ZYXEL
Your Networking Ally

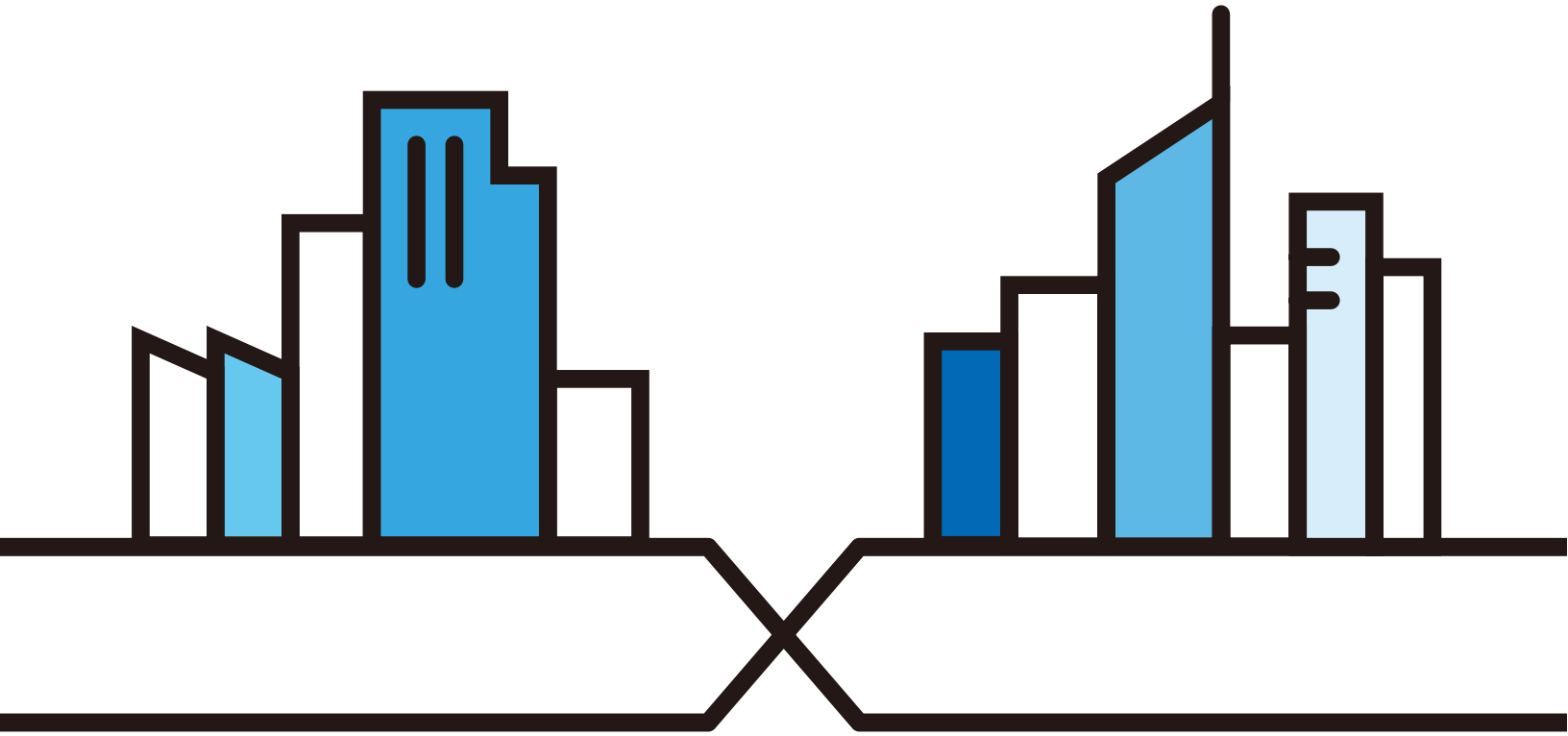
User's Guide

PX7511-B0

Wireless AX 10G PON Gateway with VoIP

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

Version 5.15 Edition 1, 10/2019



Copyright © 2019 Zyxel Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

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

- More Information

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

Document Conventions

Warnings and Notes

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

Warnings tell you about things that could harm you or your 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 PX7511-B0 in this user's guide may be referred to as the "Zyxel Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting > Routing > DNS Route** means you first click **Network Setting** in the navigation panel, then the **Routing** sub menu and finally the **DNS Route** tab to get to that screen.

Icons Used in Figures

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

Zyxel Device	Wireless Device	Laptop Computer
Switch	Firewall	Server
Internet	User	Smartphone

Contents Overview

User's Guide **16**

Introducing the Zyxel Device 17
The Web Configurator 24
Quick Start Wizard 32
Tutorials 37

Technical Reference **59**

Connection Status 60
Broadband 74
Wireless 88
Home Networking 117
Routing 137
Quality of Service (QoS) 145
Network Address Translation (NAT) 165
Dynamic DNS Setup 182
IGMP/MLD 186
VLAN Group 189
Interface Grouping 192
Firewall 198
MAC Filter 207
Parental Control 209
Scheduler Rule 215
Certificates 217
VoIP 224
Log 254
Traffic Status 257
VoIP Status 261
ARP Table 264
Routing Table 266
Multicast Status 269
WLAN Station Status 271
xPON Status 273
System 274
User Account 275
Remote Management 278
SNMP 281
Time Settings 284
Email Notification 287

Log Setting 290
Firmware Upgrade 294
Backup and Restore 296
Diagnostic 299
GPON 301

Troubleshooting and Appendices 302

Troubleshooting 303

Table of Contents

Document Conventions 3

Contents Overview 4

Table of Contents 6

Part I: User's Guide 16

Chapter 1
Introducing the Zyxel Device 17

1.1 Overview 17
1.1.1 Multi-Gigabit 17
1.2 Example Applications 17
1.2.1 Internet Access 18
1.2.2 Dual-Band WiFi 18
1.2.3 VoIP Application 19
1.3 Ways to Manage the Zyxel Device 19
1.4 Good Habits for Managing the Zyxel Device 19
1.5 Hardware 20
1.5.1 Front Panel 20
1.5.2 Rear Panel 21
1.5.3 The WPS Button 22
1.5.4 The RESET Button 23
1.5.5 The UPS Port 23

Chapter 2
The Web Configurator 24

2.1 Overview 24
2.1.1 Accessing the Web Configurator 24
2.2 Web Configurator Layout 26
2.2.1 Navigation Panel 27

Chapter 3
Quick Start Wizard 32

3.1 Overview 32
3.2 Wizard Setup 32
3.2.1 Time Zone 32
3.2.2 Internet 33

3.2.3 WiFi 35

Chapter 4
Tutorials 37

4.1 Overview 37
4.2 Setting Up a Secure Wireless Network 37
4.2.1 Configuring the Wireless Network Settings 37
4.2.2 Using WPS 39
4.2.3 Without WPS 43
4.3 Setting Up Multiple Wireless Groups 44
4.4 Configuring Static Route for Routing to Another Network 49
4.5 Configuring QoS Queue and Class Setup 51
4.6 Access the Zyxel Device Using DDNS 55
4.6.1 Registering a DDNS Account on www.dyndns.org 55
4.6.2 Configuring DDNS on Your Zyxel Device 56
4.6.3 Testing the DDNS Setting 56
4.7 Configuring the MAC Address Filter 57

Part II: Technical Reference 59

Chapter 5
Connection Status 60

5.1 Overview 60
5.1.1 Layout Icon 61
5.1.2 Connectivity 61
5.1.3 System Info 62
5.2 WiFi Settings 65
5.3 Guest WiFi Settings 67
5.4 LAN Settings 68
5.5 Parental Control 70
5.5.1 Create/Edit a Parental Control Profile 71
5.5.2 Define a Schedule 72

Chapter 6
Broadband 74

6.1 Overview 74
6.1.1 What You Can Do in this Chapter 74
6.1.2 What You Need to Know 74
6.1.3 Before You Begin 77
6.2 Broadband Settings 77
6.2.1 Add/Edit Internet Connection 78

6.3 Technical Reference 84

Chapter 7
Wireless 88

7.1 Wireless Overview 88
7.1.1 What You Can Do in this Chapter 88
7.1.2 What You Need to Know 88
7.2 Wireless General Settings 89
7.2.1 No Security 92
7.2.2 More Secure (Recommended) 92
7.3 Guest/More AP 94
7.3.1 The Edit Guest/More AP Screen 94
7.4 MAC Authentication 97
7.4.1 Add/Edit MAC Addresses 98
7.5 WPS Settings 99
7.6 WMM Settings 100
7.7 Others Settings 101
7.8 Channel Status Settings 104
7.9 Technical Reference 104
7.9.1 Wireless Network Overview 104
7.9.2 Additional Wireless Terms 106
7.9.3 Wireless Security Overview 106
7.9.4 Signal Problems 108
7.9.5 BSS 108
7.9.6 MBSSID 109
7.9.7 Preamble Type 109
7.9.8 WiFi Protected Setup (WPS) 110

Chapter 8
Home Networking 117

8.1 Home Networking Overview 117
8.1.1 What You Can Do in this Chapter 117
8.1.2 What You Need To Know 117
8.1.3 Before You Begin 119
8.2 LAN Setup 119
8.3 LAN Static DHCP 123
8.4 UPnP Settings 125
8.4.1 Turning on UPnP in Windows 7 Example 126
8.4.2 Turning on UPnP in Windows 10 Example 128
8.5 LAN Additional Subnet 130
8.6 STB Vendor ID 132
8.7 Wake on LAN 133
8.8 TFTP Server Name 133

8.9 Technical Reference 134
8.9.1 LANs, WANs and the Zyxel Device 134
8.9.2 DHCP Setup 135
8.9.3 DNS Server Addresses 135
8.9.4 LAN TCP/IP 135

Chapter 9
Routing 137

9.1 Overview 137
9.2 Static Route Settings 137
9.2.1 Add/Edit Static Route 138
9.3 DNS Route 140
9.3.1 Add DNS Route 140
9.4 Policy Route 141
9.4.1 Add/Edit Policy Route 143
9.5 RIP Settings 144

Chapter 10
Quality of Service (QoS) 145

10.1 QoS Overview 145
10.1.1 What You Can Do in this Chapter 145
10.2 What You Need to Know 146
10.3 Quality of Service General Settings 147
10.4 Queue Setup 149
10.4.1 Adding a QoS Queue 150
10.5 QoS Classification Setup 151
10.5.1 Add/Edit QoS Class 152
10.6 QoS Shaper Setup 156
10.6.1 Add/Edit a QoS Shaper 157
10.7 QoS Policer Setup 157
10.7.1 Add/Edit a QoS Policer 158
10.8 Technical Reference 160

Chapter 11
Network Address Translation (NAT) 165

11.1 NAT Overview 165
11.1.1 What You Can Do in this Chapter 165
11.1.2 What You Need To Know 165
11.2 Port Forwarding 166
11.2.1 Add/Edit Port Forwarding 168
11.3 Port Triggering 170
11.3.1 Add/Edit Port Triggering Rule 172
11.4 DMZ Settings 173

11.5 ALG Settings 174
11.6 Address Mapping 175
11.6.1 Add/Edit Address Mapping Rule 176
11.7 NAT Sessions 177
11.8 Technical Reference 178
11.8.1 NAT Definitions 178
11.8.2 What NAT Does 179
11.8.3 How NAT Works 179
11.8.4 NAT Application 180

Chapter 12
Dynamic DNS Setup 182

12.1 DNS Overview 182
12.1.1 What You Can Do in this Chapter 182
12.1.2 What You Need To Know 182
12.2 DNS Entry 183
12.2.1 Add/Edit DNS Entry 183
12.3 Dynamic DNS 184

Chapter 13
IGMP/MLD 186

13.1 IGMP/MLD Overview 186
13.1.1 What You Need To Know 186
13.2 IGMP/MLD Settings 186

Chapter 14
VLAN Group 189

14.1 Overview 189
14.1.1 What You Can Do in this Chapter 189
14.2 The VLAN Group Screen 190
14.2.1 Add/Edit a VLAN Group 190

Chapter 15
Interface Grouping 192

15.1 Interface Grouping Overview 192
15.1.1 What You Can Do in this Chapter 192
15.2 Interface Grouping Setup 192
15.2.1 Interface Group Configuration 194
15.2.2 Interface Grouping Criteria 196

Chapter 16
Firewall 198

16.1 Firewall Overview 198

16.1.1 What You Can Do in this Chapter 198
16.1.2 What You Need to Know 199
16.2 Firewall Settings 199
16.3 Protocol Settings 201
16.3.1 Add New/Edit Protocol Entry 201
16.4 Access Control 202
16.4.1 Add/Edit an ACL Rule 203
16.5 DoS Settings 205

Chapter 17
MAC Filter 207

17.1 MAC Filter Overview 207
17.2 MAC Filter Settings 207

Chapter 18
Parental Control 209

18.1 Parental Control Overview 209
18.2 Parental Control Settings 209
18.2.1 Add/Edit a Parental Control Profile 210

Chapter 19
Scheduler Rule 215

19.1 Scheduler Rule Overview 215
19.2 Scheduler Rule Settings 215
19.2.1 Add/Edit a Schedule Rule 215

Chapter 20
Certificates 217

20.1 Certificates Overview 217
20.1.1 What You Can Do in this Chapter 217
20.2 What You Need to Know 217
20.3 Local Certificates 217
20.3.1 Create Certificate Request 218
20.3.2 View Certificate Request 219
20.4 Trusted CA 221
20.4.1 View Trusted CA Certificate 222
20.4.2 Import Trusted CA Certificate 223

Chapter 21
VoIP 224

21.1 Overview 224
21.1.1 What You Can Do in this Chapter 224
21.1.2 What You Need to Know About VoIP 225

21.2 Before You Begin 225
21.3 The SIP Account Screen 226
21.3.1 The SIP Account Add/Edit Screen 226
21.4 The SIP Service Provider Screen 230
21.4.1 The SIP Service Provider Add/Edit Screen 231
21.5 The Phone Device Screen 235
21.5.1 The Phone Device Edit Screen 236
21.6 The Phone Region Screen 238
21.7 The Call Rule Screen 238
21.8 The Call History Screen 239
21.9 Technical Reference 240
21.9.1 Quality of Service (QoS) 248
21.9.2 Phone Services Overview 249

Chapter 22
Log 254

22.1 Log Overview 254
22.1.1 What You Can Do in this Chapter 254
22.1.2 What You Need To Know 254
22.2 System Log 255
22.3 Security Log 256

Chapter 23
Traffic Status 257

23.1 Traffic Status Overview 257
23.1.1 What You Can Do in this Chapter 257
23.2 WAN Status 257
23.3 LAN Status 258
23.4 NAT Status 259

Chapter 24
VoIP Status 261

24.1 The VoIP Status Screen 261

Chapter 25
ARP Table 264

25.1 ARP Table Overview 264
25.1.1 How ARP Works 264
25.2 ARP Table Settings 264

Chapter 26
Routing Table 266

26.1 Routing Table Overview 266

26.2 Routing Table Settings 266

Chapter 27
Multicast Status 269

27.1 Multicast Status Overview 269
27.2 IGMP Status 269
27.3 MLD Status 270

Chapter 28
WLAN Station Status 271

28.1 WLAN Station Status Overview 271

Chapter 29
xPON Status 273

29.1 Overview 273
29.2 xPON Status Screen 273

Chapter 30
System 274

30.1 System Overview 274
30.2 System Settings 274

Chapter 31
User Account 275

31.1 User Account Overview 275
31.2 User Account Settings 275
31.2.1 User Account Add/Edit 276

Chapter 32
Remote Management 278

32.1 Remote Management Overview 278
32.2 MGMT Services 278
32.3 Trust Domain 279
32.3.1 Add Trust Domain 280

Chapter 33
SNMP 281

33.1 SNMP Overview 281
33.2 SNMP Settings 282

Chapter 34
Time Settings 284

34.1 Time Settings Overview 284

34.2 Time 284

Chapter 35
Email Notification 287

35.1 Email Notification Overview 287
35.2 Email Notification Settings 287
35.2.1 Email Notification Edit 288

Chapter 36
Log Setting 290

36.1 Logs Setting Overview 290
36.2 Log Settings 290
36.2.1 Example Email Log 292

Chapter 37
Firmware Upgrade 294

37.1 Firmware Upgrade Overview 294
37.2 Firmware Upgrade Settings 294

Chapter 38
Backup and Restore 296

38.1 Backup/Restore Overview 296
38.2 Backup/Restore Settings 296
38.3 Reboot 298

Chapter 39
Diagnostic 299

39.1 Diagnostic Overview 299
39.1.1 What You Can Do in this Chapter 299
39.2 Diagnostic Screen 299

Chapter 40
GPON 301

40.1 Overview 301
40.2 SLID 301

Part III: Troubleshooting and Appendices 302

Chapter 41
Troubleshooting 303

41.1 Power, Hardware Connections, and LEDs 303

41.2 Zyxel Device Access and Login 304
41.3 Internet Access 305
41.4 Wireless Internet Access 306
41.5 UPnP 307

Appendix A Customer Support 308

Appendix B IPv6 314

Appendix C Services 322

Appendix D Legal Information 326

Index 334

PART I
User's Guide

CHAPTER 1
Introducing the Zyxel Device

1.1 Overview

The Zyxel Device is a GPON (Gigabit Passive Optical Network) router that offers dual-band WiFi connectivity and comes with a built-in 4-port Gigabit Ethernet switch and two phone ports to make Internet (VoIP) phone calls. The Zyxel Device also provides one 10 Gigabit Ethernet (10GbE) LAN port that supports Multi-Gigabit. See Section 1.1.1 on page 17 for more information about Multi-Gigabit.

1.1.1 Multi-Gigabit

A 10 Gigabit Ethernet port supports speeds of 10 Gbps if the connected device supports 10 Gbps and a Cat 6a (up to 100 m) or Cat 6 cable (up to 50 m) is used.

Some network devices such as gaming computers, servers, network attached storage (NAS) devices, or access points may have network cards that are capable of 2.5 Gbps or 5 Gbps connectivity.

If these devices are connected to a 1 Gbps or 10 Gbps Ethernet port, they can only transmit or receive up to 1 Gbps as speeds of 10 Gbps cannot be attained. Moreover, if network devices with 10 Gbps network cards are connected to a 10 Gbps Ethernet port, you must use Cat 6A or better Ethernet cables to achieve 10 Gbps speeds. Most buildings, at the time of writing, use Cat 5e or Cat 6 Ethernet cables.

Multi-Gigabit Ethernet ports automatically allow connections up to the speed of the connected network device (100 Mbps, 1 Gbps, 2.5 Gbps or 5 Gbps), and you just need to use a Cat 5e or Cat 6 Ethernet cable.

See the following table for the cables required and distance limitation to attain the corresponding speed.

Table 1 Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100 Mbps	100 m	100 MHz
Category 5e	1 Gbps/2.5 Gbps/5 Gbps	100 m	100 MHz
Category 6	5 Gbps/10 Gbps	50 m	250 MHz
Category 6a	10 Gbps	100 m	500 MHz
Category 7	10 Gbps	100 m	650 MHz

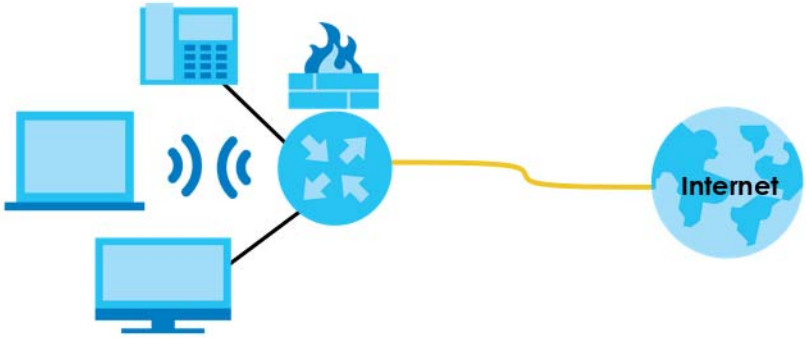
1.2 Example Applications

This section shows a few examples of using the Zyxel Device in various network environments. Note that the Zyxel Device in the figure is just an example Zyxel Device and not your actual Zyxel Device.

1.2.1 Internet Access

Your Zyxel Device provides shared Internet access by connecting a fiber optic cable provided by the ISP to the PON port. It supports OMCI (ONU Management and Control Interface) to connect to the ISP's OLT (Optical Line Terminal). Computers can connect to the Zyxel Device's LAN ports (or wirelessly) and access the Internet simultaneously.

Figure 1 Internet Access Application



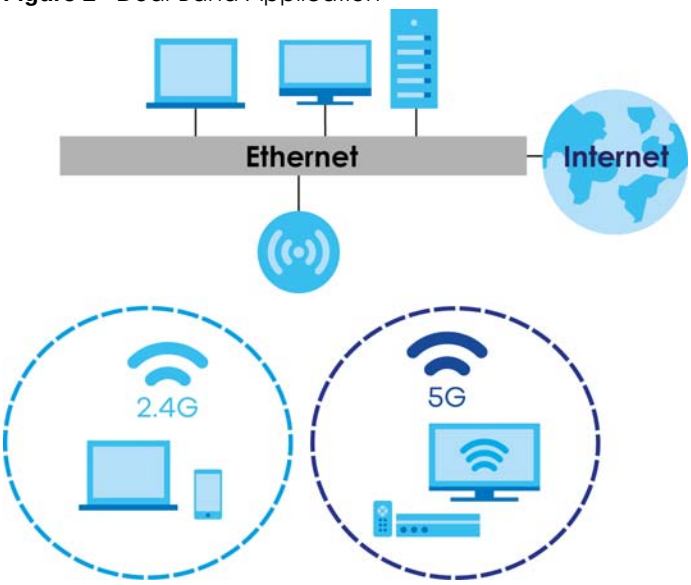
You can also configure Firewall on the Zyxel Device for secure Internet access. When the Firewall is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but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

1.2.2 Dual-Band WiFi

By default, the wireless LAN (WLAN) is enabled on the Zyxel Device. IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the Zyxel Device to access network resources.

The Zyxel Device is a dual-band gateway that can use both 2.4G and 5G networks at the same time. You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

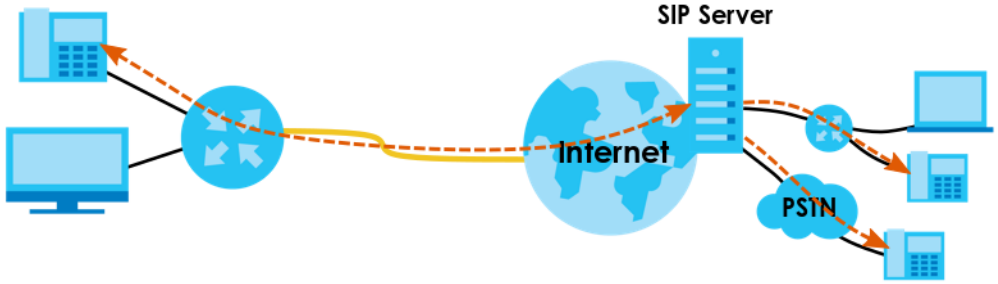
Figure 2 Dual-Band Application



1.2.3 VoIP Application

The Zyxel Device's VoIP function allows you to register up to 2 SIP (Session Initiation Protocol) accounts and use the Zyxel Device to make and receive VoIP telephone calls. The Zyxel Device sends your call to a VoIP service provider's SIP server which forwards the calls to either VoIP or PSTN phones.

Figure 3 VoIP Application



1.3 Ways to Manage the Zyxel Device

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

- Web Configurator. This is recommended for management of the Zyxel Device using a (supported) web browser.
- Simple Network Management Protocol (SNMP). Use for collecting and organizing information about the Zyxel Device and for modifying that information to change the Zyxel Device behavior.
- Secure Shell (SSH), Telnet. Use for troubleshooting the Zyxel Device by qualified personnel.
- FTP. Use FTP for firmware upgrades and configuration backup/restore.

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

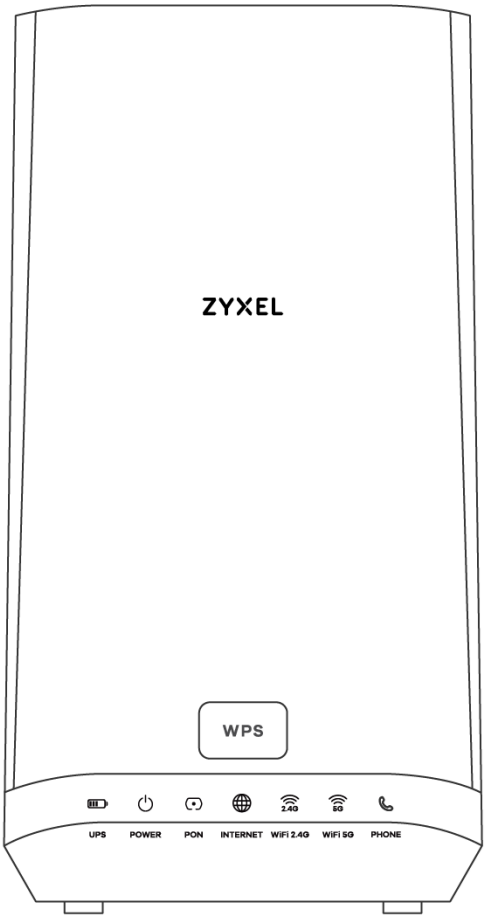
1.5 Hardware

This section describes the front and rear panels for each model. If your model is not shown here, refer to the Zyxel Device's Quick Start Guides to see the product drawings and how to make the hardware connections.

1.5.1 Front Panel

The LED indicators are located on the front panel.

Figure 4 LED Indicators



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

Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
UPS	Green	On	The main power is off, and the Zyxel Device is receiving power from the connected UPS (battery backup).
		Blinking	The Zyxel Device is not receiving backup power properly. The connected UPS may have low voltage output.
		Off	The Zyxel Device is not receiving power from the connected UPS (battery backup).

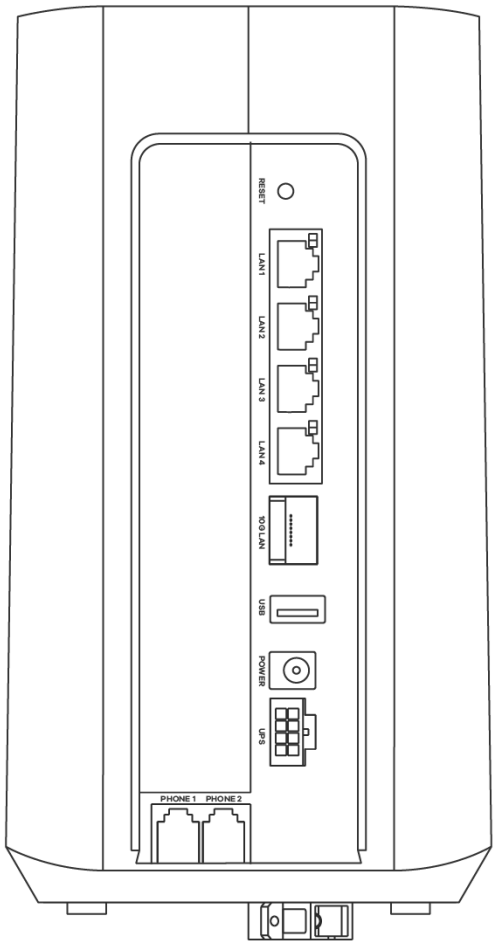
Table 2 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Zyxel Device is receiving power and ready for use.
		Blinking	The Zyxel Device is self-testing.
	Red	On	The Zyxel Device detected an error while self-testing, or there is a device malfunction.
		Blinking	The Zyxel Device is upgrading firmware.
		Off	The Zyxel Device is not receiving power.
PON	Green	On	The PON port is connected to the ISP's ONT and the Zyxel Device is receiving optical signals normally.
		Blinking	The Zyxel Device's PON port is trying to build a PON connection.
	Red	Blinking	The receive optical power (the strength of optical signals transmitted on the remote optical module) is too low.
		On	The connection to the ISP's ONT is down.
INTERNET	Green	On	The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used).
		Blinking	The Zyxel Device is sending or receiving IP traffic.
		Off	There is no Internet connection or the gateway is in bridged mode.
	Red	On	The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
2.4G WiFi	Green	On	The 2.4G wireless network is activated.
		Blinking	The Zyxel Device is communicating with 2.4G wireless clients.
		Off	The 2.4G wireless network is not activated.
5G WiFi	Green	On	The 5G wireless network is activated.
		Blinking	The Zyxel Device is communicating with 5G wireless clients.
		Off	The 5G wireless network is not activated.
PHONE	Green	On	A SIP account is registered for the phone port.
		Blinking	The telephone connected to this phone port has an incoming call or is off the hook.
		Off	The phone port does not have a SIP account registered.
	Amber	On	A SIP account is registered for the phone port, and there is a voice message in the corresponding SIP account.
		Blinking	The telephone connected to this phone port has an incoming call or is off the hook. There is a voice message in the corresponding SIP account.
WPS	Green	Blinking	The Zyxel Device is setting up a WPS connection with a wireless client.
		Off	The Zyxel Device has set up a WPS connection with a wireless client or WPS has not been enabled.

1.5.2 Rear Panel

The connection ports are located on the rear panel.

Figure 5 Rear Panel



The following table describes the items on the rear panel.

Table 3 Panel Ports and Buttons

LABEL	DESCRIPTION
Reset	Press the button to return the Zyxel Device to the factory defaults.
LAN1 ~ LAN4 10G LAN	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
USB	The USB port is reserved for future development.
Power	Connect the power adapter and press the power button to start the device.
UPS	Connect a UPS (Uninterruptible Power Supply) to the **UPS** port to have a backup power source when the main power fails.
PHONE 1/2	Connect analog phones to the **PHONE** ports to make phone calls.
PON	Connect the fiber optic cable to the **PON** port for Internet access.

1.5.3 The WPS Button

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

To activate WPS:

1 Make sure the **POWER** LED is on and not blinking.

2 Press the **WPS** button for one second and release it.

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

4 Once the connection is successfully made, the **WPS** LED will turn off.

Note: Your Zyxel Device supports both 2.4G and 5G WiFi networks, the connection to the 2.4G wireless network has priority.

1.5.4 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to the factory default (see the device label), and the LAN IP address will be "192.168.1.1".

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for more than 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.5.5 The UPS Port

You can connect a UPS to the UPS port to keep the Zyxel Device running in case the main power fails.

The following diagram and chart show the pin assignments of the UPS port on the Zyxel Device.

Figure 6 UPS Port Pin Layout

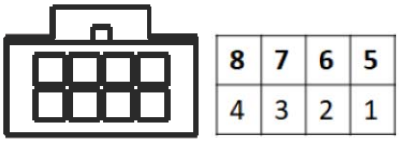


Table 4 UPS Port Pin Assignment

PIN NUMBER	DESCRIPTION
1	Power Input +12V
2	On Battery
3	Missing Battery
4	12V Power Return
5	12V Power Return
6	Replace Battery
7	Low Battery
8	NC Unused

CHAPTER 2
The Web Configurator

2.1 Overview

The Web Configurator is an HTML-based management interface that allows easy Zyxel Device setup and management via Internet browser. Use Internet Explorer 11 and later versions or Mozilla Firefox 67.0.2 and later versions or Safari 5.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

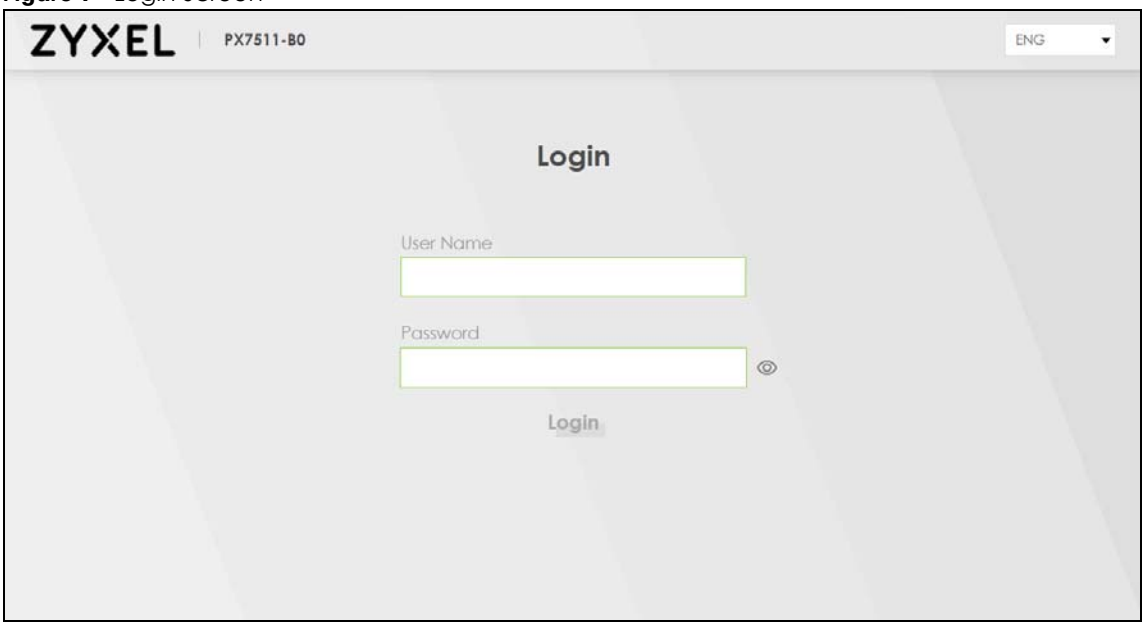
In order to use the Web Configurator you need to allow:

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

2.1.1 Accessing the Web Configurator

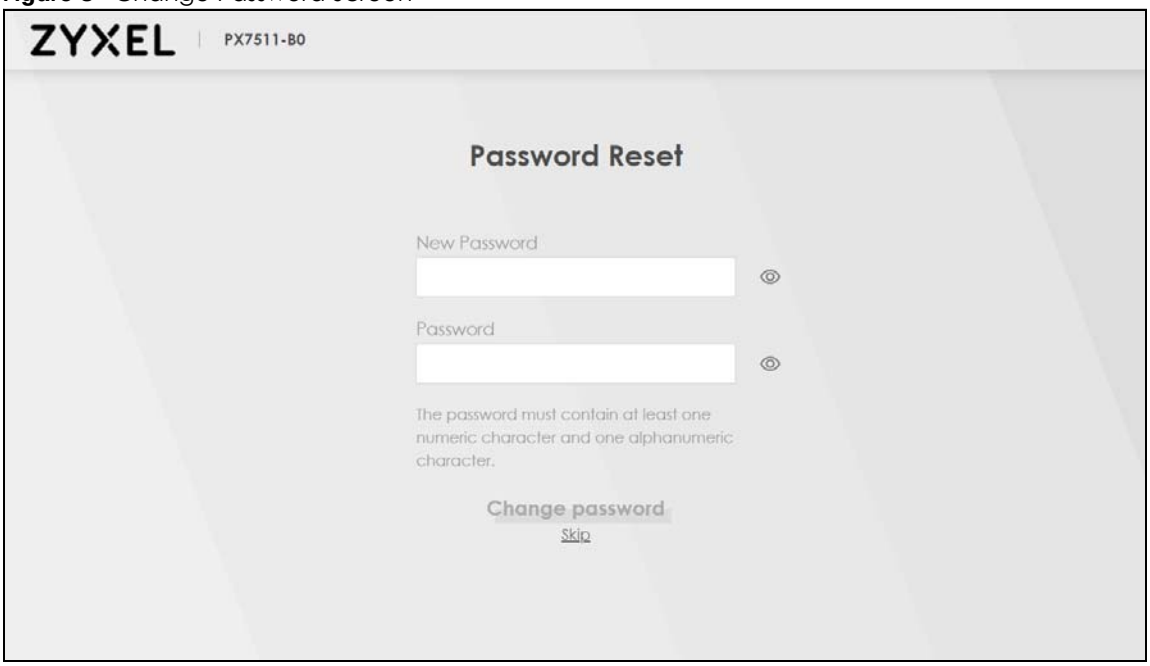
1. Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to http://192.168.1.1.
3. A login screen displays. Select the language you prefer.
4. To access the administrative Web Configurator and manage the Zyxel Device, type the default username **admin** and the randomly assigned default password (see the device label) in the login screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 7 Login Screen



5 The following screen displays when you log into the Web Configurator for the first time. Enter a new password, retype it to confirm, and click **Change password**. If you prefer to use the default password, click **Skip**.

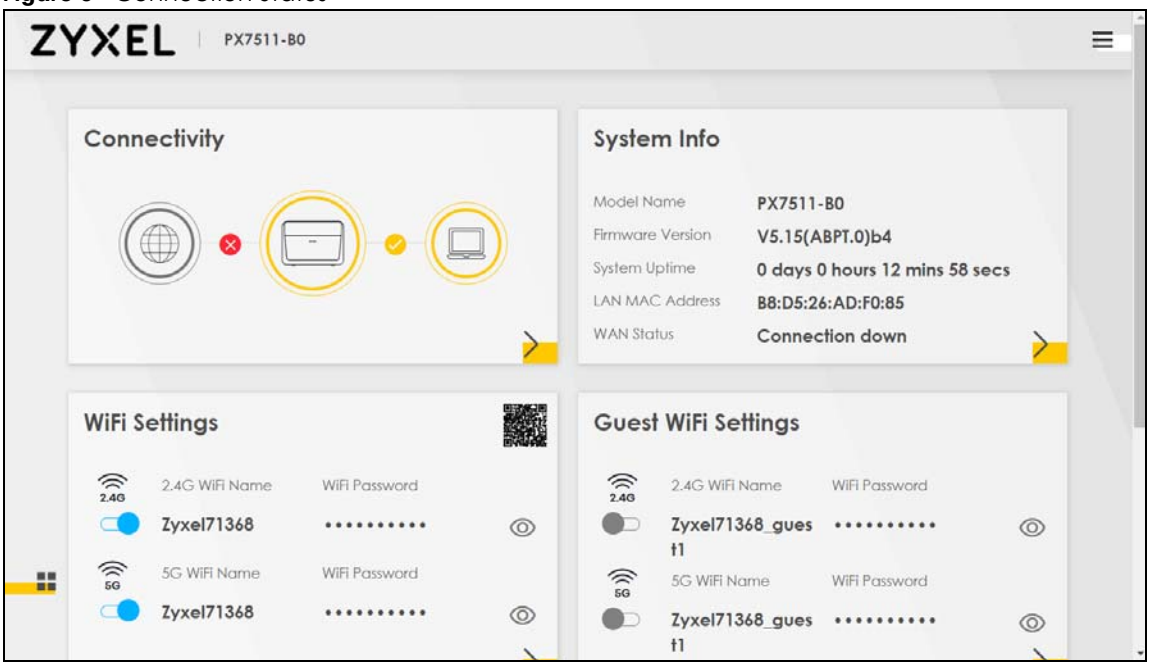
Figure 8 Change Password Screen



6 The **Wizard** screen displays when you log into the Web Configurator for the first time. Use the **Wizard** screens to configure the Zyxel Device's time zone, basic Internet access, and wireless settings. See Chapter 3 on page 32 for more information about the **Wizard** screens.

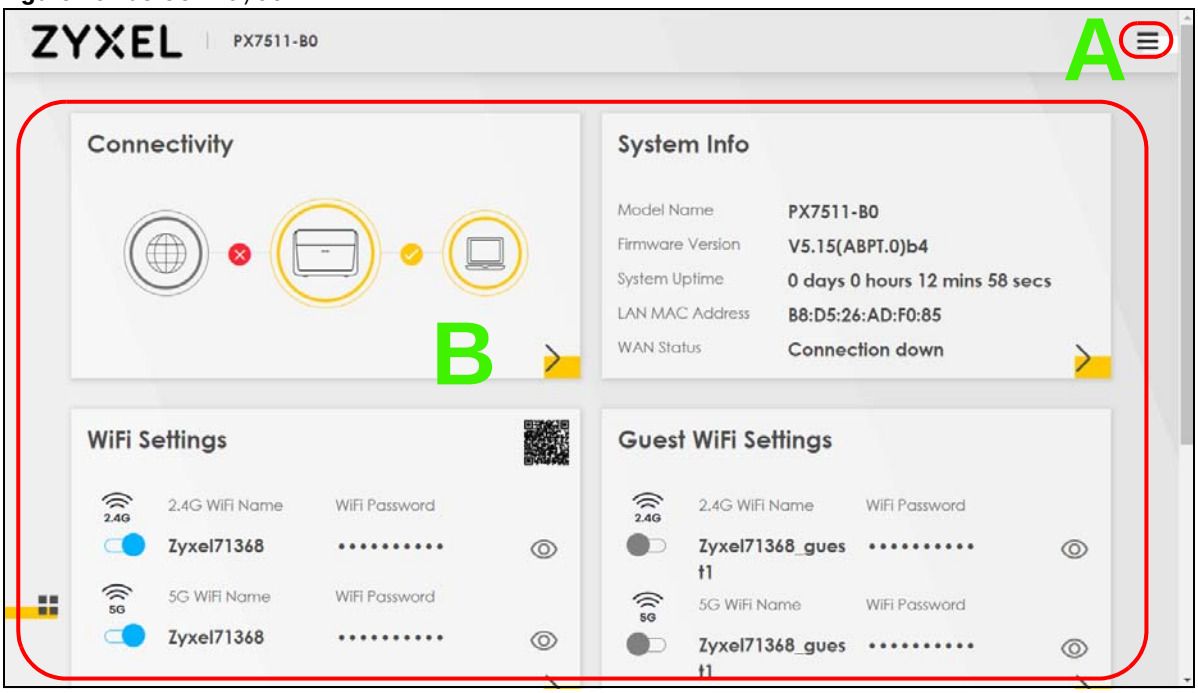
7 The **Connection Status** page appears. Use this screen to configure basic Internet access, wireless settings, and parental control settings. See Chapter 5 on page 60 for more information about the **Connection Status** screen.

Figure 9 Connection Status



2.2 Web Configurator Layout

Figure 10 Screen Layout



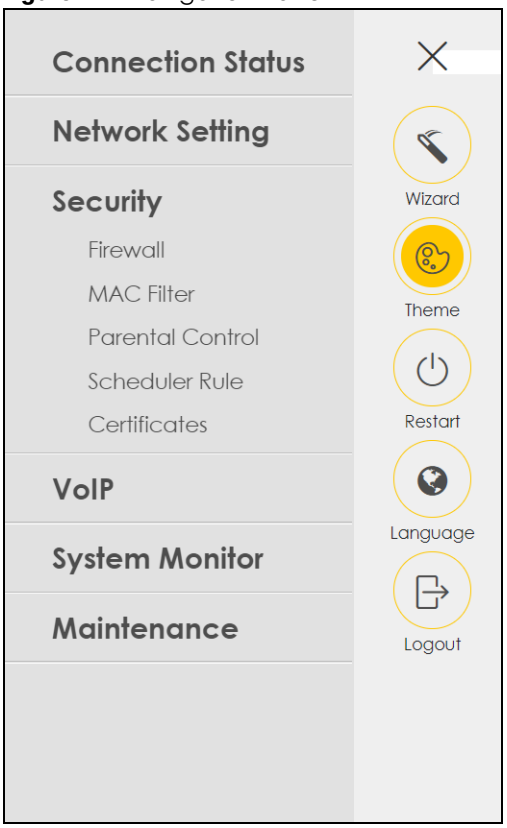
As illustrated above, the main screen is divided into these parts:

- **A** - Navigation Panel
- **B** - Main Window

2.2.1 Navigation Panel

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

Figure 11 Navigation Panel



2.2.1.1 Configuration Menus

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

Table 5 Configuration Menus Summary

LINK	TAB	FUNCTION
Connection Status		Use this screen to configure basic Internet access, wireless settings, and parental control settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.

Table 5 Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to configure the WiFi settings and WLAN authentication/ security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the Zyxel Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	WMM	Use this screen to enable or disable WiFi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan WiFi channel noises and view the results.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	STB Vendor ID	Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses.
	Wake on LAN	Use this screen to remotely turn on a device on the local network.
	TFTP Server Name	Use DHCP option 66 to identify a TFTP server name.
Routing	Static Route	Use this screen to view and set up static routes on the Zyxel Device.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Route	Use this screen to configure policy routing on the Zyxel Device.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
	Policer Setup	Use this screen to configure QoS policers.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Triggering	Use this screen to change your Zyxel Device's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable the ALGs (Application Layer Gateways) in the Zyxel Device to allow applications to operate through NAT.
	Address Mapping	Use this screen to change your Zyxel Device's 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.

Table 5 Configuration Menus Summary (continued)

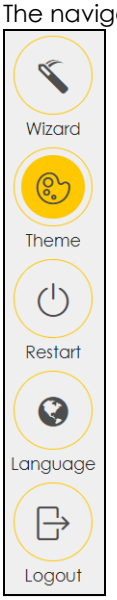
LINK	TAB	FUNCTION
IGMP/MLD	IGMP/MLD	Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN.
VLAN Group	VLAN Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to create multiple networks on the Zyxel Device.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Parental Control	Parental Control	Use this screen to limit the time a user can access the Internet and block the users on your network from accessing certain web sites.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
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.
VoIP		
SIP	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the Zyxel Device.
	SIP Service Provider	Use this screen to configure the SIP server information, and other SIP settings, such as QoS for VoIP calls, outbound proxy, DTMF mode and SIP timers..
Phone	Phone Device	Use this screen to control which SIP account(s) each phone uses to handle outgoing and incoming calls.
	Regine	Use this screen to select your location and call service mode.
Call Rule	Call Rule	Use this screen to configure speed dial for SIP phone numbers that you call often.
Call History	Call History	Use this screen to view detailed information for each outgoing call you made or each incoming call from someone calling you. You can also view a summary list of received, dialed and missed calls.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
	NAT	Use this screen to view NAT statistics for connected hosts.

Table 5 Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
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.
Multicast Status	IGMP Status	Use this screen to view the status of all IGMP settings on the Zyxel Device.
	MLD Status	Use this screen to view the status of all MLD settings on the Zyxel Device.
WLAN Station Status	WLAN Station Status	Use this screen to view the wireless stations that are currently connected to the Zyxel Device.
xPON Status	xPON Status	Use this screen to view the fiber optical transceiver's TX power and RX power level and its temperature.
Maintenance		
System	System	Use this screen to set Device name and Domain name.
User Account	User Account	Use this screen to change user password on the Zyxel Device.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** > **MGMT Services** screen.
SNMP	SNMP	Use this screen to configure SNMP (Simple Network Management Protocol) settings.
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 Setting	Use this screen to change your Zyxel Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems.
GPON	SLID	Use this screen to change your Zyxel Device's Subscriber Location ID (SLID) setting. The SLID identifies your device to the GPON service provider's Optical Line Terminal (OLT).

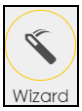
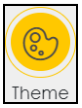
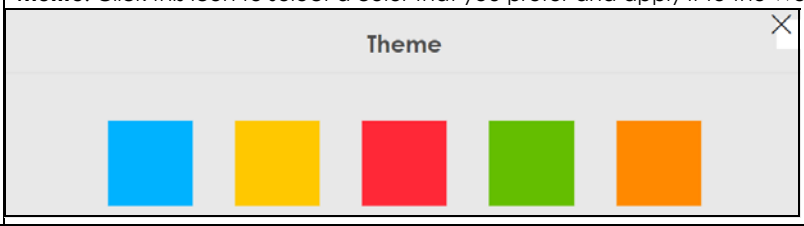
2.2.1.2 Icons

The navigation panel provides some icons on the right hand side.



The icons provide the following functions.

Table 6 Web Configurator Icons

ICON	DESCRIPTION
	**Wizard**: Click this icon to open screens where you can configure the Zyxel Device's time zone Internet access, and wireless settings. See Chapter 3 on page 32 for more information about the **Wizard** screens.
	**Theme**: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
	Restart: Click this icon to reboot the Zyxel Device without turning the power off.
	Language: Select the language you prefer.
	Logout: Click this icon to log out of the Web Configurator.

CHAPTER 3
Quick Start Wizard

3.1 Overview

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

Note: See the technical reference chapters (starting on Chapter 4 on page 37) for background information on the features in this chapter.

3.2 Wizard Setup

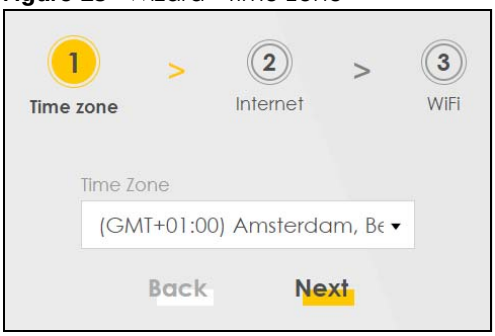
You can click the **Wizard** icon in the navigation panel to open the **Wizard** screens. See Section 2.2.1 on page 27 for more information about the navigation panel. After you click the **Wizard** icon, the following screen appears. Click **Let's Go** to proceed with settings on time zone, basic Internet access, and wireless networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can also click **Skip** to leave the **Wizard** screens.

Figure 12 Wizard - Home

3.2.1 Time Zone

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

Figure 13 Wizard - Time Zone



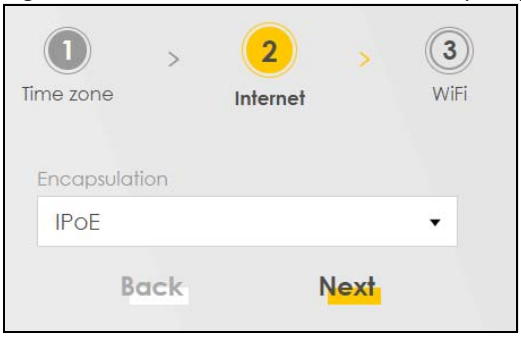
3.2.2 Internet

1 The Zyxel Device will check the Internet status automatically, and determine your connection type. Click **Next** to proceed. You can also click **Skip** to pass Internet settings in the **Wizard**.

Figure 14 Wizard - Internet

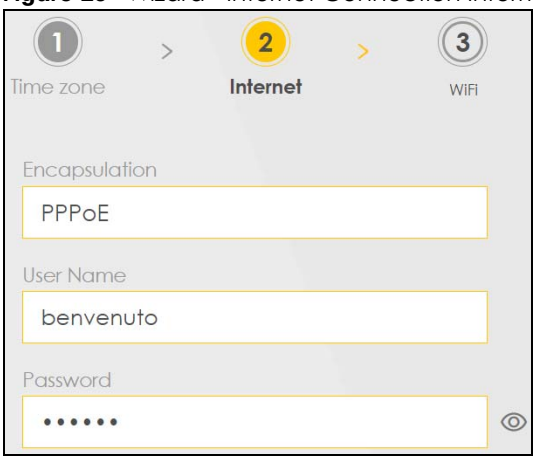
2 If the following screen displays, select the encapsulation type your ISP uses. Click **Next**.

Figure 15 Wizard - Internet Information (IPoE)



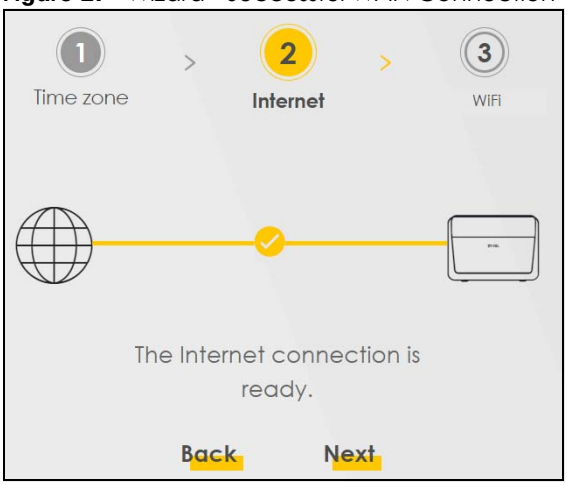
Enter your Internet connection information. The screen and fields to enter may vary depending on your current connection type. Click **Next**.

Figure 16 Wizard - Internet Connection Information (PPPoE)



3 Click **Next** when the Zyxel Device has a successful Internet connection.

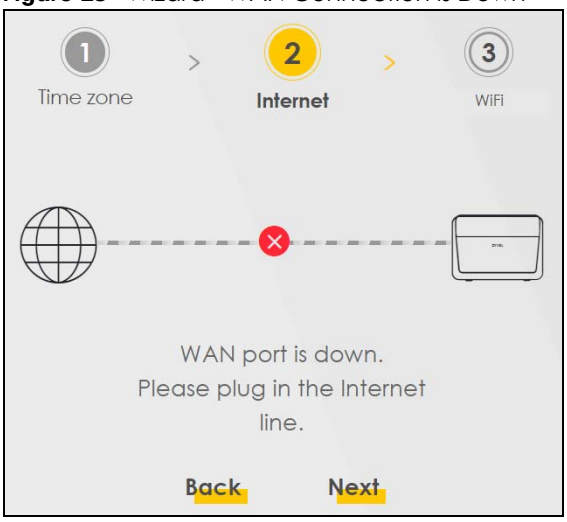
Figure 17 Wizard - Successful WAN Connection



Unsuccessful Internet Connection

The following screen displays when the Zyxel Device did not detect a WAN connection. Connect a fiber optic cable to the PON port for Internet access if you have not connected any.

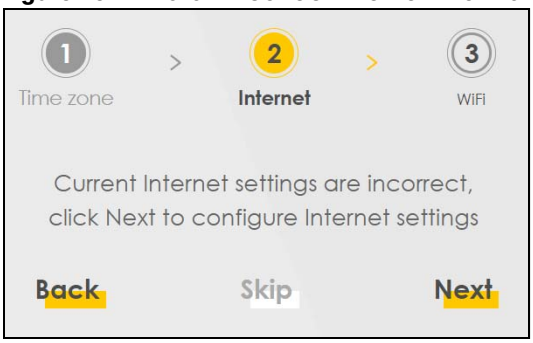
Figure 18 Wizard - WAN Connection is Down



Incorrect Internet Information

If the following screen displays, click **Next** to configure the Internet settings.

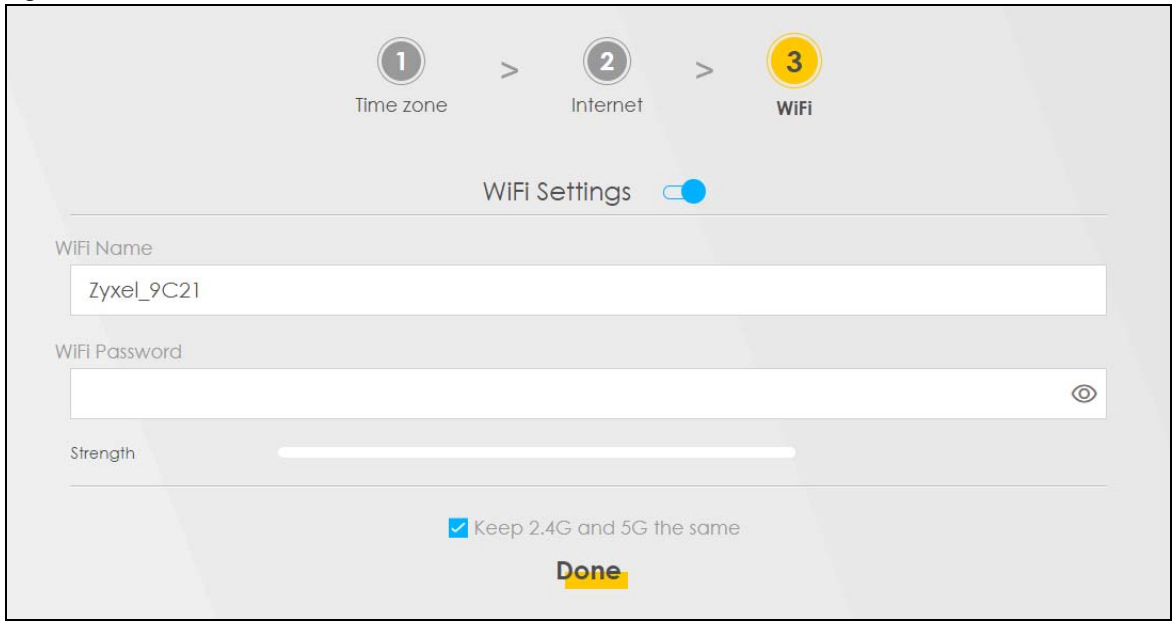
Figure 19 Wizard - Incorrect Internet Information



3.2.3 WiFi

Turn WiFi on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the Zyxel Device.
Click the **Keep 2.4G and 5G the same** check box to use the same SSID for 2.4G and 5G wireless networks. Otherwise, deselect the check box to have two different SSIDs for 2.4G and 5G wireless networks. The screen and fields to enter may vary when you select or deselect the check box.
Click **Done** to complete the setup.

Figure 20 Wizard - WiFi



CHAPTER 4
Tutorials

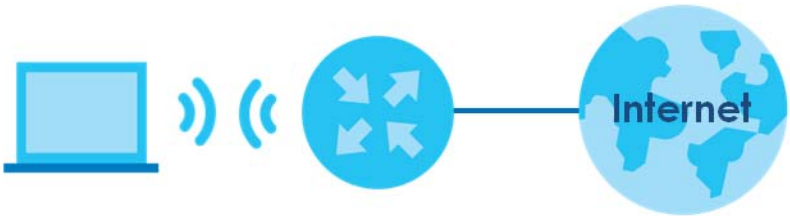
4.1 Overview

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

- Setting Up a Secure Wireless Network, see page 37
- Setting Up Multiple Wireless Groups, see page 44
- Configuring Static Route for Routing to Another Network, see page 49
- Configuring QoS Queue and Class Setup, see page 51
- Access the Zyxel Device Using DDNS, see page 55
- Configuring the MAC Address Filter, see page 57

4.2 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the Zyxel Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



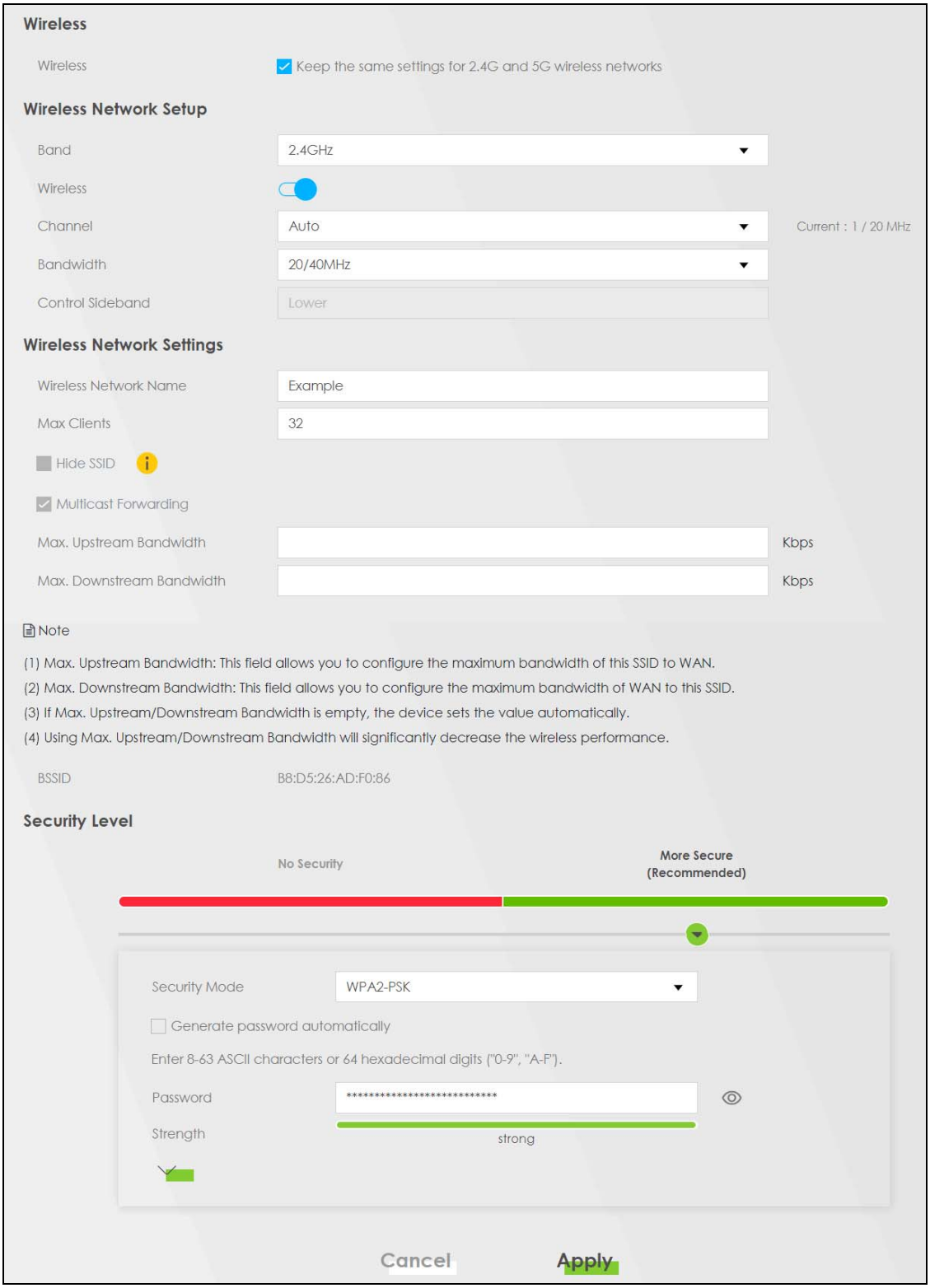
Thomas has to configure the wireless network settings on the Zyxel Device. Then he can set up a wireless network using WPS (Section 4.2.2 on page 39) or manual configuration (Section 4.2.3 on page 43).

4.2.1 Configuring the Wireless Network Settings

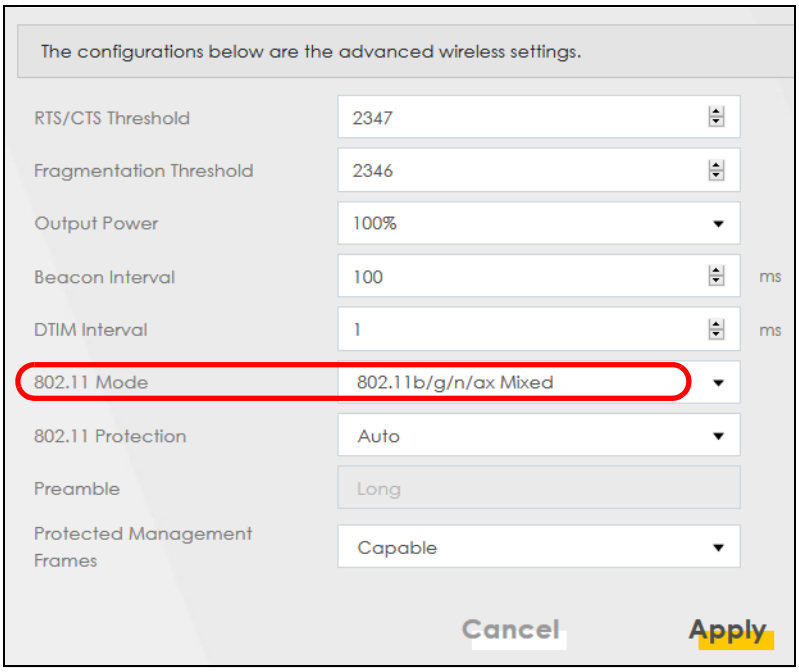
This example uses the following parameters to set up a wireless network.

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

1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see page 37). Click **Apply**.



2 Go to the **Wireless > Others** screen and select **802.11b/g/n/ax Mixed** in the **802.11 Mode** field. Click **Apply**.



Thomas can now use the WPS feature to establish a wireless connection between his notebook and the Zyxel Device (see Section 4.2.2 on page 39). He can also use the notebook's wireless client to search for the Zyxel Device (see Section 4.2.3 on page 43).

4.2.2 Using WPS

This section gives you an example of how to set up a wireless network using WPS. This example uses the Zyxel Device as the AP and a WPS-enabled Android smartphone as the wireless client.

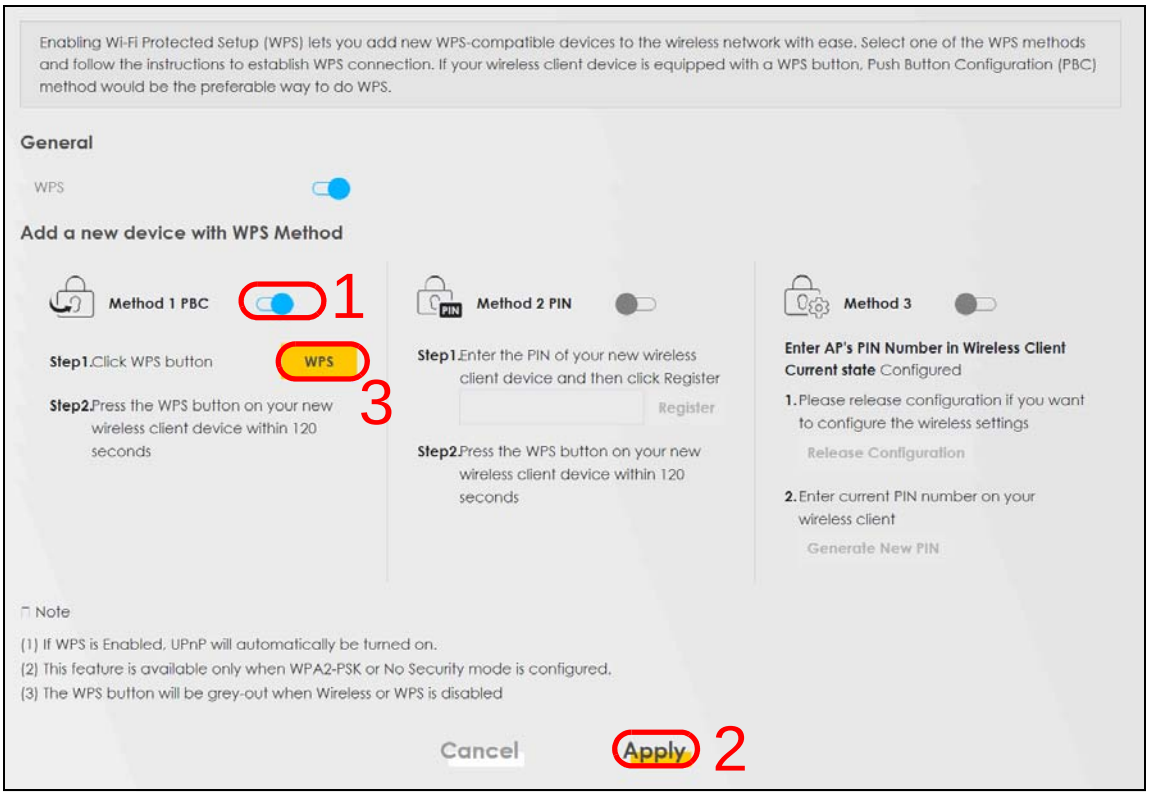
There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section on page 39. This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the Zyxel Device's interface. See Section on page 41. This is the more secure method, since one device can authenticate the other.

Push Button Configuration (PBC)

1 Make sure that your Zyxel Device is turned on and your notebook is within the cover range of the wireless signal.

2 Push and hold the **WPS** button located on the Zyxel Device's front panel for one second. Alternatively, you may log into the Zyxel Device's Web Configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function for method 1 and click **Apply**. Then click the **Connect** button.



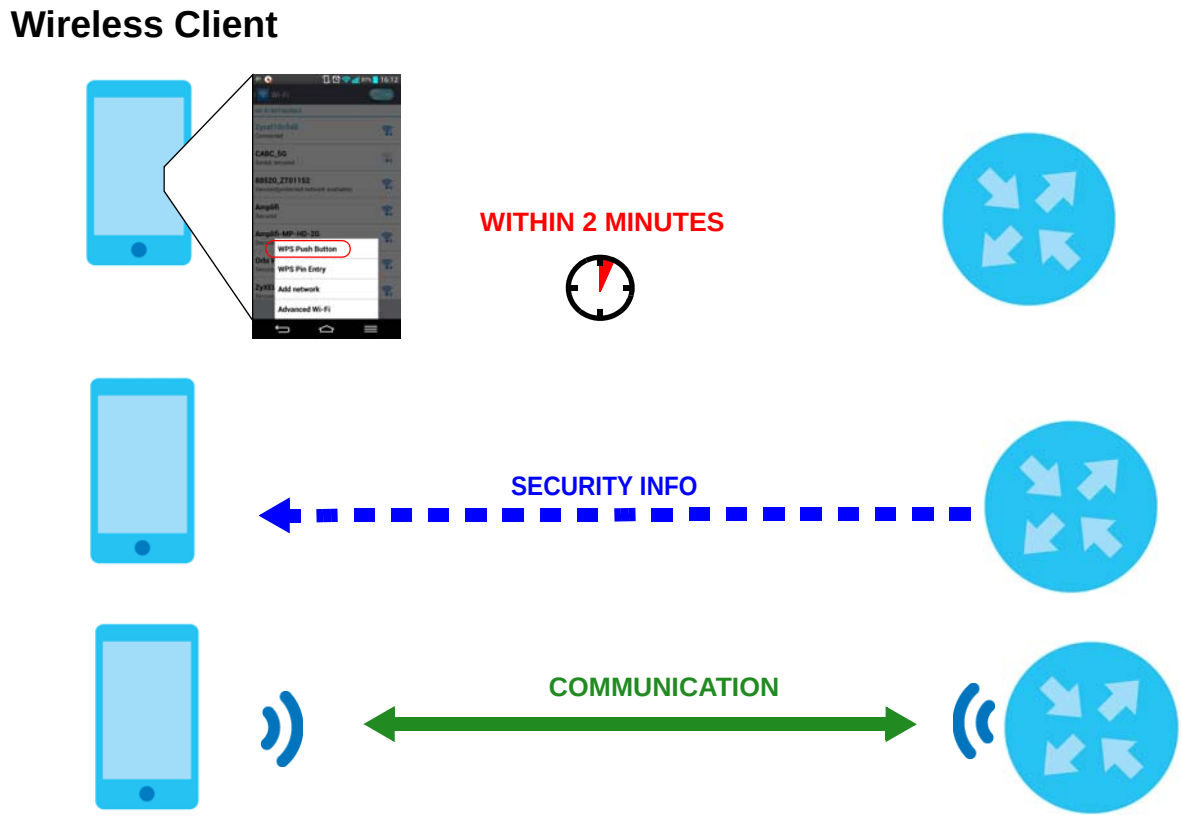
Note: Your Zyxel Device has a WPS button located on its side panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It does not matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The Zyxel Device sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Zyxel Device securely.

The following figure shows you how to set up wireless network and security by pressing a button on both Zyxel Device and wireless client (the Android phone in this example).

Figure 21 Example WPS Process: PBC Method

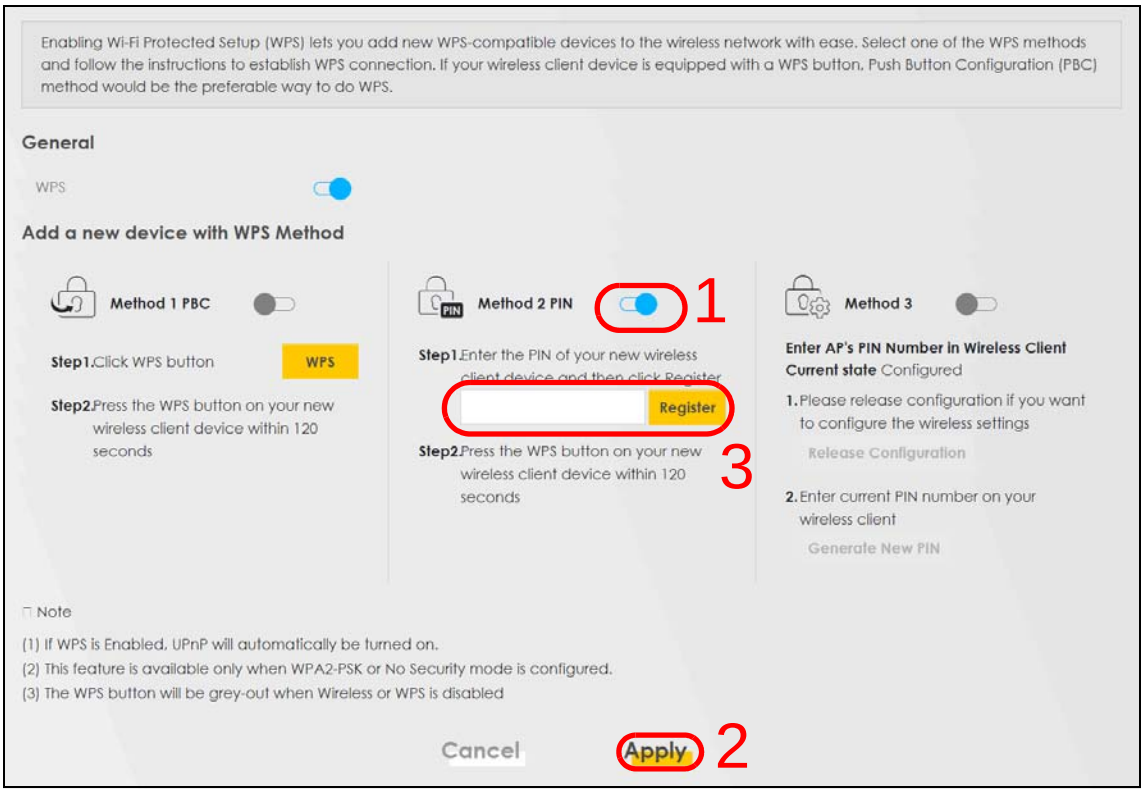


PIN Configuration

When you use the PIN configuration method, you need to check the client's PIN number and use the Zyxel Device's configuration interface.

1 Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap **WPS PIN Entry** to get a PIN number.

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

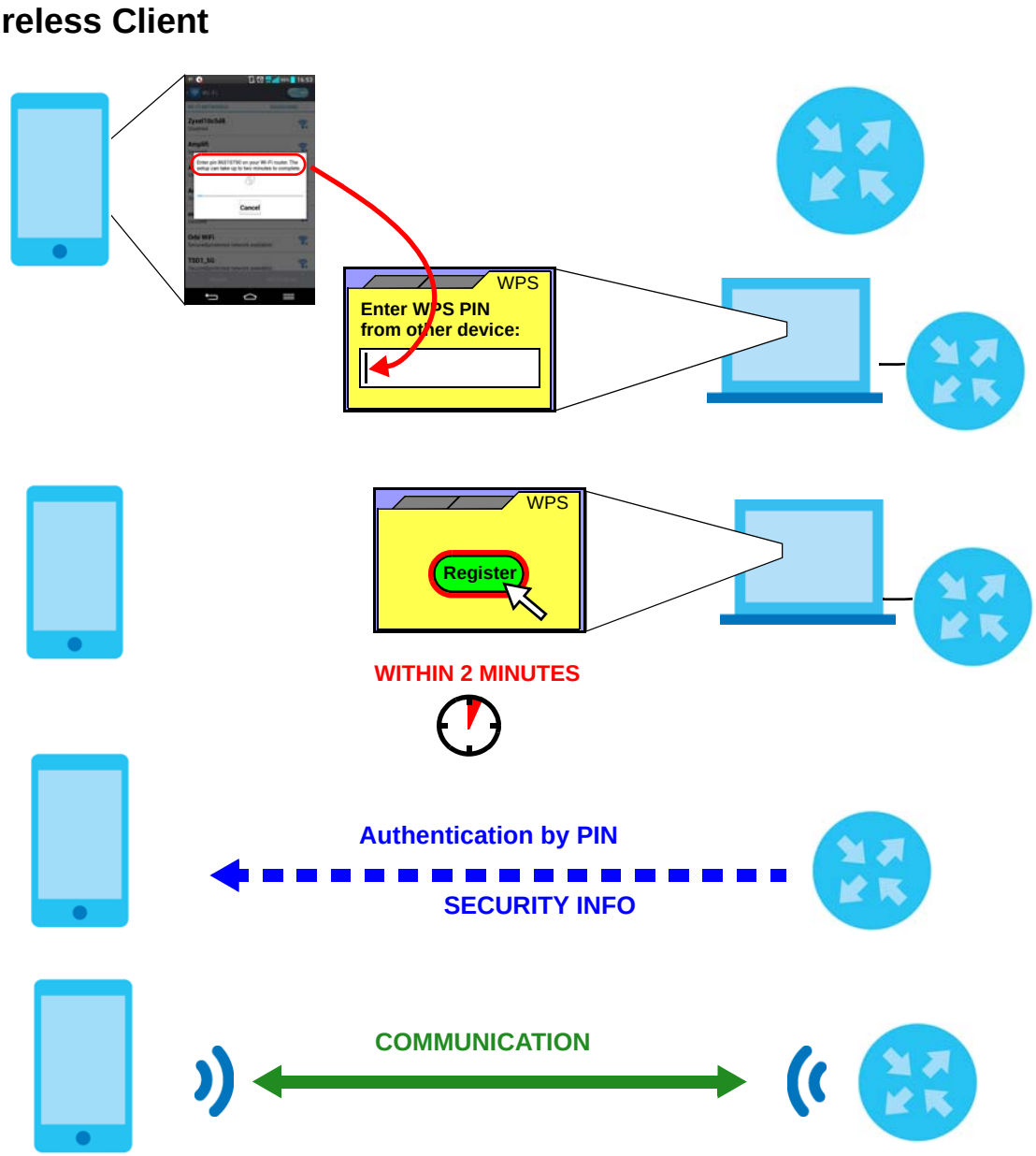


3 Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.

The Zyxel Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Zyxel Device securely.

The following figure shows you how to set up wireless network and security on Zyxel Device and wireless client (Android smartphone in this example) by using the PIN method.

Figure 22 Example WPS Process: PIN Method



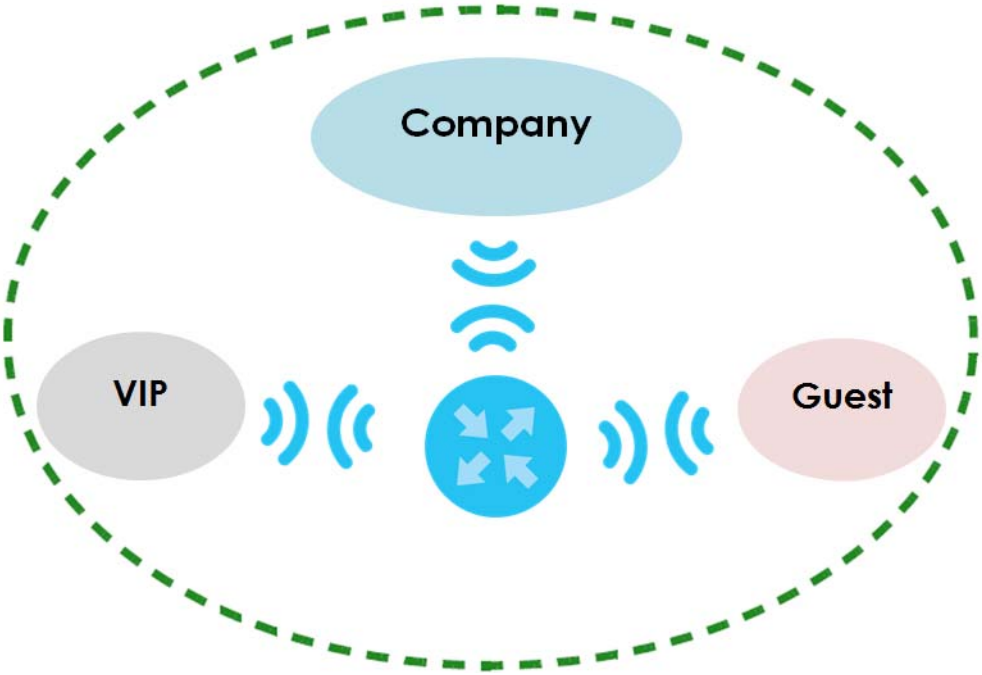
4.2.3 Without WPS

Use the wireless adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish a wireless Internet connection.

Note: The Zyxel Device supports IEEE 802.11a/b/g/n/ac/ax wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

4.3 Setting Up Multiple Wireless Groups

Company A wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own SSID and security mode.



- Employees in Company A will use a general **Company** wireless network group.
- Higher management level and important visitors will use the **VIP** group.
- Visiting guests will use the **Guest** group, which has a different SSID and password.

Company A will use the following parameters to set up the wireless network groups.

	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK	WPA2-PSK
Pre-Shared Key	ForCompanyOnly	123456789	guest123

1 Click **Network Setting > Wireless** to open the **General** screen. Use this screen to set up the company's general wireless network group. Configure the screen using the provided parameters and click **Apply**.

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 the same settings for 2.4G and 5G wireless networks

Wireless Network Setup

Band: 2.4GHz

Wireless

Channel: Auto — Current : / MHz

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Company

Max Clients: 32

Hide SSID — Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.

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.

BSSID

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: For CompanyOnly

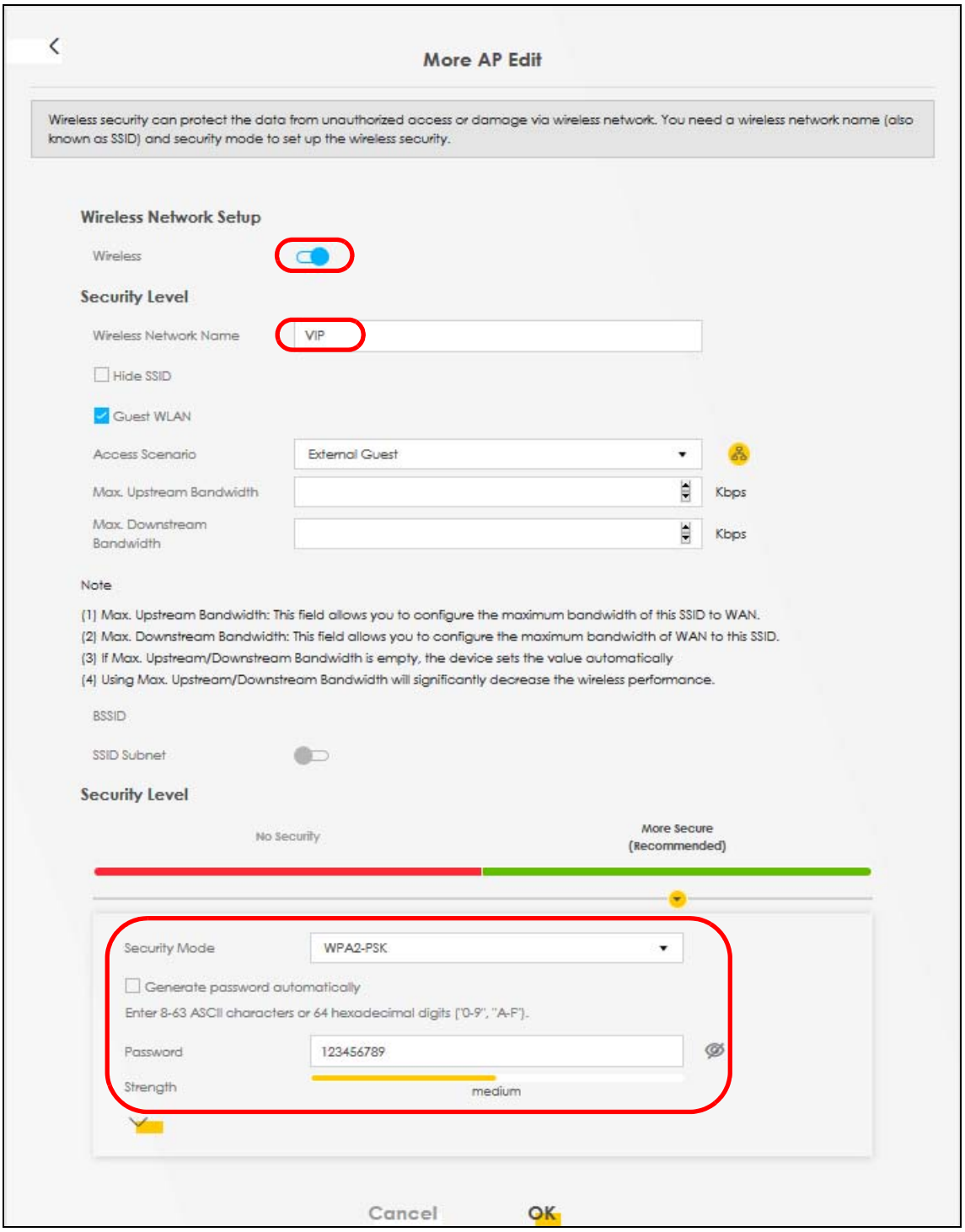
Strength: strong

Cancel Apply

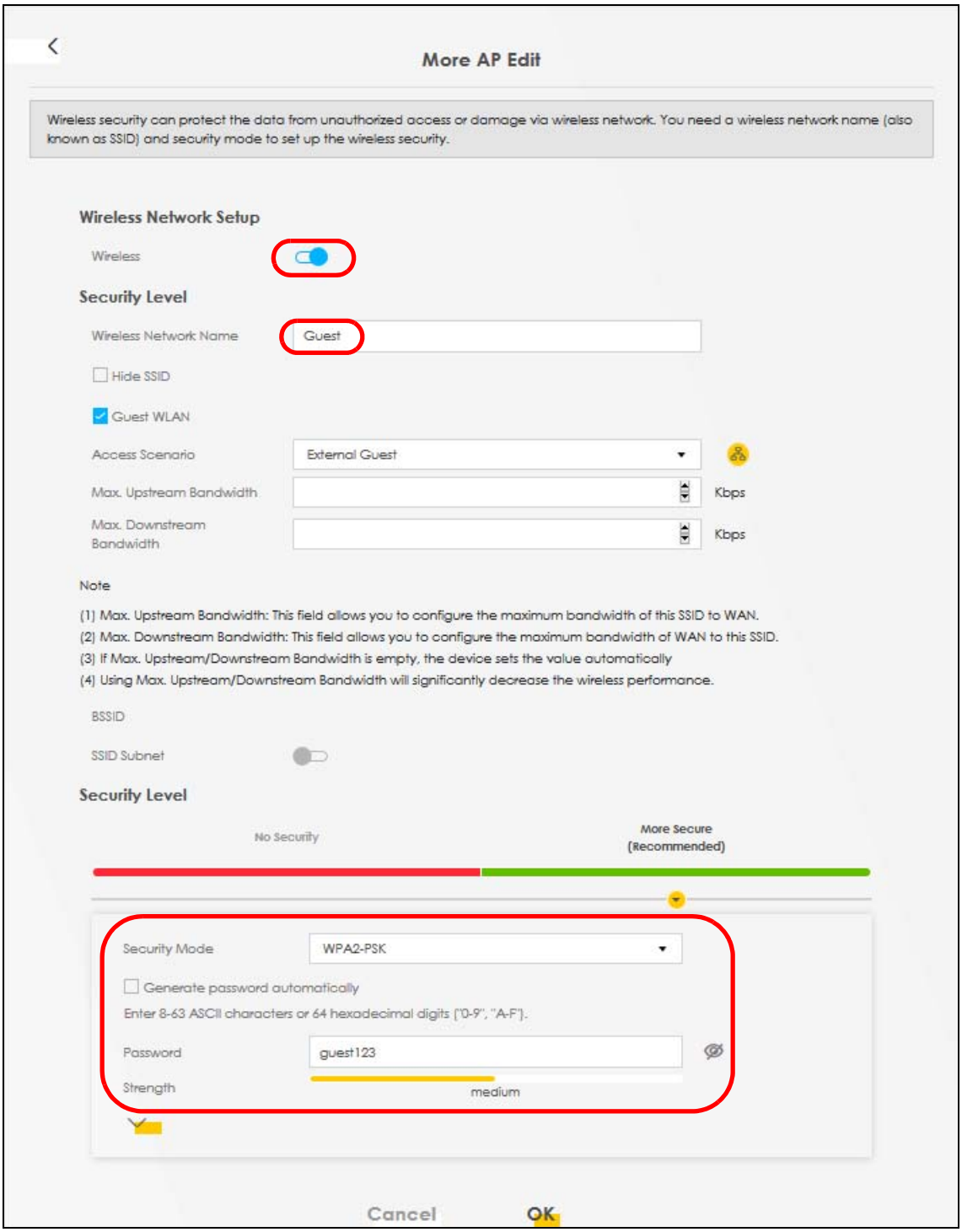
2 Click **Network Setting > Wireless > Guest/More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.

#	Status	SSID	Security	Guest WLAN	Modify
1		Zyxel_9DE5_guest1	WPA2-Personal	External Guest	
2		Zyxel_9DE5_guest2	WPA2-Personal	External Guest	
3		Zyxel_9DE5_guest3	WPA2-Personal	External Guest	

3 Configure the screen using the provided parameters and click **Apply**.



4 In the **Guest/More AP** screen, click the **Edit** icon to configure the third wireless network group. Configure the screen using the provided parameters and click **Apply**.



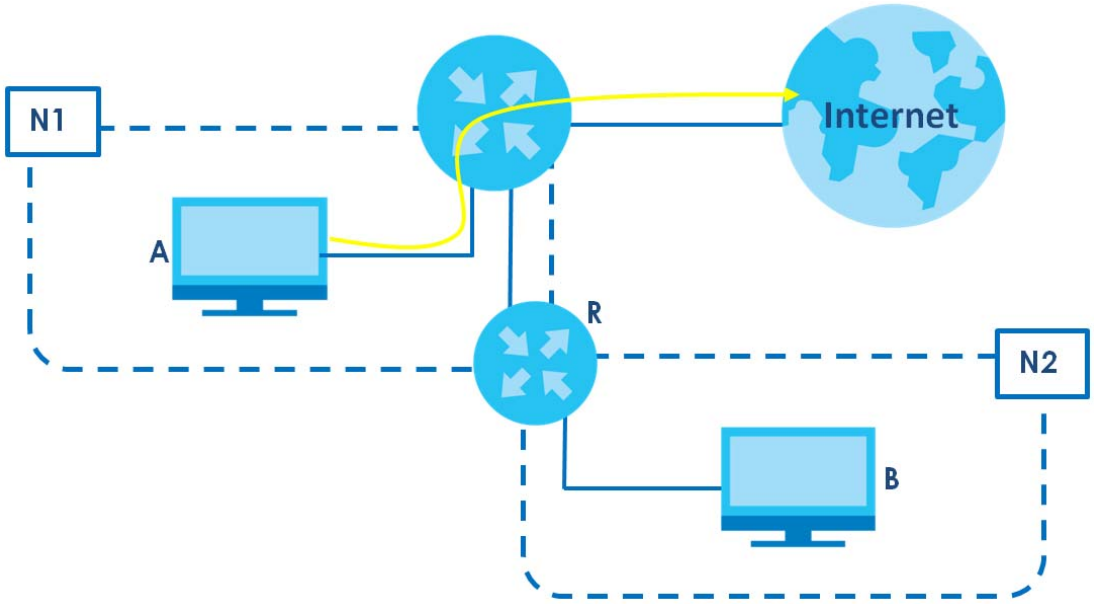
5 Check the status of **VIP** and **Guest** in the **Guest/More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

#	Status	SSID	Security	Guest WLAN	Modify
1		Home&Life SuperWIFI-F0FD_guest1	WPA2-Personal	External Guest	
2		VIP	WPA2-Personal	External Guest	
3		Guest	WPA2-Personal	External Guest	

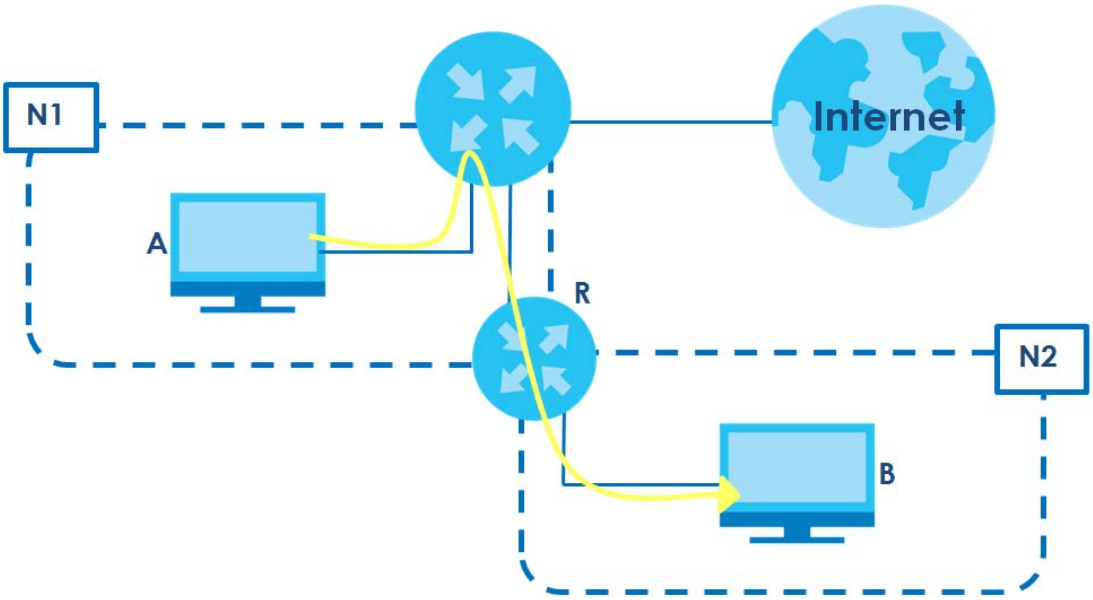
4.4 Configuring Static Route for Routing to Another Network

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 7 IP Settings in this Tutorial

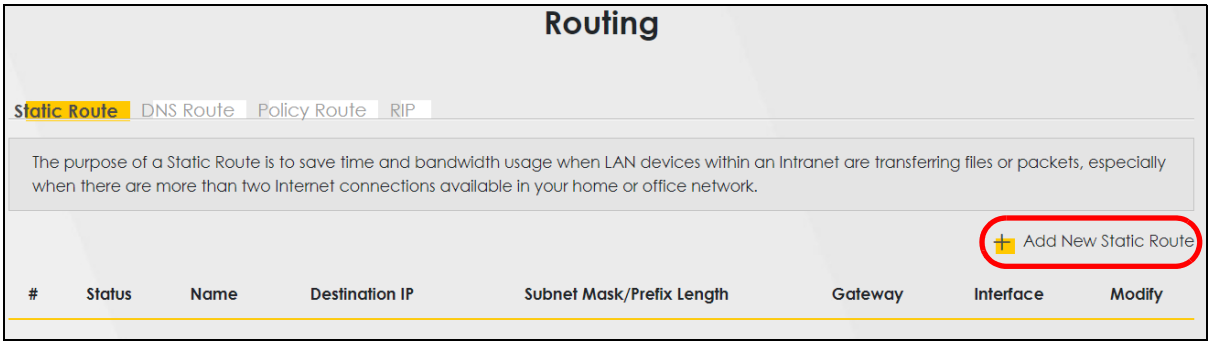
DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	192.168.1.1
IP Type	IPv4
Use Interface	Ethernet
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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 Create a new static route using the following settings:

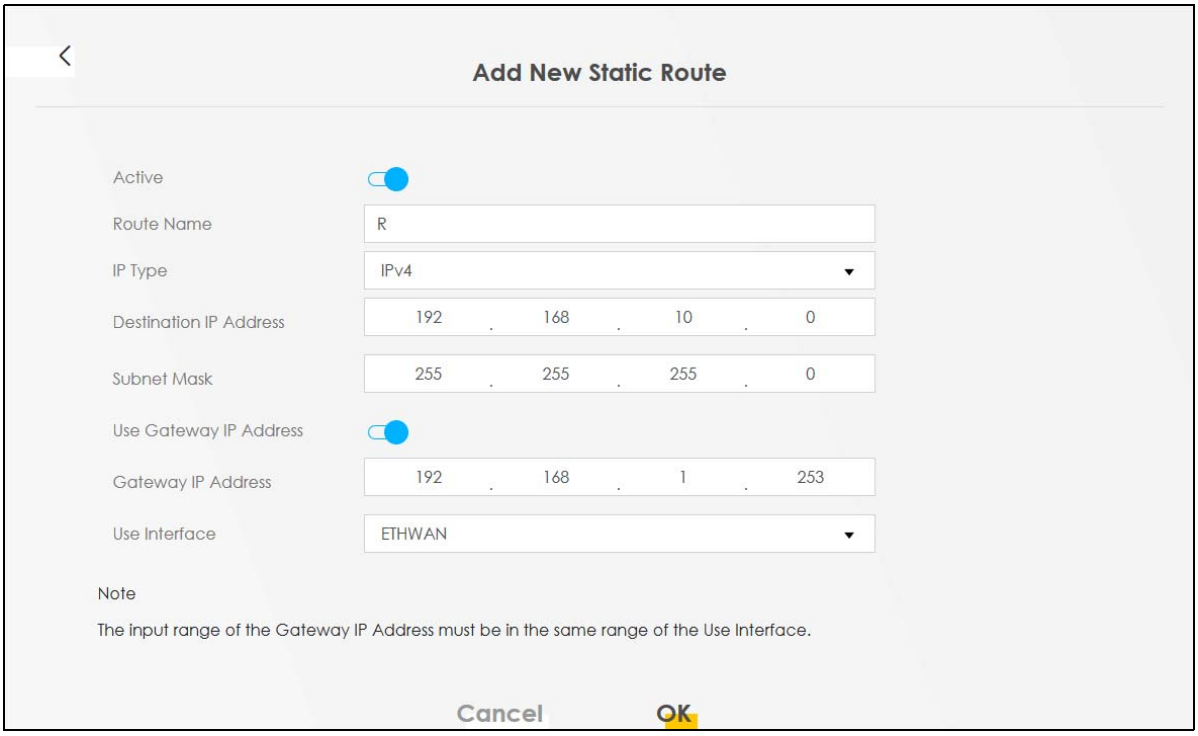
4a Click the **Active** button to enable this static route. When the switch goes to the right ( ), the function is enabled. Enter the **Route Name** as **R**.

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 **ETHWAN** as the **Use Interface**.



4a 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.

4.5 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

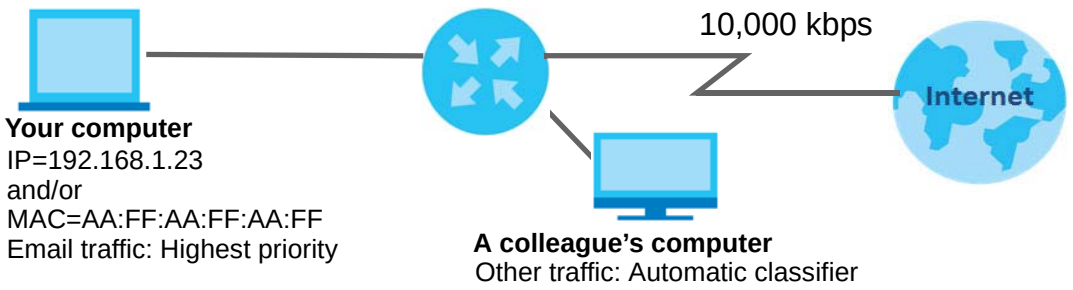
Let us say you are a team leader of a small sales branch office. You want to prioritize email traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and email archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that email traffic gets the highest priority with at least 5,000 kbps. You can do the following:

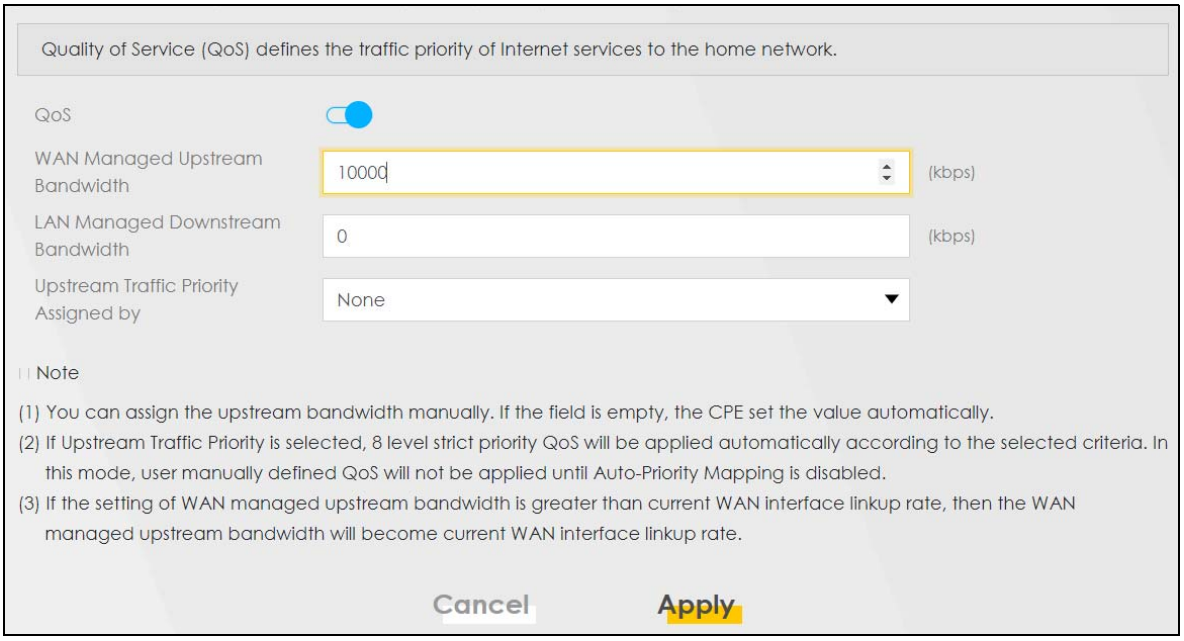
- Configure a queue to assign the highest priority queue (1) to email traffic going to the WAN interface, so that email traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the Zyxel Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the Zyxel Device.



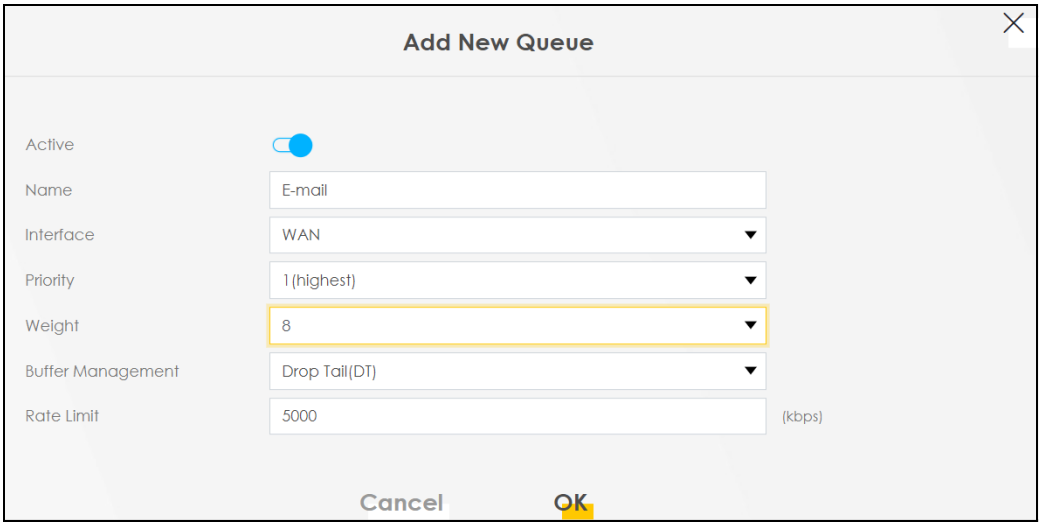
1 Click **Network Setting > QoS > General** and click the **QoS** button to enable. When the switch goes to the right ( ), the function is enabled. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Zyxel Device automatically determine this figure). Click **Apply**.



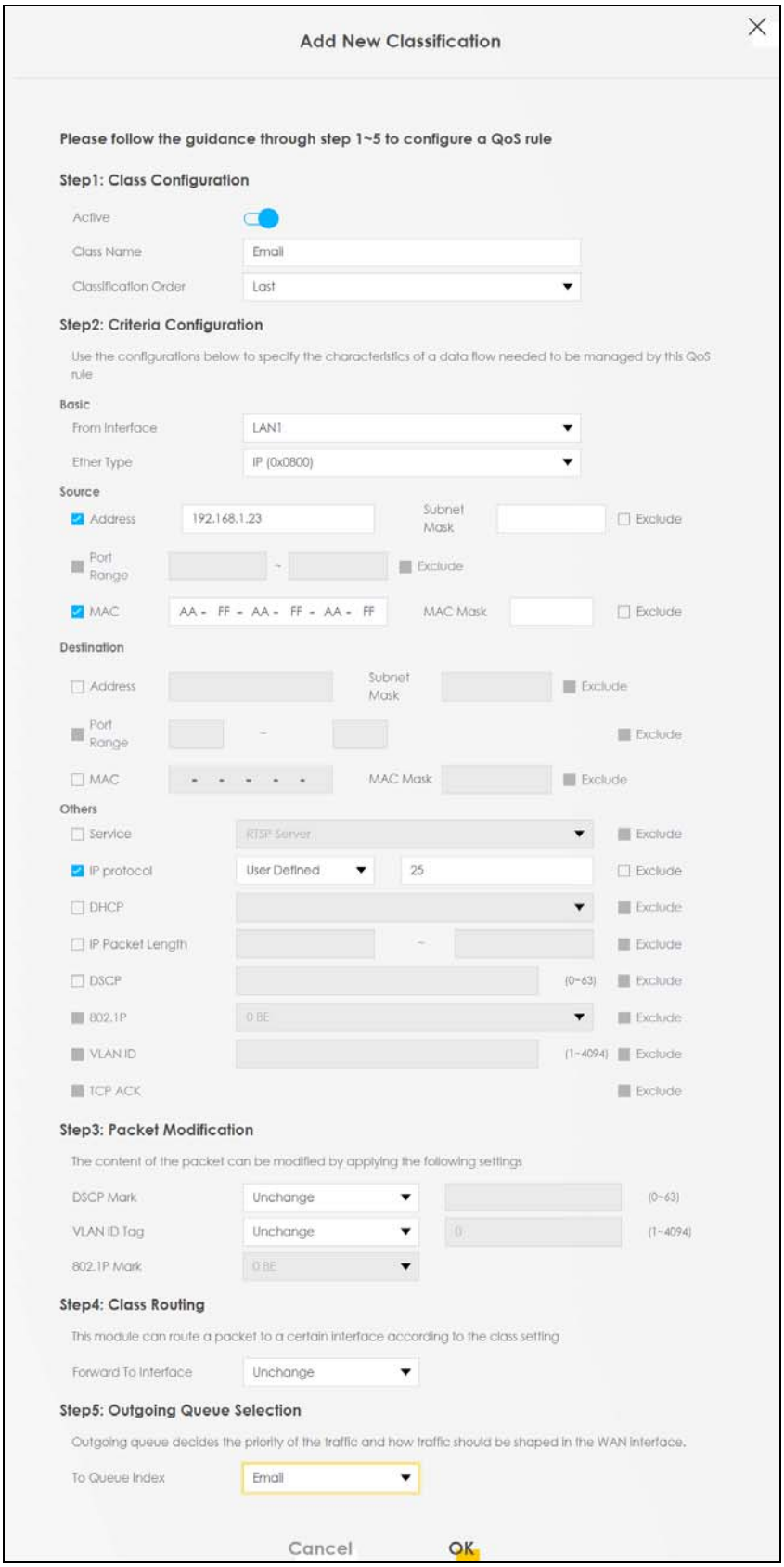
2 Click **Network** > **Queue Setup** > **Add new Queue** to create a new queue. In the screen that opens, click the **Active** field to enable. When the switch goes to the right ( ), the function is enabled. Enter or select the following values:

- **Name**: Email

- **Interface**: **WAN**
- **Priority**: 1 (High)
- **Weight**: 8
- **Rate Limit**: 5,000 (kbps)



3 Click **Network** > **QoS** > **Classification Setup** > **Add new Classification** to create a new class. Select **Enable** in the **Active** field and follow the settings as shown in the screen below.

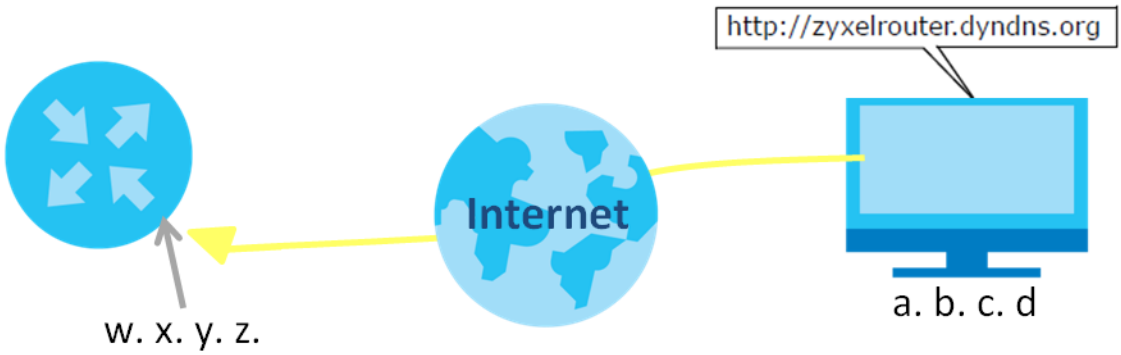

Add New Classification
Please follow the guidance through step 1~5 to configure a QoS rule
Step1: Class Configuration
Active
Class Name
Email
Classification Order
Last
Step2: Criteria Configuration
Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule
Basic
From Interface
LAN1
Ether Type
IP (0x0800)
Source
Address
192.168.1.23
Subnet Mask
Exclude
Port Range
Exclude
MAC
AA - FF - AA - FF - AA - FF
MAC Mask
Exclude
Destination
Address
Subnet Mask
Exclude
Port Range
Exclude
MAC
MAC Mask
Exclude
Others
Service
RTSP Server
Exclude
IP protocol
User Defined
25
Exclude
DHCP
Exclude
IP Packet Length
Exclude
DSCP
(0~63)
Exclude
802.1P
0 BE
Exclude
VLAN ID
(1~4094)
Exclude
TCP ACK
Exclude
Step3: Packet Modification
The content of the packet can be modified by applying the following settings
DSCP Mark
Unchange
(0~63)
VLAN ID Tag
Unchange
0
(1~4094)
802.1P Mark
0 BE
Step4: Class Routing
This module can route a packet to a certain interface according to the class setting
Forward To Interface
Unchange
Step5: Outgoing Queue Selection
Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface.
To Queue Index
Email
Cancel
OK

Class Name	Give a class name to this traffic, such as **Email** in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **LAN1** for this example.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.
MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
To Queue Index	Link this to an item in the **Network Setting > QoS > Queue Setup** screen, which is the **Email** queue created in this example.

This maps email traffic coming from port 25 to the highest priority, which you have created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to the **Email** queue (see the **Source** fields).

4.6 Access 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.

This tutorial covers:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your Zyxel Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

4.6.1 Registering 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.

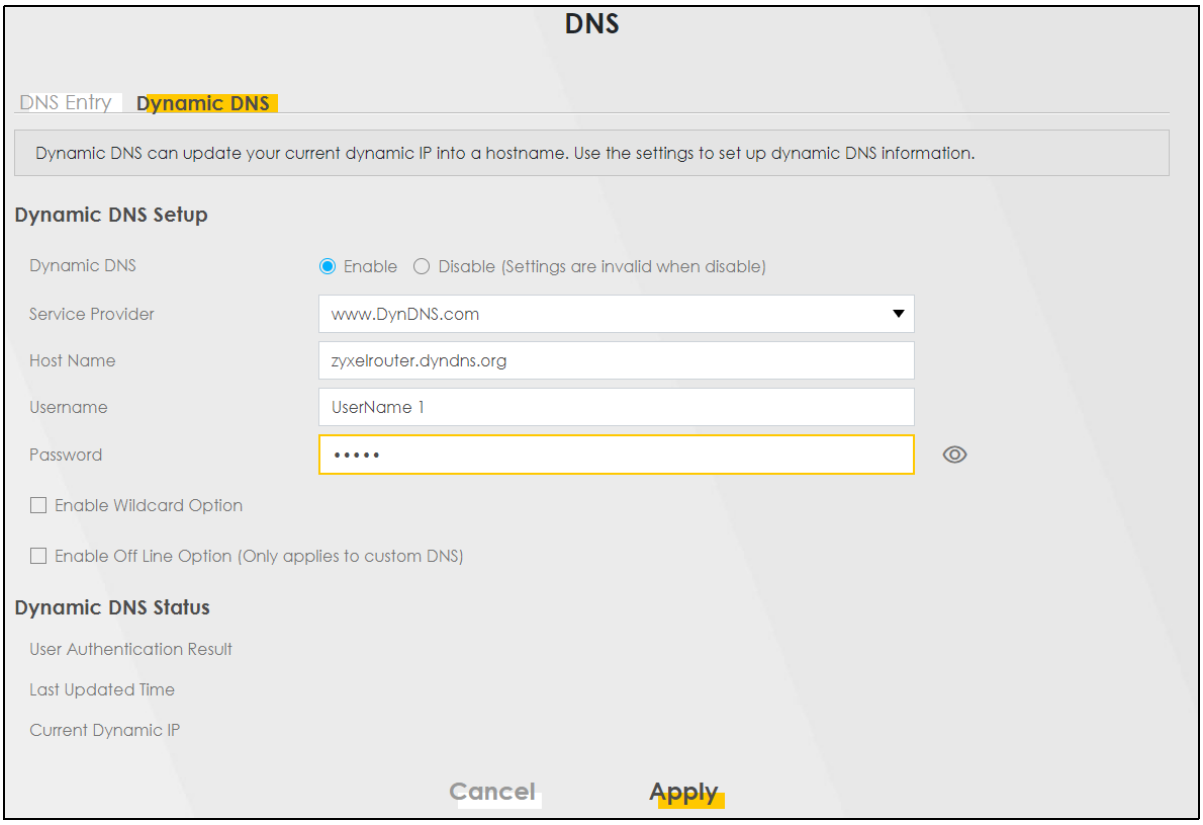
- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the Zyxel Device later.

4.6.2 Configuring 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**.

4.6.3 Testing 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.

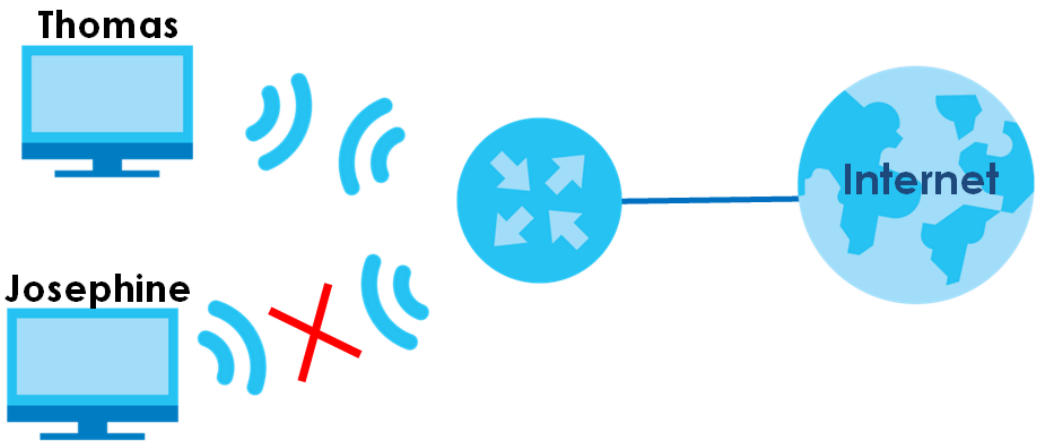
2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

4.7 Configuring the MAC Address Filter

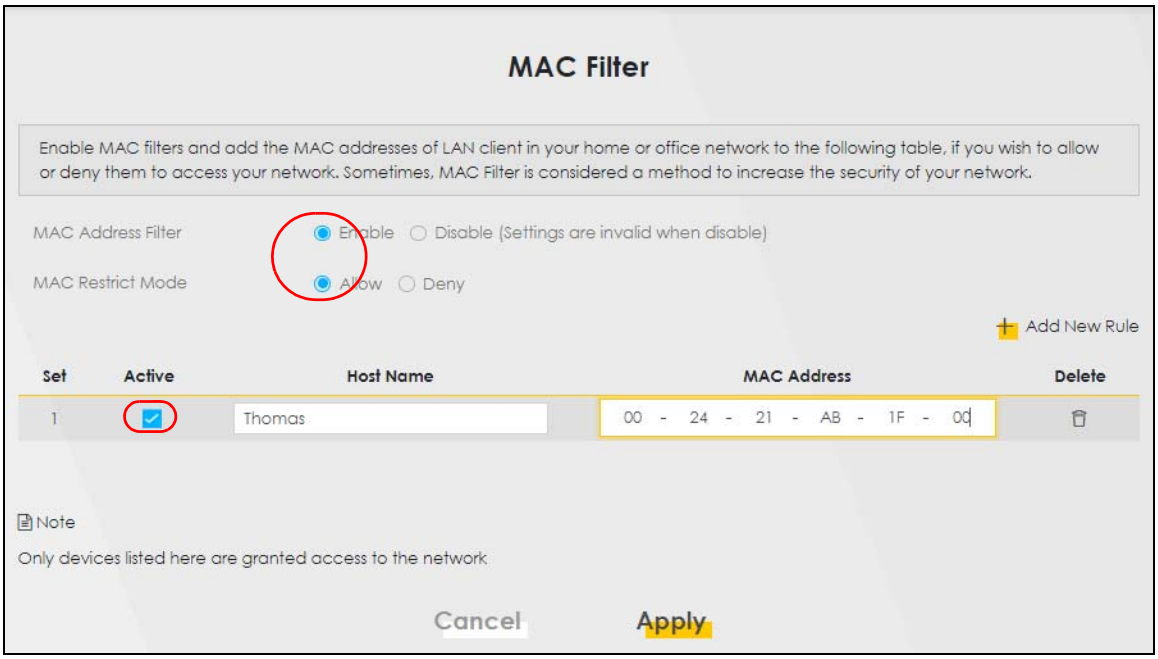
Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the Zyxel Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



1 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.

2 Select **Allow**. Click **Add a new setting** to add a new entry. Then enter the host name and MAC address of Thomas' computer in this screen. Click **Apply**.



Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the Zyxel Device.

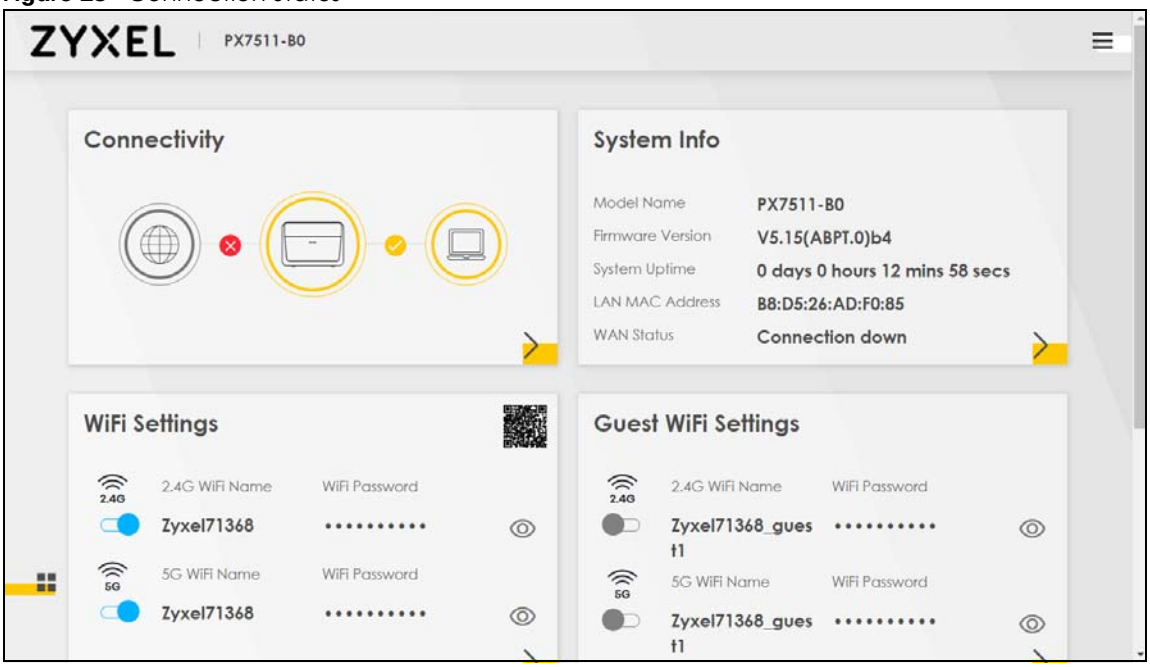
Part II
Technical Reference

CHAPTER 5
Connection Status

5.1 Overview

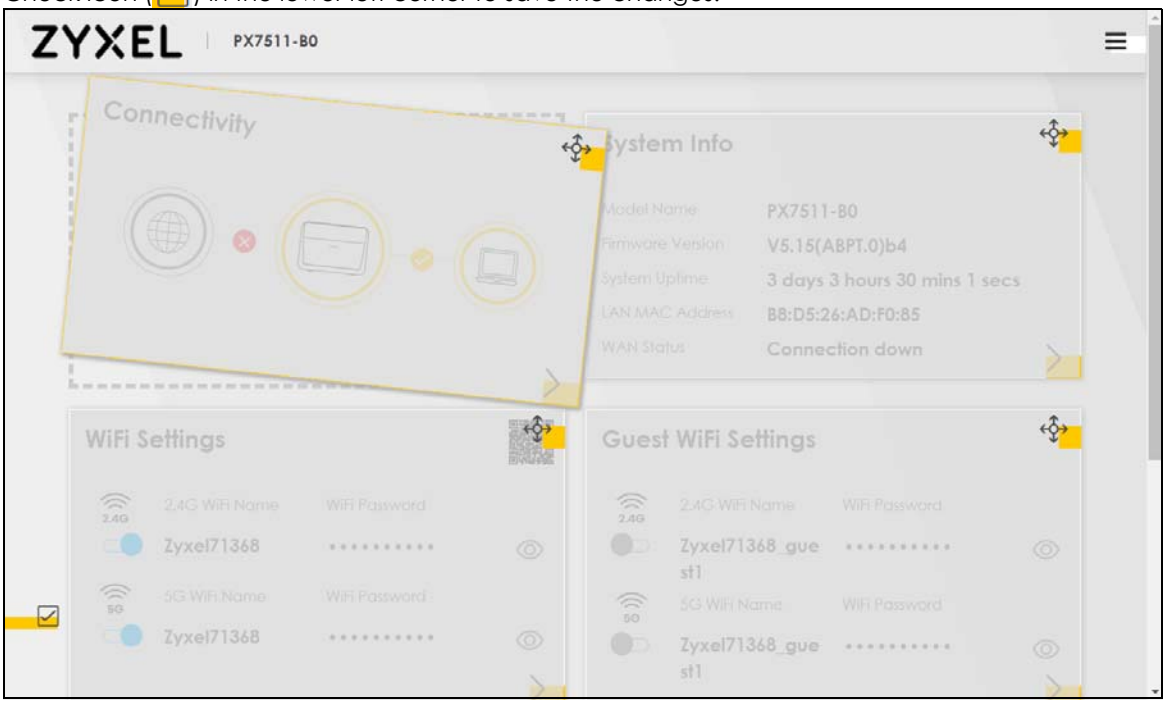
After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access, wireless settings, and parental control settings in this screen. It also shows the network status of the Zyxel Device and computers/devices connected to it.

Figure 23 Connection Status



5.1.1 Layout Icon

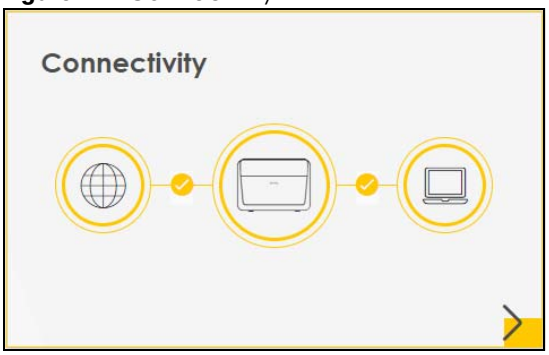
Click this icon ( ) to arrange the screen order. Select a block and hold it to move around. Click the Check icon ( ) in the lower left corner to save the changes.



5.1.2 Connectivity

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

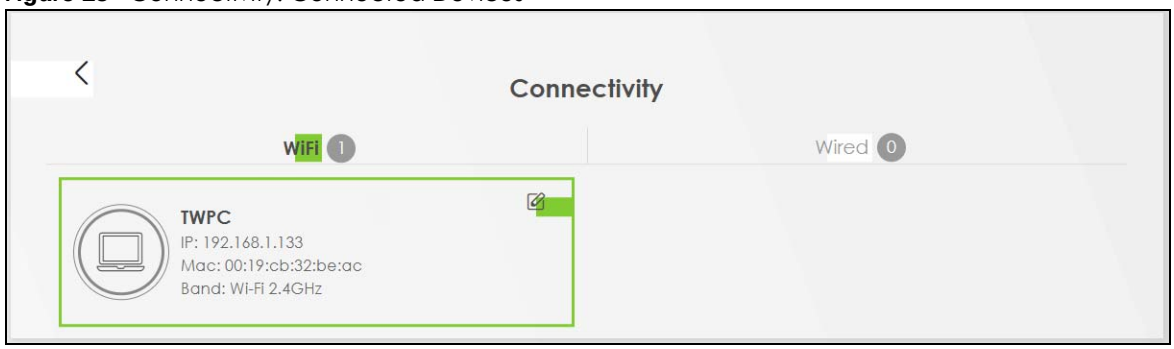
Figure 24 Connectivity



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

Place your mouse within the device block, and an Edit icon ( ) will appear. Click the Edit icon to change the icon and name of a connected device.

Figure 25 Connectivity: Connected Devices



5.1.2.1 Icon and Device Name

You can change the icon and name of a connected device by clicking the device's Edit icon. Select an icon and/or enter a name in the **Device Name** field for a connected device. Click **Save** to save your changes.

Figure 26 Connectivity: Edit

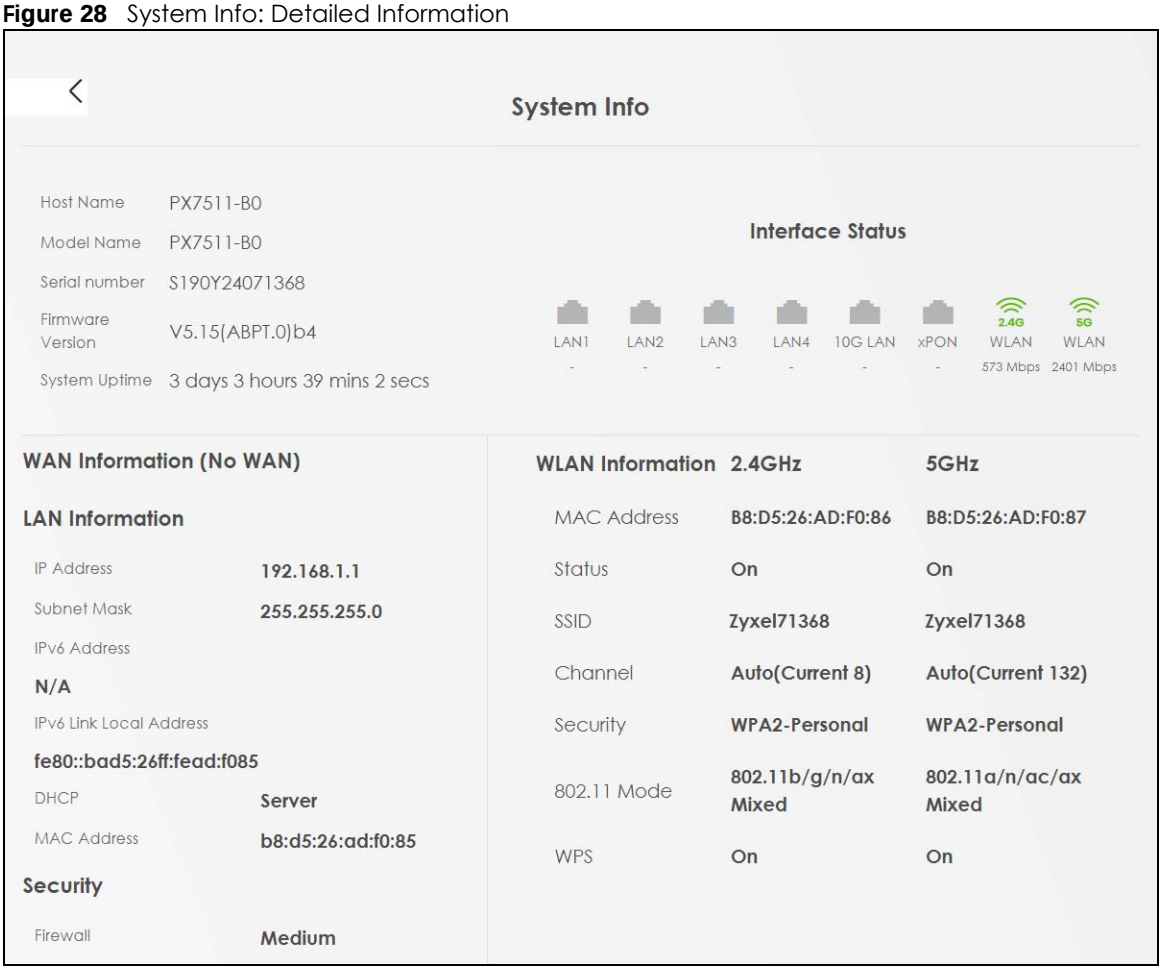
5.1.3 System Info

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

Figure 27 System Info

Click the Arrow icon ( ) to open the following screen. Use this screen to view more information on the status of your firewall and interfaces (WAN, LAN, and wireless LAN).

Figure 28 System Info: Detailed Information



Each field is described in the following table.

Table 8 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.

Table 8 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
Firmware Version	This is the current version of the firmware inside the Zyxel Device.
System Up Time	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Interface Status Virtual ports are shown here. You can see whether the ports are in use and their transmission rate.	
WAN Information (These fields display when you have a WAN connection.)	
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IPv4 address of the Zyxel Device in the WAN. Click the **Release** button to release the IP address provided by a DHCP server.
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.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
Primary DNSv6 server	This field displays the first DNS server IPv6 address assigned by the ISP.
Secondary DNSv6 server	This field displays the second DNS server IPv6 address assigned by the ISP.
LAN Information	
IP Address	This is the current IPv4 address of the Zyxel Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Address	This field displays 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.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: **Server** - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The Zyxel Device is not providing any DHCP services to the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
Security	
Firewall	This displays the firewall's current security level.
WLAN 2.4G/5G Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) address of the wireless interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a wireless LAN.
Channel	This is the channel number used by the wireless interface now.

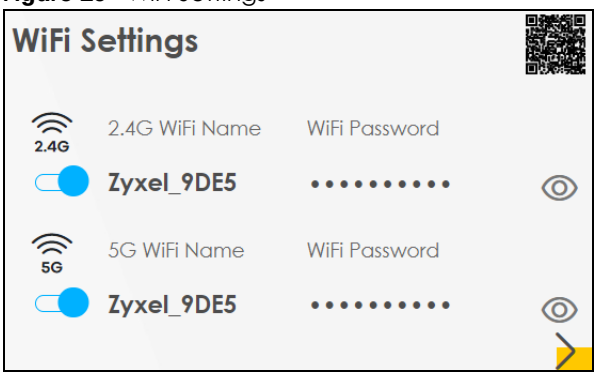
Table 8 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.

5.2 WiFi Settings

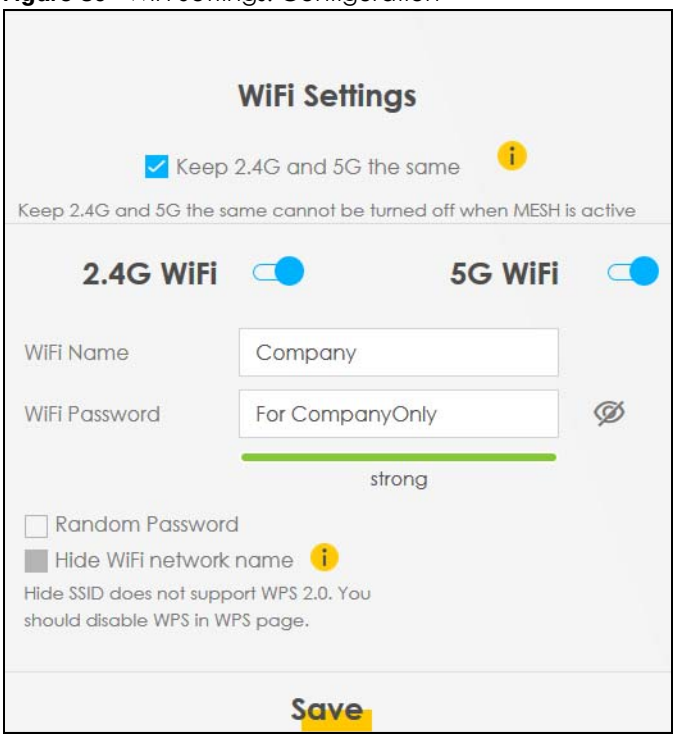
Use this screen to enable or disable the main 2.4G and/or 5G wireless networks. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the main wireless networks. If you want to show or hide your WiFi passwords, click the Eye icon ( ).

Figure 29 WiFi Settings



Click the Arrow icon ( ) to open the following screen. Use this screen to configure the SSIDs and/or passwords for your main wireless networks. Select **Keep 2.4G and 5G the same** to use the same SSID for 2.4 GHz and 5 GHz bands.

Figure 30 WiFi Settings: Configuration



Each field is described in the following table.

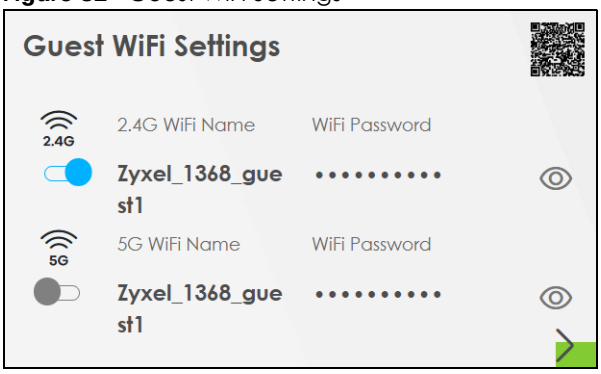
Table 9 WiFi Settings: Configuration

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

5.3 Guest WiFi Settings

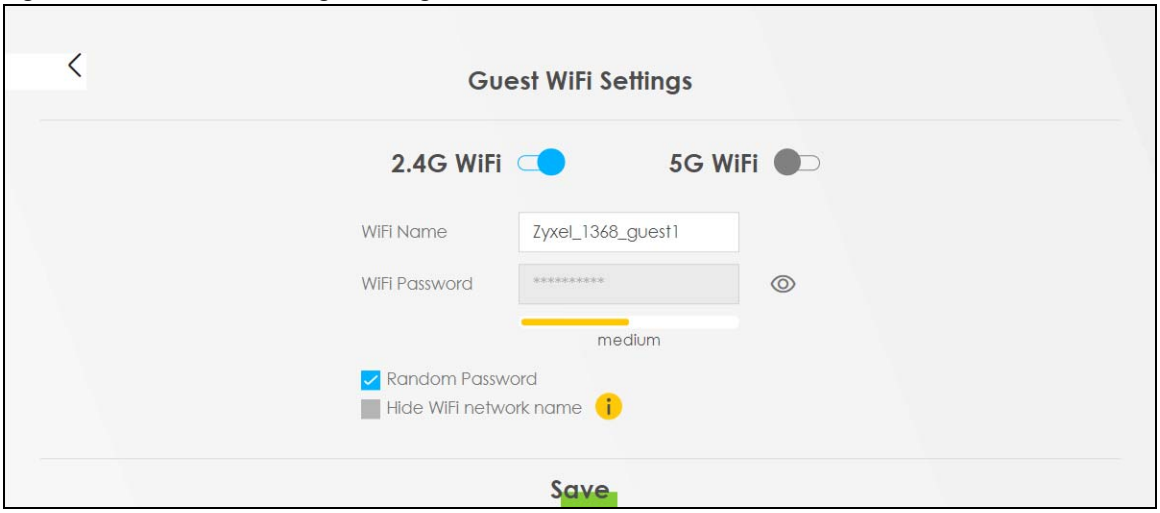
Use this screen to enable or disable the guest 2.4G and/or 5G wireless networks. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the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

Figure 31 Guest WiFi Settings



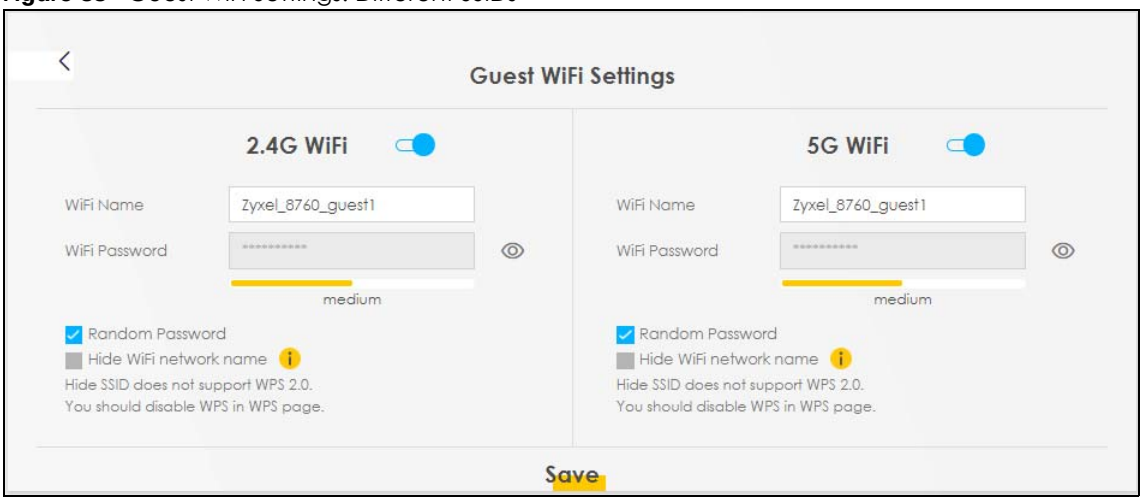
Click the Arrow icon ( ) to open the following screen. Use this screen to configure the SSIDs and/or passwords for your guest wireless networks.

Figure 32 Guest WiFi Settings: Configuration



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

Figure 33 Guest WiFi Settings: Different SSIDs



Each field is described in the following table.

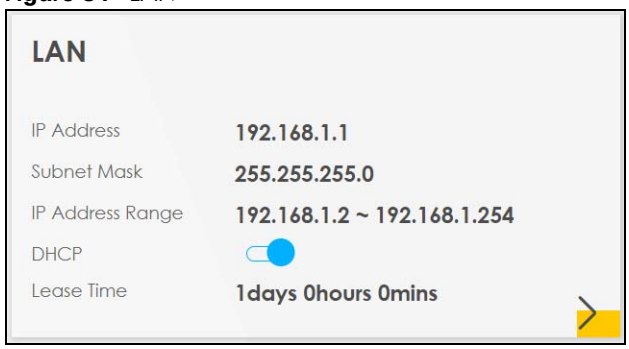
Table 10 WiFi Settings: Configuration

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

5.4 LAN Settings

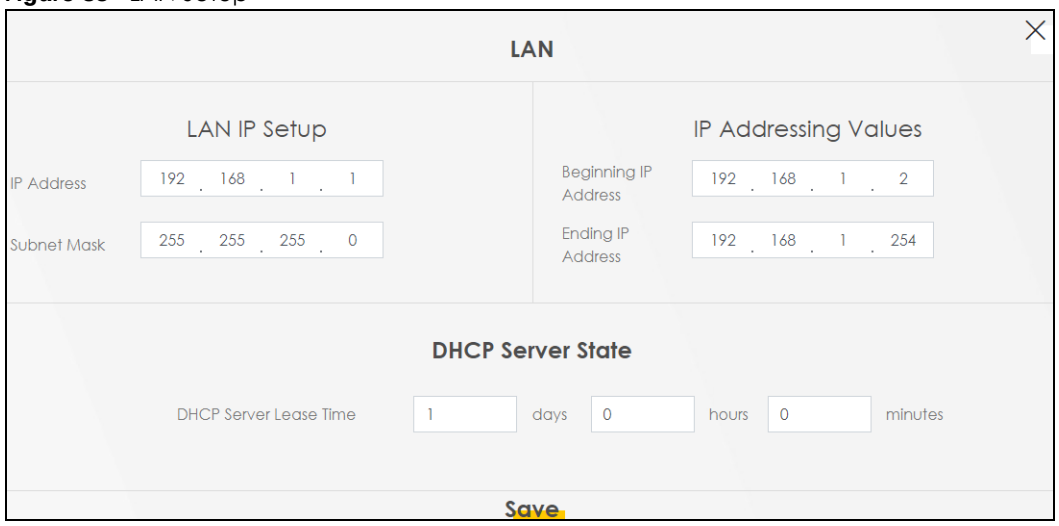
Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device.

Figure 34 LAN



Click the Arrow icon ( ) to open the following screen. Use this screen to configure the LAN IP address and DHCP setting for your Zyxel Device.

Figure 35 LAN Setup



Each field is described in the following table.

Table 11 Status Screen

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 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	

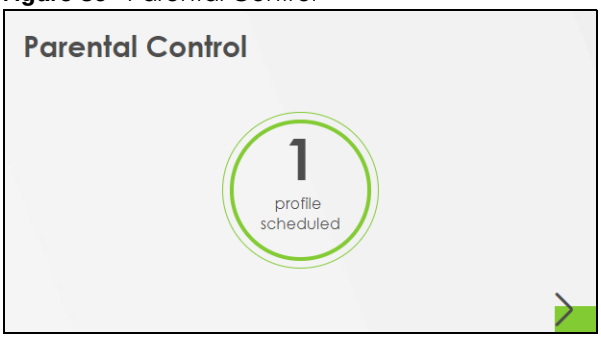
Table 11 Status Screen (continued)

LABEL	DESCRIPTION
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
Save	Click **Save** to save your changes.

5.5 Parental Control

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

Figure 36 Parental Control



Click the Arrow icon ( ) to open the following screen. Use this screen to enable parental control and add more profiles. Add a profile to create restricted access schedules. Go to the **Security** > **Parental Control** > **Add New PCP/Edit** screen to configure URL filtering settings to block the users on your network from accessing certain web sites.

Figure 37 Parental Control: Scheduled Profile (no profile)

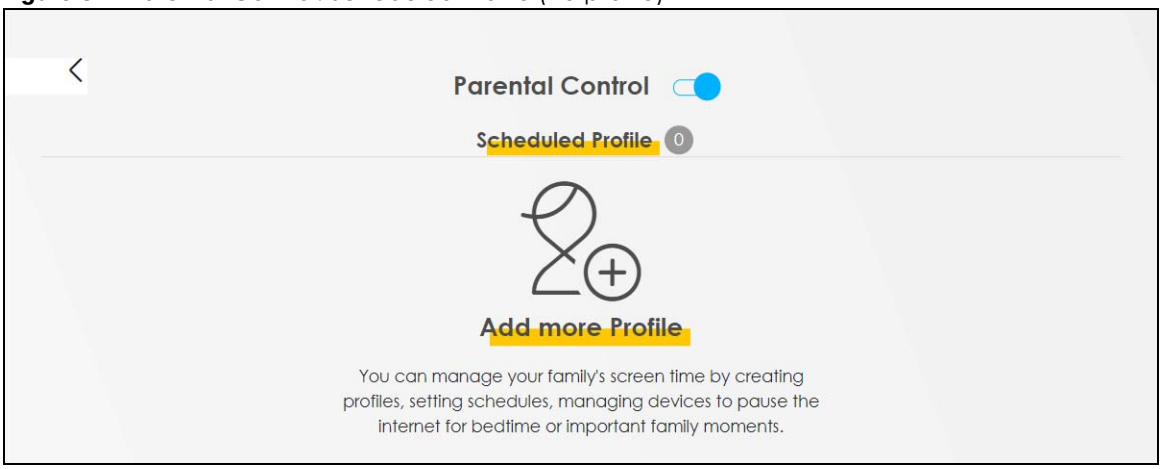
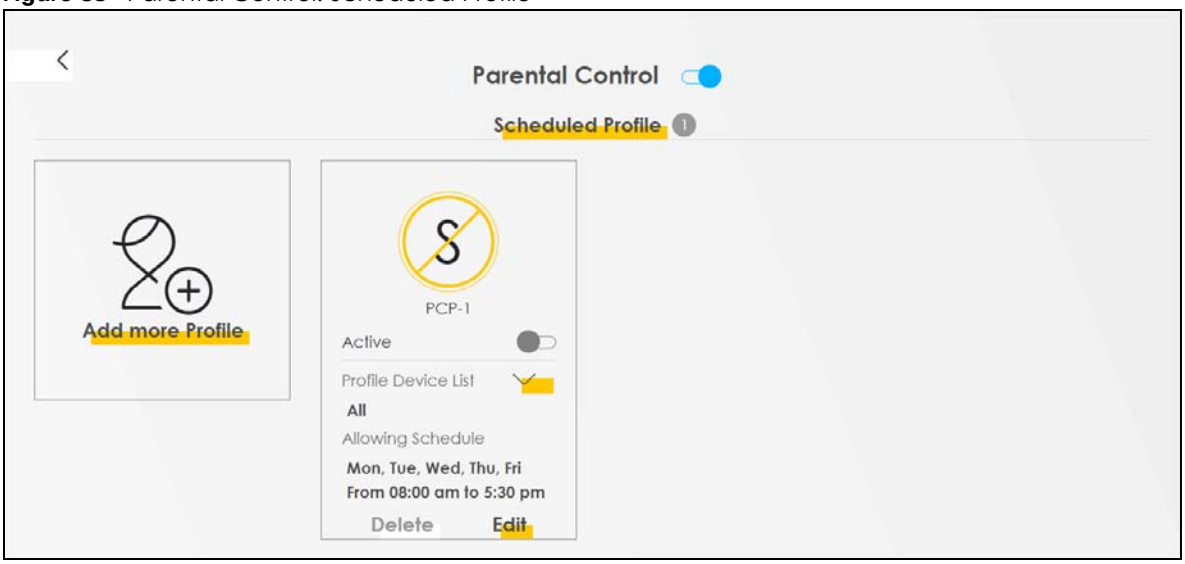


Figure 38 Parental Control: Scheduled Profile



Each field is described in the following table.

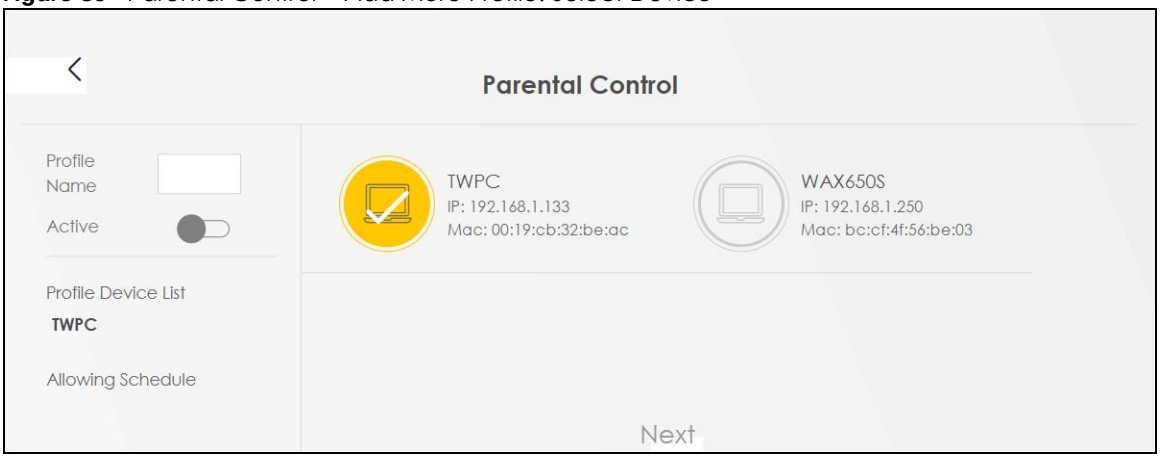
Table 12 Parental Control: Schedule

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not.
Scheduled Profile	This screen shows all the created profile(s). Click to view more information about the profile. You can click **Delete** to remove the profile or click **Edit** to change the profile settings. Only the **Add more Profile** button displays if there is no profile created.
Add more Profile	Click this button to create a new profile.

5.5.1 Create/Edit a Parental Control Profile

Click **Add more Profile** to create a profile or click **Edit** of an existing profile to change its settings. Use this screen to add a device(s) in a profile and block Internet access on the profile device(s).

Figure 39 Parental Control > Add More Profile: Select Device



Each field is described in the following table.

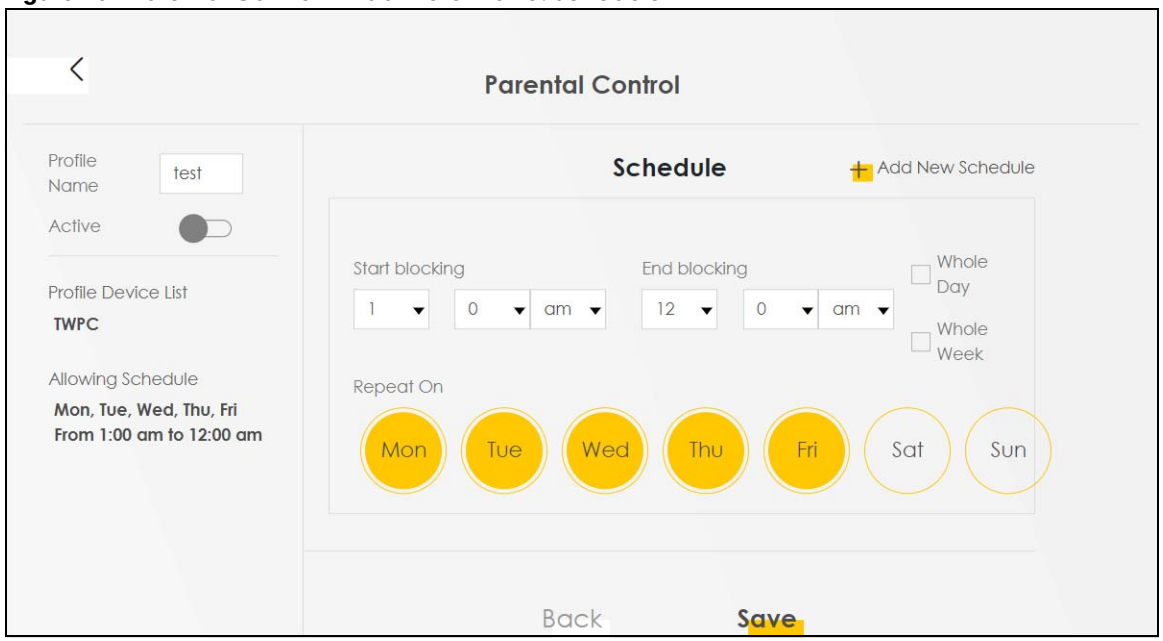
Table 13 Parental Control > Add More Profile: Select Device

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable the profile. When the switch goes to the right , the profile is enabled. Otherwise, it is disabled.
Profile Device List	This field shows the devices selected on the right for this profile.
Allowing Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
	Select the device(s) on your network for this profile and click **Next.**

5.5.2 Define a Schedule

This screen allows you to define time periods and days during which Internet access is blocked on the profile device(s).

Figure 40 Parental Control > Add More Profile: Schedule



Each field is described in the following table.

Table 14 Parental Control > Add More Profile: Schedule

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable the profile. When the switch goes to the right , the profile is enabled. Otherwise, it is disabled.
Profile Device List	This field shows the devices selected on the right for this profile.
Allowing Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
Schedule	
Add New Schedule	Click this to add a new block for scheduling.

Table 14 Parental Control > Add More Profile: Schedule (continued)

LABEL	DESCRIPTION
Start/End blocking	Select the time period when Internet access is blocked on the profile device(s). Select **Whole Week** and the scheduler rule will be activated for every day of the week.
Repeat On	Select the days when Internet access is blocked on the profile device(s).
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save your changes.

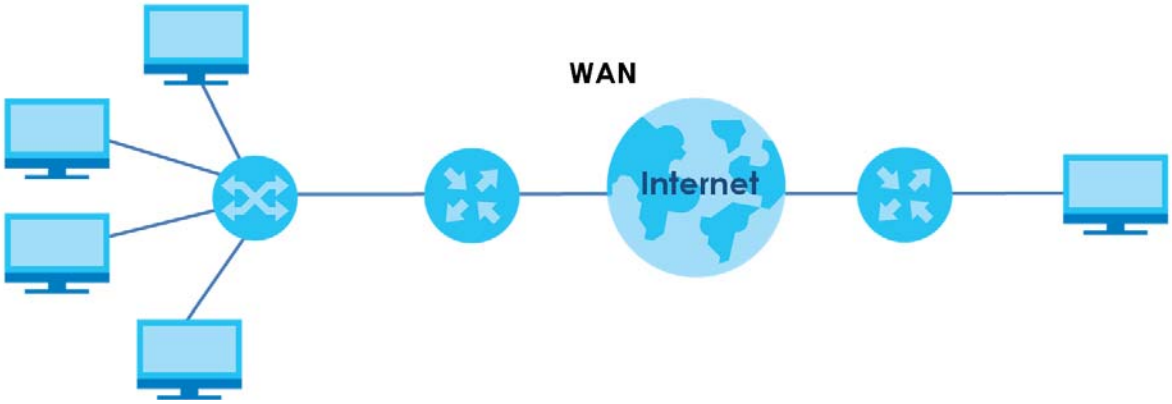
CHAPTER 6
Broadband

6.1 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 41 LAN and WAN



6.1.1 What You Can Do in this Chapter

Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 6.2 on page 77).

Table 15 WAN Setup Overview

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

6.1.2 What You Need to Know

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

WAN IP Address

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

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

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 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).

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

IPv6 Subnet Masking

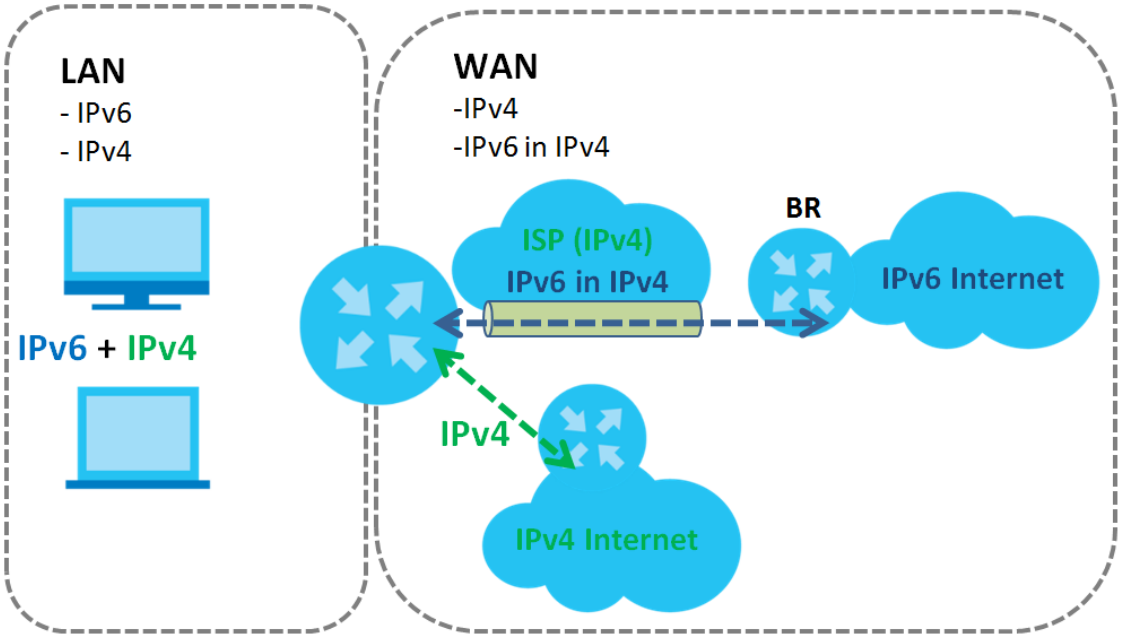
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example,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

IPv6 Rapid Deployment

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

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

Figure 42 IPv6 Rapid Deployment

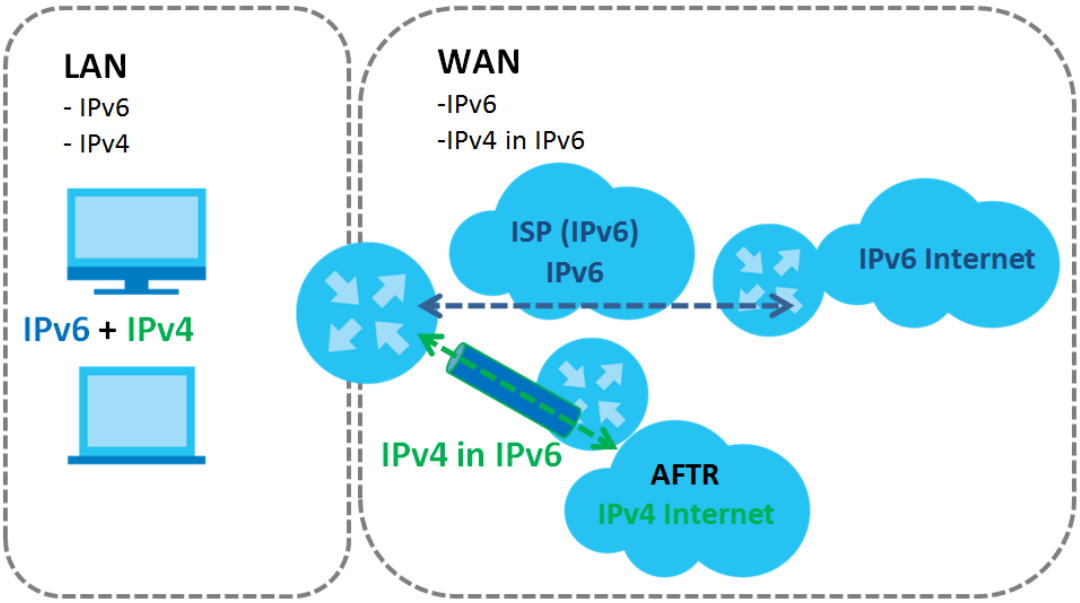


Dual Stack Lite

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

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

Figure 43 Dual Stack Lite



6.1.3 Before You Begin

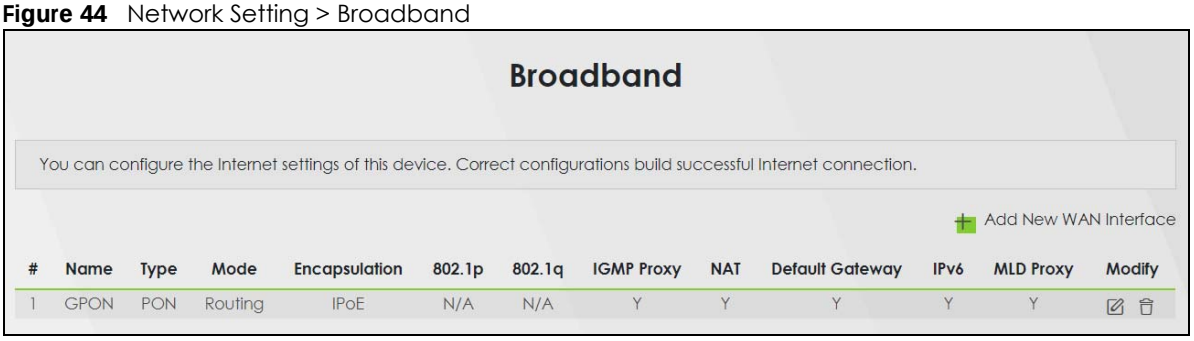
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

6.2 Broadband Settings

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

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

Figure 44 Network Setting > Broadband



The following table describes the labels in this screen.

Table 16 Network Setting > Broadband

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

6.2.1 Add/Edit Internet Connection

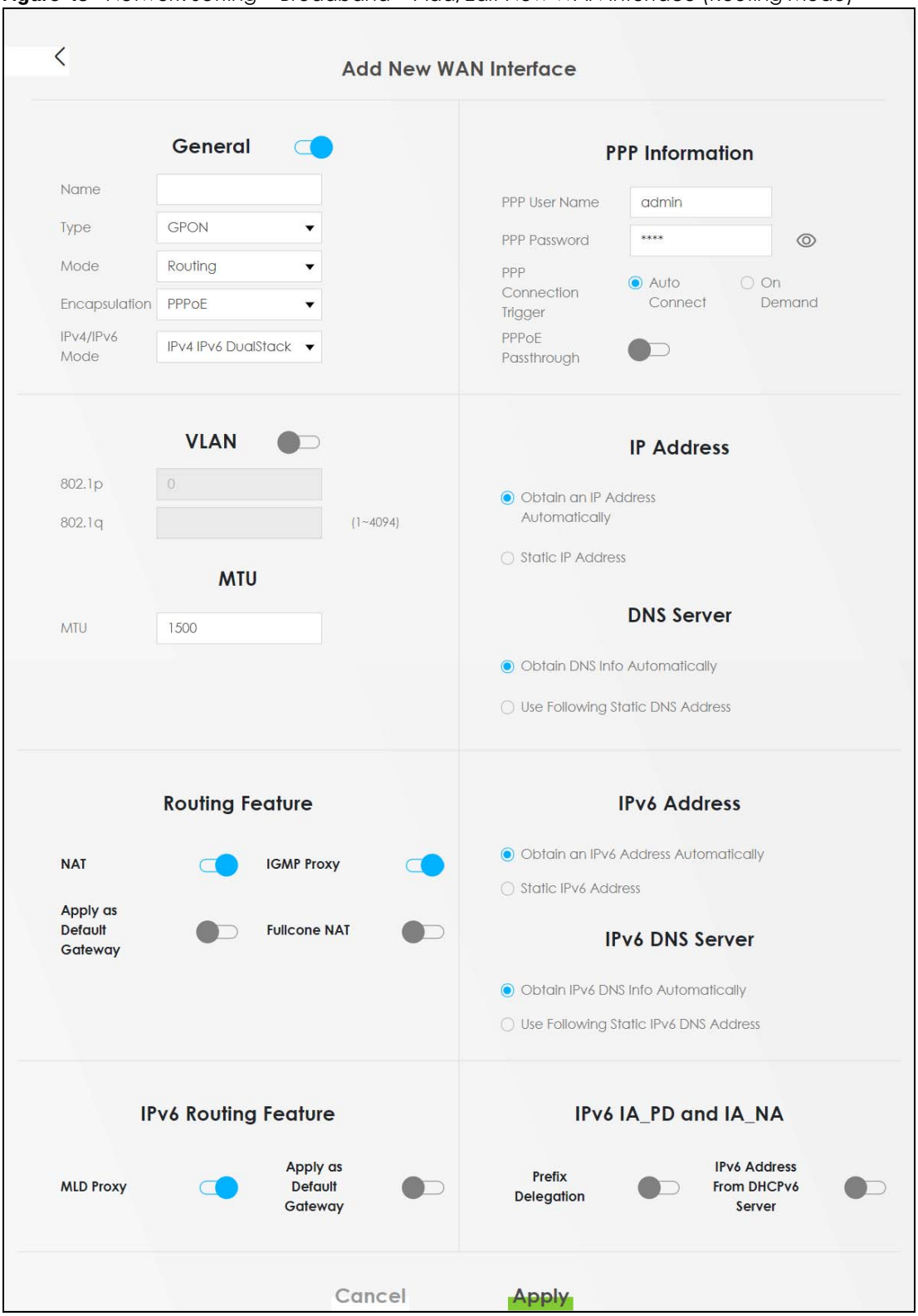
Click **Add New WAN Interface** in the **Broadband** screen or the Edit icon next to an existing WAN interface to open the following screen. Use this screen to configure a WAN connection. The screen varies depending on the mode, encapsulation, and IPv6/IPv4 mode you select.

6.2.1.1 Routing Mode

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

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

Figure 45 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)



The following table describes the labels in this screen.

Table 17 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Name	Specify a descriptive name for this connection.
Type	This field shows **GPON** and indicates a broadband connection to a PON (Passive Optical Network).
Mode	Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. The choices are **PPPoE** and **IPoE**.
IPv4/IPv6 Mode	Select **IPv4 Only** if you want the Zyxel Device to run IPv4 only. Select **IPv4 IPv6 DualStack** to allow the Zyxel Device to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the Zyxel Device to run IPv6 only.
PPP Information (This is available only when you select **Routing** in the **Mode** field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select **password unmask** to show your entered password in plain text.
PPP Connection Trigger	Select when to have the Zyxel Device establish the PPP connection. **Auto Connect** - select this to not let the connection time out. **On Demand** - select this to automatically bring up the connection when the Zyxel Device receives packets destined for the Internet.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not available if you select **Auto Connect** in the **PPP Connection Trigger** field.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the Zyxel Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Zyxel Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
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 traffic through this connection.
IP Address (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	

Table 17 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP. This is available only when you set **Encapsulation** to **IPoE**.
Gateway IP Address	Enter the gateway IP address provided by your ISP. This is available only when you set **Encapsulation** to **IPoE**.
DNS Server (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
	Select **Obtain DNS Info Automically** 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 (This is available only when you select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
NAT	Click this switch to activate or deactivate NAT on this connection. When the switch goes to the right , the function is enabled. Otherwise, it is not.
IGMP Proxy	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Click this switch to have the Zyxel Device act as an IGMP proxy on this connection. When the switch goes to the right , the function is enabled. Otherwise, it is not. This allows the Zyxel Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Click this switch to have the Zyxel Device use the WAN interface of this connection as the system default gateway. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Fullcone NAT Enable	Click this switch to enable or disable full cone NAT on this connection. When the switch goes to the right , the function is enabled. Otherwise, it is not. This field is available only when you activate **NAT**. In full cone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.
DHCPC Options (This is available only when you set **Encapsulation** to **IPoE** and select **IPv4 Only** or **IPv4 IPv6 DualStack** in the **IPv4/IPv6 Mode** field.)	
Request Options	Select **Option 43** to have the Zyxel Device automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server. Select **Option 121** to have the Zyxel Device push static routes to clients.
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.

Table 17 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
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 (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.)	
Obtain an IPv6 Address Automatically	Select **Obtain an IPv6 Address Automatically** if you want to have the Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select **Static IPv6 Address** if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.
IPv6 DNS Server (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. Configure the IPv6 DNS server in the following section.)	
Obtain IPv6 DNS Info Automatically	Select **Obtain IPv6 DNS Info Automatically** to have the Zyxel Device get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select **Use Following Static IPv6 DNS Address** to have the Zyxel Device use the IPv6 DNS server addresses you configure manually.
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.
IPv6 Routing Feature (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. You can enable IPv6 routing features in the following section.)	
MLD Proxy Enable	Select this check box to have the Zyxel Device act as an MLD proxy on this connection. This allows the Zyxel Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway.
DS-Lite	This is available only when you select **IPv6 Only** in the **IPv4/IPv6 Mode** field. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 76 for more information. Click this switch to let local computers use IPv4 through an ISP's IPv6 network. When the switch goes to the right , the function is enabled. Otherwise, it is not.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
6RD	The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 76 for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network. When the switch goes to the right , the function is enabled. Otherwise, it is not.

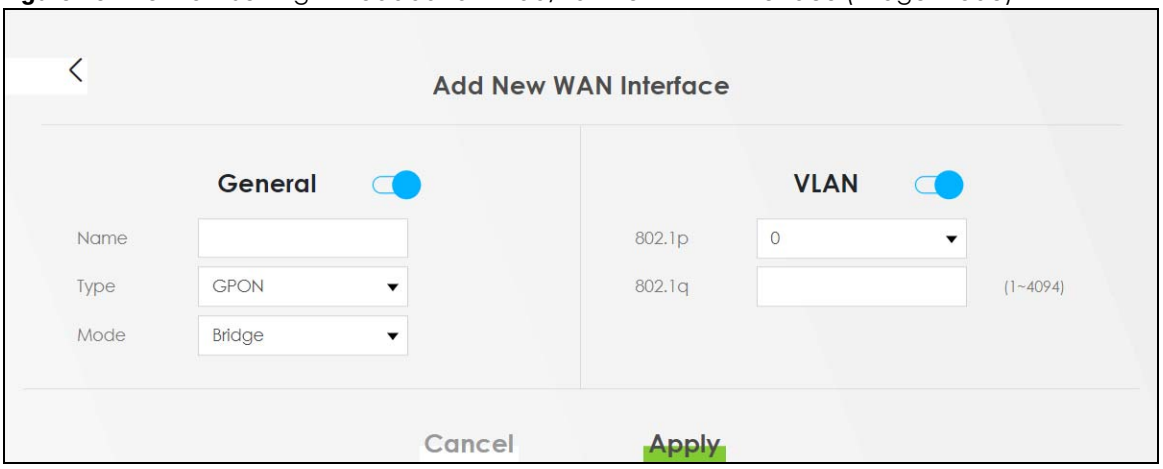
Table 17 Network Setting > Broadband > Add/Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
	Select **Manually Configured** if you have the IPv4 address of the relay server. Otherwise, select **Automatically configured by DHCPC** to have the Zyxel Device detect it automatically through DHCP. The **Automatically configured by DHCPC** option is configurable only when you set the method of encapsulation to **IPoE**.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
Border Relay IPv4 Address	When you select **Manually Configured**, specify the relay server's IPv4 address in this field.
IPv6 IA_PD and IA_NA (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.)	
Prefix Delegation	Click this switch to use DHCP PD (Prefix Delegation) which enables the Zyxel Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses. When the switch goes to the right , the function is enabled. Otherwise, it is disabled.
IPv6 Address From DHCPv6 Server	Click this switch to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Zyxel Device using the IPv6 prefix from a Router Advertisement (RA). When the switch goes to the right , the function is enabled. Otherwise, it is disabled.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

6.2.1.2 Bridge Mode

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

Figure 46 Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode)



The following table describes the fields in this screen.

Table 18 Network Setting > Broadband > Add/Edit New WAN Interface (Bridge Mode)

LABEL	DESCRIPTION
General	Click this switch to enable or disable the interface. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Name	Enter a service name of the connection.
Type	This field shows **GPON** and indicates a broadband connection to a PON (Passive Optical Network).
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right , the function is enabled. Otherwise, it 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 0 to 4094) for traffic through this connection.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

6.3 Technical Reference

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

Encapsulation

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

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Zyxel Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Zyxel Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

IP Address Assignment

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

Introduction to VLANs

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

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

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

Introduction to IEEE 802.1Q Tagged VLAN

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

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

used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

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

Multicast

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

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

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

DNS Server Address Assignment

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

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

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.

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

IPv6 Prefix and Prefix Length

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

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

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

CHAPTER 7
Wireless

7.1 Wireless Overview

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

7.1.1 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 wireless connection.

- Use the **General** screen to enable WiFi, enter the SSID and select the wireless security mode (Section 7.2 on page 89).
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device (Section 7.3 on page 94).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device (Section 7.4 on page 97).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 7.5 on page 99).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 7.6 on page 100).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold (Section 7.7 on page 101).
- Use the **Channel Status** screen to scan WiFi channel noises and view the results (Section 7.8 on page 104).

7.1.2 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 7.9 on page 104 for advanced technical information on wireless networks.

7.2 Wireless General Settings

Use this screen to enable WiFi, enter the SSID and select the wireless security mode. These are basic elements for starting a wireless service. It's recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

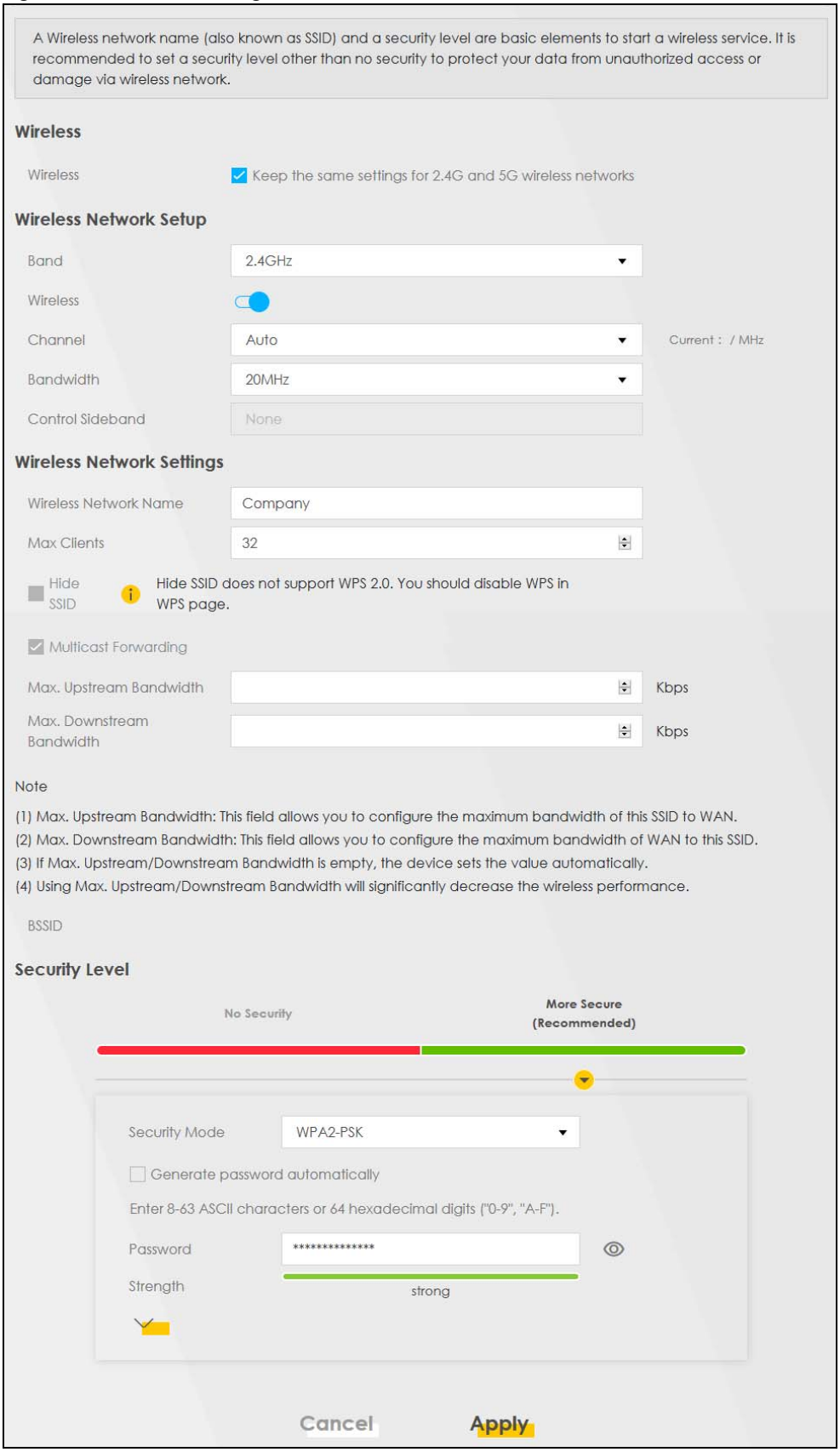
Note: If you are configuring the Zyxel Device from a computer connected to WiFi and you change the Zyxel Device's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Zyxel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

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

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

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

Figure 47 Network Setting > Wireless > General



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

Table 19 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	Select **Keep the same settings for 2.4G and 5G wireless networks** and the 2.4 GHz and 5 GHz wireless networks will use the same SSID and wireless security settings.
Wireless Network Setup	
Band	This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax wireless clients while **5GHz** is used by IEEE 802.11a/n/ac/ax wireless clients.
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue , the function is enabled. Otherwise, it is not.
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use **Auto** to have the Zyxel Device automatically determine a channel to use.
Bandwidth	Select whether the Zyxel Device uses a wireless channel width of **20MHz**, **40MHz, 20MHz/40MHz**, **20MHz/40MHz/80MHz** or **20MHz/40MHz/80MHz/160MHz**. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. Because not all devices support 40 MHz and/or 160 MHz channels, select **20/40MHz** or **20MHz/40MHz/80MHz/160MHz** to allow the Zyxel Device to adjust the channel bandwidth automatically.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz** or **20MHz/40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This check box is grayed out if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen.
Multicast Forwarding	Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
Security Level	

Table 19 Network Setting > Wireless > General (continued)

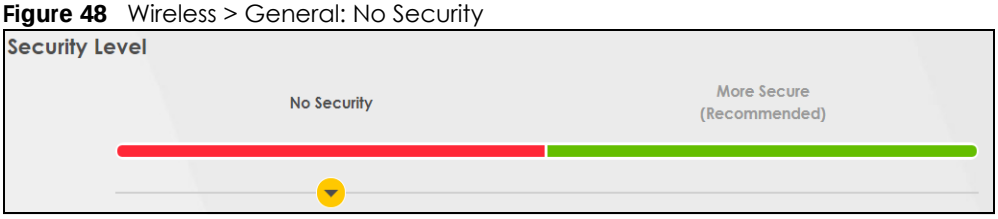
LABEL	DESCRIPTION
Security Mode	Select **More Secure (Recommended)** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

7.2.1 No Security

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

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

Figure 48 Wireless > General: No Security



The following table describes the labels in this screen.

Table 20 Wireless > General: No Security

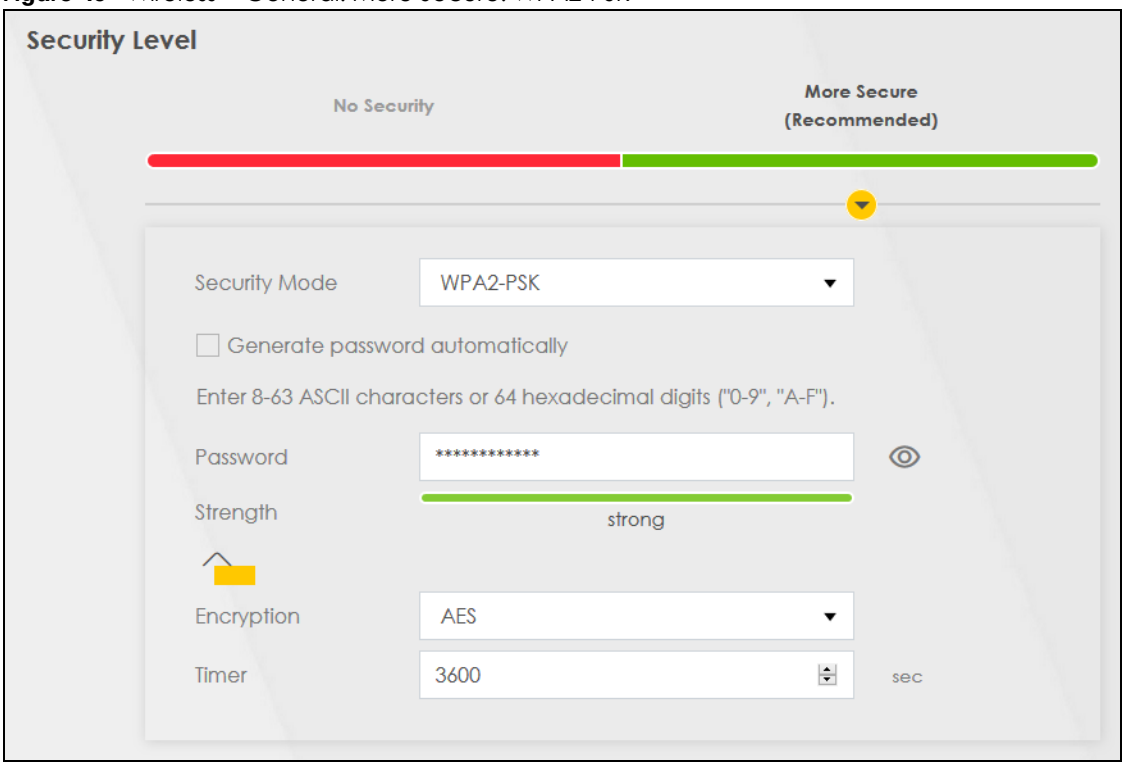
LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all wireless connections without data encryption or authentication.

7.2.2 More Secure (Recommended)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the Zyxel Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a 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.

Click **Network Setting** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA2-PSK** or **WPA2-EAP** from the **Security Mode** list.

Figure 49 Wireless > General: More Secure: WPA2-PSK



The following table describes the labels in this screen.

Table 21 Wireless > General: More Secure: WPA2-PSK

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

7.3 Guest/More AP

This screen allows you to configure a guest wireless network that allows access to the Internet only through the Zyxel Device. You can also configure additional wireless networks, each with different security settings, in this screen.

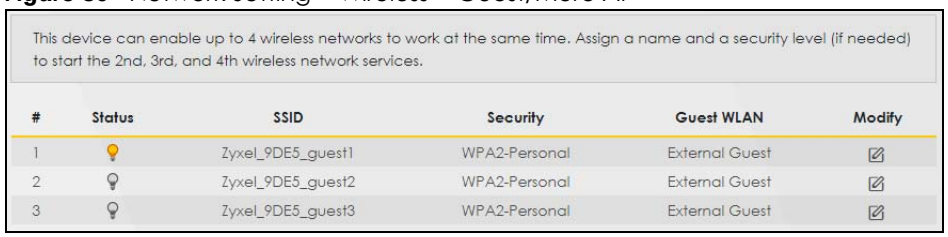
Click **Network Setting > Wireless** > **Guest/More AP**. The following screen displays.

The following table introduces the supported wireless networks.

Table 22 Supported Wireless Networks

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

Figure 50 Network Setting > Wireless > Guest/More AP



The following table describes the labels in this screen.

Table 23 Network Setting > Wireless > Guest/More AP

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

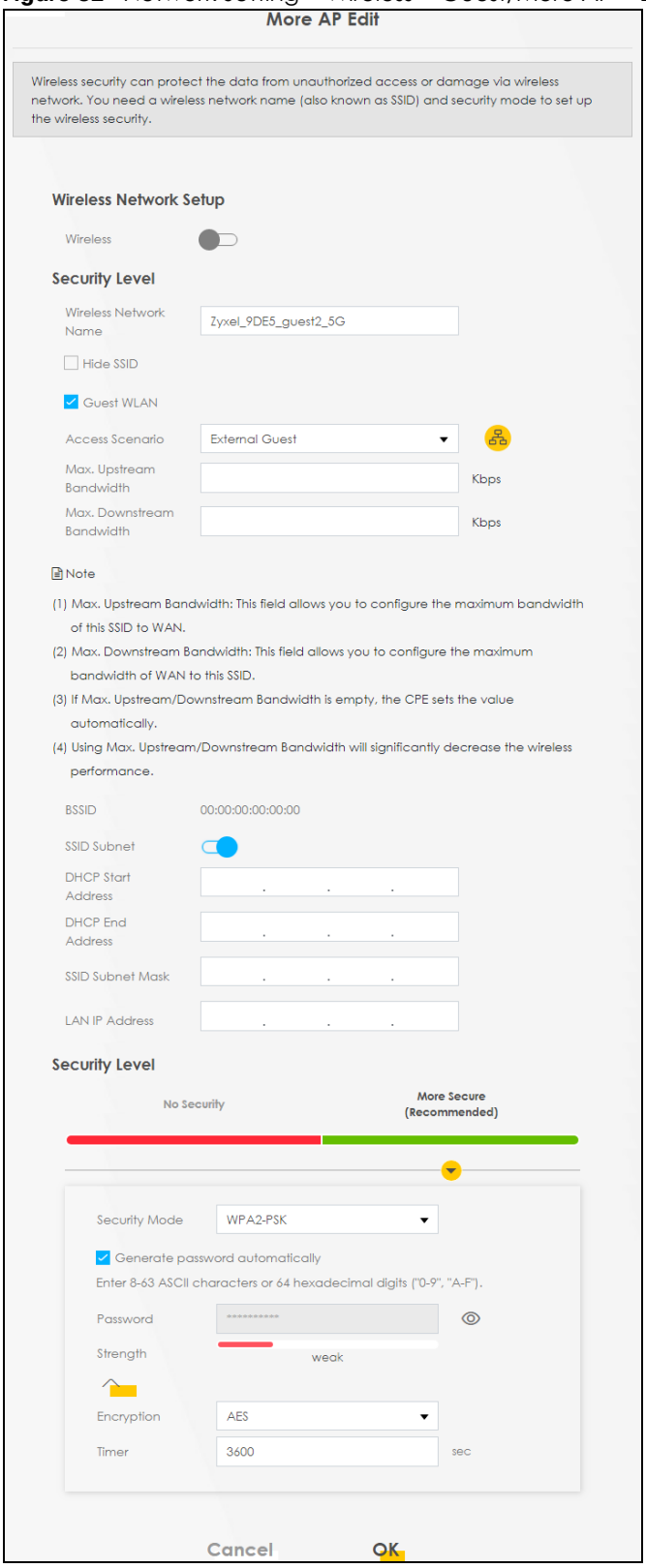
7.3.1 The Edit Guest/More AP Screen

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

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

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

Figure 51 Network Setting > Wireless > Guest/More AP > Edit



The following table describes the fields in this screen.

Table 24 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue , the function is enabled; otherwise, it is not.
Security Level	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WiFis for home and external clients. Select the WiFi type in the **Access Scenario** field.
Access Scenario	If you select **Home Guest**, clients can connect to each other directly. If you select **External Guest**, clients are blocked from connecting to each other directly.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
SSID Subnet	Click on this switch to **Enable** this function if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients. This option cannot be used if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen or if the **Keep the same settings for 2.4G and 5G wireless networks** check box is selected in **Network Setting** > **Wireless** > **General**.
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool. The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	Select **More Secure (Recommended)** to add security on this wireless network. The wireless clients which want to associate to this network must have the same wireless security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 92 for more details about this field.
Security Mode	Select **WPA2-PSK** from the drop-down list box.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.

Table 24 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it is hidden.
	Click this to show more fields in this section. Click again to hide them.
Encryption	This field shows the **AES** type of data encryption.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

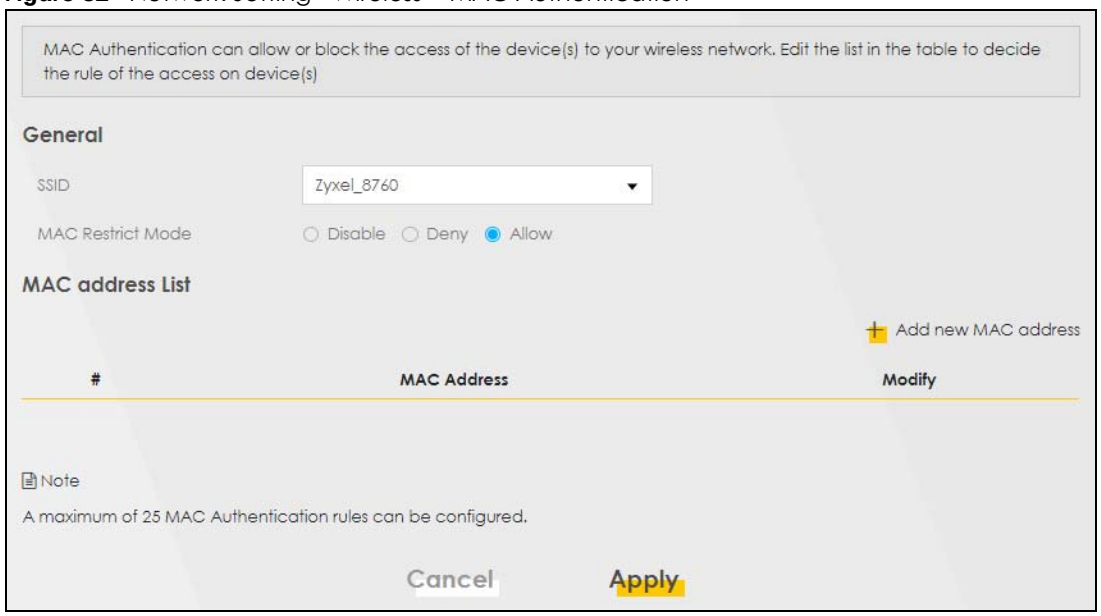
7.4 MAC Authentication

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

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

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

Figure 52 Network Setting> Wireless > MAC Authentication



The following table describes the labels in this screen.

Table 25 Network Setting > Wireless > MAC Authentication

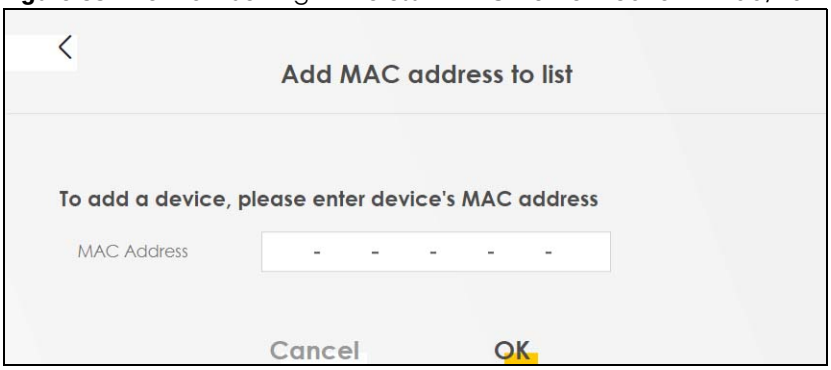
LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device. Select **Allow** to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device.
MAC Address List	
Add New MAC Address	This field is available when you select **Deny** or **Allow** in the **MAC Restrict Mode** field. Click this if you want to add a new MAC address entry to the MAC filter list below.
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless 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 restore your previously saved settings.
Apply	Click **Apply** to save your changes.

7.4.1 Add/Edit MAC Addresses

Click **Add new MAC address** in the **Network Setting** > **Wireless** > **MAC Authentication** screen to add a new MAC address. You can also click the Edit icon next to a MAC authentication rule to edit the rule.

Enter the MAC addresses of the wireless 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.

Figure 53 Network Setting> Wireless > MAC Authentication > Add/Edit



7.5 WPS Settings

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. See Section 7.9.8.3 on page 112 for more information about WPS.

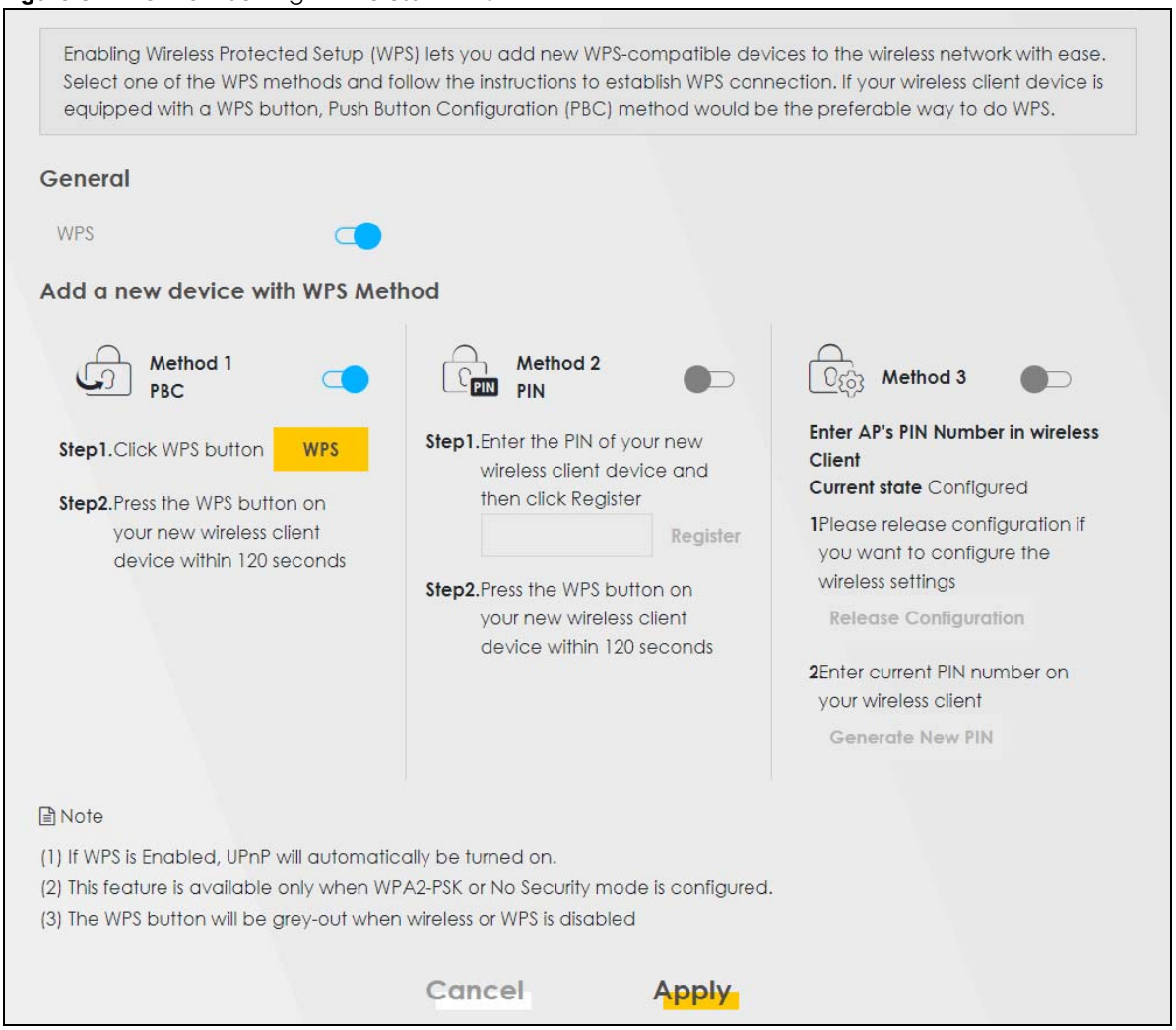
Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile (see Section 7.2 on page 89).

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

Note: The WPS switch is grayed out when WiFi is disabled.

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

Figure 54 Network Setting > Wireless > WPS



The following table describes the labels in this screen.

Table 26 Network Setting > Wireless > WPS

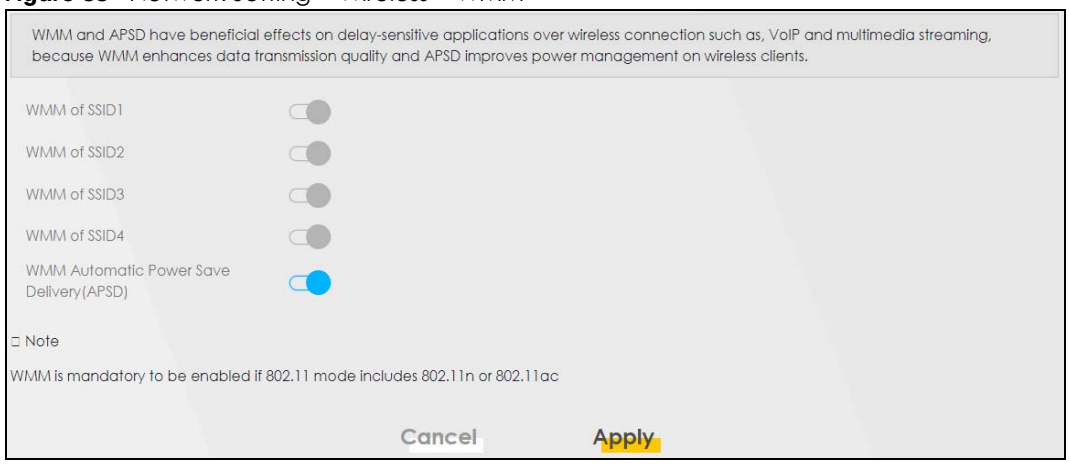
LABEL	DESCRIPTION
General	
WPS	Click this switch to activate or deactivate WPS on this Zyxel Device. When the switch turns blue , the function is enabled. Otherwise, it is not.
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (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 wireless device (within wireless range of the Zyxel Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the Zyxel Device. Click this switch and 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 wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Zyxel Device.
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the Zyxel Device into the client. Click this switch and 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 wireless and wireless 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.

7.6 WMM Settings

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 55 Network Setting > Wireless > WMM



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 27 Network Setting > Wireless > WMM

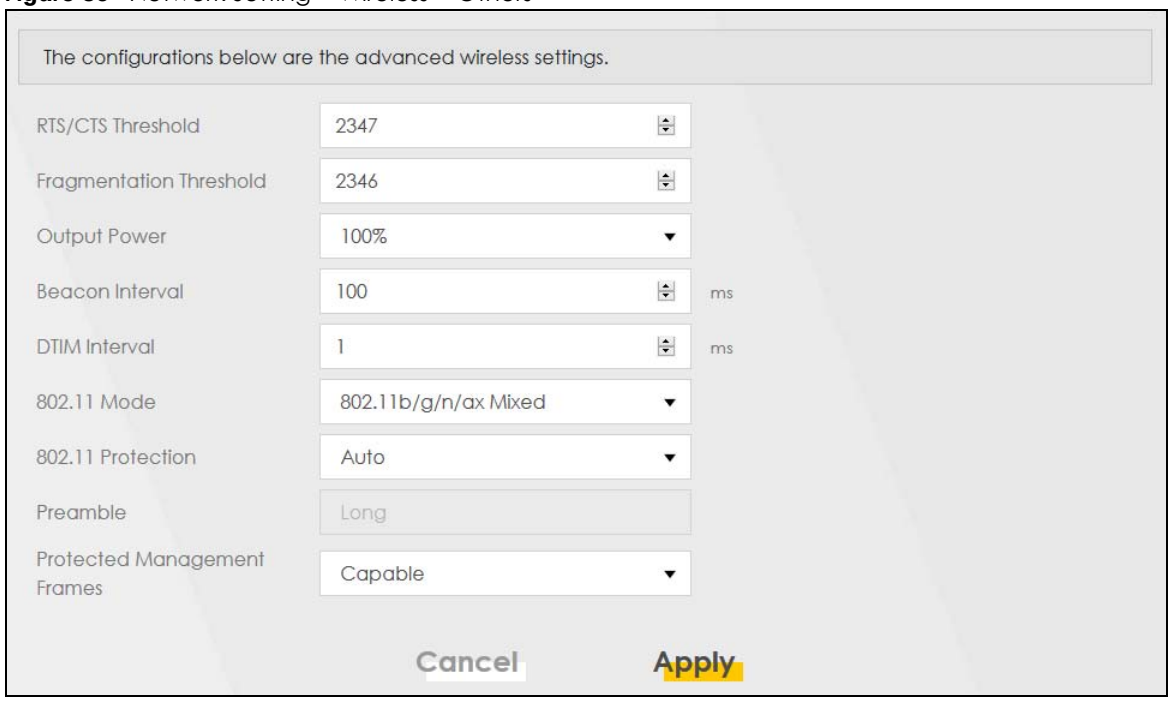
LABEL	DESCRIPTION
WMM of SSID1~4	Select **On** to have the Zyxel Device automatically give the wireless network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to voice and video, which makes them 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 wireless 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.

7.7 Others Settings

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 7.9.2 on page 106 for detailed definitions of the terms listed in this screen.

Figure 56 Network Setting > Wireless > Others



The following table describes the labels in this screen.

Table 28 Network Setting > Wireless > Others

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

Table 28 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Mode	For 2.4 GHz frequency WiFi devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n/ax Mixed** to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. For 5 GHz frequency WiFi devices: • Select **802.11a Only** to allow only IEEE 802.11a compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11ac Only** to allow only IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. • Select **802.11a/n Mixed** to allow either IEEE 802.11a or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11n/ac Mixed** to allow either IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac Mixed** to allow IEEE 802.11a, IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac/ax Mixed** to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 7.9.7 on page 109 for more information. This field is configurable only when you set **802.11 Mode** to **802.11b** or **802.11b/g Mixed**.
Protected Management Frames	This option is only available when using **WPA2-PSK** as the **Security Mode** and **AES** Encryption in **Network Setting > Wireless > General**. Management frame protection (MFP) helps prevent wireless DoS attacks. Select **Disable** if you do not want to use MFP. Select **Capable** to encrypt management frames of wireless clients that support MFP. Clients that do not support MFP will still be allowed to join the wireless network, but remain unprotected. Select **Required** to allow only clients that support MFP to join the wireless network.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

7.8 Channel Status Settings

Use the **Channel Status** screen to scan WiFi channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **Scan** to scan the wireless LAN channels. You can view the results in the **Channel Scan Result** section.

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 57 Network Setting > Wireless > Channel Status

7.9 Technical Reference

This section discusses WiFis in depth. For more information, see Appendix B on page 283.

7.9.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.

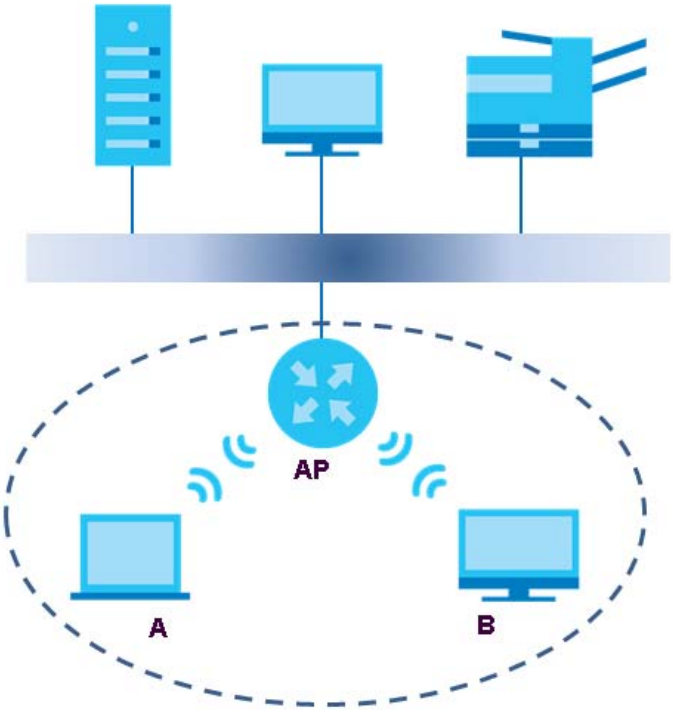
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 58 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless 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 wireless network must follow these basic guidelines.

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

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

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

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

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

Radio Channels

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

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

7.9.2 Additional Wireless Terms

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

Table 29 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless 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 wireless 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 wireless devices never have to get permission to send information to the Zyxel Device.
Preamble	A preamble affects the timing in your wireless 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 wireless device is allowed to use the wireless 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.

7.9.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless 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 wireless data network, or understand the data carried on it.

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

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

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless 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 wireless security you can set up in the wireless network.

7.9.3.1 SSID

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

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

7.9.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless 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 wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless 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 wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless 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.

7.9.3.3 User Authentication

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

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

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

7.9.3.4 Encryption

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

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

7.9.4 Signal Problems

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

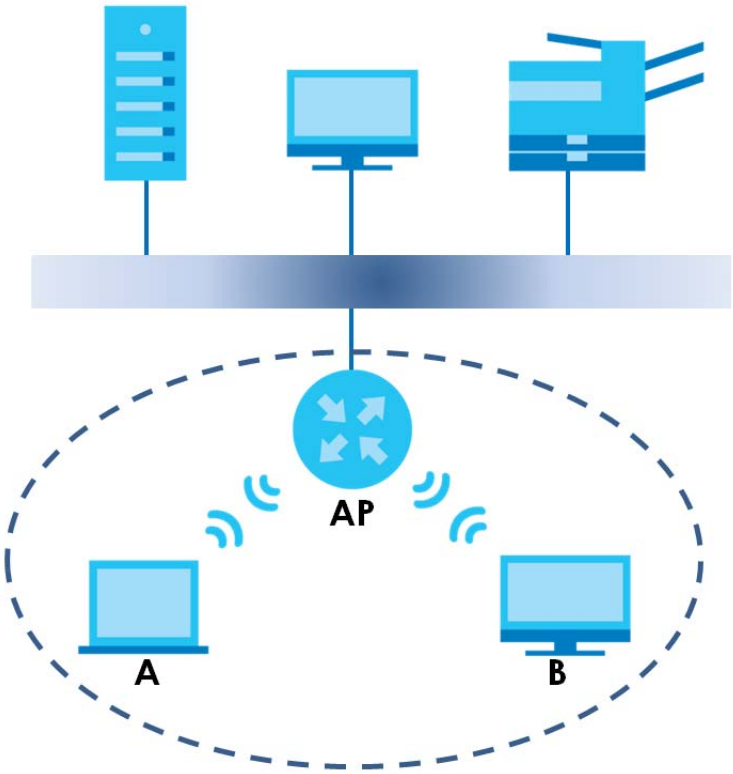
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters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

7.9.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

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

Figure 59 Basic Service set



7.9.6 MBSSID

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

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

7.9.6.1 Notes on Multiple BSSs

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

7.9.7 Preamble Type

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

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

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

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

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

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

7.9.8 WiFi Protected Setup (WPS)

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

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

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

7.9.8.1 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 7.6 on page 100).
3. Press the button on one of the devices (it doesn't matter which). For the Zyxel Device you must press the WPS button for more than five seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

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

7.9.8.2 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 wireless 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.

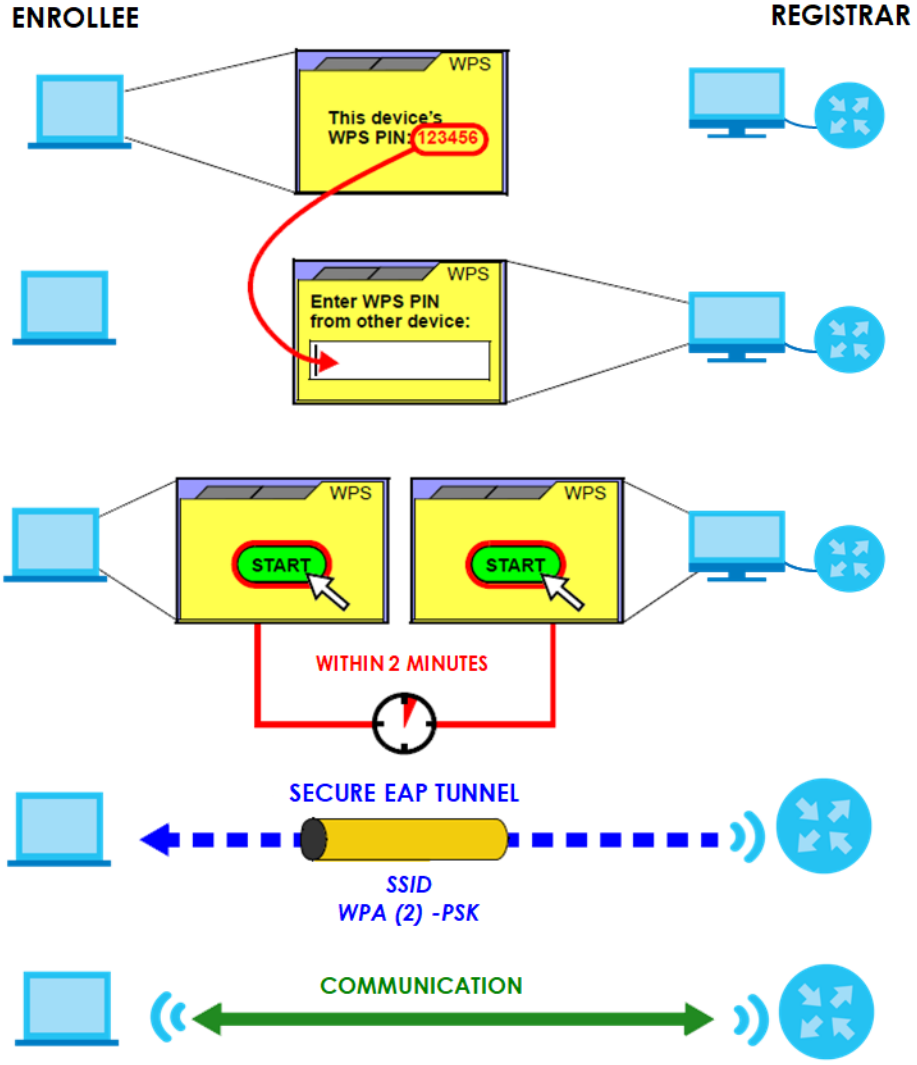
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

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 for 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 for how to find the WPS PIN - for the Zyxel Device, see Section 7.5 on page 99).
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 wireless client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

Figure 60 Example WPS Process: PIN Method

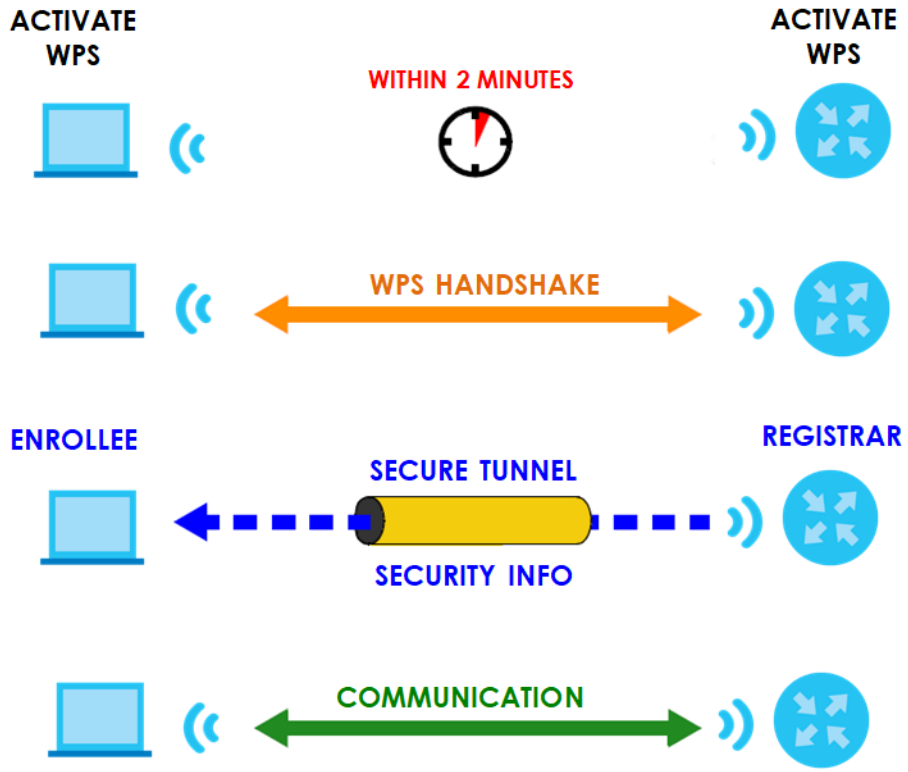


7.9.8.3 How WPS Works

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 61 How WPS works



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

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

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

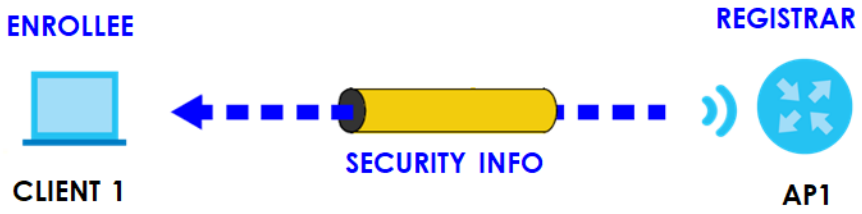
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless 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.

7.9.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

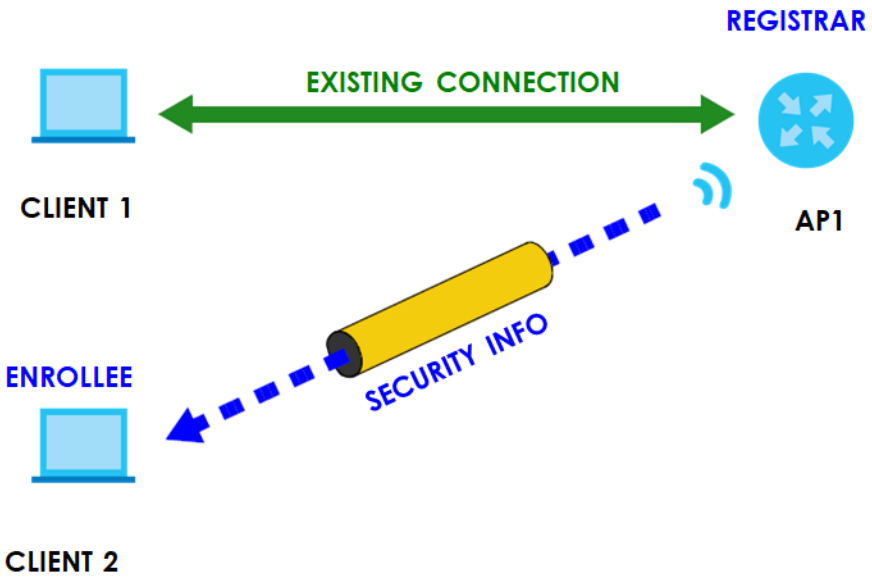
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 62 WPS: Example Network Step 1



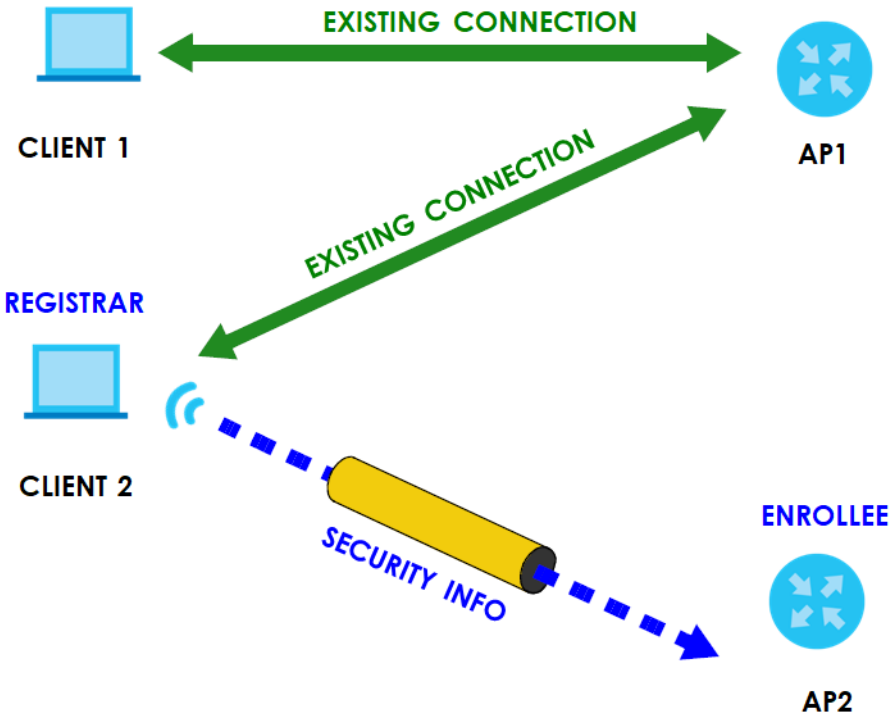
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 63 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 64 WPS: Example Network Step 3



7.9.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- 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 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 works between only two devices simultaneously, 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 wireless 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.

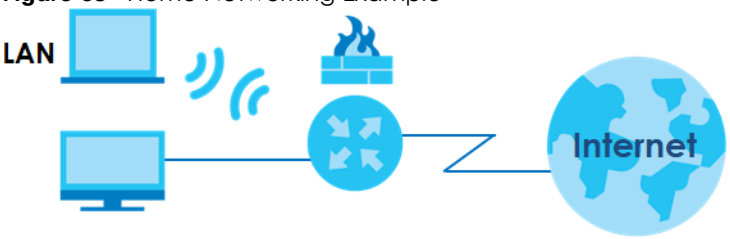
CHAPTER 8
Home Networking

8.1 Home Networking Overview

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

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.

Figure 65 Home Networking Example



8.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device (Section 8.2 on page 119).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 8.3 on page 123).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the Zyxel Device (Section 8.4 on page 125).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 8.5 on page 130).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses (Section 8.6 on page 132).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. (Section 8.7 on page 133).
- Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. (Section 8.8 on page 133).

8.1.2 What You Need To Know

8.1.2.1 About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, and so on) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your Zyxel Device an IP address, subnet mask, DNS and other routing information when it is turned on.

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 networking device before you can access it.

RADVD (Router Advertisement Daemon)

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

8.1.2.2 About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows 10). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

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

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

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

See the Chapter 11 on page 165 for more information on NAT.

Cautions with UPnP

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

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

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

UPnP and Zyxel

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

See Section 8.4.1 on page 126 for examples of installing and using UPnP.

Finding Out More

See Section 8.9 on page 134 for technical background information on LANs.

8.1.3 Before You Begin

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

8.2 LAN Setup

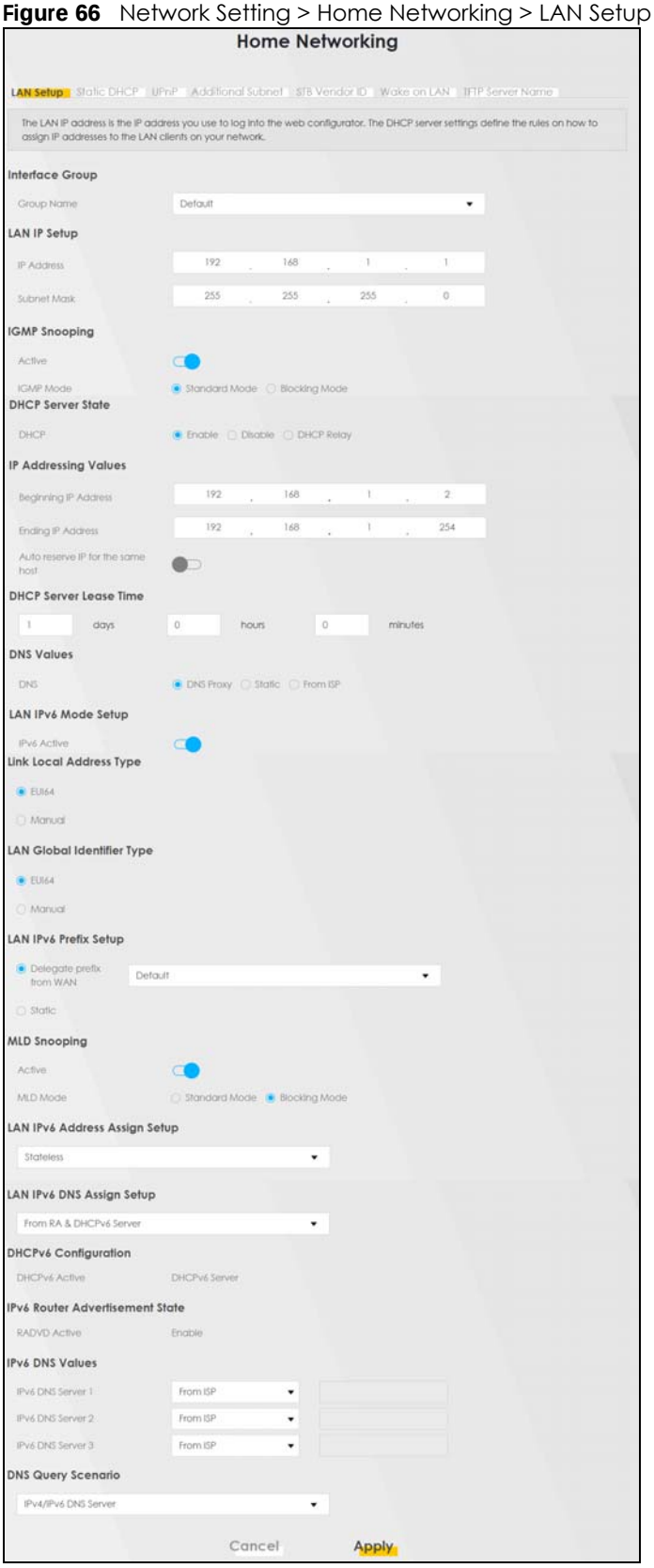
Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

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

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

Figure 66 Network Setting > Home Networking > LAN Setup



The following table describes the fields in this screen.

Table 30 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See Chapter 15 on page 192 for how to create a new interface group.
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.
IGMP Snooping	
Active	Select **Enable** to allow the Zyxel Device to passively learn multicast group.
IGMP Mode	Select **Standard Mode** to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
DHCP Server State	
DHCP	Select **Enable** to have the Zyxel Device act as a DHCP server or DHCP relay agent. Select **Disable** to stop the DHCP server on the Zyxel Device. Select **DHCP Relay** to have the Zyxel Device forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select **DHCP Relay** in the **DHCP** field.
IP Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.
IP Addressing Values	This field is only available when you select **Enable** in the **DHCP** field.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Click this switch to have the Zyxel Device record DHCP IP addresses with the MAC addresses the IP addresses are assigned to. When the switch goes to the right , the function is enabled. Otherwise, it is not. The Zyxel Device assigns the same IP address to the same MAC address when the host requests an IP address again through DHCP.
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select **Enable** in the **DHCP** field.
DNS	Select the type of service that you are registered for from your DNS service provider (**From ISP**). Select **DNS Proxy** if you have the DNS proxy service. The Zyxel Device redirects clients' DNS queries to a DNS server for resolving domain names. Select **Static** if you have the static DNS service.

Table 30 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Server 1/2	Enter the first and second DNS (Domain Name System) server IP addresses the Zyxel Device passes to the DHCP clients.
LAN IPv6 Mode Setup	
IPv6 Active	Click this switch to enable or disable the IPv6 mode and configure IPv6 settings on the Zyxel Device. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Link Local Address Type	
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	
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	
Delegate prefix from WAN	Select this option and specify a WAN interface (connection) through which the Zyxel Device automatically obtains an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 prefix for the Zyxel Device's LAN IPv6 address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
Active	Click this switch to enable or disable MLD Snooping on the Zyxel Device. When the switch goes to the right , the function is enabled. Otherwise, it is not. This allows the Zyxel Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
MLD Mode	Select **Standard Mode** to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: • **Stateless**: The Zyxel Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • **Stateful**: The Zyxel Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: • **From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements. • **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. • **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. **DHCPv6 Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 Address Values This section is available only when you select **Stateful** in the **LAN IPv6 Address Assign Setup** field.	

Table 30 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
IPv6 Start Address	Enter the first of the contiguous addresses in the IPv6 address pool.
IPv6 End Address	Enter the last of the contiguous addresses in the IPv6 address pool.
IPv6 Domain Name	Enter the domain name that is assigned to DHCPv6 clients.
IPv6 DNS Values	
IPv6 DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns IPv6 DNS server information. Select **User-Defined** if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. 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.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

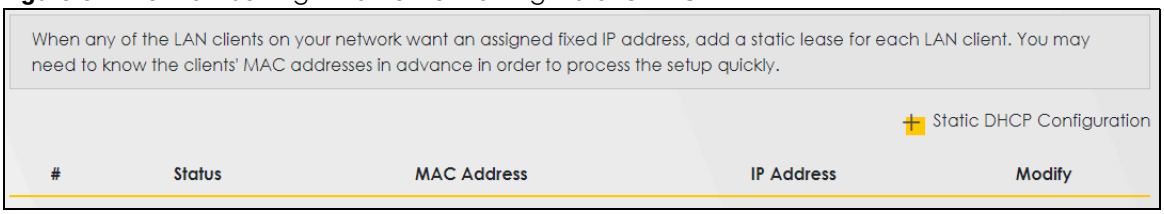
8.3 LAN Static DHCP

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.

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 67 Network Setting > Home Networking > Static DHCP



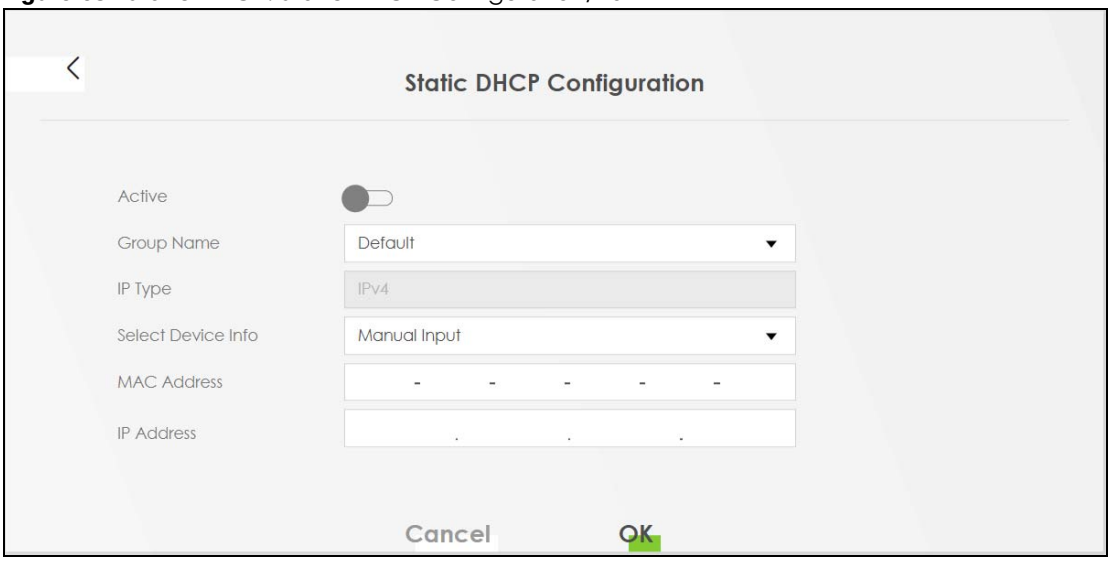
The following table describes the labels in this screen.

Table 31 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to add a new 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 have the IP address field editable and change it. Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

If you click **Static DHCP Configuration** in the **Static DHCP** screen or the **Edit** icon next to a static DHCP entry, 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 68 Static DHCP: Static DHCP Configuration/Edit



The following table describes the labels in this screen.

Table 32 Static DHCP: Static DHCP Configuration/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the connection between the client and the Zyxel Device. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Chapter 15 on page 192 for how to create a new interface group.

Table 32 Static DHCP: Static DHCP Configuration/Edit (continued)

LABEL	DESCRIPTION
IP Type	This field displays **IPv4** for the type of the DHCP IP address. At the time of writing, it is not allowed to select other type.
Select Device Info	Select a device or computer from the drop-down list or select **Manual Input** to manually enter a device's MAC address and IP address in the following fields.
MAC Address	If you select **Manual Input**, enter the MAC address of a computer on your LAN.
IP Address	If you select **Manual Input**, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

8.4 UPnP Settings

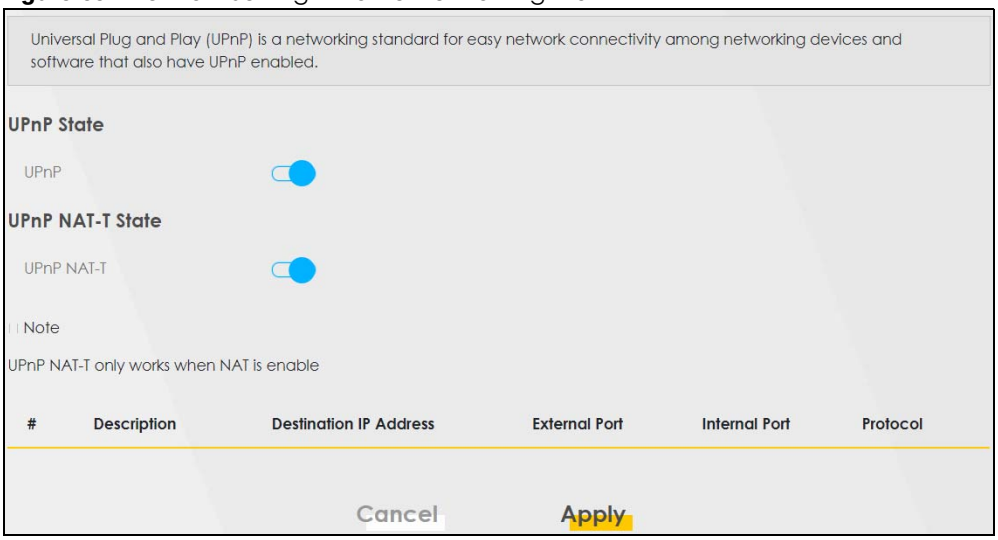
Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. A device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

See Section 8.4.1 on page 126 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.

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

Figure 69 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

Table 33 Network Setting > Home Networking > UPnP

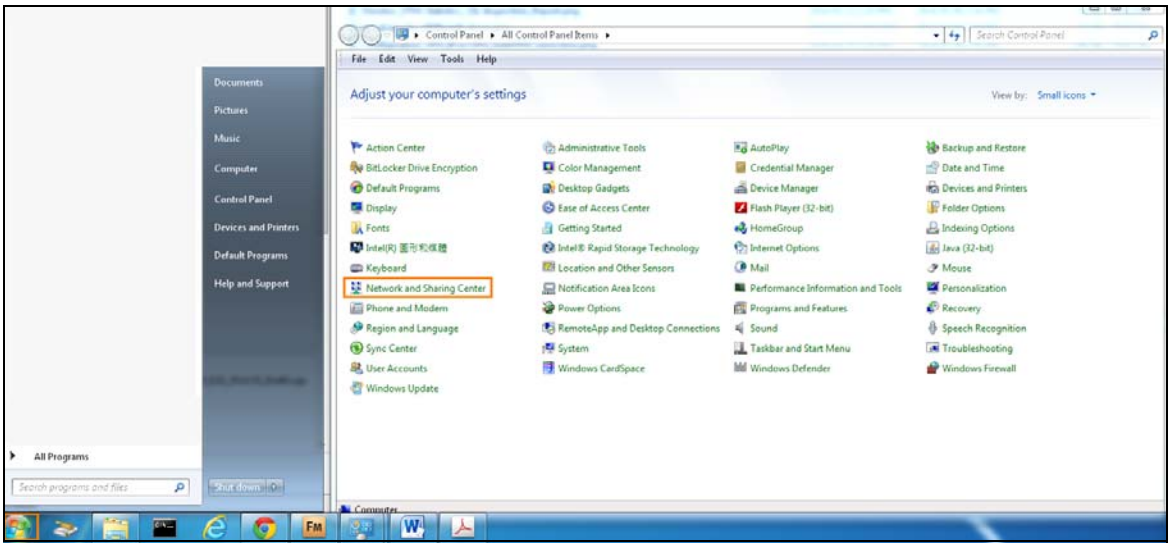
LABEL	DESCRIPTION
UPnP State	
UPnP	Click this switch to enable or disable UPnP. When the switch goes to the right , the function is enabled. Otherwise, it is not. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T State	
UPnP NAT-T	Click this switch to allow UPnP-enabled applications to automatically configure the Zyxel Device so that they can communicate through the Zyxel Device by using NAT traversal. When the switch goes to the right , the function is enabled. Otherwise, it is not. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. The table below displays the NAT port forwarding rules added automatically by UPnP NAT-T.
#	This is the index number of the UPnP NAT-T connection.
Description	This is the description of the UPnP NAT-T connection.
Destination IP Address	This is the IP address of the other connected UPnP-enabled device.
External Port	This is the external port number that identifies the service.
Internal Port	This is the internal port number that identifies the service.
Protocol	This is the transport layer protocol used for the service.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.4.1 Turning on UPnP in Windows 7 Example

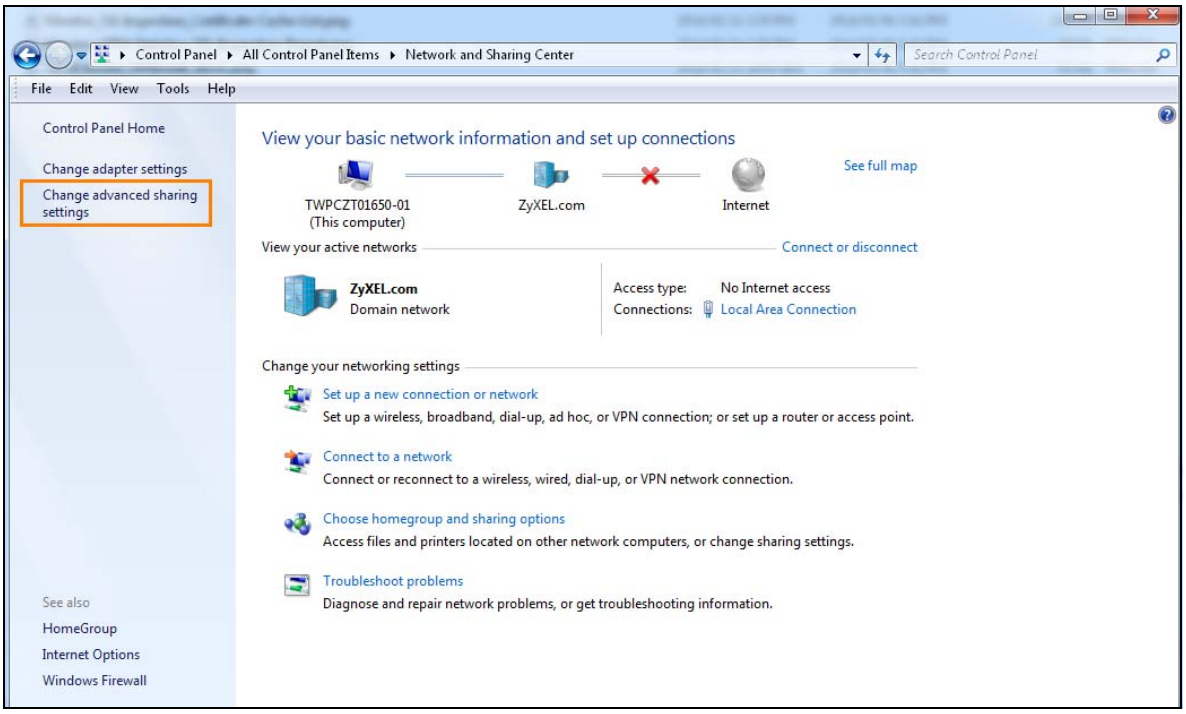
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device in **Network Setting > Home Networking > UPnP**.

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

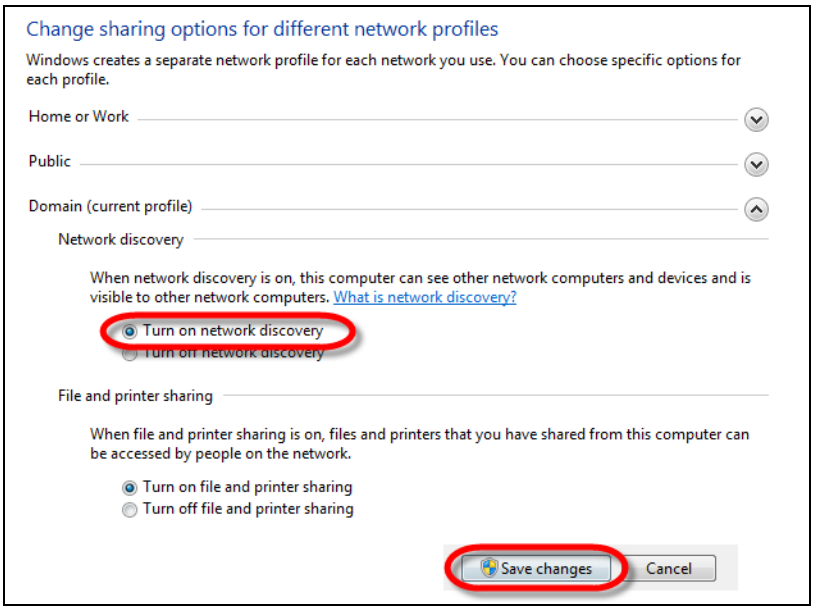
1 Click the start icon, **Control Panel** and then the **Network and Sharing Center.**



2 Click **Change Advanced Sharing Settings**.



3 Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.

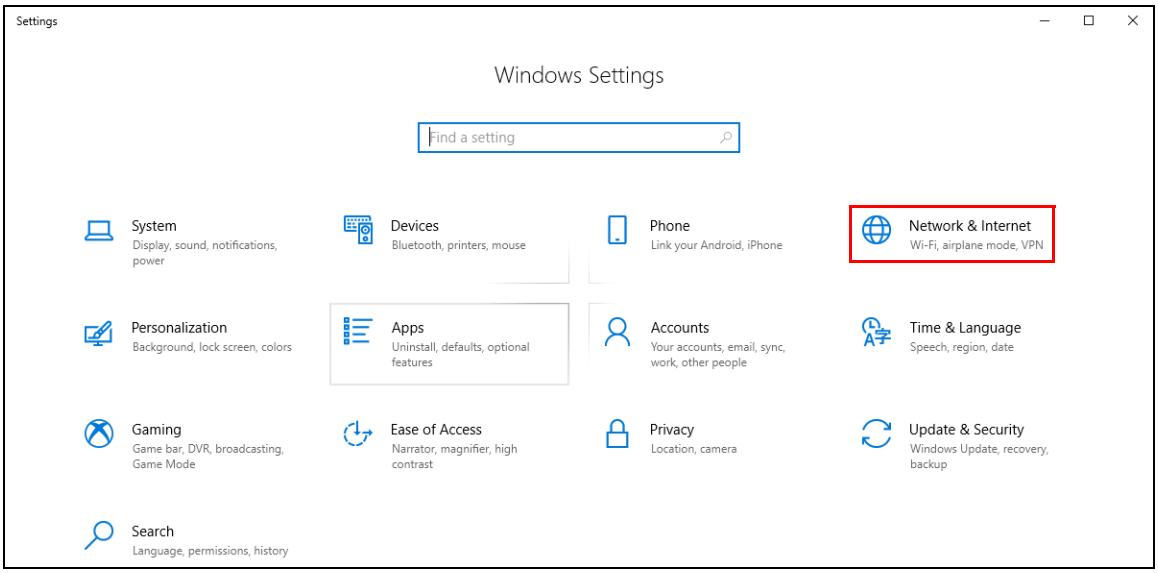


8.4.2 Turning on UPnP in Windows 10 Example

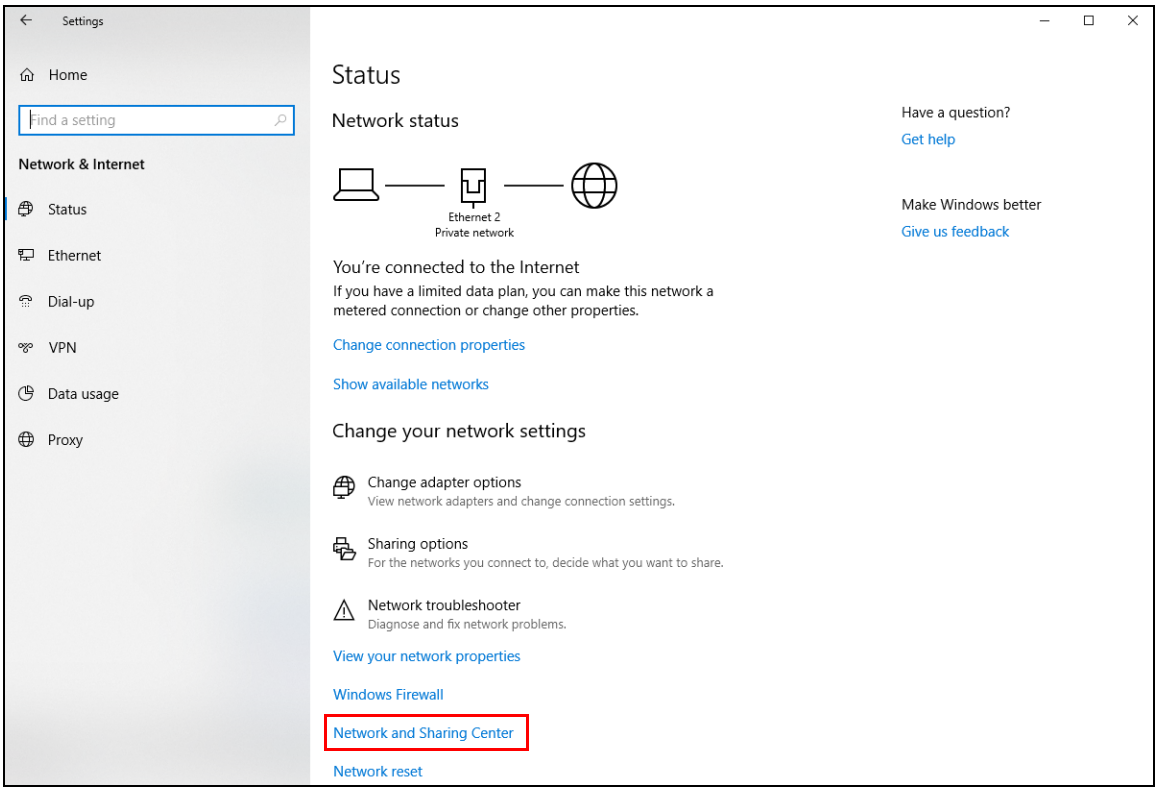
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device in **Network Setting > Home Networking > UPnP**.

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

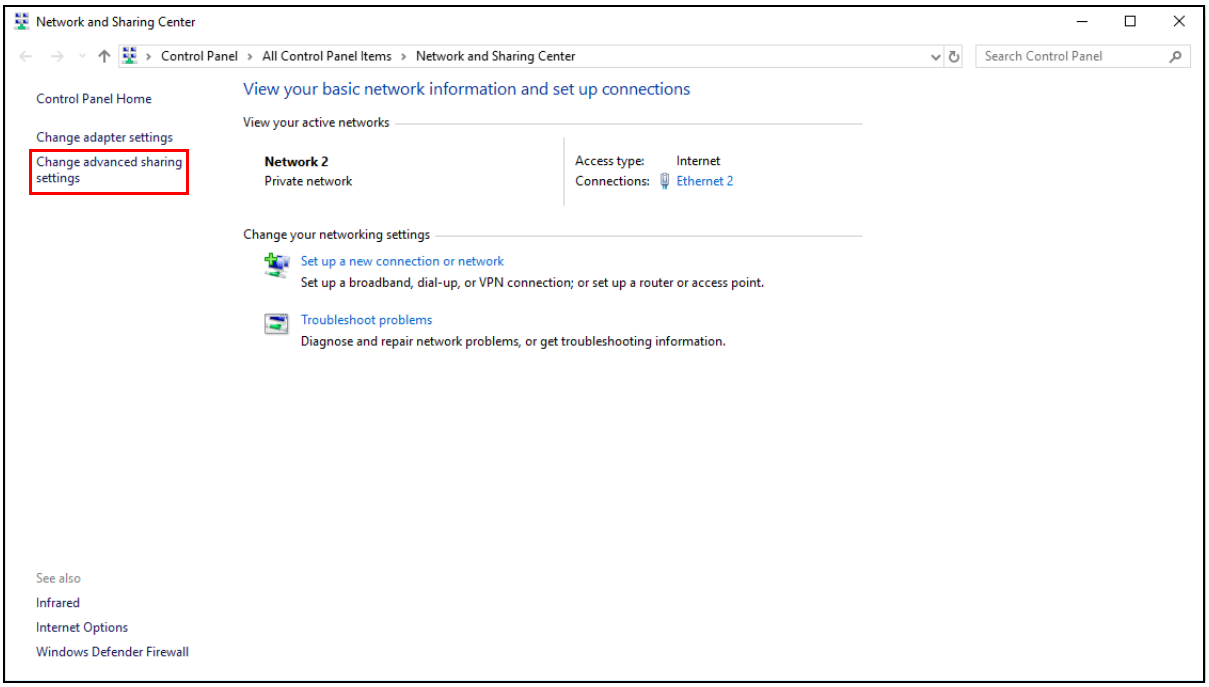
1 Click the start icon, **Settings** and then **Network & Internet**.



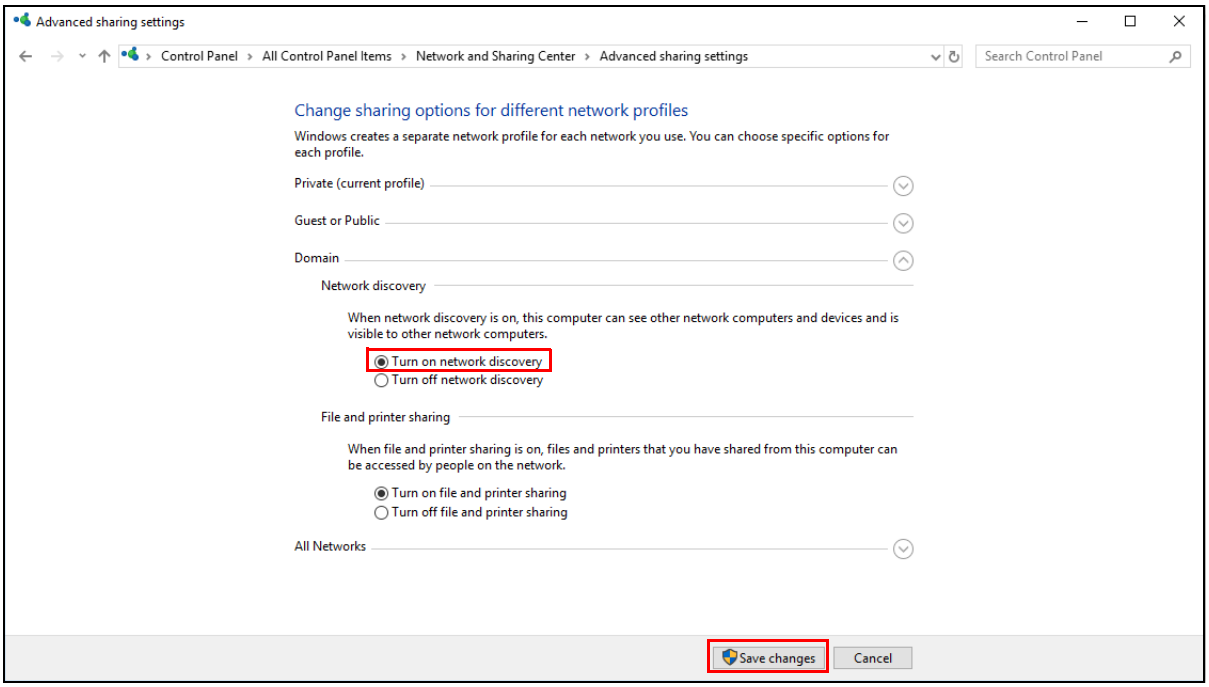
2 Click **Network and Sharing Center**.



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.



8.5 LAN Additional Subnet

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

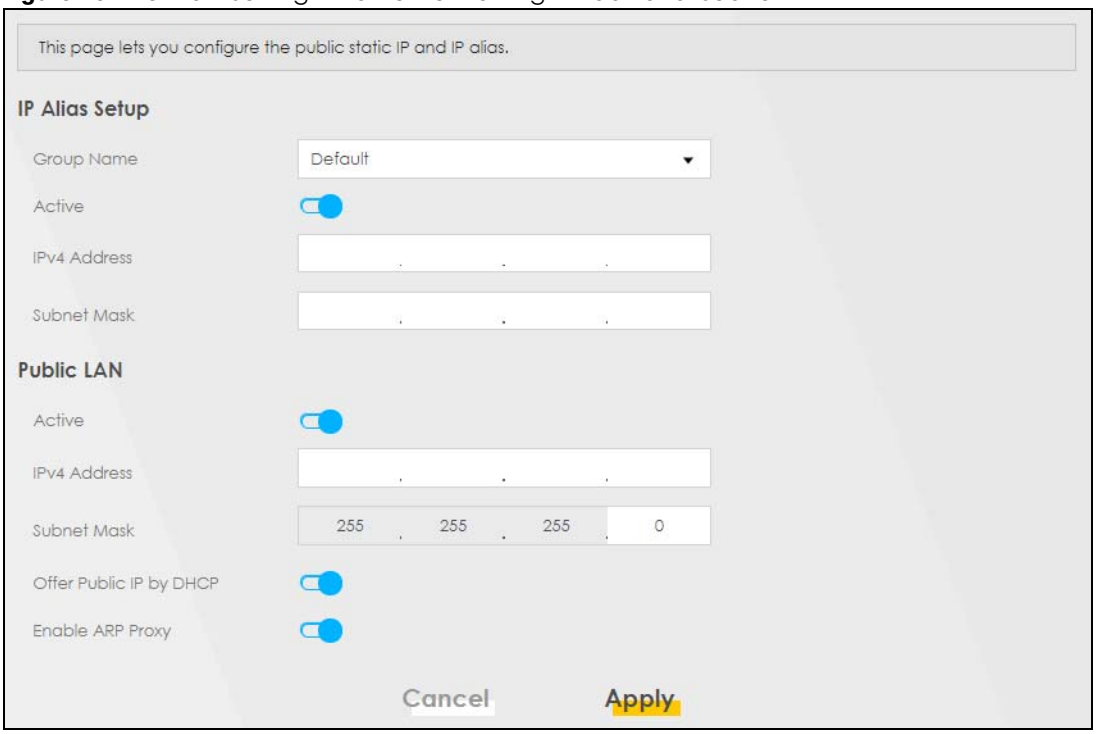
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Zyxel Device supports multiple logical LAN interfaces via its physical Ethernet interface

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

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

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

Figure 70 Network Setting > Home Networking > Additional Subnet



The following table describes the labels in this screen.

Table 34 Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Chapter 15 on page 192 for how to create a new interface group.
Active	Click this switch to configure a LAN network for the Zyxel Device. When the switch goes to the right , the following fields will be configurable. Otherwise, they are not.
IPv4 Address	Enter the IP address of your Zyxel Device in dotted decimal notation.
Subnet Mask	Your Zyxel Device will automatically calculate the subnet mask based on the IPv4 address that you assign. Unless you are implementing subnetting, use this value computed by the Zyxel Device.
Public LAN	
Active	Click this switch to enable or disable the Public LAN feature. When the switch goes to the right , the function is enabled. Otherwise, it is not. Your ISP must support Public LAN and static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.

Table 34 Network Setting > Home Networking > Additional Subnet (continued)

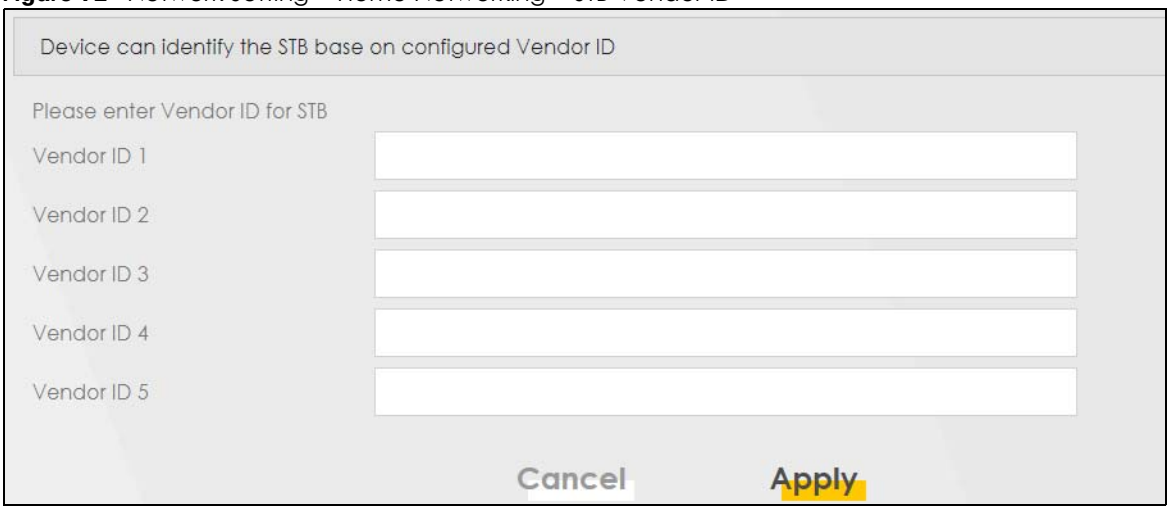
LABEL	DESCRIPTION
Offer Public IP by DHCP	Click this switch to enable or disable the Zyxel Device to provide public IP addresses by DHCP server. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Enable ARP Proxy	Click this switch to enable or disable the ARP (Address Resolution Protocol) proxy. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.6 STB Vendor ID

Use this screen to configure the Vendor IDs of connected Set Top Boxes (STBs) so the Zyxel Device can automatically create static DHCP entries for them when they request IP addresses.

Click **Network Setting** > **Home Networking** > **STB Vendor ID** to open this screen.

Figure 71 Network Setting > Home Networking > STB Vendor ID



The following table describes the labels in this screen.

Table 35 Network Setting > Home Networking > STB Vendor ID

LABEL	DESCRIPTION
Vendor ID 1~5	These are STB's Vendor Class Identifiers (DHCP option 60). A Vendor Class Identifier is usually used to inform the DHCP server a DHCP client's vendor and functionality.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

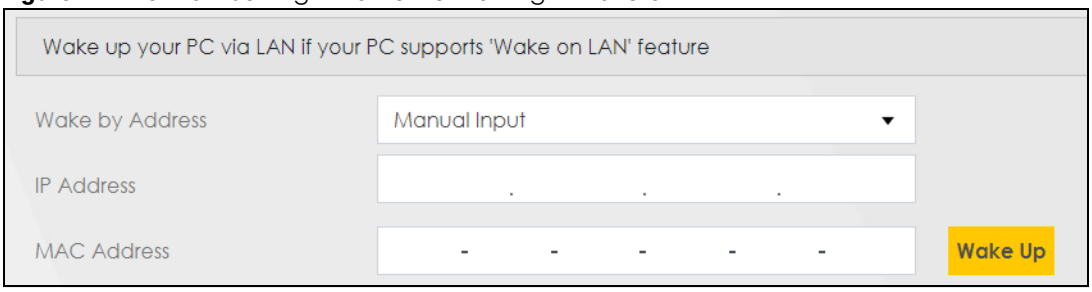
8.7 Wake on LAN

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

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

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

Figure 72 Network Setting > Home Networking > Wake on LAN



The following table describes the labels in this screen.

Table 36 Network Setting > Home Networking > Wake on LAN

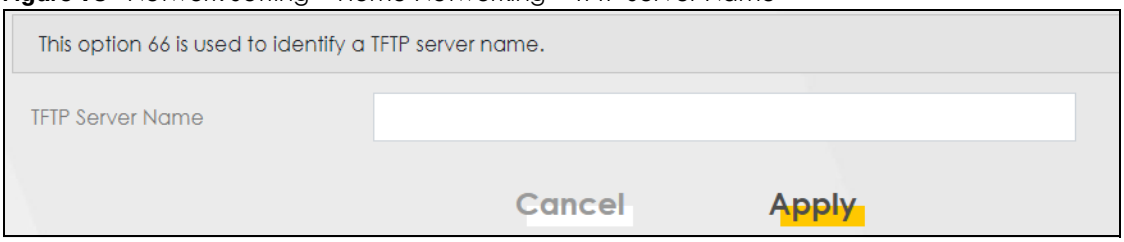
LABEL	DESCRIPTION
Wake by Address	Select **Manual Input** and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the Zyxel Device's ARP table. If you select an IP address, the MAC address of the device with the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

8.8 TFTP Server Name

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

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

Figure 73 Network Setting > Home Networking > TFTP Server Name



The following table describes the labels in this screen.

Table 37 Network Setting > Home Networking > TFTP Server Name

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

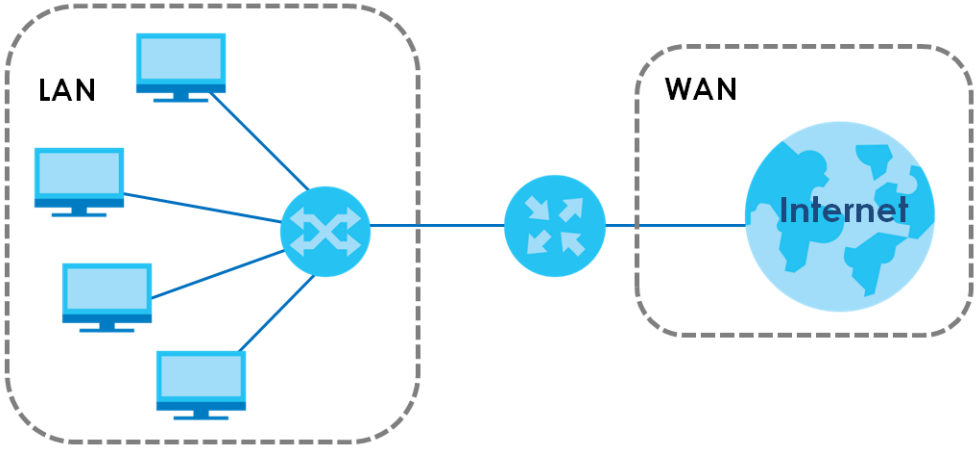
8.9 Technical Reference

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

8.9.1 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 74 LAN and WAN IP Addresses



8.9.2 DHCP Setup

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

IP Pool Setup

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

8.9.3 DNS Server Addresses

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

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

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

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

8.9.4 LAN TCP/IP

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

IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and

you must enable the Network Address Translation (NAT) feature of the Zyxel Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

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

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

Private IP Addresses

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

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

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

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

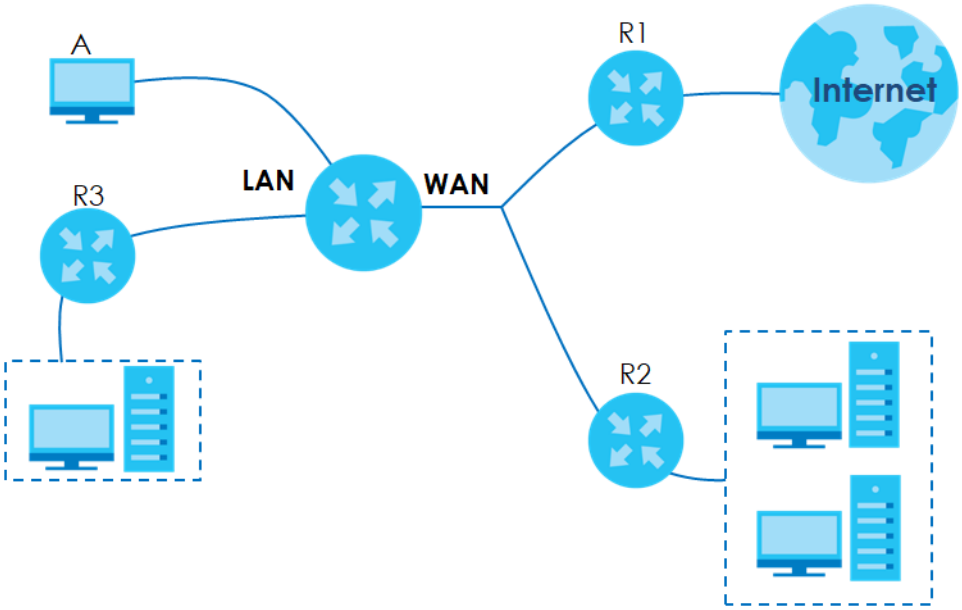
CHAPTER 9
Routing

9.1 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.

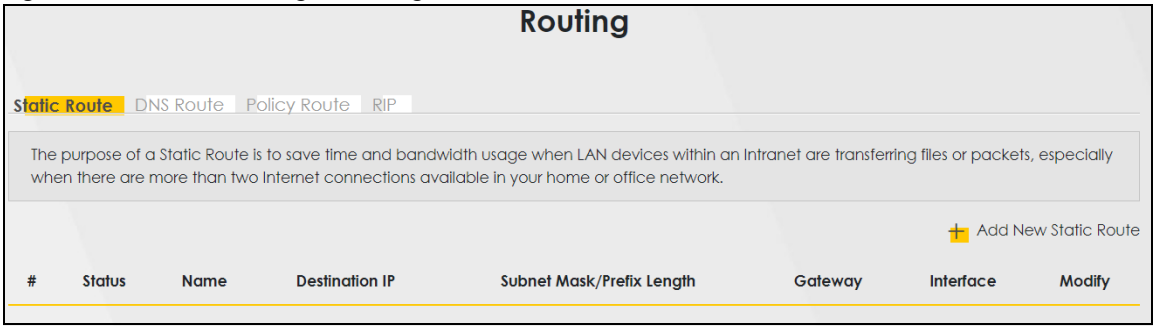
Figure 75 Example of Routing Topology



9.2 Static Route Settings

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. Click **Network Setting > Routing > Static Route** to open the following screen.

Figure 76 Network Setting > Routing > Static Route



The following table describes the labels in this screen.

Table 38 Network Setting > Routing > Static Route

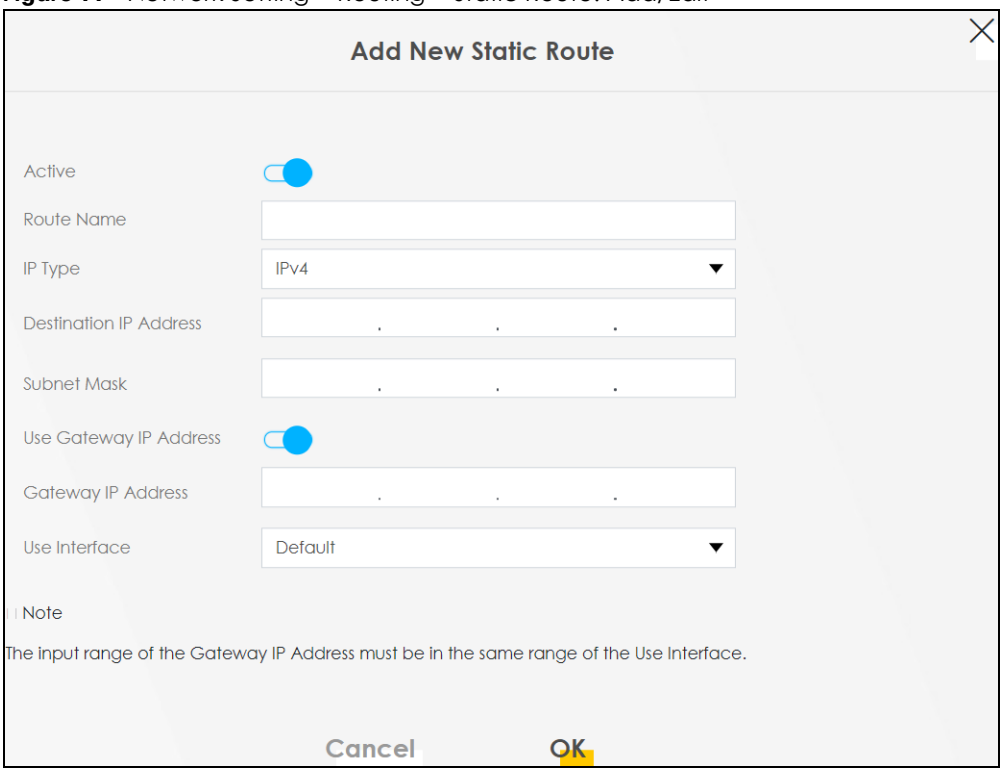
LABEL	DESCRIPTION
Add New Static Route	Click this to configure a new static route.
#	This is the index number of the entry.
Status	This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active.
Name	This is the name that describes or identifies this 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 used for this static route.
Modify	Click the **Edit** icon to edit the static route on the Zyxel Device. Click the **Delete** icon to remove a static route from the Zyxel Device. A window displays asking you to confirm that you want to delete the route.

9.2.1 Add/Edit Static Route

Use this screen to add or edit a static route. Click **Add new static route** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

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

Figure 77 Network Setting > Routing > Static Route: Add/Edit



The following table describes the labels in this screen.

Table 39 Network Setting > Routing > Static Route: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable this static route. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Route Name	Enter a descriptive name for the static route.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
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.
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

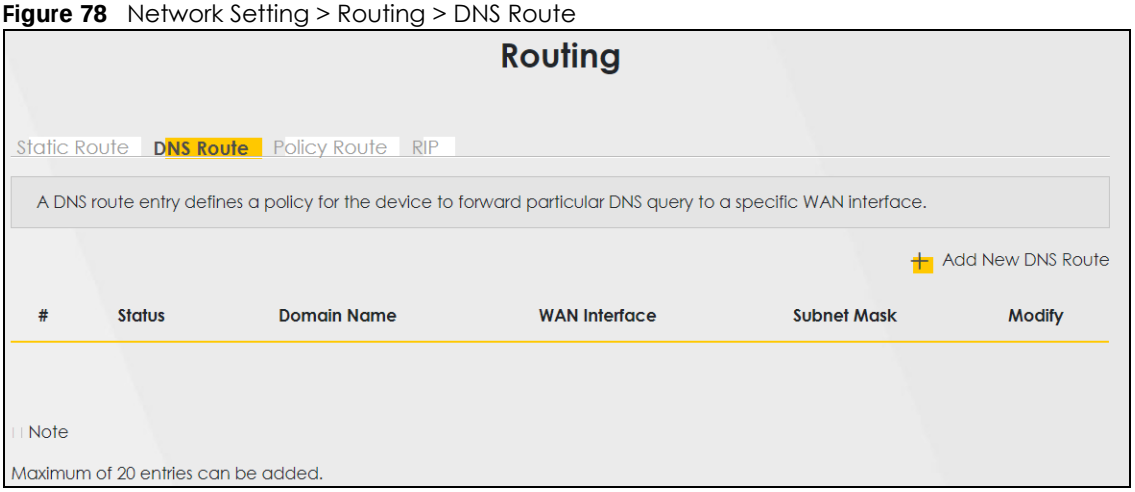
9.3 DNS Route

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.

Note: A maximum of 20 DNS routes can be added.

Click **Network Setting > Routing > DNS Route** to open the following screen.

Figure 78 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

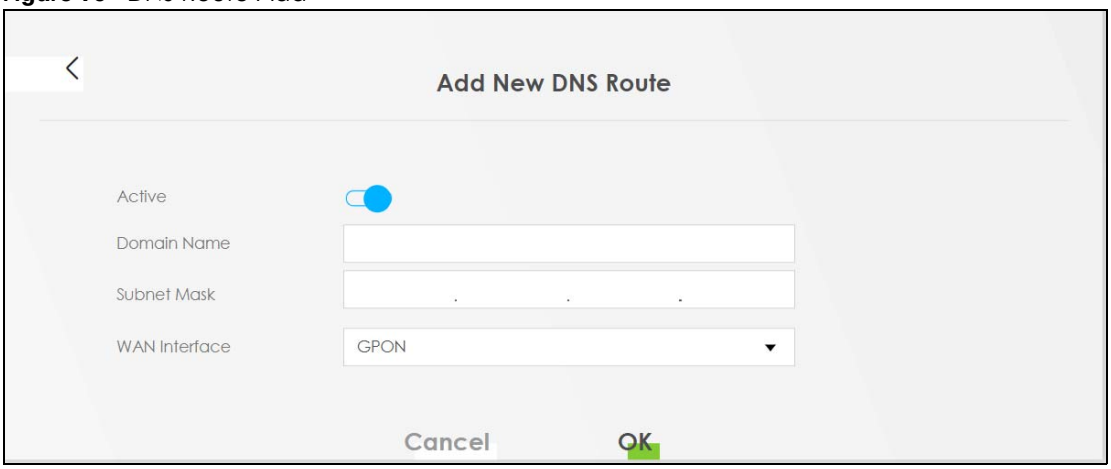
Table 40 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to add a new DNS route.
#	This is the index number of a DNS route.
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.
Domain Name	This is the host name or domain name of the DNS route entry.
WAN Interface	This is the WAN connection through which the Zyxel Device forwards DNS requests for this domain name.
Subnet Mask	This is the subnet mask of the DNS route entry.
Modify	Click the **Edit** icon to modify the DNS route. Click the **Delete** icon to delete the DNS route.

9.3.1 Add DNS Route

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **Network Setting > Routing > DNS Route** screen. The screen shown next appears.

Figure 79 DNS Route Add



The following table describes the labels in this screen.

Table 41 DNS Route Add

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the DNS route. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Domain Name	Enter the domain name of the DNS route entry.
Subnet Mask	Enter the subnet mask of the DNS route entry.
WAN Interface	Select the WAN connection through which the Zyxel Device forwards DNS requests for this domain name. **ETHWAN** means the wireless cellular interface.
Cancel	Click this to exit this screen without saving any changes.
OK	Click this to save your changes.

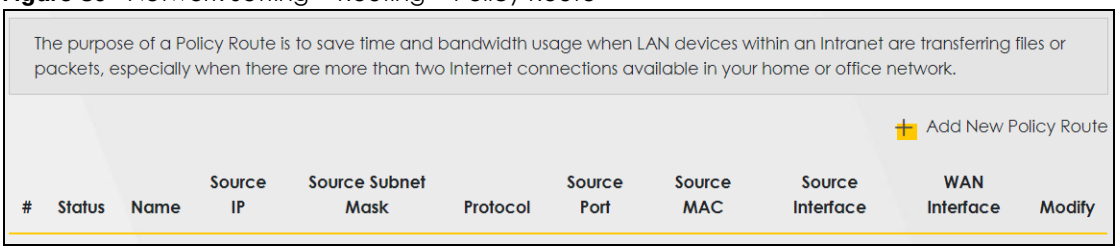
9.4 Policy Route

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. Policy routes allow the Zyxel Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

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

The **Policy Route** screen let you view and configure routing policies on the Zyxel Device. Click **Network Setting > Routing > Policy Route** to open the following screen.

Figure 80 Network Setting > Routing > Policy Route



The following table describes the labels in this screen.

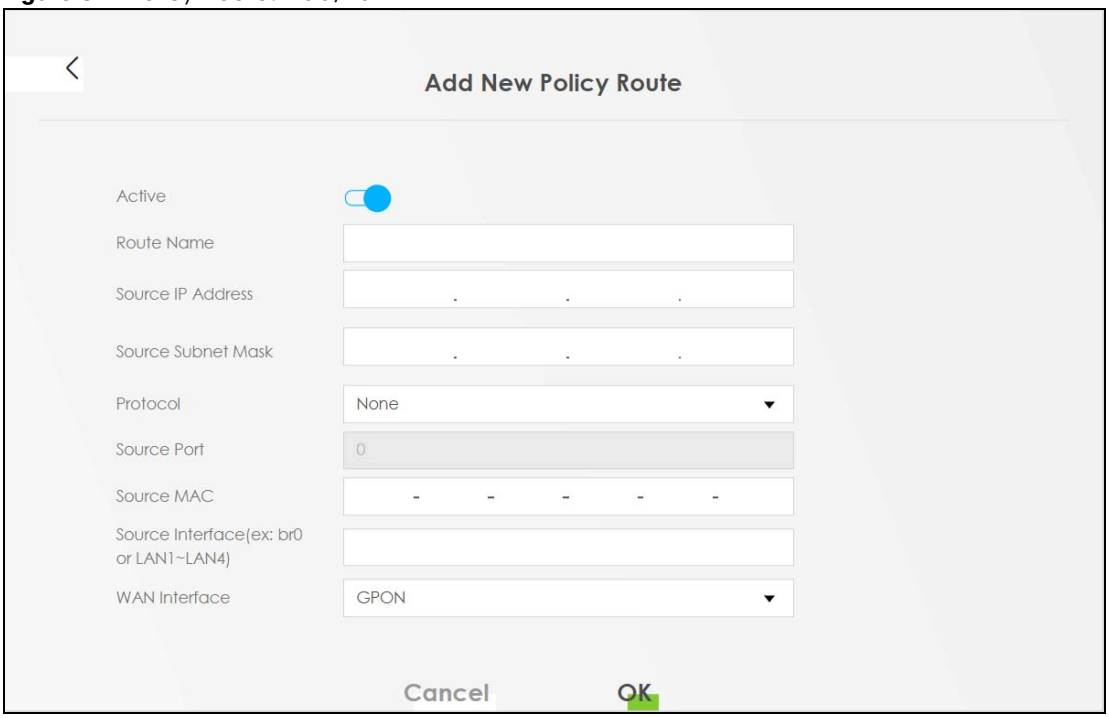
Table 42 Network Setting > Routing > Policy Route

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.

9.4.1 Add/Edit Policy Route

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

Figure 81 Policy Route: Add/Edit



The following table describes the labels in this screen.

Table 43 Policy Route: Add/Edit

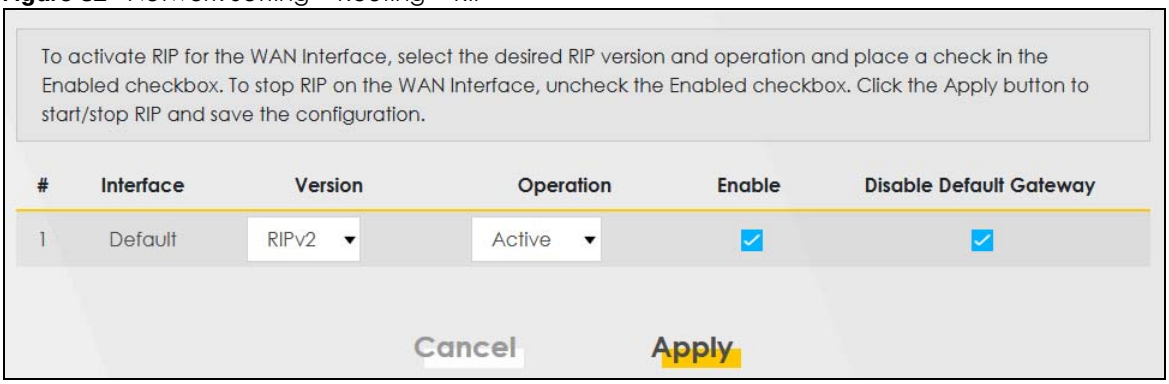
LABEL	DESCRIPTION
Active	Click this switch to enable or disable the policy route. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Route Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (ex: br0 or LAN1~LAN4)	Type the name of the interface from which the matched traffic is sent.
WAN Interface	This field shows **ETHWAN** as the WAN interface through which the traffic is sent.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

9.5 RIP Settings

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

Click **Network Setting > Routing > RIP** to open the **RIP** screen.

Figure 82 Network Setting > Routing > RIP



The following table describes the labels in this screen.

Table 44 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select **Passive** to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the check box to activate the settings.
Disable Default Gateway	Select the check box to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 10
Quality of Service (QoS)

10.1 QoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

Configure QoS on the Zyxel Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1. Configure classifiers to sort traffic into different flows.
2. Assign priority and define actions to be performed for a classified traffic flow.

The Zyxel Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video. There are eight priority levels, with 1 having the highest priority.

This chapter contains information about configuring QoS and editing classifiers.

10.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 10.3 on page 147).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 10.4 on page 149).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers (Section 10.5 on page 151).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface (Section 10.6 on page 156).
- The **Policer Setup** screen lets you control incoming traffic transmission rate and bursts (Section 10.7 on page 157).

10.2 What You Need to Know

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

QoS versus CoS

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

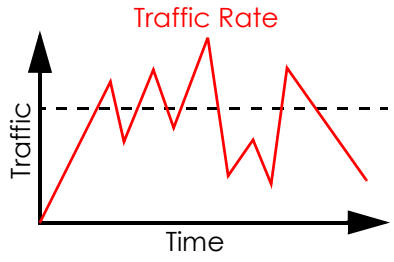
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

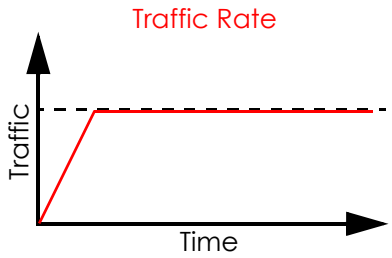
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Zyxel Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



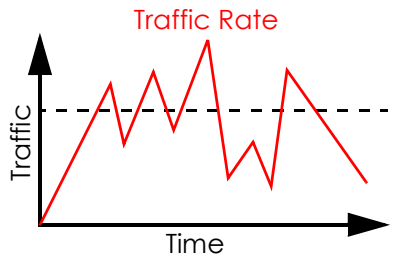
(Before Traffic Shaping)



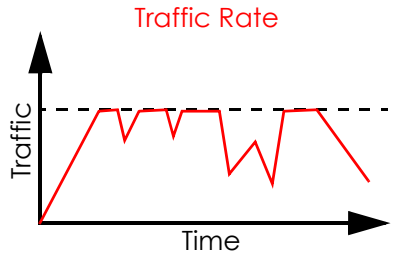
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

The Zyxel Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 10.8 on page 160 for more information on each metering algorithm.

10.3 Quality of Service General Settings

Click **Network Setting > QoS > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See Section 10.1 on page 145 for more information.

When one of the following situations happens, the current WAN linkup rate will be used instead:

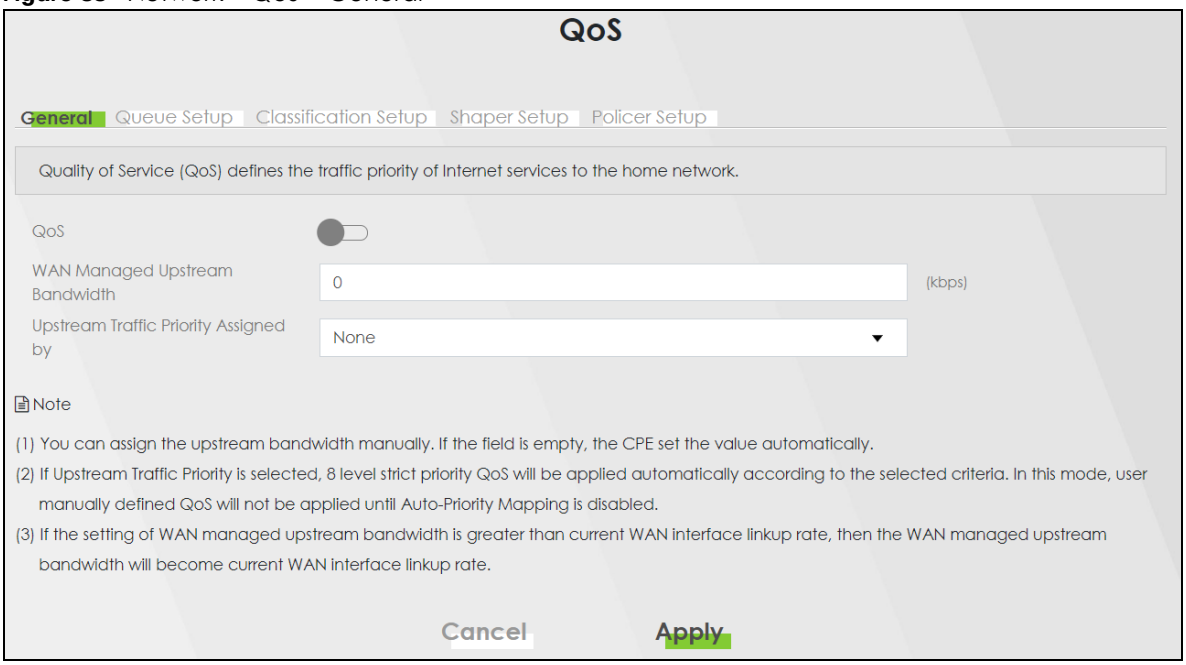
1. **WAN Managed Upstream Bandwidth** is set to 0
2. **WAN Managed Upstream Bandwidth** is empty
3. **WAN Managed Upstream Bandwidth** is higher than the current WAN interface linkup rate

Note: Manually defined QoS is ignored when **Upstream Traffic Priority** is selected.

Note: **Upstream Traffic Priority** automatically assigns a traffic priority level based on the selected criteria.

Note: To have your QoS settings configured in other **QoS** screens take effect, select **None** in the **Upstream Traffic Priority Assigned by** field.

Figure 83 Network > QoS > General



The following table describes the labels in this screen.

Table 45 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Select the **Enable** check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interfaces' actual transmission speed. The Zyxel Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed. You can also set this number lower than the interfaces' actual transmission speed. This will cause the Zyxel Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the Zyxel Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.
Upstream traffic priority Assigned by	Select how the Zyxel Device assigns priorities to various upstream traffic flows. • **None:** Disables auto priority mapping and has the Zyxel Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • **Ethernet Priority:** Automatically assign priority based on the IEEE 802.1p priority level. • **IP Precedence:** Automatically assign priority based on the first three bits of the TOS field in the IP header. • **Packet Length:** Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, Internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

10.4 Queue Setup

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

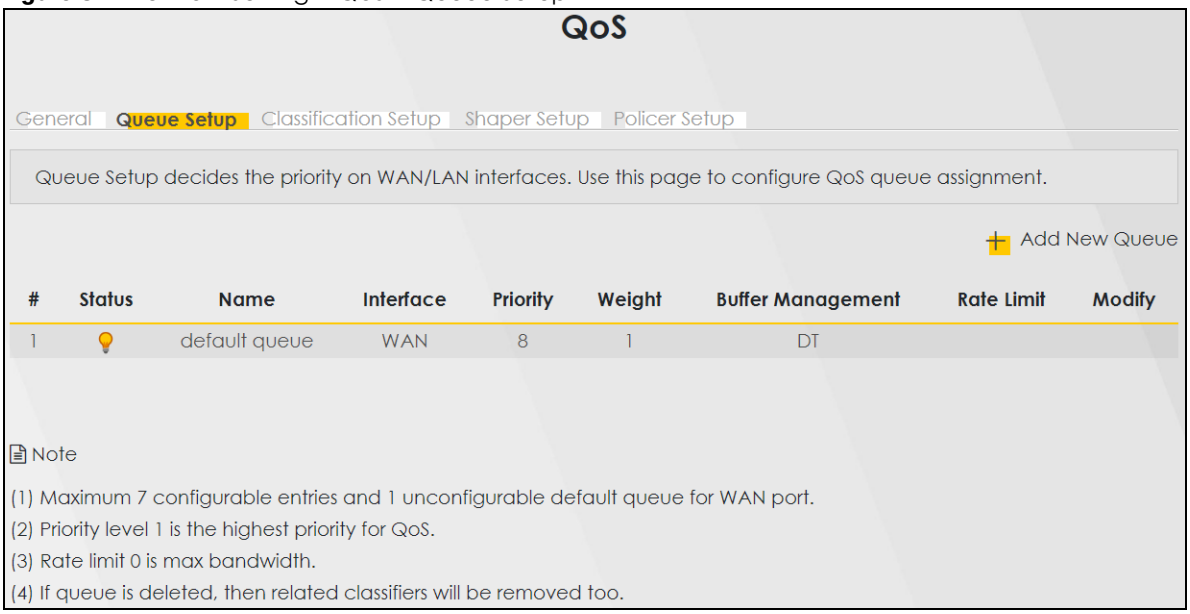
Use this screen to configure QoS queue assignment to decide the priority on WAN/LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

Note: Configure the priority level for a QoS queue from 1 to 8. The smaller the number in the **Priority** column, the higher the priority.

Note: The corresponding classifier(s) will be removed automatically if a queue is deleted.

Note: Rate limit 0 means there's no rate limit on a queue.

Figure 84 Network Setting > QoS > Queue Setup



The following table describes the labels in this screen.

Table 46 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add New Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue. The lower the number, the higher the priority level.
Weight	This shows the weight of this queue.

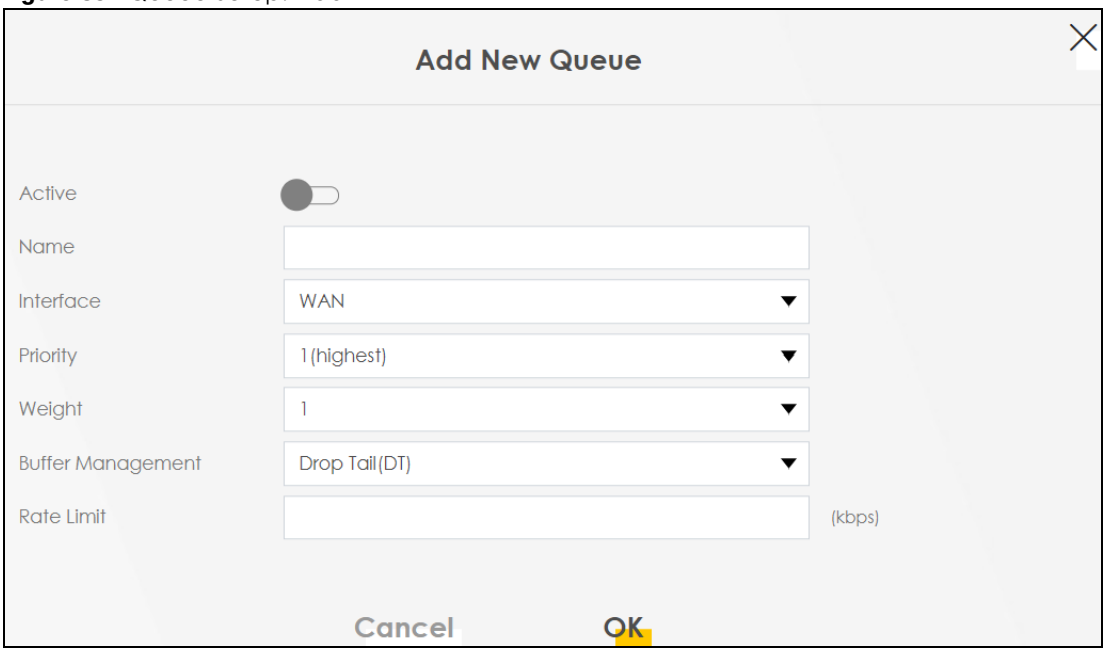
Table 46 Network Setting > QoS > Queue Setup (continued)

LABEL	DESCRIPTION
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Zyxel Device should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue. Rate limit 0 means there's no rate limit on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

10.4.1 Adding a QoS Queue

Click **Add New Queue** or the **Edit** icon in the **Queue Setup** screen to configure a queue.

Figure 85 Queue Setup: Add



The following table describes the labels in this screen.

Table 47 Queue Setup: Add

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the queue. When the switch turns blue , the function is enabled. Otherwise, it is not.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.