notice>

for Zyxel Network products, please go to: https://www.zyxel.com/form/gpl_oss_software_notice.shtml

Index

A

- access
 - troubleshooting [288](#)
- Access Control (Rules) screen [198](#)
- ACS [269](#)
- activation
 - firewalls [195](#)
- Address Resolution Protocol [246](#)
- Any_WAN
 - Remote Management [264](#)
 - TR-069 traffic [270](#)
- APN information
 - obtain [101](#)
- APN Settings [103](#)
- Application Layer Gateway (ALG) [177](#)
- applications
 - Internet access [18](#)
 - wireless WAN [17](#)
- applications, NAT [182](#)
- ARP Table [246](#), [248](#)
- authentication [134](#)
- Authentication Type
 - APN [103](#), [105](#)
- Auto Configuration Server, see ACS [269](#)

B

- backup
 - configuration [282](#)
- backup configuration [282](#)
- Backup/Restore screen [282](#)
- Band Configuration screen [106](#)
- blinking LEDs [25](#)
- Broadband [94](#)

C

- CA [219](#)
- CCMs [285](#)
- Cellular Band screen [106](#)
- Cellular SIM screen [105](#)
- Cellular WAN [264](#)
 - TR-069 traffic [270](#)
- Cellular WAN screen [100](#), [101](#), [102](#)
- certificate
 - details [221](#)
 - factory default [214](#)
 - file format [220](#)
 - file path [218](#)
 - import [214](#), [217](#)
 - public and private keys [220](#)
 - verification [220](#)
- certificate request
 - create [214](#)
 - view [215](#)
- certificates [213](#)
 - advantages [220](#)
 - authentication [213](#)
 - CA [213](#), [219](#)
 - creating [214](#)
 - public key [213](#)
 - replacing [214](#)
 - storage space [214](#)
 - thumbprint algorithms [221](#)
 - trusted CAs [218](#)
 - verifying fingerprints [220](#)
- Certification Authority [213](#)
- Certification Authority, see CA
- certifications [311](#)
 - viewing [313](#)
- CFM [285](#)
 - CCMs [285](#)
 - link trace test [285](#)
 - loopback test [285](#)
 - MA [285](#)
 - MD [285](#)
 - MEP [285](#)

- MIP [285](#)
- client list [147](#)
- configuration
 - backup [282](#)
 - firewalls [195](#)
 - restoring [283](#)
 - static route [187](#)
- Connectivity Check Messages, see CCMs
- contact information [297](#)
- copyright [308](#)
- Create Certificate Request screen [214](#)
- creating certificates [214](#)
- CTS threshold [128](#), [134](#)
- customer support [297](#)
- customized service [197](#)
 - add [197](#)
- customized services [198](#)

D

- data fragment threshold [128](#), [134](#)
- Data Roaming
 - enable [102](#)
- DDoS [195](#)
- Denials of Service, see DoS
- DHCP [143](#)
- DHCP Server State [145](#)
- diagnostic [285](#)
- diagnostic screens [285](#)
- digital IDs [213](#)
- disclaimer [308](#)
- DMZ screen [176](#)
- DNS [143](#)
- DNS Values [145](#)
- Domain Name [183](#)
- domain name system, see DNS
- DoS [194](#)
 - thresholds [194](#)
- DoS protection blocking
 - enable [202](#)
- dynamic DNS [185](#)
 - wildcard [186](#)
- Dynamic Host Configuration Protocol, see DHCP

- DYNDNS wildcard [186](#)

E

- ECHO [183](#)
- email
 - log example [278](#)
 - log setting [278](#)
- Extended Service Set IDentification [117](#), [121](#)

F

- factory defaults
 - reset [283](#)
- filters
 - MAC address [123](#), [135](#)
- Finger services [183](#)
- firewall
 - enhancing security [203](#)
 - LAND attack [195](#)
 - security considerations [204](#)
 - traffic rule direction [201](#)
- Firewall DoS screen [201](#)
- Firewall General screen [196](#)
- firewall rules
 - direction of travel [202](#)
- firewalls [194](#), [195](#)
 - actions [201](#)
 - configuration [195](#)
 - customized service [197](#)
 - customized services [198](#)
 - DDoS [195](#)
 - DoS [194](#)
 - thresholds [194](#)
 - ICMP [195](#)
 - Ping of Death [195](#)
 - rules [202](#)
 - security [203](#)
- firmware [280](#)
 - version [84](#)
- Firmware Upgrade screen [280](#)
- firmware upload [280](#)
- firmware version
 - check [281](#)

fragmentation threshold [128, 134](#)

FTP [170, 183](#)

unusable [291](#)

G

General wireless LAN screen [115](#)

H

HTTP [183](#)

I

ICMP [195](#)

IGA [181](#)

ILA [181](#)

Import Certificate screen [218](#)

importing trusted CAs [218](#)

Inside Global Address, see IGA

Inside Local Address, see ILA

Internet

no access [292](#)

wizard setup [47](#)

Internet access [17, 18](#)

wizard setup [47](#)

Internet Blocking [82](#)

Internet connection

slow or erratic [293](#)

Internet Control Message Protocol, see ICMP

Internet Protocol version 6, see IPv6

IP address

WAN [95](#)

IP address access control [266](#)

IP alias

NAT applications [183](#)

IP Passthrough mode [110](#)

IP Passthrough screen [41, 110, 111, 112](#)

IPv4 firewall [196](#)

IPv6 [302](#)

addressing [302](#)

EUI-64 [304](#)

global address [302](#)

interface ID [304](#)

link-local address [302](#)

Neighbor Discovery Protocol [302](#)

ping [302](#)

prefix [302](#)

prefix length [302](#)

unspecified address [303](#)

IPv6 firewall [196](#)

L

LAN [142](#)

client list [147](#)

MAC address [130, 148](#)

status [85, 93](#)

LAN IP address [145](#)

LAN IPv6 Mode Setup [145](#)

LAN Setup screen [143](#)

LAN subnet mask [145](#)

LAND attack [195](#)

LBR [285](#)

limitations

wireless LAN [136](#)

WPS [141](#)

link trace [285](#)

Link Trace Message, see LTM

Link Trace Response, see LTR

listening port [229](#)

Local Area Network, see LAN

local certificate

TR-069 client [270](#)

Local Certificates screen [213](#)

Log Setting screen [276](#)

login [37](#)

password [37](#)

Login screen

no access [288](#)

logs [237, 240, 253, 276](#)

Loop Back Response, see LBR

loopback [285](#)

LTM [285](#)

LTR [285](#)

M

MA [285](#)
MAC address [124, 130, 148](#)
 filter [123, 135](#)
 LAN [148](#)
MAC Authentication screen [119, 123](#)
MAC Filter [205](#)
Maintenance Association, see MA
Maintenance Domain, see MD
Maintenance End Point, see MEP
managing the device
 good habits [20](#)
 using FTP, see FTP
MD [285](#)
MEP [285](#)
MGMT Services screen [263, 264](#)
Multi_WAN
 Remote Management [264](#)
 TR-069 traffic [270](#)

N

NAT [181](#)
 applications [182](#)
 IP alias [183](#)
 default server [176](#)
 DMZ host [176](#)
 example [182](#)
 global [181](#)
 IGA [181](#)
 ILA [181](#)
 inside [181](#)
 local [181](#)
 multiple server example [170](#)
 outside [181](#)
 port number [183](#)
 services [183](#)
NAT ALG screen [177, 178, 180](#)
NAT example [184](#)
Network Address Translation, see NAT
network disconnect
 temporary [281](#)
network map [41, 82](#)
network type

 select [107](#)
NNTP [183](#)
Nslookup test [286](#)

O

Others screen [127](#)

P

password [37](#)
 admin [288](#)
 good habit [20](#)
 lost [288](#)
 user [288](#)
PBC [136](#)
PIN Protection [106](#)
PIN, WPS [137](#)
 example [138](#)
Ping of Death [195](#)
Ping test [286](#)
Ping/TraceRoute/Nslookup screen [285](#)
PLMN Configuration screen [107](#)
PoE injector [18](#)
Point-to-Point Tunneling Protocol, see PPTP
POP3 [183](#)
port forwarding rule
 add/edit [171](#)
Port Forwarding screen [170, 171](#)
Port Triggering
 add new rule [175](#)
Port Triggering screen [173](#)
ports [25](#)
PPTP [183](#)
preamble [129, 134](#)
problem
 troubleshooting [287](#)
Protocol (Customized Services) screen [197](#)
Protocol Entry
 add [197](#)
Push Button Configuration, see PBC
push button, WPS [136](#)

R

- Reboot screen [284](#)
- remote management
 - TR-069 [269](#)
- Remote Procedure Calls, see RPCs [269](#)
- RESET Button [33](#)
- reset to factory defaults [283](#)
- restart system [284](#)
- restore default settings
 - after firmware upgrade [281](#)
- restoring configuration [283](#)
- RFC 1058, see RIP
- RFC 1389, see RIP
- RFC 1631 [169](#)
- RFC 3164 [237](#)
- RIP [168](#)
- router features [17](#), [18](#)
- Routing Information Protocol, see RIP
- Routing Table screen [248](#)
- RPPCs [269](#)
- RTS threshold [128](#), [134](#)

S

- security
 - network [203](#)
 - wireless LAN [134](#)
- Security Log [238](#)
- Security Parameter Index, see SPI
- service access control [264](#), [266](#)
- Service Set [117](#), [121](#)
- services
 - port forwarding [183](#)
- setup
 - firewalls [195](#)
 - static route [187](#)
- SIM card
 - status [87](#), [255](#)
- SIM configuration [105](#)
- SMTP [183](#)
- SNMP [183](#)
- SNMP trap [183](#)

- SPI [195](#)
- SSH
 - unusable [291](#)
- SSID [135](#)
- static DHCP [147](#)
 - configuration [149](#)
- Static DHCP screen [147](#)
- static route [159](#), [168](#)
 - configuration [187](#)
- status [82](#)
 - firmware version [84](#)
 - LAN [85](#), [93](#)
 - WAN [84](#)
 - wireless LAN [85](#)
- status indicators [25](#)
- syslog
 - protocol [237](#)
 - severity levels [237](#)
- syslog logging
 - enable [277](#)
- syslog server
 - name or IP address [278](#)
- system
 - firmware [280](#)
 - version [84](#)
 - password [37](#)
 - status [82](#)
 - LAN [85](#), [93](#)
 - WAN [84](#)
 - wireless LAN [85](#)
 - time [271](#)

T

- Telnet
 - unusable [291](#)
- thresholds
 - data fragment [128](#), [134](#)
 - DoS [194](#)
 - RTS/CTS [128](#), [134](#)
- time [271](#)
- TR-069 [269](#)
 - authentication [270](#)
- TR-069 Client screen [269](#)
- Trace Route test [286](#)

troubleshooting [287](#)

Trust Domain

add [266](#)

Trust Domain screen [265](#)

Trusted CA certificate

view [218](#)

Trusted CA screen [217](#)

Turning on UPnP

Windows 7 example [150](#)

U

Universal Plug and Play, see UPnP

upgrading firmware [280](#)

UPnP [149](#)

forum [143](#)

security issues [143](#)

state [150](#)

usage confirmation [143](#)

UPnP screen [149](#)

UPnP-enabled Network Device

auto-discover [153](#)

SSID [135](#)

status [85](#)

WPS [136, 138](#)

example [139](#)

limitations [141](#)

PIN [137](#)

push button [136](#)

Wireless tutorial [55](#)

wizard setup

Internet [47](#)

WMM screen [126](#)

WPS [136, 138](#)

example [139](#)

limitations [141](#)

PIN [137](#)

example [138](#)

push button [136](#)

WPS screen [124](#)

W

WAN

status [84](#)

Wide Area Network, see WAN [94](#)

warranty [313](#)

note [314](#)

Web Configurator

login [37](#)

password [37](#)

WEP Encryption [118](#)

Wireless General screen [115](#)

wireless LAN [114](#)

authentication [134](#)

example [133](#)

fragmentation threshold [128, 134](#)

limitations [136](#)

MAC address filter [123, 135](#)

preamble [129, 134](#)

RTS/CTS threshold [128, 134](#)

security [134](#)