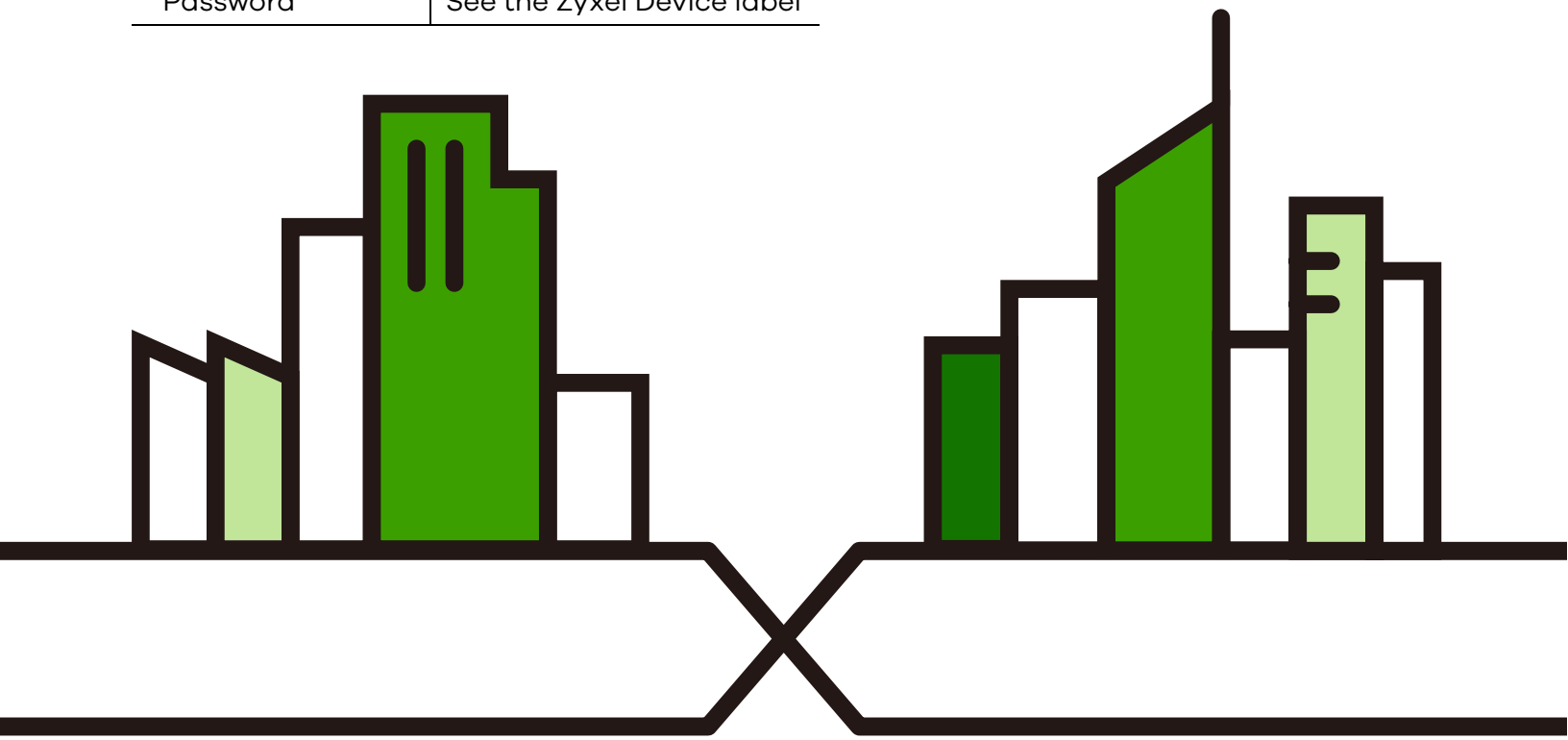
# User's Guide

# NBG7510

Dual-Band WiFi 6 AX1800 Router

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

Version 1.0 Ed 3, 10/2022



Copyright © 2022 Zyxel and/or its affiliates. All Rights Reserved.

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

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

## Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the Zyxel Device.
- More Information
- Go to *support.zyxel.com* to find other information on the Zyxel Device.

# Document Conventions

## Warnings and Notes

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

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

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

## Syntax Conventions

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

## Icons Used in Figures

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

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

# Contents Overview

**User's Guide** ..... **14**

Introducing the Zyxel Device ..... 15
Hardware ..... 25
Web Configurator ..... 31
Quick Start ..... 40
Tutorials ..... 44
Rover App Tutorials ..... 72

**Technical Reference** ..... **92**

Connection Status ..... 93
Broadband ..... 105
Wireless ..... 117
Home Networking ..... 143
Routing ..... 166
Network Address Translation (NAT) ..... 175
DNS ..... 192
Firewall ..... 196
MAC Filter ..... 207
Scheduler Rule ..... 209
Log ..... 211
Traffic Status ..... 214
ARP Table ..... 218
Routing Table ..... 220
WLAN Station Status ..... 223
Operating Mode ..... 225
System ..... 226
User Account ..... 227
Remote Management ..... 229
Time Settings ..... 233
Email Notification ..... 236
Log Setting ..... 239
Firmware Upgrade ..... 243
Backup/Restore ..... 246
Diagnostic ..... 250

**Troubleshooting and Appendices** ..... **252**

Troubleshooting ..... 253

# Table of Contents

**Document Conventions** ..... 3

**Contents Overview** ..... 4

**Table of Contents** ..... 5

**Part I: User's Guide** ..... 14

**Chapter 1**
**Introducing the Zyxel Device** ..... 15

1.1 Overview ..... 15
1.2 Applications for the Zyxel Device ..... 16
1.3 Mesh ..... 18
1.3.1 Network Controller ..... 18
1.3.2 Dual-Band WiFi ..... 19
1.3.3 AP Steering ..... 20
1.3.4 Band Steering ..... 21
1.3.5 Daisy Chain ..... 21
1.4 Operating Modes for the Zyxel Device ..... 22
1.4.1 Standard (Router) Mode ..... 22
1.4.2 AP (Bridge) Mode ..... 23
1.5 Ways to Manage the Zyxel Device ..... 23
1.6 Good Habits for Managing the Zyxel Device ..... 24

**Chapter 2**
**Hardware** ..... 25

2.1 LED ..... 25
2.2 Ports and Buttons ..... 27
2.3 How to Reset the Zyxel Device ..... 28
2.4 How to Enable WiFi/WPS ..... 28
2.5 Wall Mounting ..... 28

**Chapter 3**
**Web Configurator** ..... 31

3.1 Overview ..... 31
3.1.1 Access the Web Configurator ..... 31
3.2 Web Configurator Layout ..... 33
3.2.1 Settings Icon ..... 33

3.2.2 Widget Icon ..... 38

**Chapter 4**
**Quick Start ..... 40**

4.1 Overview ..... 40
4.2 Quick Start Setup ..... 40
4.3 Quick Start Setup – Time Zone ..... 40
4.4 Quick Start Setup – Internet Connection ..... 41
4.4.1 Successful Internet Connection ..... 41
4.4.2 Unsuccessful Internet Connection ..... 42
4.5 Quick Start Setup – WiFi ..... 42
4.6 Quick Start Setup – Finish ..... 43

**Chapter 5**
**Tutorials ..... 44**

5.1 Overview ..... 44
5.2 Wired Network Setup ..... 44
5.2.1 Setting Up an Ethernet Connection ..... 44
5.3 WiFi Network Setup ..... 46
5.3.1 Changing Security on a WiFi Network ..... 47
5.3.2 Connecting to the Zyxel Device's WiFi Network Using WPS ..... 49
5.3.3 Setting Up a Guest Network ..... 52
5.3.4 Setting Up Two Guest WiFi Networks on Different WiFi Bands ..... 56
5.4 Network Security ..... 61
5.4.1 Configuring a Firewall Rule ..... 61
5.4.2 Parental Control ..... 63
5.4.3 Configuring a MAC Address Filter ..... 68
5.5 Device Maintenance ..... 69
5.5.1 Backing up the Device Configuration ..... 69
5.5.2 Restoring the Device Configuration ..... 70

**Chapter 6**
**Rover App Tutorials ..... 72**

6.1 Overview ..... 72
6.2 What You Can Do ..... 72
6.3 WiFi Network Scenario ..... 72
6.3.1 Connect the Rover Router to the WRE6605 Repeater ..... 73
6.4 Wired Network Scenarios ..... 74
6.4.1 Scenario 1: Connect your Rover AP to the Rover Router ..... 74
6.4.2 Scenario 2: Connect the Rover Router to the WRE6605 AP ..... 75
6.5 Network Management with the Rover App ..... 77
6.6 Home Settings ..... 77
6.7 General WiFi and Guest Settings ..... 78

6.7.1 Setting Up General WiFi Settings ..... 79
6.7.2 Setting Up Guest WiFi Settings ..... 82
6.8 Devices Settings ..... 84
6.9 Parental Control Settings ..... 87
6.10 Others Settings ..... 89

**Part II: Technical Reference ..... 92**

**Chapter 7**
**Connection Status ..... 93**

7.1 Connection Status Overview ..... 93
7.1.1 Connectivity ..... 93
7.1.2 Icon and Device Name ..... 93
7.1.3 System Info ..... 94
7.1.4 WiFi Settings ..... 96
7.2 Guest WiFi Settings ..... 98
7.2.1 LAN ..... 100
7.3 The Parental Control Screen ..... 101
7.3.1 Create a Parental Control Profile ..... 102
7.3.2 Define a Schedule ..... 103

**Chapter 8**
**Broadband ..... 105**

8.1 Overview ..... 105
8.1.1 What You Can Do in this Chapter ..... 105
8.1.2 What You Need to Know ..... 106
8.1.3 Before You Begin ..... 108
8.2 Broadband Settings ..... 108
8.2.1 Edit Internet Connection ..... 109
8.3 Technical Reference ..... 114

**Chapter 9**
**Wireless ..... 117**

9.1 Overview ..... 117
9.1.1 What You Can Do in this Chapter ..... 117
9.1.2 What You Need to Know ..... 117
9.2 Wireless General Settings ..... 118
9.2.1 No Security ..... 121
9.2.2 More Secure (Recommended) ..... 121
9.3 Guest/More AP Screen ..... 122
9.3.1 The Edit Guest/More AP Screen ..... 123

9.4 MAC Authentication ..... 126
9.5 WPS ..... 127
9.6 WMM ..... 128
9.7 Others Screen ..... 129
9.8 Channel Status ..... 132
9.9 Mesh ..... 132
9.10 Mesh Topology ..... 133
9.11 Technical Reference ..... 134
9.11.1 WiFi Network Overview ..... 134
9.11.2 Additional Wireless Terms ..... 135
9.11.3 WiFi Security Overview ..... 135
9.11.4 Signal Problems ..... 137
9.11.5 BSS ..... 137
9.11.6 MBSSID ..... 138
9.11.7 Preamble Type ..... 138
9.11.8 WiFi Protected Setup (WPS) ..... 139

**Chapter 10**
**Home Networking ..... 143**

10.1 Overview ..... 143
10.1.1 What You Can Do in this Chapter ..... 143
10.1.2 What You Need To Know ..... 143
10.1.3 Before You Begin ..... 145
10.2 LAN Setup ..... 145
10.3 Static DHCP ..... 149
10.3.1 Before You Begin ..... 150
10.4 UPnP ..... 151
10.5 LAN Additional Subnet ..... 152
10.6 Wake on LAN ..... 154
10.7 TFTP Server Name ..... 155
10.8 Technical Reference ..... 156
10.8.1 DHCP Setup ..... 156
10.8.2 DNS Server Addresses ..... 156
10.8.3 LAN TCP/IP ..... 157
10.9 Turn on UPnP in Windows 10 Example ..... 158
10.9.1 Auto-discover Your UPnP-enabled Network Device ..... 160
10.10 Web Configurator Easy Access in Windows 10 ..... 163

**Chapter 11**
**Routing ..... 166**

11.1 Overview ..... 166
11.2 Configure Static Route ..... 166
11.2.1 Add or Edit Static Route ..... 167

11.3 DNS Route ..... 171
11.3.1 Add or Edit DNS Route ..... 172
11.4 Policy Route ..... 172
11.4.1 Add or Edit Policy Route ..... 173

**Chapter 12**
**Network Address Translation (NAT) ..... 175**

12.1 Overview ..... 175
12.1.1 What You Can Do in this Chapter ..... 175
12.1.2 What You Need To Know ..... 175
12.2 Port Forwarding ..... 176
12.2.1 Port Forwarding ..... 176
12.2.2 Add or Edit Port Forwarding ..... 177
12.3 Port Triggering ..... 179
12.3.1 Add or Edit Port Triggering Rule ..... 181
12.4 DMZ ..... 182
12.5 ALG ..... 183
12.6 Address Mapping ..... 184
12.6.1 Address Mapping Screen ..... 184
12.6.2 Add New Rule Screen ..... 185
12.7 Sessions ..... 187
12.8 Technical Reference ..... 187
12.8.1 NAT Definitions ..... 188
12.8.2 What NAT Does ..... 188
12.8.3 How NAT Works ..... 189
12.8.4 NAT Application ..... 189

**Chapter 13**
**DNS ..... 192**

13.1 DNS Overview ..... 192
13.1.1 What You Can Do in this Chapter ..... 192
13.1.2 What You Need To Know ..... 193
13.2 DNS Entry ..... 193
13.2.1 Add or Edit DNS Entry ..... 194
13.3 Dynamic DNS ..... 194

**Chapter 14**
**Firewall ..... 196**

14.1 Overview ..... 196
14.1.1 What You Need to Know About Firewall ..... 196
14.2 Firewall ..... 197
14.2.1 What You Can Do in this Chapter ..... 198
14.3 Firewall General Settings ..... 198

14.4 Protocol (Customized Services) ..... 199
14.4.1 Add Customized Service ..... 200
14.5 Access Control (Rules) ..... 200
14.5.1 Add New ACL Rule ..... 201
14.6 DoS ..... 203
14.7 Firewall Technical Reference ..... 204
14.7.1 Firewall Rules Overview ..... 204
14.7.2 Guidelines For Security Enhancement With Your Firewall ..... 205
14.7.3 Security Considerations ..... 205

**Chapter 15**
**MAC Filter ..... 207**

15.1 MAC Filter Overview ..... 207
15.2 MAC Filter ..... 207
15.2.1 Add New Rule ..... 208

**Chapter 16**
**Scheduler Rule ..... 209**

16.1 Scheduler Rule Overview ..... 209
16.2 Scheduler Rule Settings ..... 209
16.2.1 Add or Edit a Schedule Rule ..... 210

**Chapter 17**
**Log ..... 211**

17.1 Log Overview ..... 211
17.1.1 What You Can Do in this Chapter ..... 211
17.1.2 What You Need To Know ..... 211
17.2 System Log ..... 212
17.3 Security Log ..... 213

**Chapter 18**
**Traffic Status ..... 214**

18.1 Traffic Status Overview ..... 214
18.1.1 What You Can Do in this Chapter ..... 214
18.2 WAN Status ..... 214
18.3 LAN Status ..... 216
18.4 NAT Status ..... 217

**Chapter 19**
**ARP Table ..... 218**

19.1 ARP Table Overview ..... 218
19.1.1 How ARP Works ..... 218
19.2 ARP Table ..... 218

**Chapter 20**
**Routing Table ..... 220**

20.1 Routing Table Overview ..... 220
20.2 Routing Table ..... 220

**Chapter 21**
**WLAN Station Status ..... 223**

21.1 WLAN Station Status Overview ..... 223

**Chapter 22**
**Operating Mode ..... 225**

22.1 Overview ..... 225

**Chapter 23**
**System ..... 226**

23.1 System Overview ..... 226
23.2 System ..... 226

**Chapter 24**
**User Account ..... 227**

24.1 User Account Overview ..... 227
24.2 User Account ..... 227

**Chapter 25**
**Remote Management ..... 229**

25.1 Overview ..... 229
25.1.1 What You Can Do in this Chapter ..... 229
25.2 MGMT Services ..... 229
25.3 Trust Domain ..... 231
25.4 Add Trust Domain ..... 231

**Chapter 26**
**Time Settings ..... 233**

26.1 Time Settings Overview ..... 233
26.2 Time ..... 233

**Chapter 27**
**Email Notification ..... 236**

27.1 Email Notification Overview ..... 236
27.2 Email Notification ..... 236
27.2.1 E-mail Notification Edit ..... 237

**Chapter 28**
**Log Setting .....239**

28.1 Log Setting Overview ..... 239
28.2 Log Setting ..... 239
28.2.1 Example Email Log ..... 241

**Chapter 29**
**Firmware Upgrade .....243**

29.1 Overview ..... 243
29.2 Firmware Upgrade ..... 243
29.3 Module Upgrade ..... 244

**Chapter 30**
**Backup/Restore .....246**

30.1 Backup/Restore Overview ..... 246
30.2 Backup/Restore ..... 246
30.3 Reboot ..... 249

**Chapter 31**
**Diagnostic.....250**

31.1 Diagnostic Overview ..... 250
31.1.1 What You Can Do in this Chapter ..... 250
31.2 Diagnostic ..... 250

**Part III: Troubleshooting and Appendices..... 252**

**Chapter 32**
**Troubleshooting.....253**

32.1 Overview ..... 253
32.2 Power and Hardware Problems ..... 253
32.3 Device Access Problems ..... 254
32.4 Internet Problems ..... 257
32.5 WiFi Problems ..... 258
32.6 UPnP Problems ..... 258

Appendix A Customer Support ..... 260

Appendix B IPv6..... 265

Appendix C Services..... 271

Appendix D Legal Information ..... 275

**Index .....281**

# PART I
# User's Guide

# CHAPTER 1
# Introducing the Zyxel Device

## 1.1 Overview

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

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

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

Table 1 Features Supported

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

# 1.2 Applications for the Zyxel Device

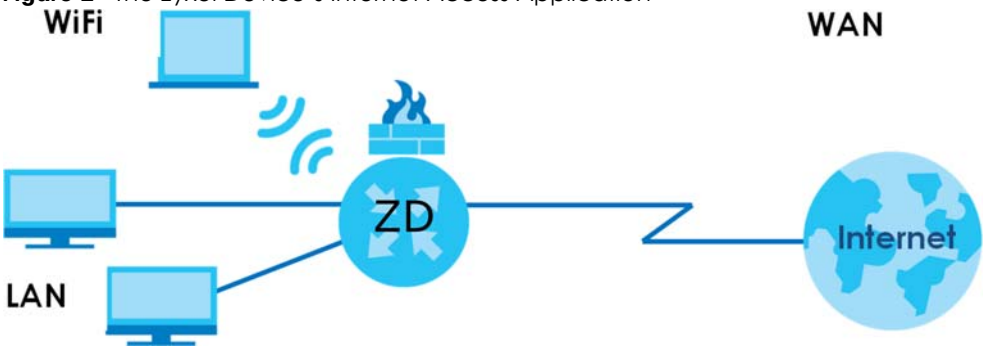
The Zyxel Device supports the following features.

## Internet Access

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

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

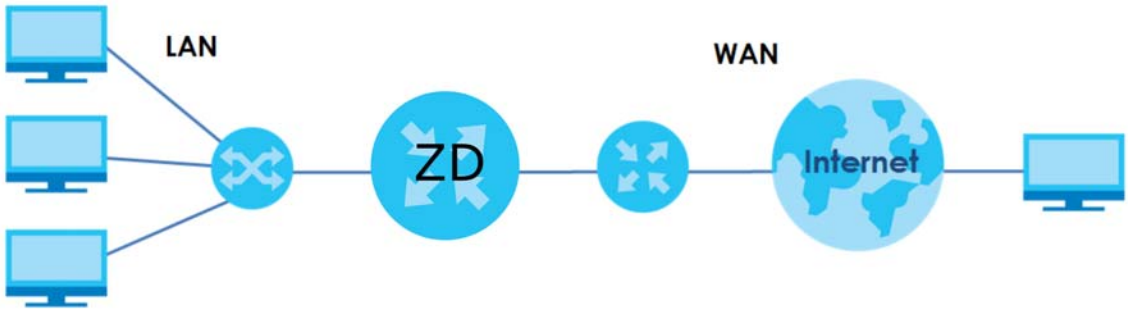
**Figure 1** The Zyxel Device's Internet Access Application




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

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

**Figure 2** The Zyxel Device's Internet Access Application: Ethernet WAN



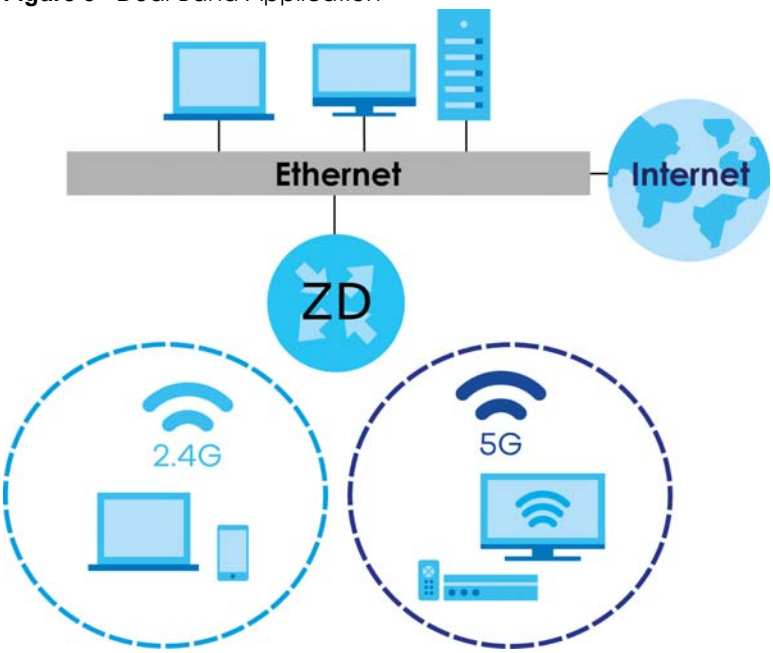

## Dual-Band WiFi

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

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

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

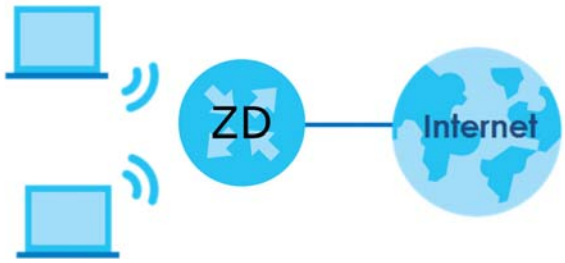
**Figure 3** Dual-Band Application




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

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

**Figure 4** WiFi Access Example




## Guest WiFi

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

## IPv6 and IPv6 Firewall

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and support IPv6 rapid deployment (6RD).

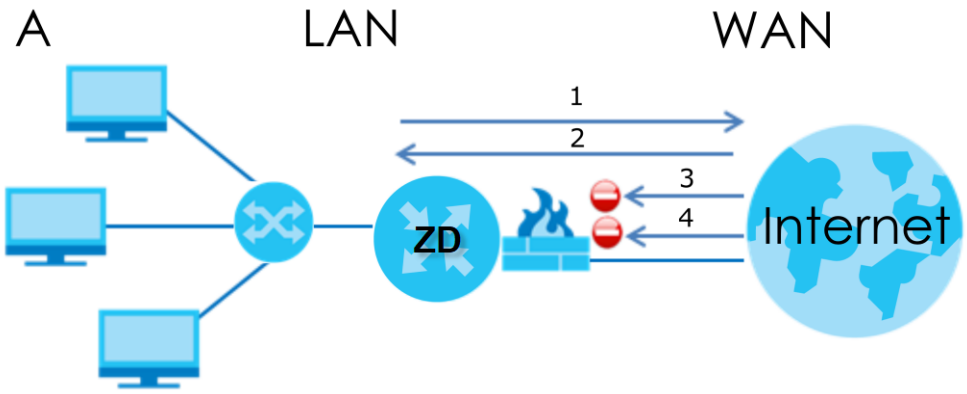
Consequently, you can enable and create IPv6 firewall rules to filter IPv6 traffic.

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

- allows traffic that originates from your LAN computers to go to all other networks
- blocks traffic that originates on other networks from going to the LAN

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

**Figure 5** Firewall Default Action




# 1.3 Mesh

An Mesh network is composed of three key components.

(A) A router works as a controller to manage and optimize the Mesh network.

(B) One or more devices in the Mesh network function as APs or WiFi Extenders to extend the WiFi communication range.

(C) Multiple client devices connect to the Mesh network for Internet connections.

## 1.3.1 Network Controller

The Mesh Router is the Network Controller and the Extender is also known as a Satellite.

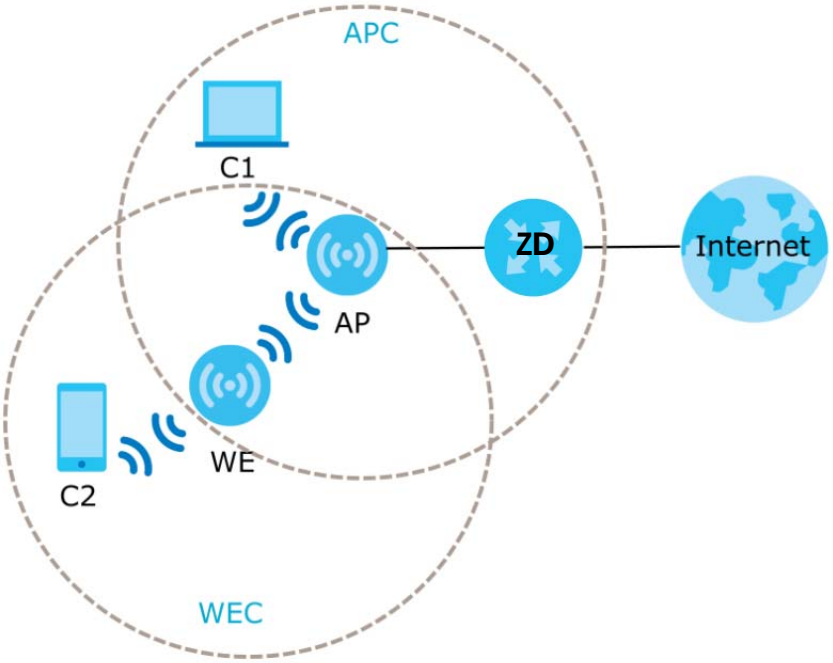
The Zyxel Device functions as a controller to coordinate and optimize WiFi activity In the Mesh network. The controller collects Channel Availability Check responses and scan reports from the APs or WiFi Extenders. Then, the controller selects the best channel and the final optimized topology based on the current situation.

The Mesh network uses AP steering and Band steering mechanisms to improve WiFi performance. AP steering allows WiFi clients to roam seamlessly in an Mesh network. Band steering allows 2.4 GHz / 5 GHz dual-band WiFi clients to move from one band to another less busy band. For AP steering to work, the controller and the devices in the Mesh network must use the same SSID and password. For band steering

to work, the SSIDs and passwords of 2.4GHz and 5GHz must be identical. See Section 1.3.3 on page 20 and Section 1.3.4 on page 21 for more information. The controller synchronizes the SSIDs and passwords during auto-configuration.

- The Zyxel Device connects to an AP using an Ethernet cable to expand the WiFi coverage.
- The Zyxel Device connects to a WiFi extender using WiFi. You can place the WiFi extender between the Zyxel Device and the WiFi clients who require WiFi but are not in the coverage of the Zyxel Device.

**Figure 6** Mesh Application




The following table describes the icons used in the figure.

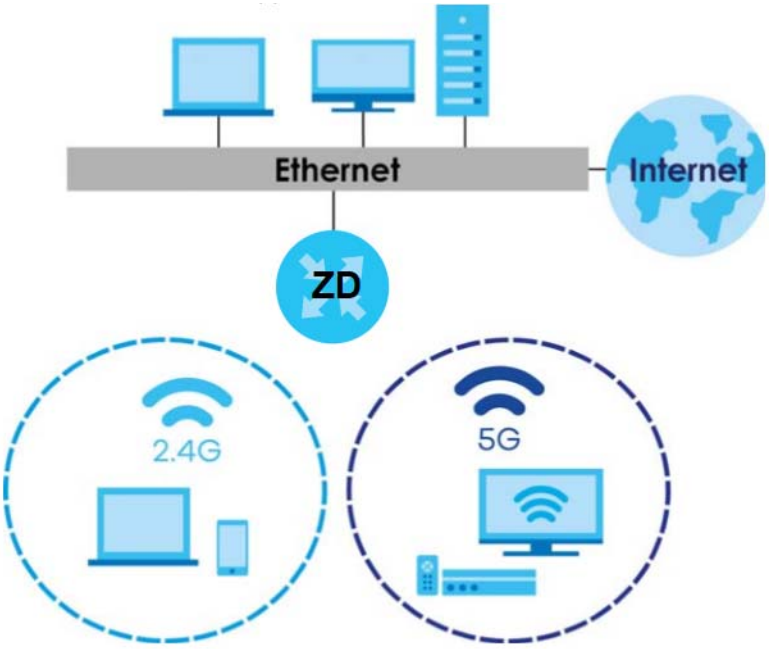
Table 2 Mesh Application

| LABEL | DESCRIPTION |
|---|---|
| ZD | Router Controller |
| AP | Access Point |
| WE | WiFi Extender |
| C1 | Client1 |
| C2 | Client2 |
| APC | Access Point coverage area |
| WEC | WiFi Extender coverage area |

## 1.3.2 Dual-Band WiFi

The Zyxel Device is a dual-band device that can use both 2.4 GHz and 5 GHz at the same time. IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the Zyxel Device to access network resources. 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 7** Dual-Band Application

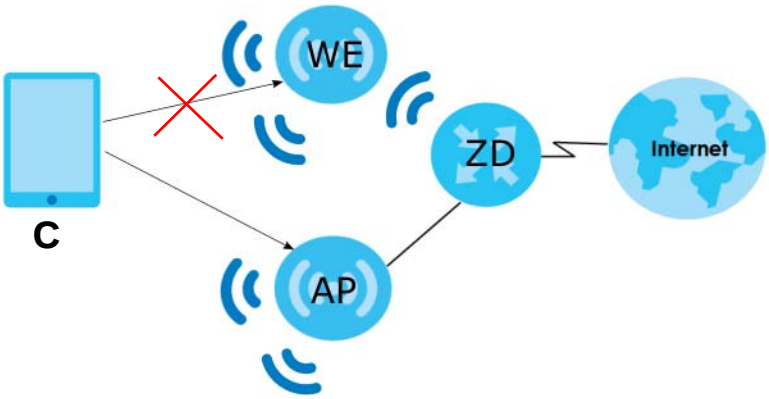



## 1.3.3 AP Steering

AP steering allows WiFi clients to roam seamlessly in the Mesh network. AP steering helps monitor WiFi clients and drops their connections to optimize the Zyxel Device bandwidth when the clients are idle or have a low signal. When a WiFi client is dropped, it has the opportunity to reconnect to an AP or WiFi Extender with a stronger signal.

In the following example, the controller (**ZD**) drops the connection between the client device (**C**) and the WiFi Extender (**WE**) so that the client device (**C**) can connect to the Access Point (**AP**), which has a stronger signal.

**Figure 8** AP Steering Application

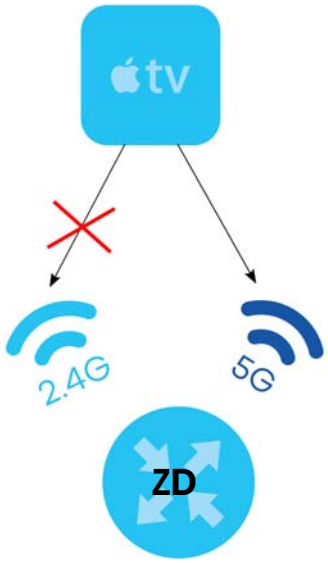


## 1.3.4 Band Steering

Band steering allows 2.4 GHz/5 GHz dual-band WiFi clients to move from one band to another. The controller detects if the client device are dual-band compatible. If a client device supports dual-band WiFi and the 2.4 GHZ band is congested, its 2.4 GHz connection is dropped so that it can connect to the less congested 5 GHz band.

In the following example, the Apple TV is a dual-band client device that uses the 5 GHz band.

**Figure 9** Band Steering Application




## 1.3.5 Daisy Chain

You can add more APs or WiFi Extenders to your Mesh network to form a daisy chain. Daisy chain refers to the connection from the Zyxel Device to up to three APs or WiFi Extenders to extend the WiFi connection from the router to the client.

- If the Zyxel Device has a wired downlink connection, the device connected to the Zyxel Device must be an AP.
- If the Zyxel Device has a WiFi downlink connection, the device connected to the Zyxel Device must be a WiFi Extender.

Here are some example scenarios of the Zyxel Device's daisy chain connection:

**Figure 10** Scenario 1: Three APs

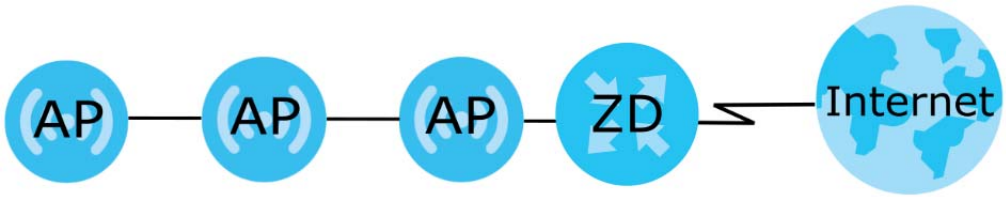


**Figure 11** Scenario 2: Two APs and one WE

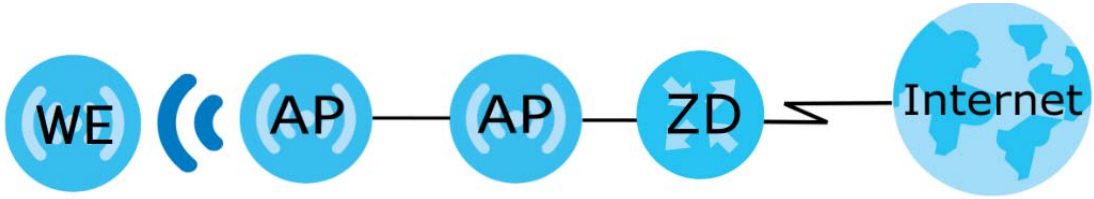



**Figure 12** Scenario 3: One AP and two WEs

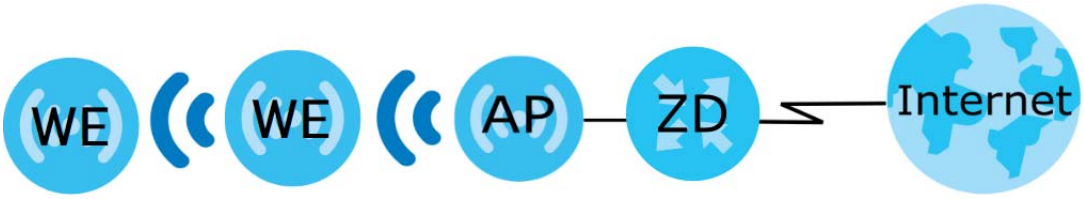
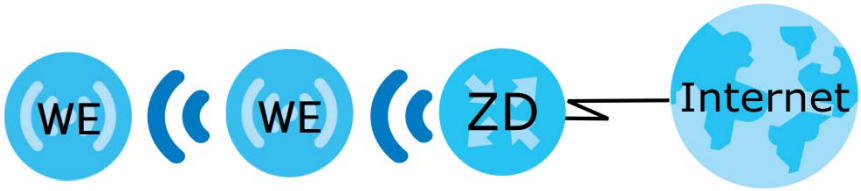


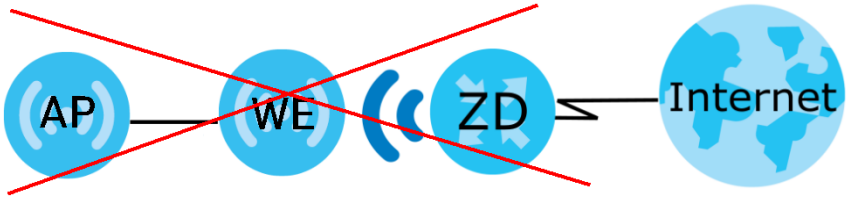

**Figure 13** Scenario 4: Two WEs




Note: We do not recommend connecting more than three APs or WiFi Extenders in your daisy chain network.

Note: If one of the WiFi Extenders has a WiFi uplink connection, we do not recommend linking the other WiFi Extenders in your daisy chain network with a wired connection.

**Figure 14** Not Recommended Connection Example



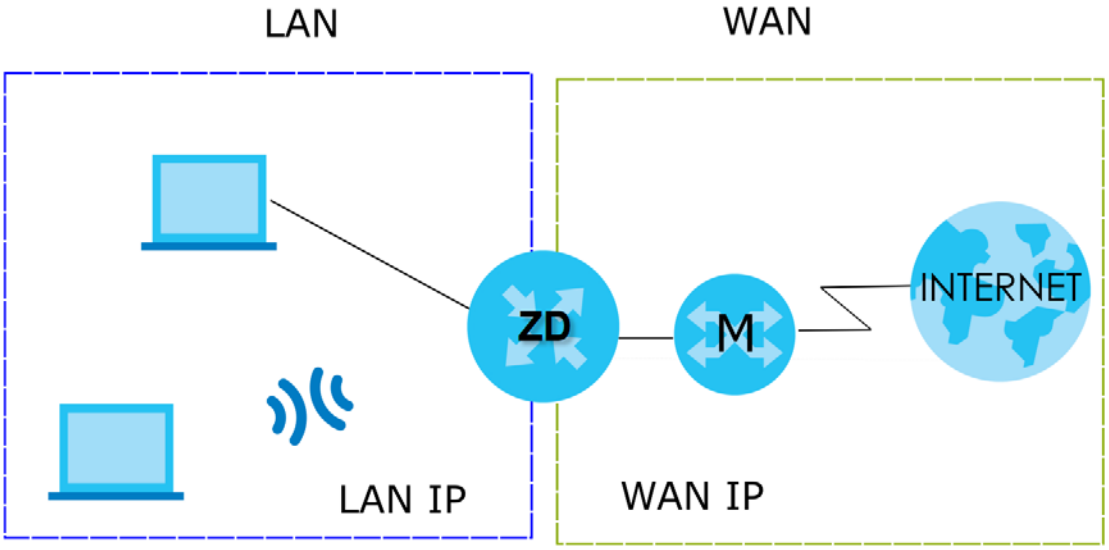

# 1.4 Operating Modes for the Zyxel Device

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

## 1.4.1 Standard (Router) Mode

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

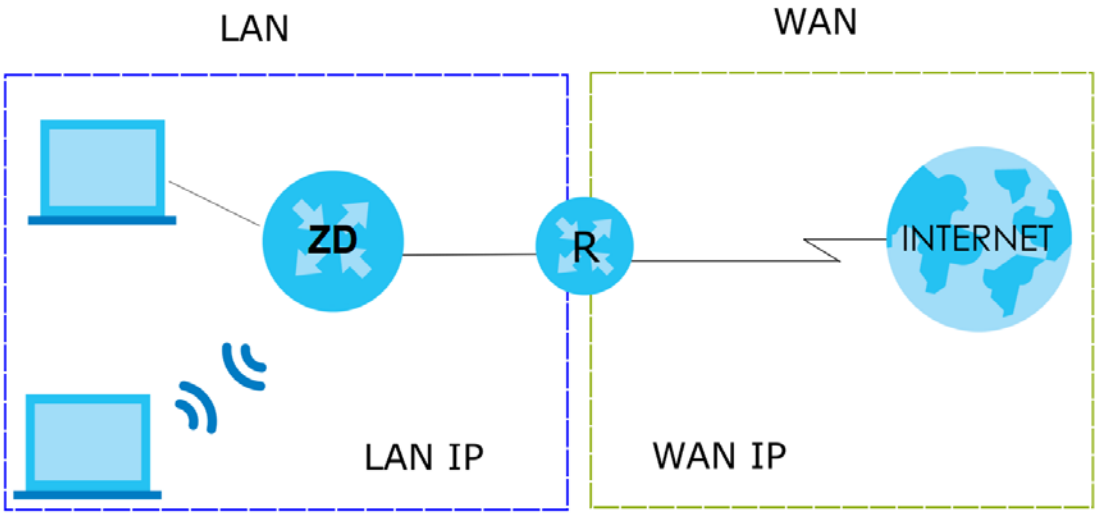
**Figure 15** Standard Mode Example




### 1.4.2 AP (Bridge) Mode

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

**Figure 16** AP Mode Example




## 1.5 Ways to Manage the Zyxel Device

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

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

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

## 1.6 Good Habits for Managing the Zyxel Device

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

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

# CHAPTER 2
# Hardware

This chapter describes the LED and Ports and Buttons on the Zyxel Device.

## 2.1 LED

After you connect the power to the Zyxel Device, view the LED to ensure proper functioning of the Zyxel Device and as an aid to troubleshooting.

**Figure 17** LED

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

Table 3 LED Behavior

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

## 2.2 Ports and Buttons

The following figure shows the ports and buttons on the Zyxel Device.

**Figure 18** Ports and Buttons

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

Table 4 Panel Ports and Buttons

| LABEL | DESCRIPTION |
|---|---|
| WIFI/WPS | Press the **WIFI/WPS** button for 1.5 - 4 seconds to quickly setup a secure WiFi connection between the Zyxel Device and a WPS-compatible client device. |
| RESET | Press the button for more than 5 seconds to return the Zyxel Device to the factory defaults. |
| LAN1 – LAN3 | Connect computers or other Ethernet devices to Ethernet LAN ports for Internet access. |
| WAN | For the Zyxel Device, connect an Ethernet cable to the WAN port for Internet access. |
| DC12V | Connect a power adapter to start the device. |

## 2.3 How to Reset the Zyxel Device

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

1. Make sure the LED lights blue (not blinking).
2. Locate the RESET hole.
3. Insert a thin object into the RESET hole for more than 5 seconds or until the LED begins to blink red and blue and then release it. The LED will blink blue when the defaults have been restored and the Zyxel Device restarts.

## 2.4 How to Enable WiFi/WPS

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

To activate WiFi/WPS:

1. Make sure the **POWER** LED lights blue and not blinking.
2. Press the **WiFi/WPS** button for 1.5-4 seconds and release it.
3. Press the WPS button on another WPS-enabled client device within range of the Zyxel Device within 120 seconds. The LED flashes purple while the Zyxel Device sets up a WPS connection with the client device.
4. Once the connection is successfully made, the LED will light up in blue.

## 2.5 Wall Mounting

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

**Figure 19** Wall Mounting Screw Specifications

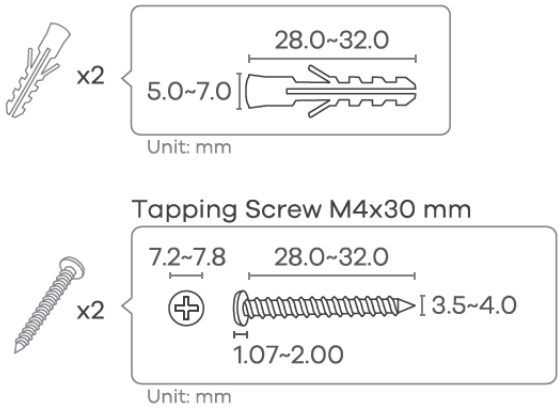



Table 5 Wall Mounting Information

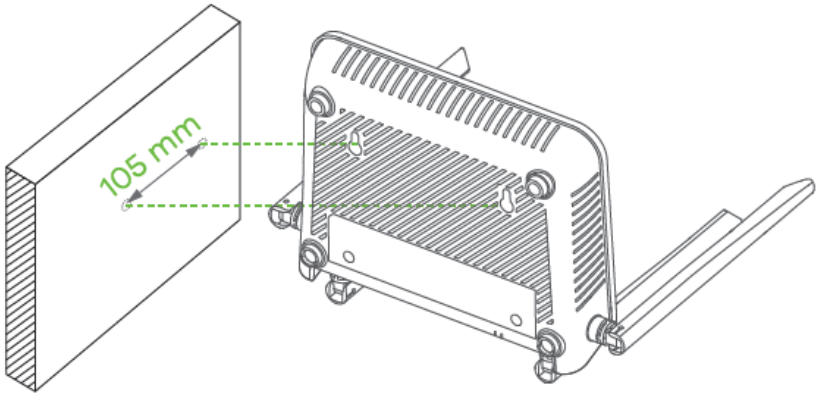
| | |
|---|---|
| Distances between holes | 105 mm |
| M4 Screws | Two |
| Screw Anchors | Two |

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

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

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

**Figure 20** Wall Mounting Distance

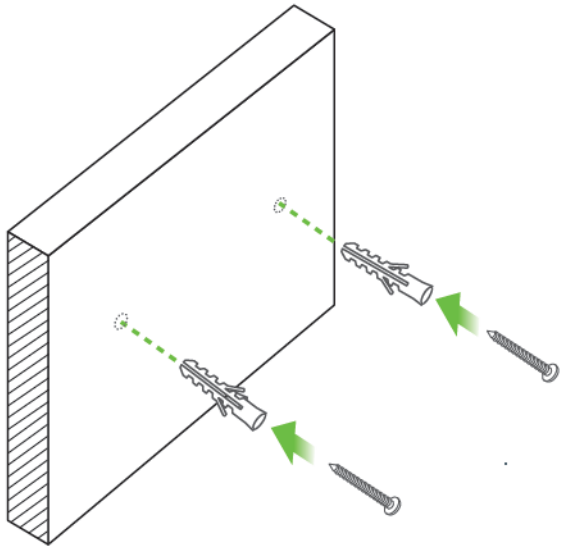



**Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.**

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

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

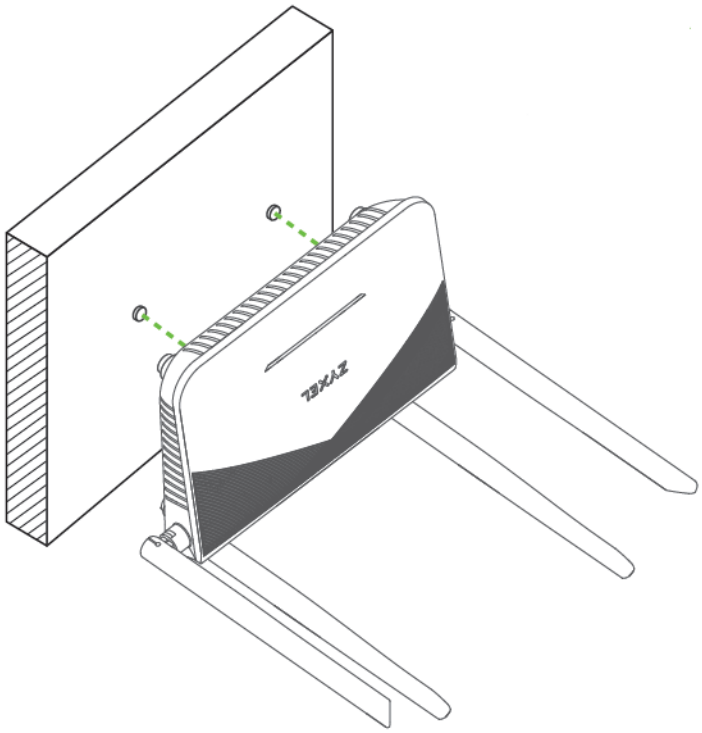
**Figure 21** Wall Mounting Anchors



4 Make sure the screws are fastened well enough to hold the weight of the Zyxel Device with the connection cables.

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

**Figure 22** Wall Mounting Device



# CHAPTER 3
# Web Configurator

## 3.1 Overview

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

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

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

### 3.1.1 Access the Web Configurator

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

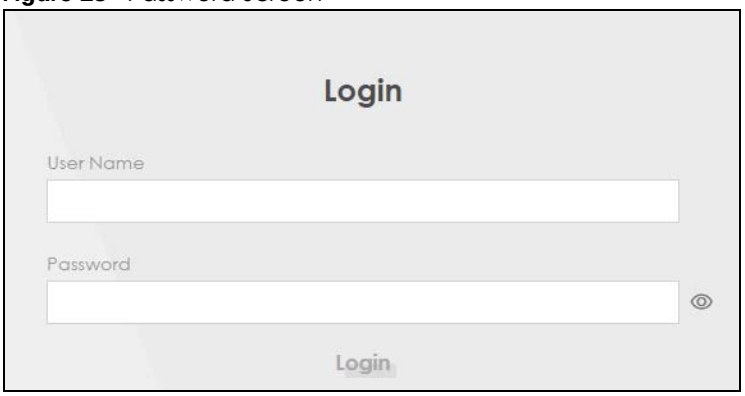
2 Make sure your computer has an IP address in the same subnet as the Zyxel Device.

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

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

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

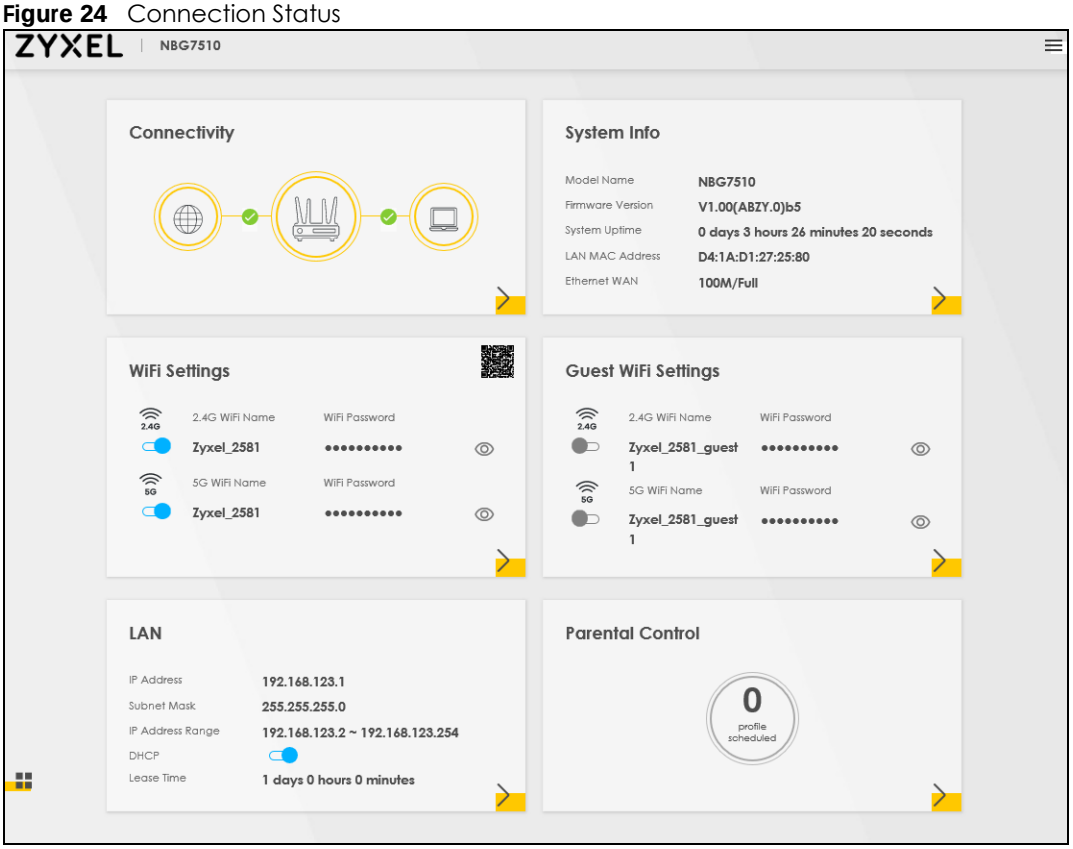
**Figure 23** Password Screen



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

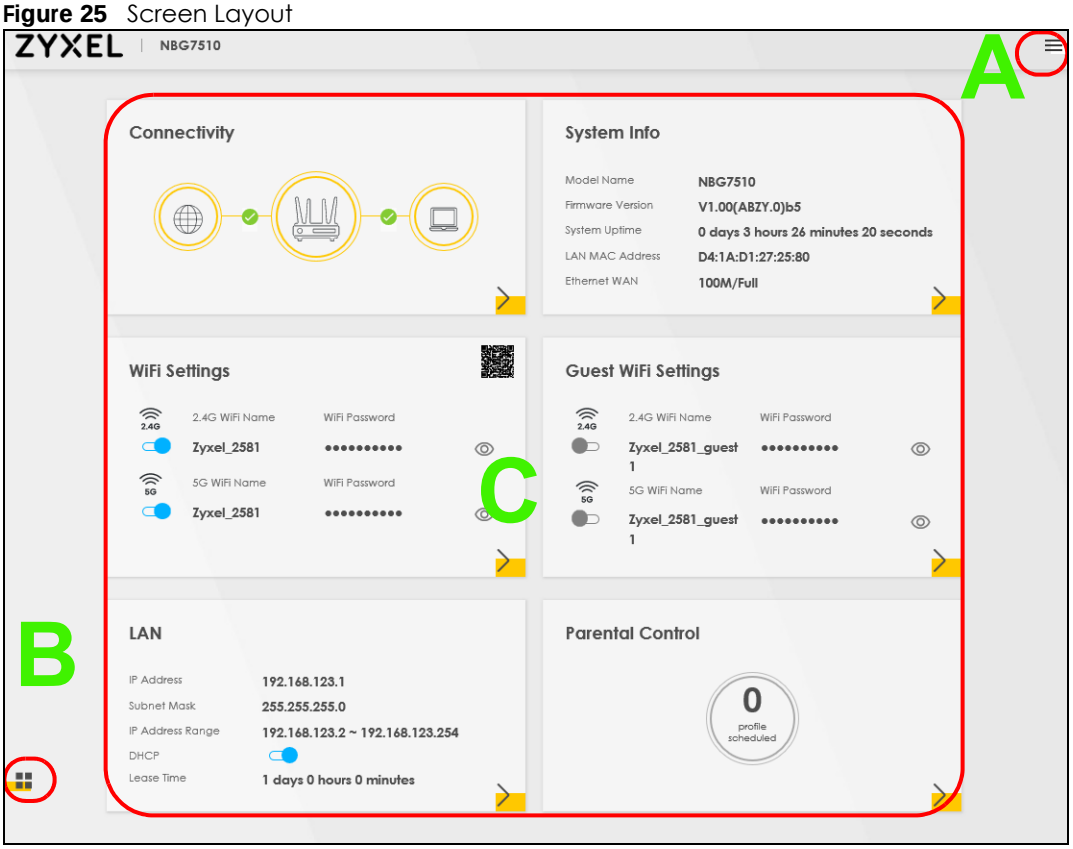
6 The **Connection Status** screen appears. Use this screen to configure basic Internet access and WiFi settings.

**Figure 24** Connection Status



# 3.2 Web Configurator Layout

**Figure 25** Screen Layout




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

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

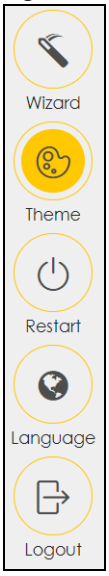
## 3.2.1 Settings Icon

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

### 3.2.1.1 Side Bar

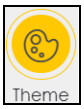
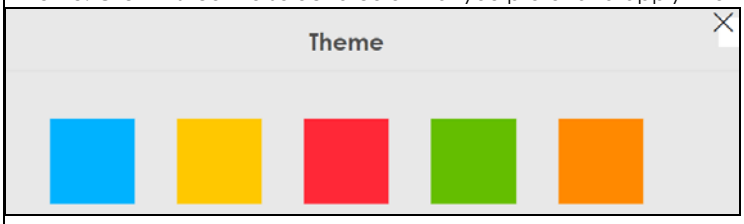
The side bar provides some icons on the right hand side.

**Figure 26** Side Bar




The icons provide the following functions.

Table 6 Web Configurator Icons in the Title Bar

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

### 3.2.1.2 Navigation Panel

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

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

**Figure 27** Navigation Panel

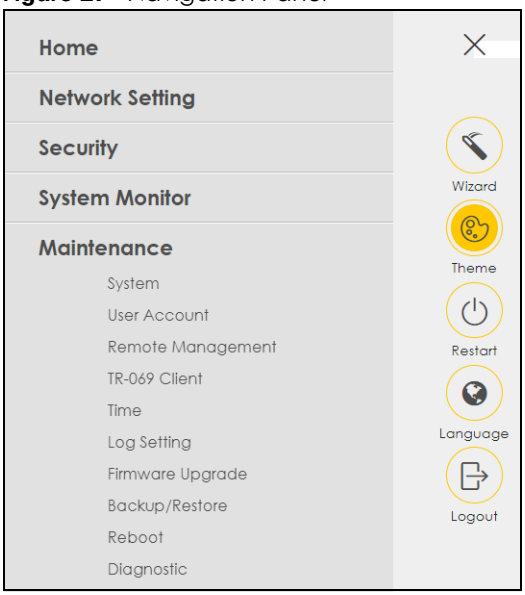



Table 7 Navigation Panel Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| Connection Status | | Use this screen to configure basic Internet access, wireless settings, and parental control settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it. |
| Network Setting | | |
| Broadband | Broadband | Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections. |
| Wireless | General | Use this screen to configure the wireless LAN settings and WLAN authentication or security settings. |
| | Guest/More AP | Use this screen to configure multiple BSSs on the Zyxel Device. |
| | MAC Authentication | Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device. |
| | WPS | Use this screen to configure and view your WPS (WiFi Protected Setup) settings. |
| | WMM | Use this screen to enable or disable WiFi MultiMedia (WMM). |
| | Others | Use this screen to configure advanced wireless settings. |
| | Channel Status | Use this screen to scan wireless LAN channel noises and view the results. |
| | Mesh | Use this screen to enable or disable Mesh. |
| | Mesh Topology | Use this screen to configure the MAC address of the extender connected to the Zyxel Device. |
| 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. |

Table 7 Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| | Additional Subnet | Use this screen to configure IP alias and public static IP. |
| | Wake on LAN | Use this screen to remotely turn on a device on the local network. |
| | TFTP Server Name | Use DHCP option 66 to identify a TFTP server name. |
| Routing | Static Route | Use this screen to view and set up static routes on the Zyxel Device. |
| | DNS Route | Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. |
| | Policy Route | Use this screen to configure policy routing on the Zyxel Device. |
| NAT | Port Forwarding | Use this screen to make your local servers visible to the outside world. |
| | Port Triggering | Use this screen to change your Zyxel Device's port triggering settings. |
| | DMZ | Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen. |
| | ALG | Use this screen to enable the ALGs (Application Layer Gateways) in the Zyxel Device to allow applications to operate through NAT. |
| | Address Mapping | Use this screen to change your Zyxel Device's IP address mapping settings. |
| | Sessions | Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the Zyxel Device. |
| DNS | DNS Entry | Use this screen to view and configure DNS routes. |
| | Dynamic DNS | Use this screen to allow a static hostname alias for a dynamic IP address. |
| Security | | |
| Firewall | General | Use this screen to configure the security level of your firewall. |
| | Protocol | Use this screen to add Internet services and configure firewall rules. |
| | Access Control | Use this screen to enable specific traffic directions for network services. |
| | DoS | Use this screen to activate protection against Denial of Service (DoS) attacks. |
| MAC Filter | MAC Filter | Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device. |
| Scheduler Rule | Scheduler Rule | Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced. |
| System Monitor | | |
| Log | System Log | Use this screen to view the status of events that occurred to the Zyxel Device. You can export or email the logs. |

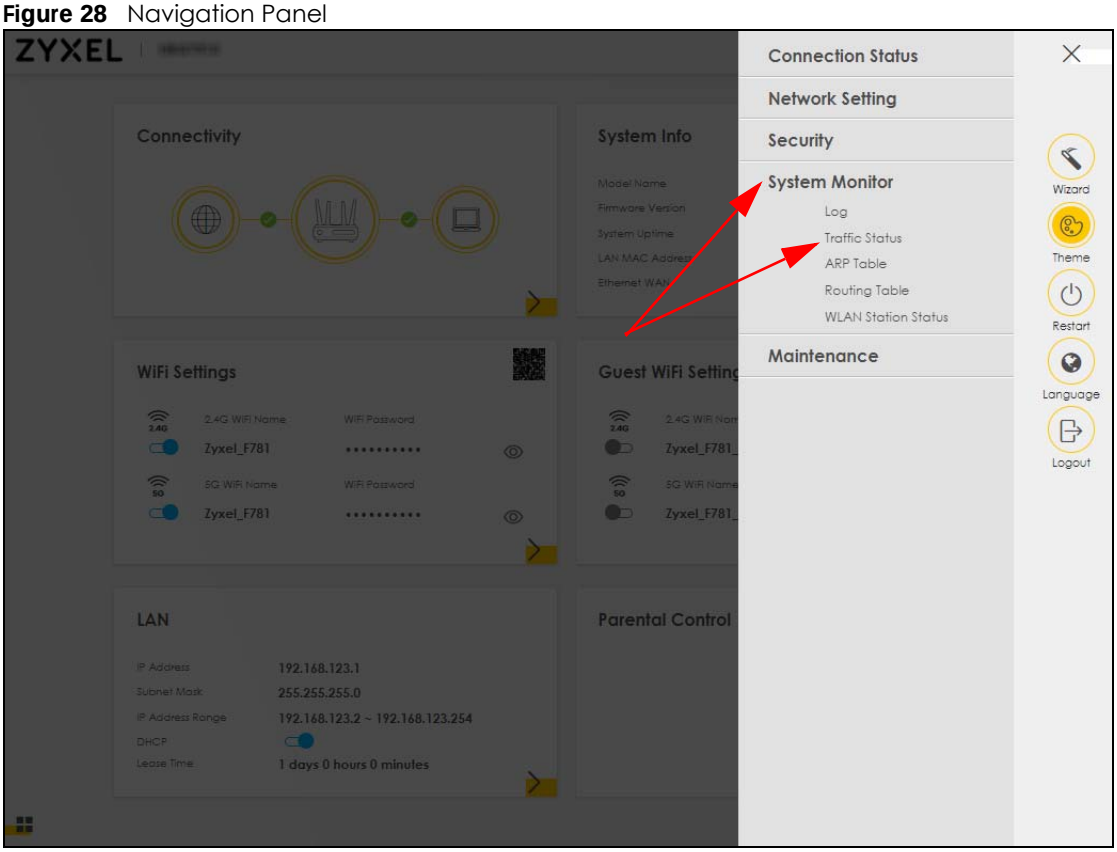
Table 7 Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| | Security Log | Use this screen to view all security related events. You can select the level and category of the security events in their proper drop-down list window.<br>Levels include:<br>• Emergency<br>• Alert<br>• Critical<br>• Error<br>• Warning<br>• Notice<br>• Informational<br>• Debugging<br>Categories include:<br>• Account<br>• Attack<br>• Firewall<br>• MAC Filter |
| Traffic Status | WAN | Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device. |
| | LAN | Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device. |
| | NAT | Use this screen to view NAT statistics for connected hosts. |
| ARP table | ARP table | Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection. |
| Routing Table | Routing Table | Use this screen to view the routing table on the Zyxel Device. |
| WLAN Station Status | WLAN Station Status | Use this screen to view the wireless stations that are currently associated to the Zyxel Device's wireless LAN. |
| Maintenance | | |
| Operating Mode | Operating Mode | Use this screen to change the operating mode of the Zyxel Device. |
| System | System | Use this screen to set the Zyxel Device name and Domain name. |
| User Account | User Account | Use this screen to change the user password on the Zyxel Device. |
| Remote Management | MGMT Services | Use this screen to enable specific traffic directions for network services. |
| | Trust Domain | Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** screen. |
| Time | Time | Use this screen to change your Zyxel Device's time and date. |
| E-mail Notification | E-mail Notification | Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device. |
| Log Settings | Log Settings | Use this screen to change your Zyxel Device's log settings. |
| Firmware Upgrade | Firmware Upgrade | Use this screen to upload firmware to your Zyxel Device. |
| Backup/Restore | Backup/Restore | Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings. |
| Reboot | Reboot | Use this screen to reboot the Zyxel Device without turning the power off. |
| Diagnostic | Ping&Traceroute &Nslookup | Use this screen to identify problems with the Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems. |

### 3.2.1.3 Dashboard

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

**Figure 28** Navigation Panel

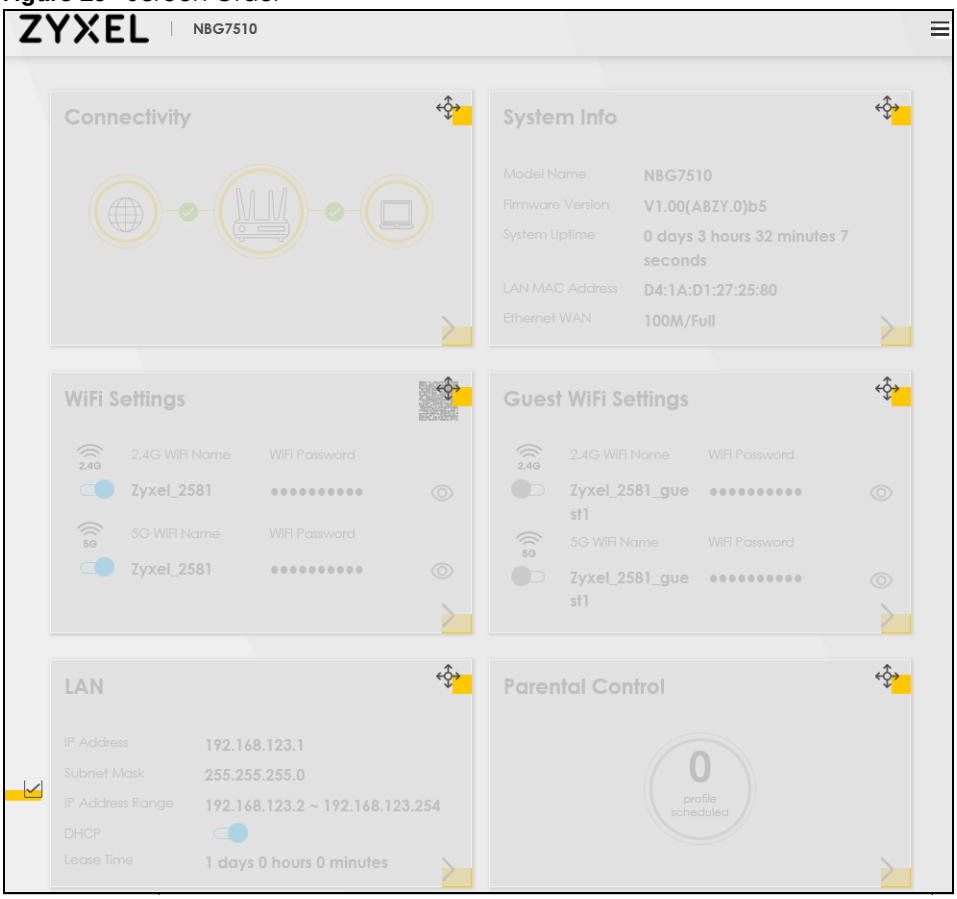



## 3.2.2 Widget Icon

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

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

**Figure 29** Screen Order



# CHAPTER 4
# Quick Start

## 4.1 Overview

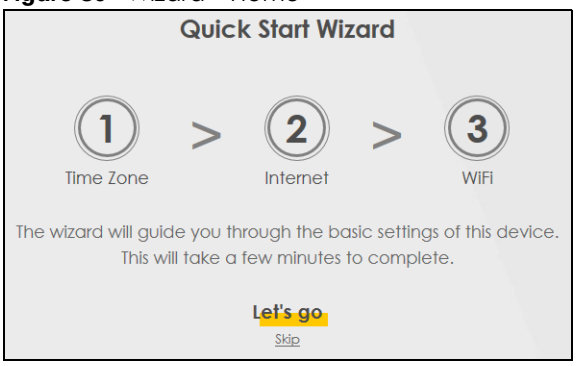
Use the **Wizard** screens to configure the Zyxel Device's time zone and wireless settings.

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

## 4.2 Quick Start Setup

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

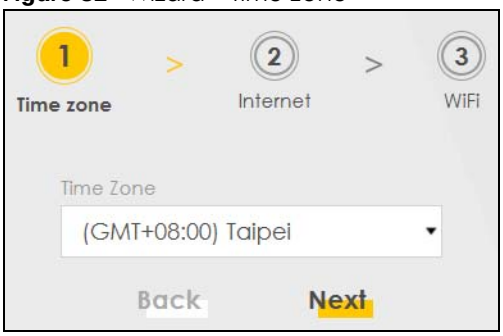
**Figure 30** Wizard – Home




## 4.3 Quick Start Setup – Time Zone

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

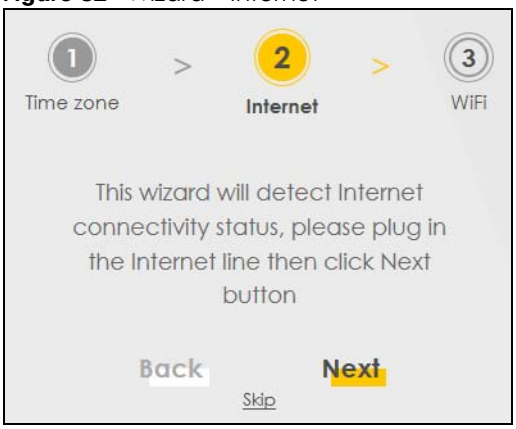
**Figure 31** Wizard – Time Zone




# 4.4 Quick Start Setup – Internet Connection

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

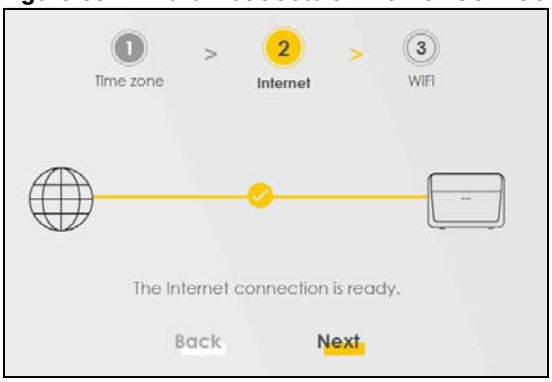
**Figure 32** Wizard – Internet




## 4.4.1 Successful Internet Connection

The Zyxel Device has Internet access.

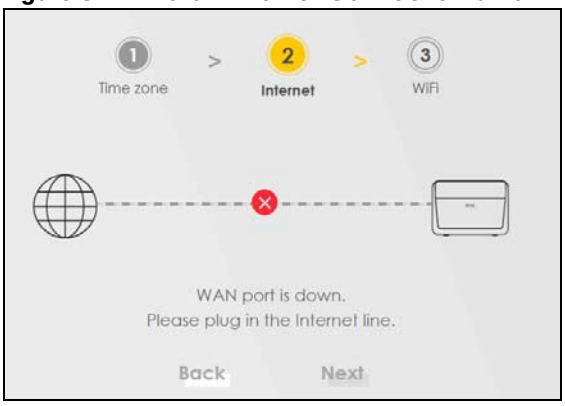
**Figure 33** Wizard – Successful Internet Connection



### 4.4.2 Unsuccessful Internet Connection

The Zyxel Device did not detect a WAN connection.

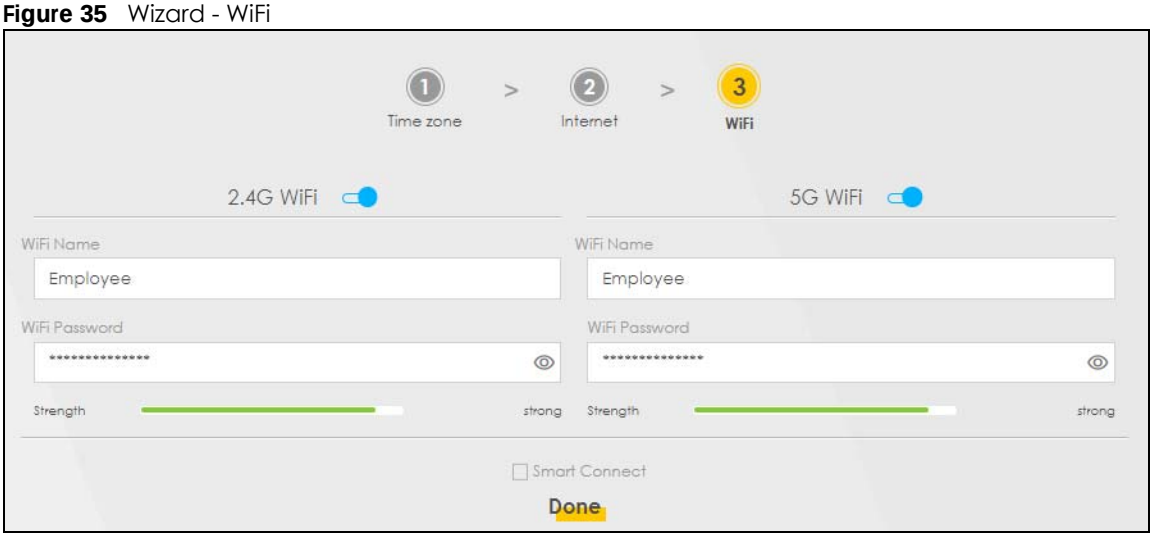
**Figure 34** Wizard – Internet Connection is Down




## 4.5 Quick Start Setup – WiFi

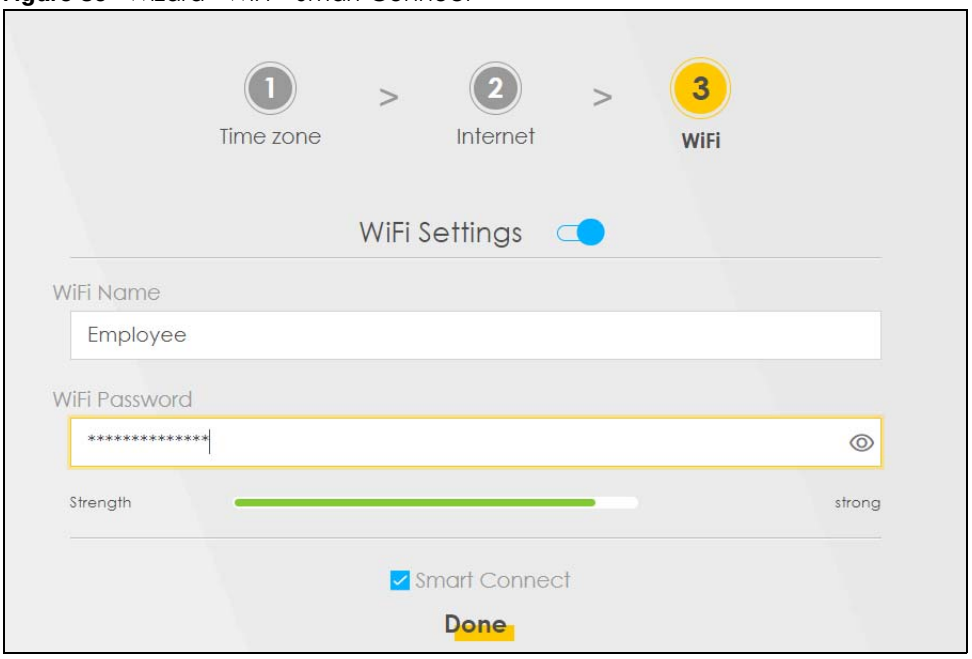
Turn WiFi on or off. If you keep it on, record the **WiFi Name** and **Password** in this screen so you can configure your WiFi clients to connect to the Zyxel Device. If you want to show or hide your WiFi password, click the Eye icon ( ).

**Figure 35** Wizard - WiFi




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

**Figure 36** Wizard - WiFi – Smart Connect




## 4.6 Quick Start Setup – Finish

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

# CHAPTER 5
# Tutorials

## 5.1 Overview

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

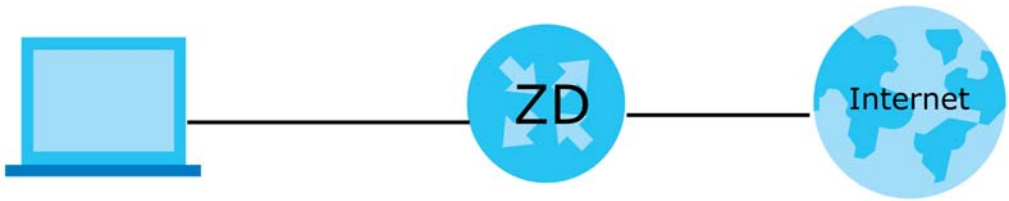
- Wired Network Setup
- WiFi Network Setup
- Network Security
- Device Maintenance

## 5.2 Wired Network Setup

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

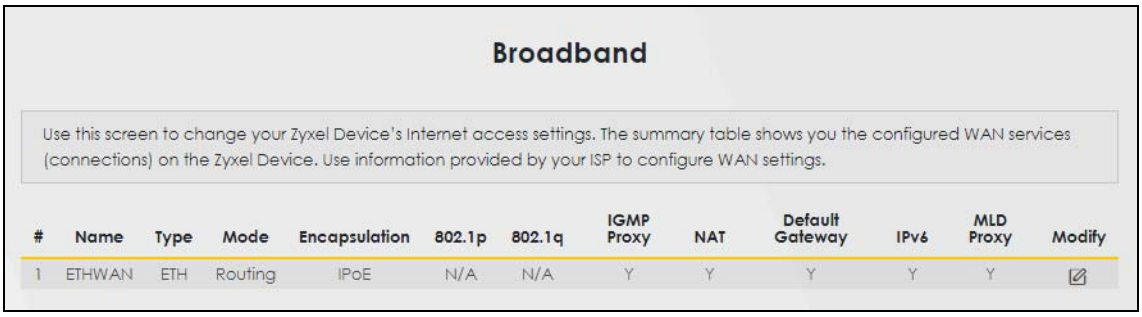
### 5.2.1 Setting Up an Ethernet Connection

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




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

2 Go to **Network Setting** > **Broadband** and then the following screen appears. Click the Modify icon to edit the information.




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

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

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

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

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

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

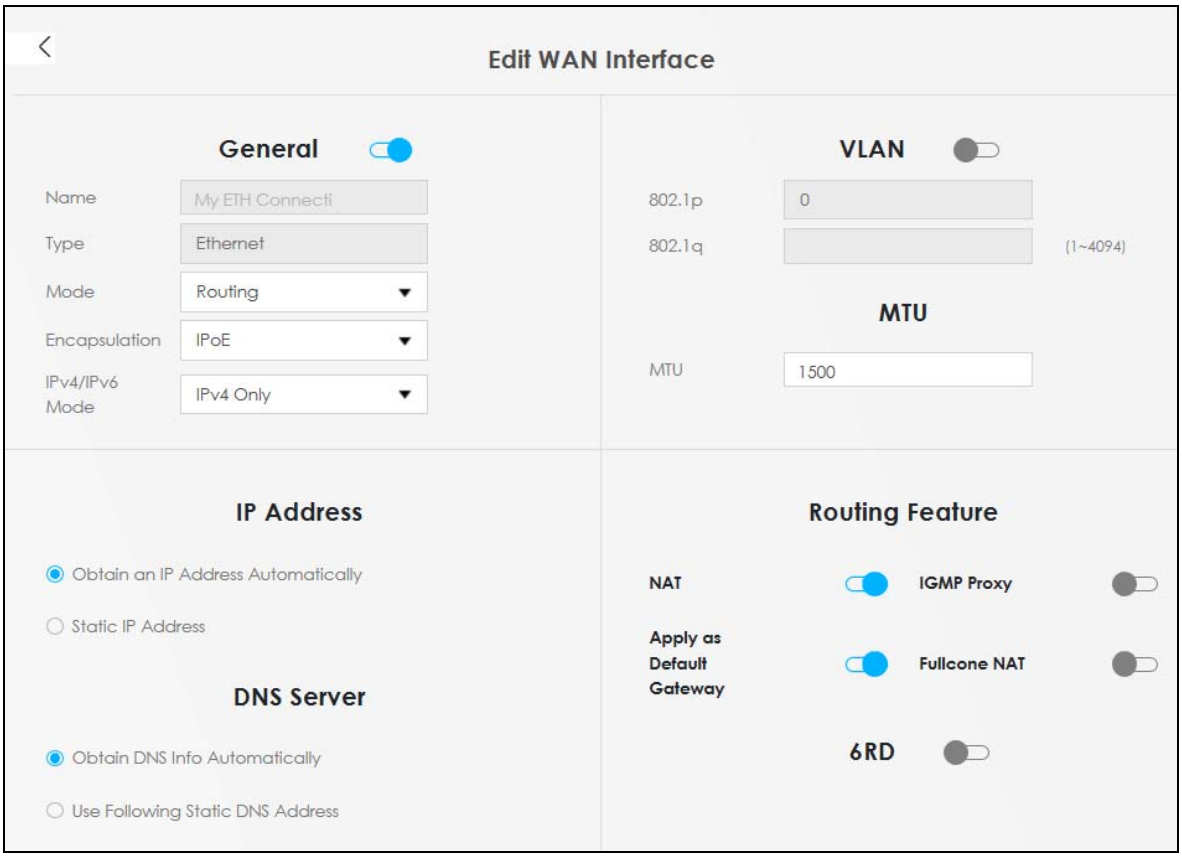
**4d** Choose the **Encapsulation** specified by your Internet service provider. For this example, select **IPoE** as the WAN encapsulation type.

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

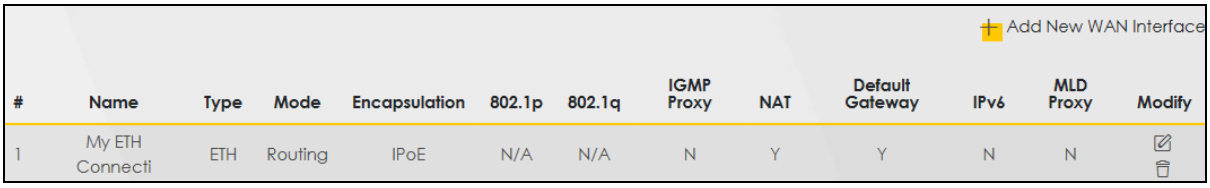
**5** Under **Routing Feature**, enable **NAT** and **Apply as Default Gateway**.

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

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




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

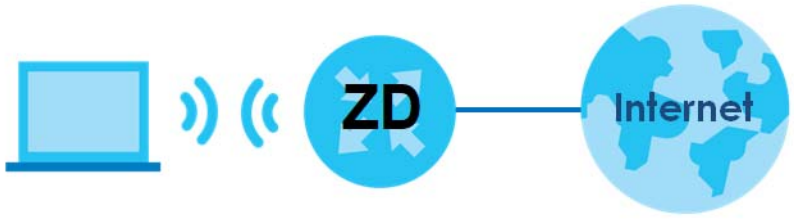



| # | Name | Type | Mode | Encapsulation | 802.1p | 802.1q | IGMP Proxy | NAT | Default Gateway | IPv6 | MLD Proxy | Modify |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | My ETH Connecti | ETH | Routing | IPoE | N/A | N/A | N | Y | Y | N | N | |

# 5.3 WiFi Network Setup

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

**Figure 37** WiFi Network Setup




See the label on the Zyxel Device for the WiFi network settings and then connect manually to the Zyxel Device. Alternatively, you can set up a WiFi network using WPS. See Section 5.3.2 on page 49.

## 5.3.1 Changing Security on a WiFi Network

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

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

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

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. We recommend that you select **More Secure** to enable **WPA3-SAE/WPA2-PSK** data encryption.

**Wireless**

Wireless: Smart Connect

**Wireless Network Setup**

Band: 2.4GHz

Wireless

Channel: Auto — Current: 5 / 40 MHz

Bandwidth: 20/40MHz

Control Sideband: Upper

**Wireless Network Settings**

Wireless Network Name: Example

Max Clients: 32

Hide SSID

Multicast Forwarding

Note

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

BSSID: D4:1A:D1:3F:F8:01

**Security Level**

No Security | More Secure (Recommended)

Security Mode: WPA2-PSK

Generate password automatically

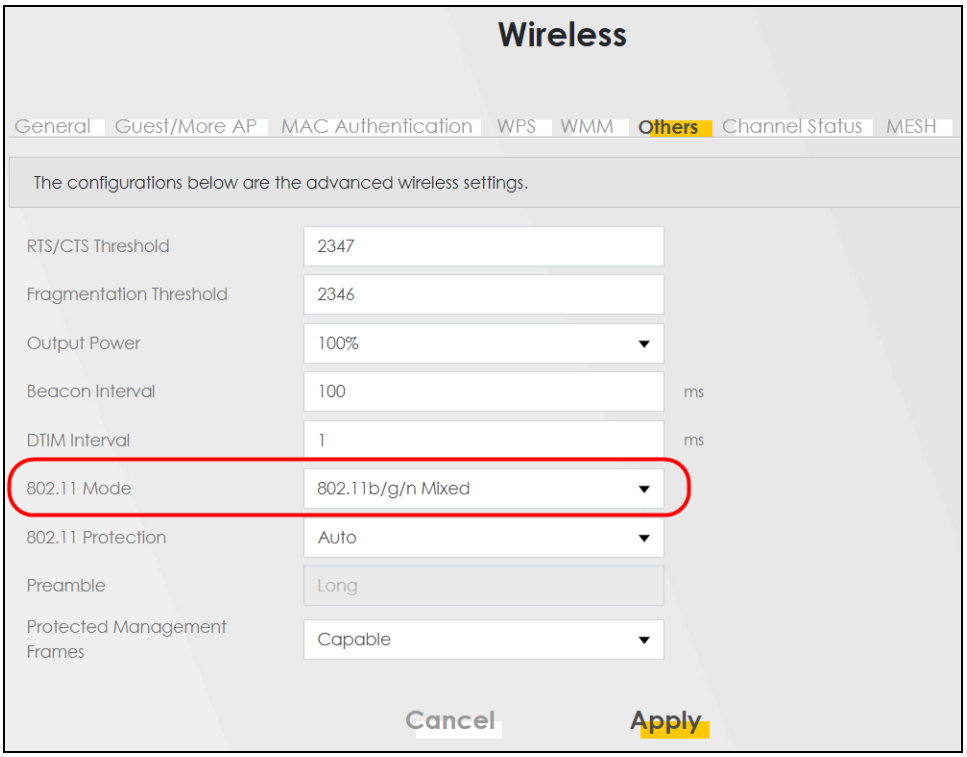
Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password: DoNotStealMyWiFi

Strength: strong

Cancel Apply

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




You can now use the WPS feature to establish a WiFi connection between your notebook and the Zyxel Device (see Section 5.3.2 on page 49). Now use the new security settings to connect to the Internet through the Zyxel Device using WiFi.

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

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

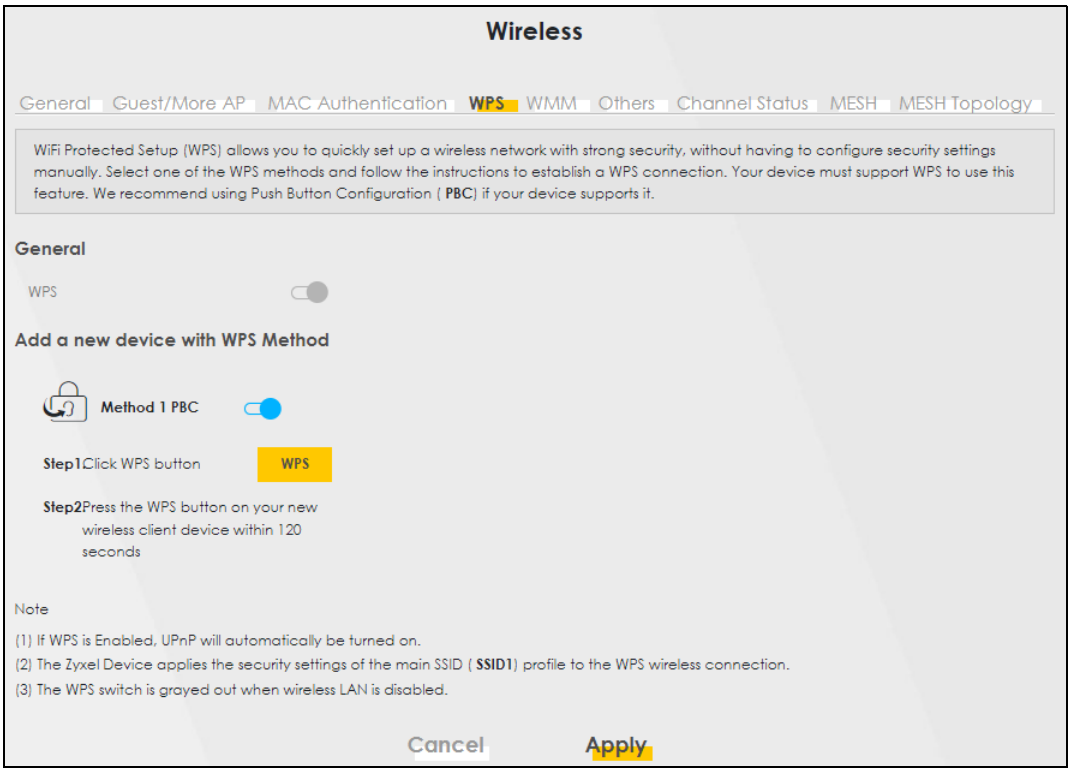
- **Push Button Configuration (PBC)** – Connect to the WiFi network by pressing a button. See Section 5.3.2.1 on page 49. This is the simplest method.

### 5.3.2.1 WPS Push Button Configuration (PBC)

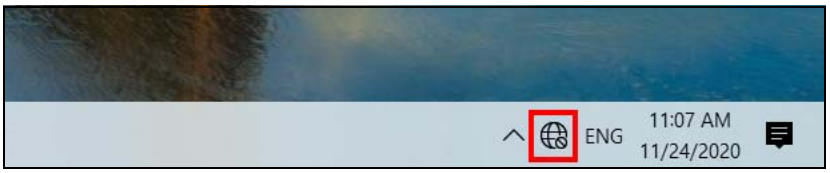
This example shows how to connect to the Zyxel Device's WiFi network from a notebook computer running Windows 10.

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

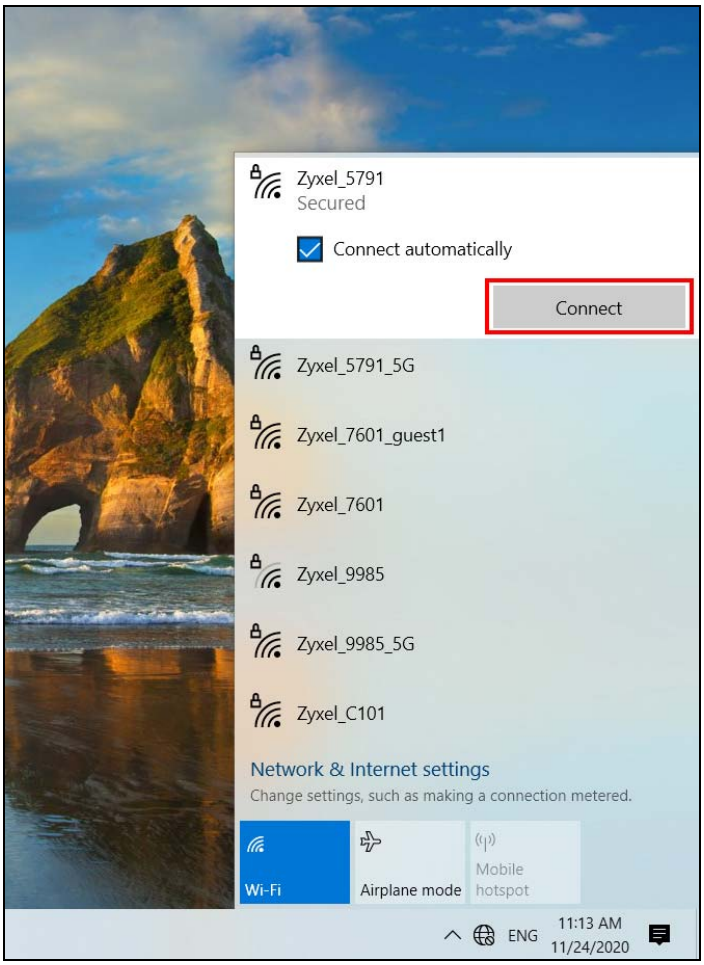
2 Push and hold the **WPS** button located on the Zyxel Device until the **WiFi** or **WPS** LED starts blinking slowly. Alternatively, log into the Zyxel Device's Web Configurator, and then go to the **Network Setting** > **Wireless** > **WPS** screen. Enable **WPS** and **Method 1 PBC**, click **Apply**,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



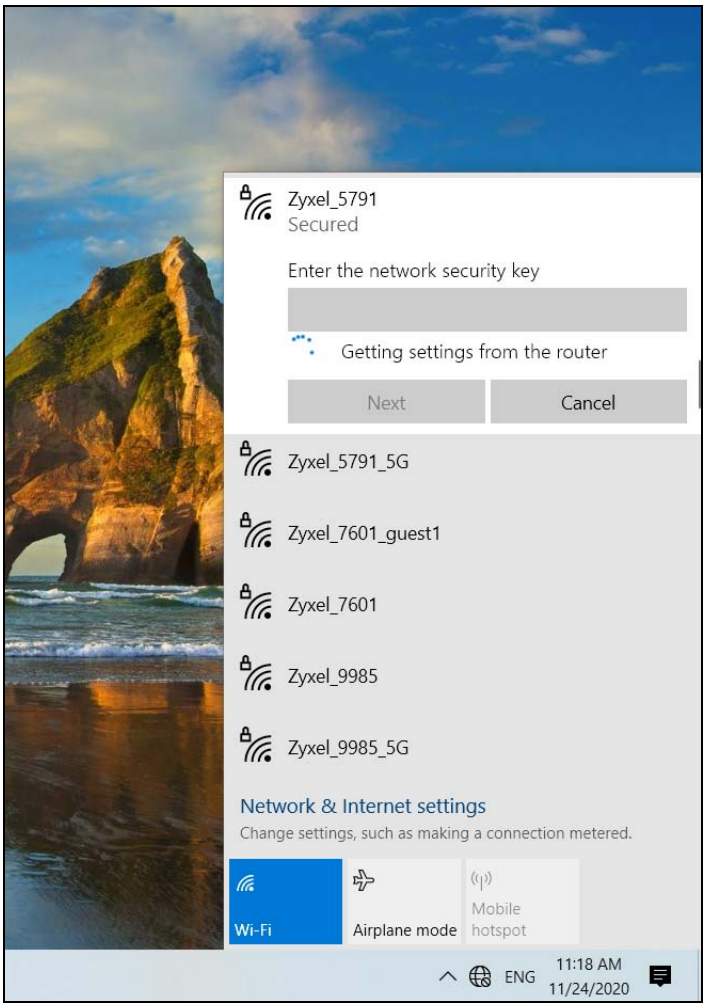

**3** In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.




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



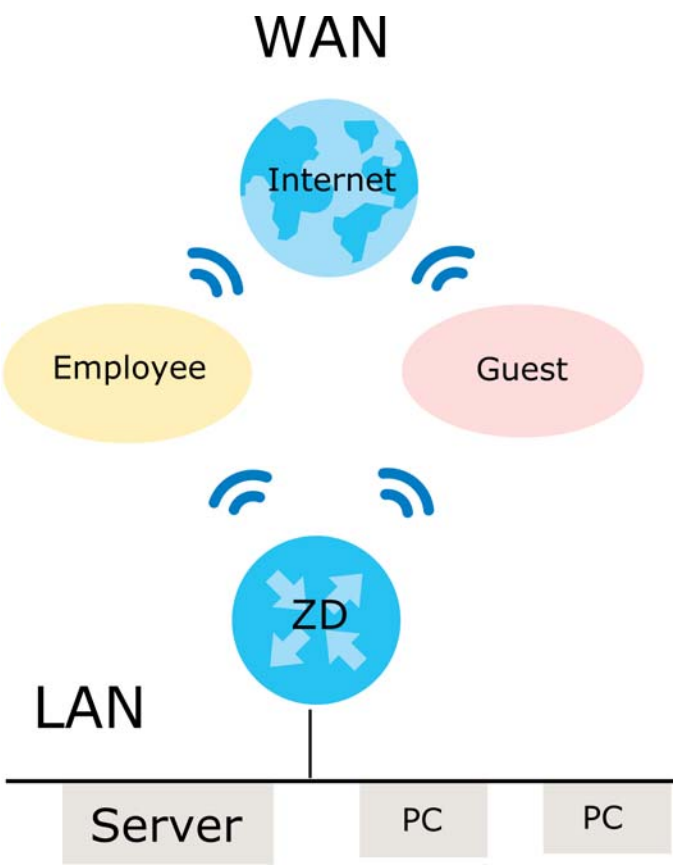

The Zyxel Device sends the WiFi network settings to Windows using WPS. Windows displays "Getting settings from the router".




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

## 5.3.3 Setting Up a Guest Network

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

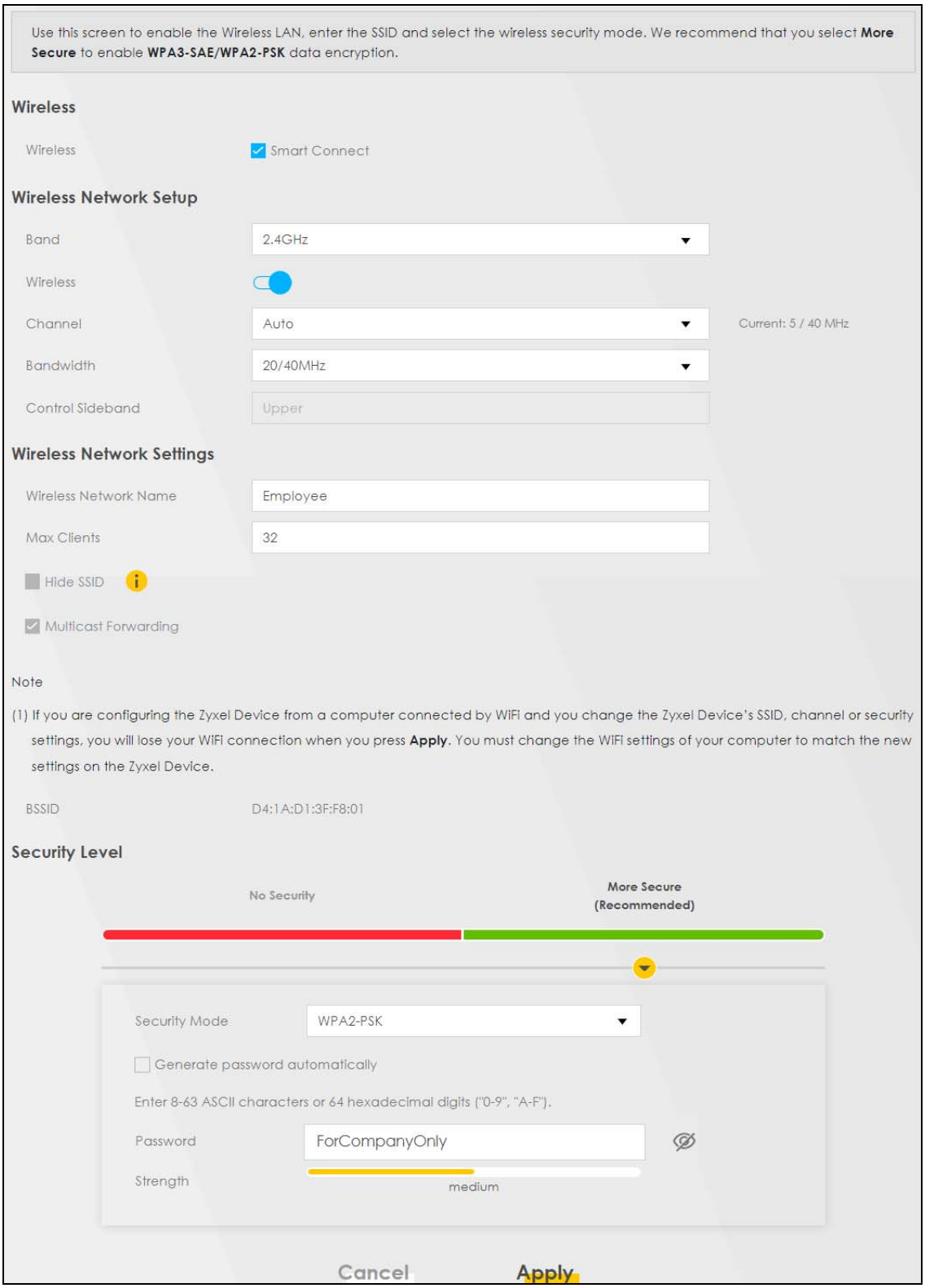



- Employees using the **General** WiFi network group will have access to the local network and the Internet.
- Visitors using the **Guest** WiFi network group with a different SSID and password will have access to the Internet only.

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

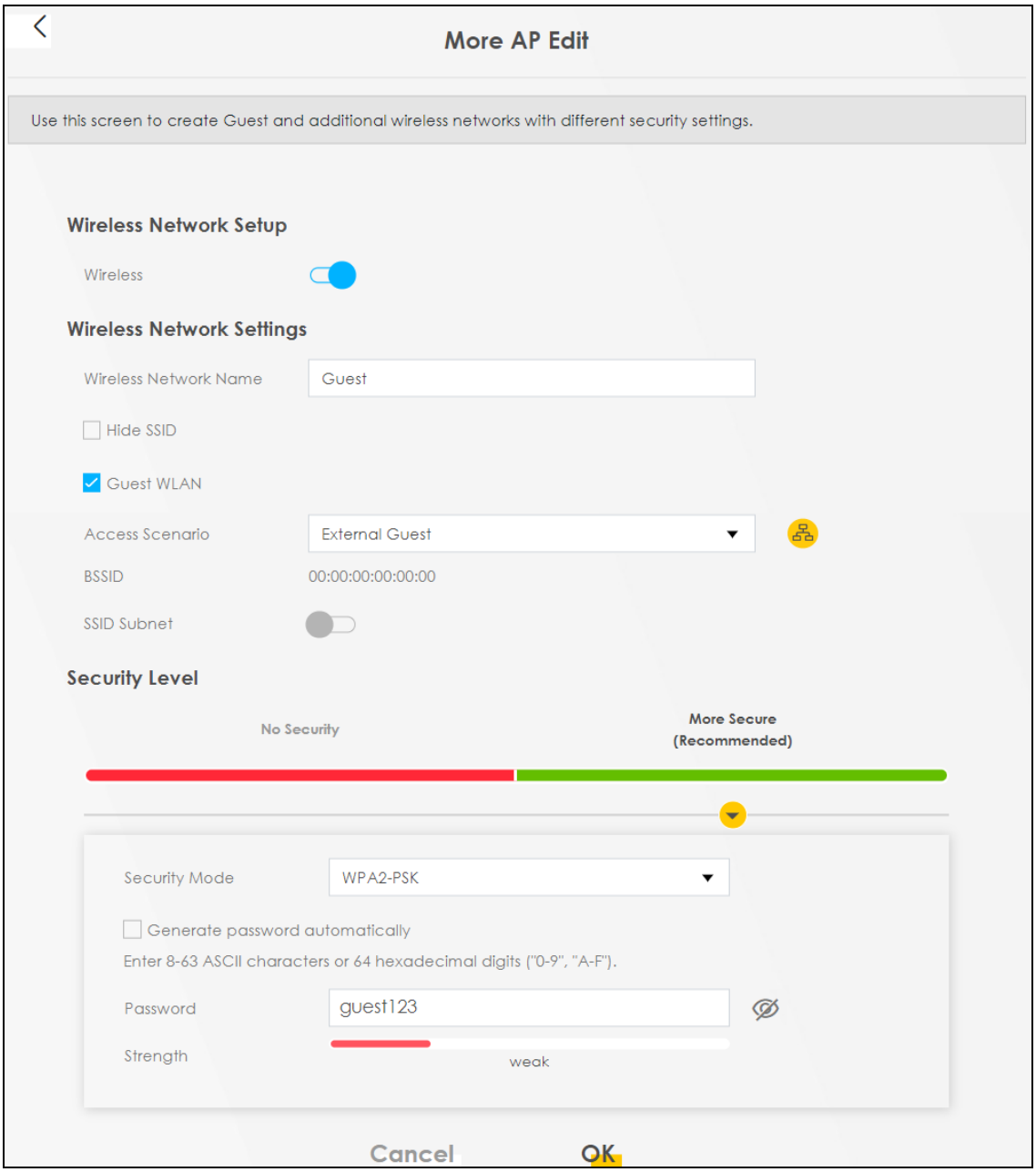
| | GENERAL | GUEST |
|---|---|---|
| **2.4/5G SSID** | Employee | Guest |
| **Security Level** | More Secure | More Secure |
| **Security Mode** | WPA2-PSK | WPA2-PSK |
| **Pre-Shared Key** | ForCompanyOnly | guest123 |

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

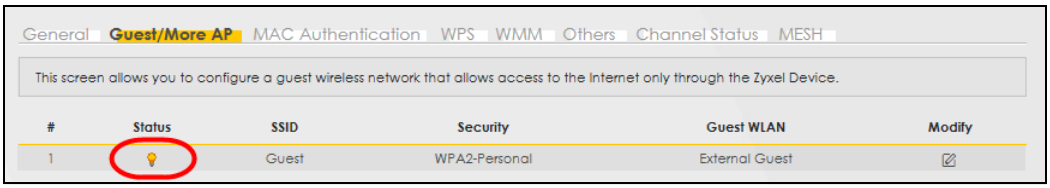



2 Go to the **Network Setting** > **Wireless** > **Guest/More AP** screen. Click the **Modify** icon to configure the second WiFi network group.

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

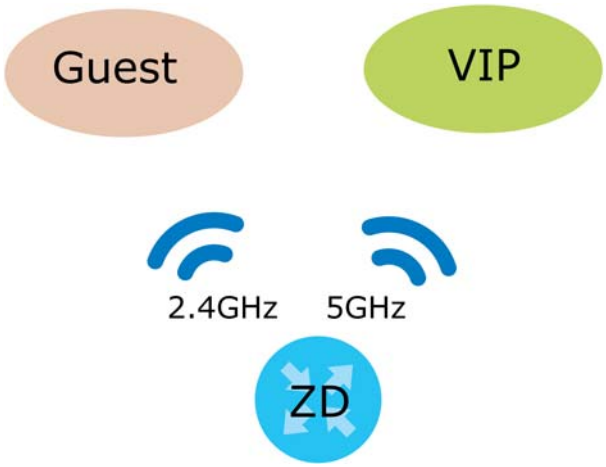



4 Check the status of **Guest** in the **Guest/More AP** screen. A yellow bulb under **Status** means the SSID is active and ready for WiFi access.




## 5.3.4 Setting Up Two Guest WiFi Networks on Different WiFi Bands

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




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

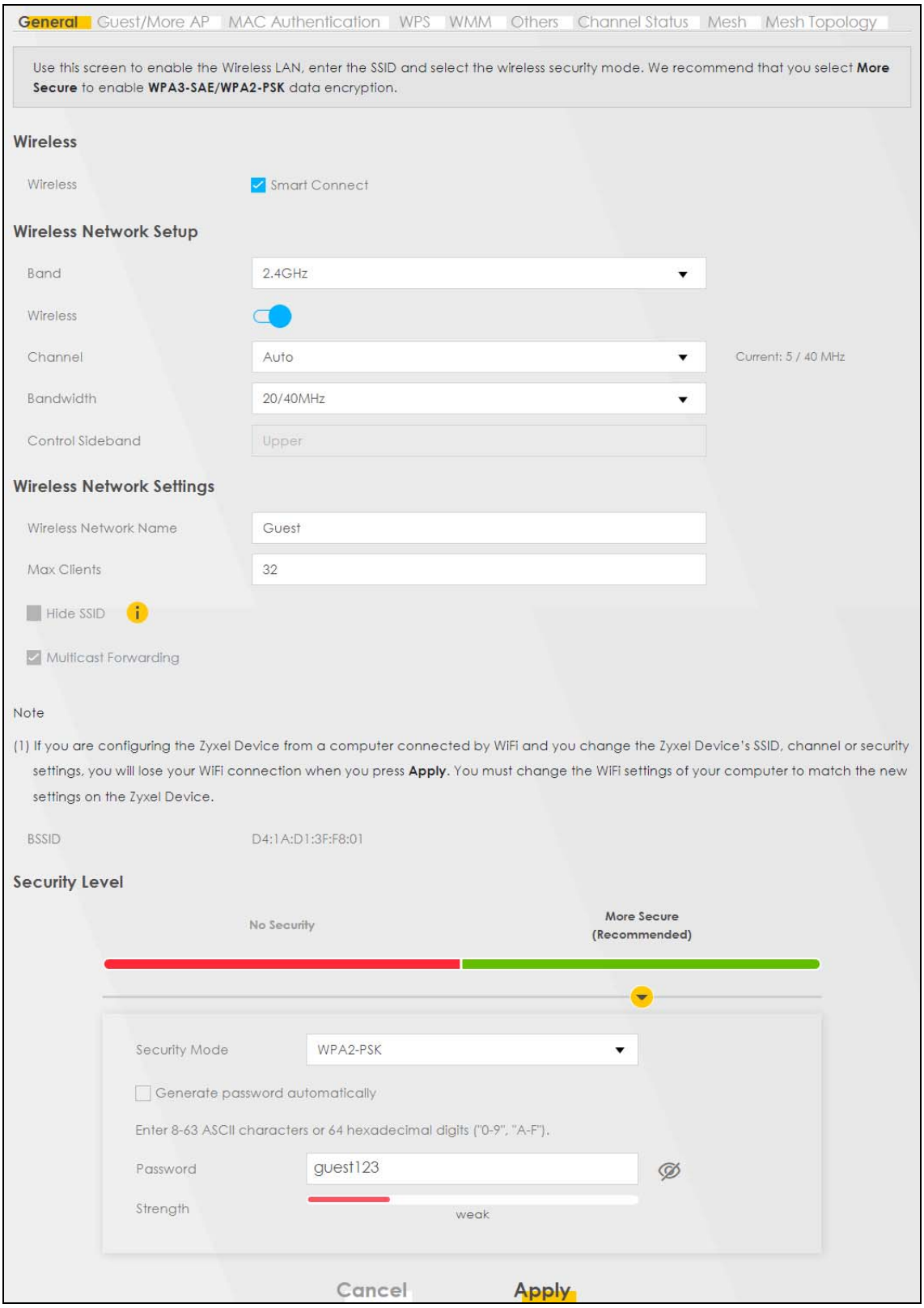
The Company will use the following parameters to set up the WiFi network groups.

Table 8 WiFi Settings Parameters Example

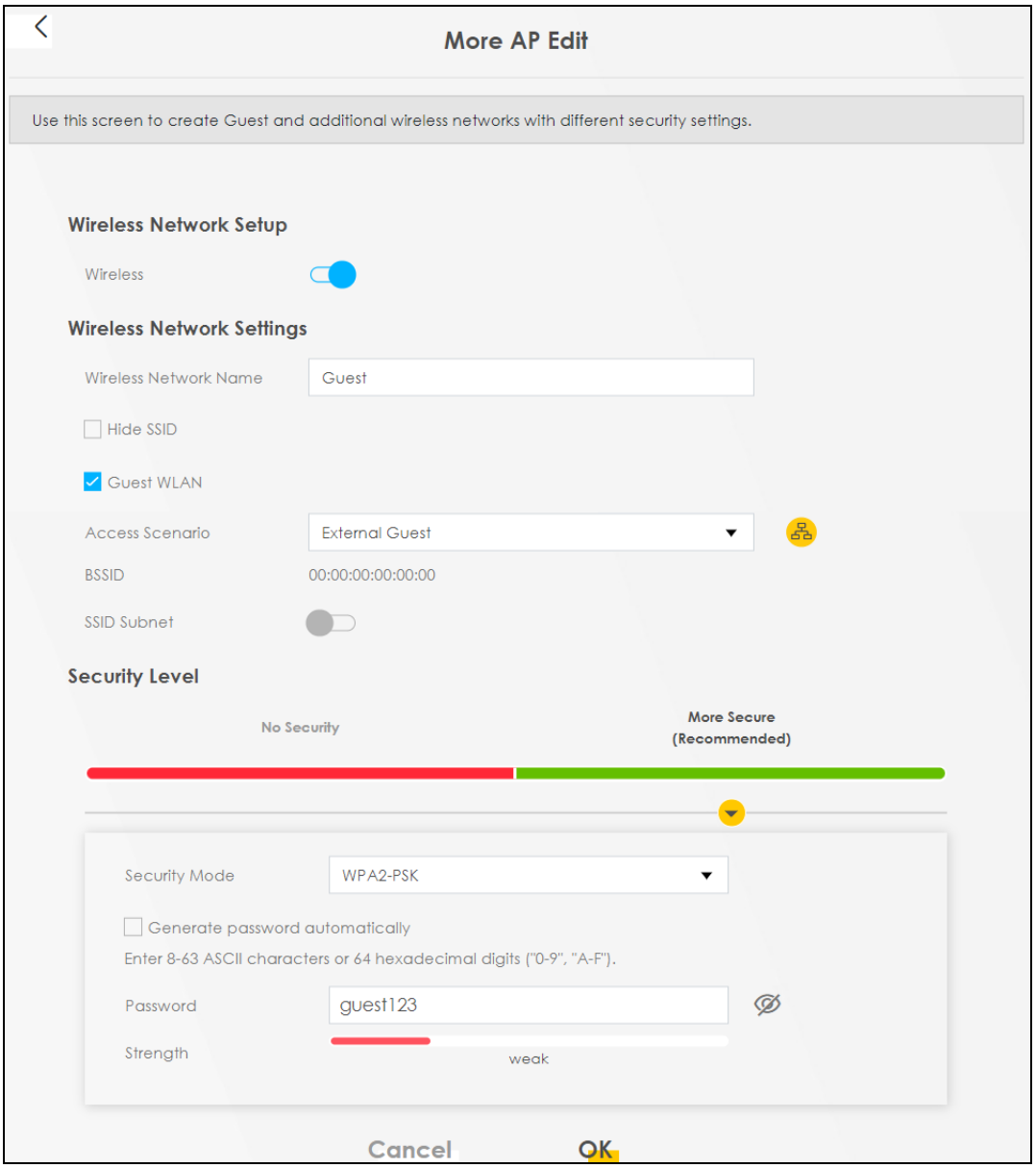
| BAND | 2.4G | 5G |
|---|---|---|
| SSID | Guest | VIP |
| Security Mode | WPA2-PSK | WPA2-PSK |
| Pre-Shared Key | guest123 | 123456789 |

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

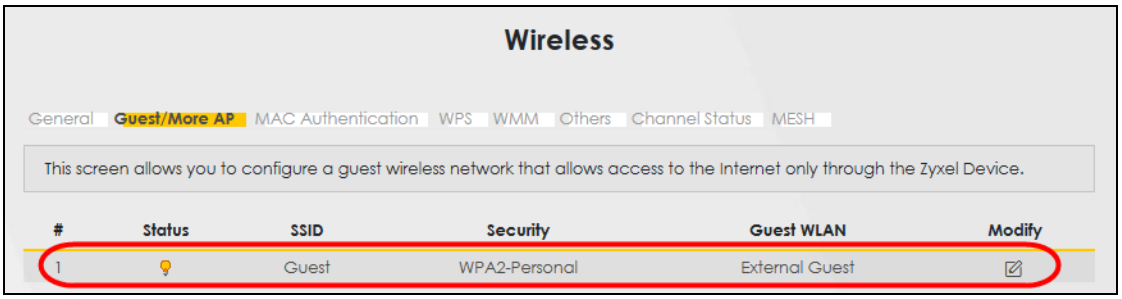
Note: You will not be able to configure the 2.4G and 5G Guest WiFi settings separately if **Smart Connect** is enabled.



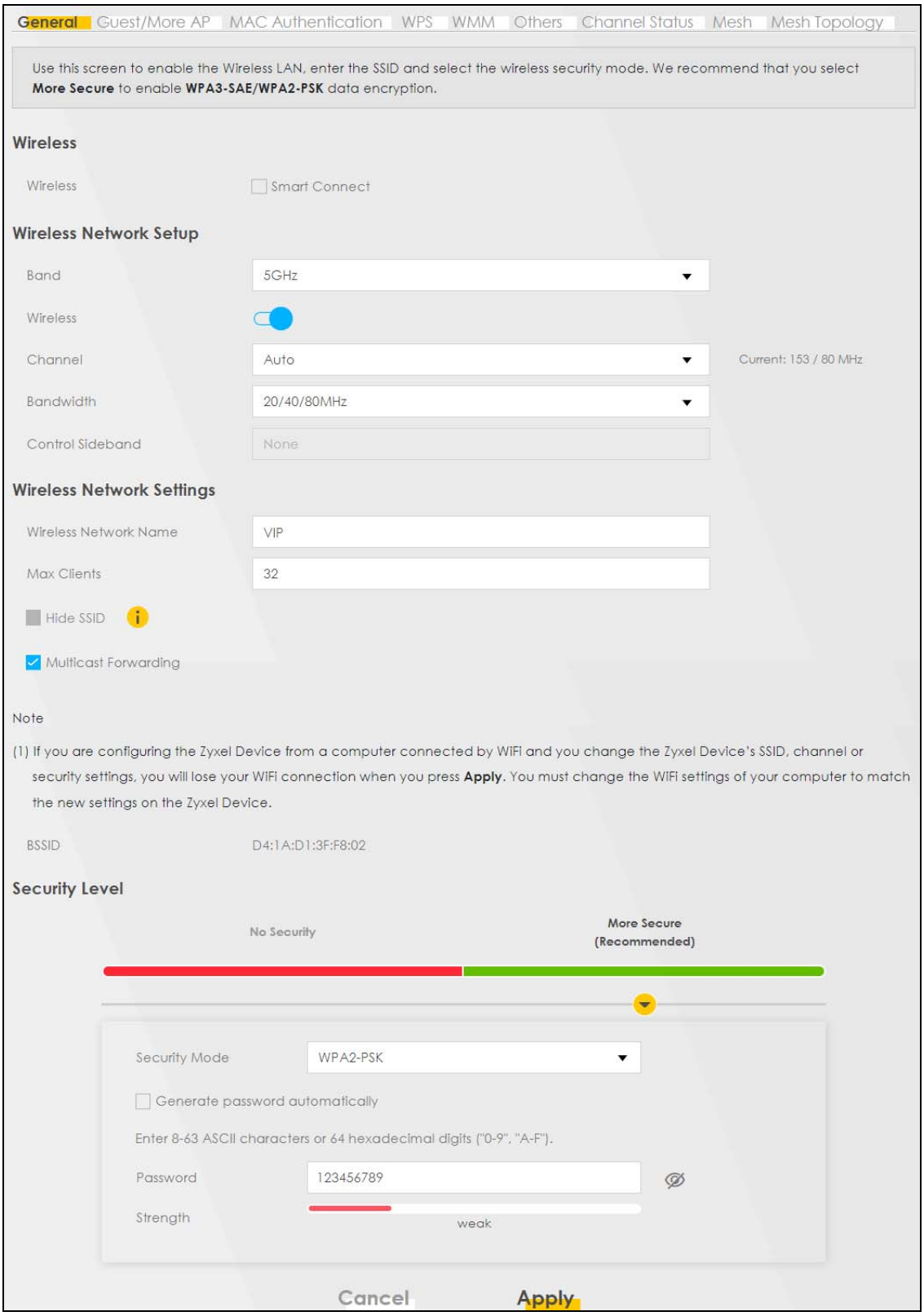

2 Go to the **Wireless** > **Guest/More AP** screen and click the **Modify** icon. The following screen appears. Configure the **Security Mode** and **Password** using the provided parameters and click **OK**.



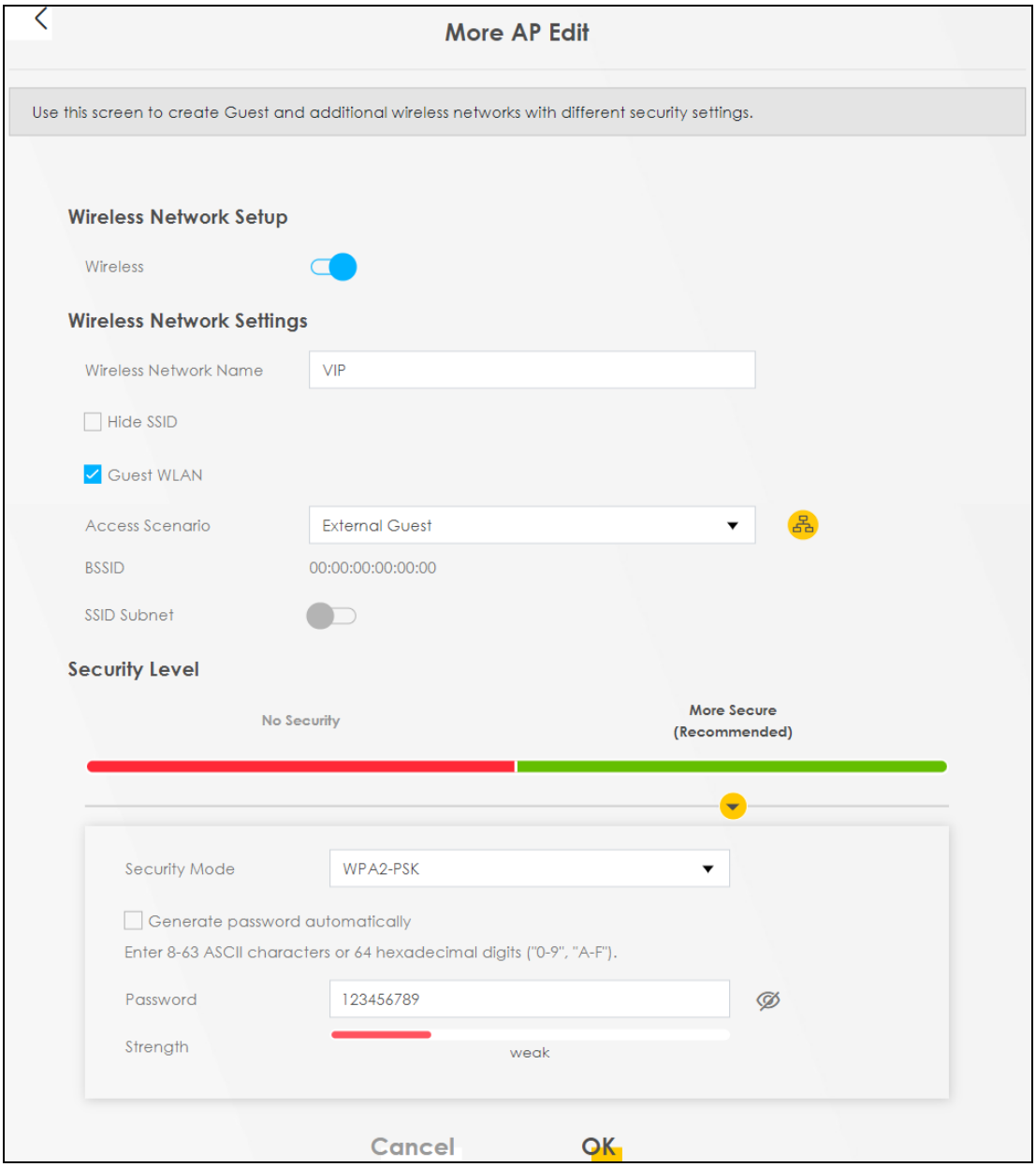

The 2.4GHz **Guest** WiFi network is now configured.



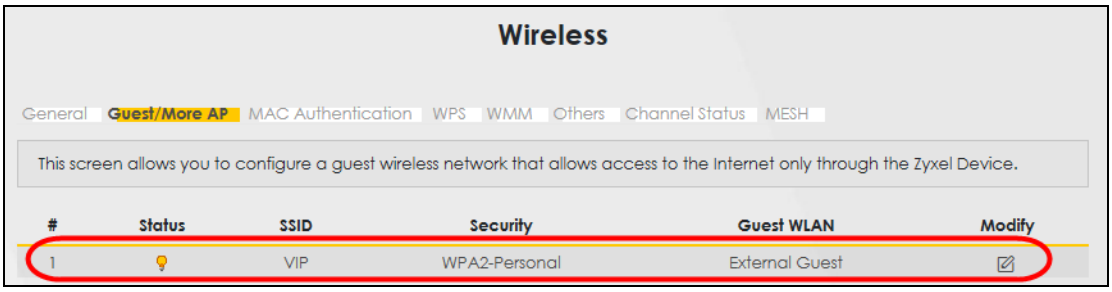

3 Go to the **Wireless** > **General** screen and set **Band** to **5GHz** to configure the 5G Guest WiFi settings for **VIP**. Click **OK**.




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




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



# 5.4 Network Security

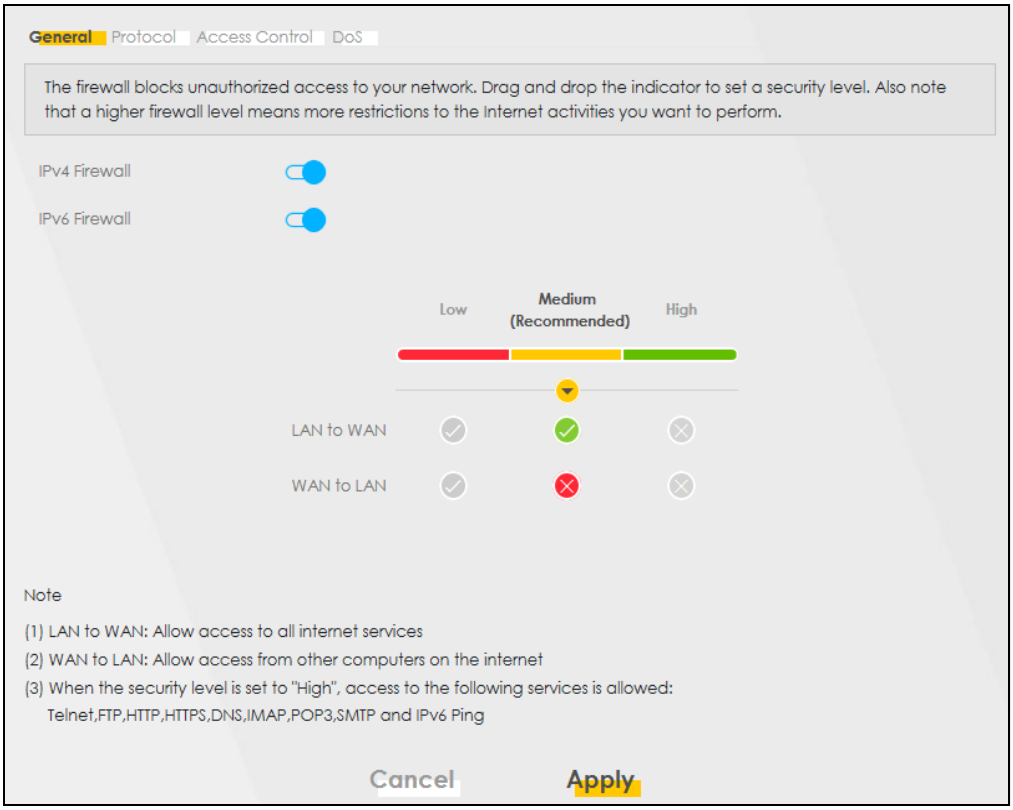
This section shows you how to configure a Firewall rule, Parental Control rule, and MAC Filter rule.

## 5.4.1 Configuring a Firewall Rule

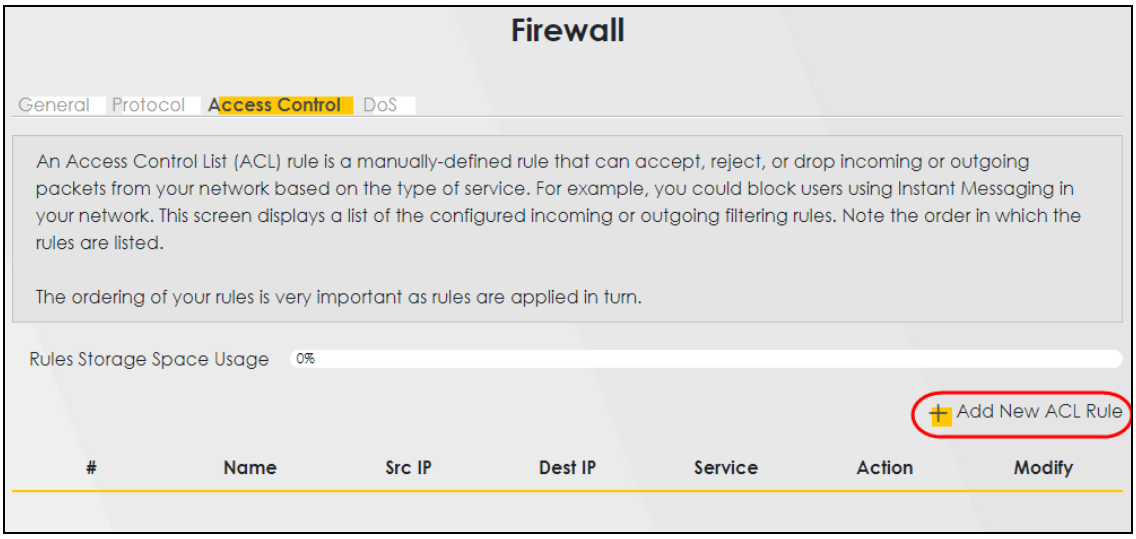
You can enable the firewall to protect your LAN computers from malicious attacks from the Internet.

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

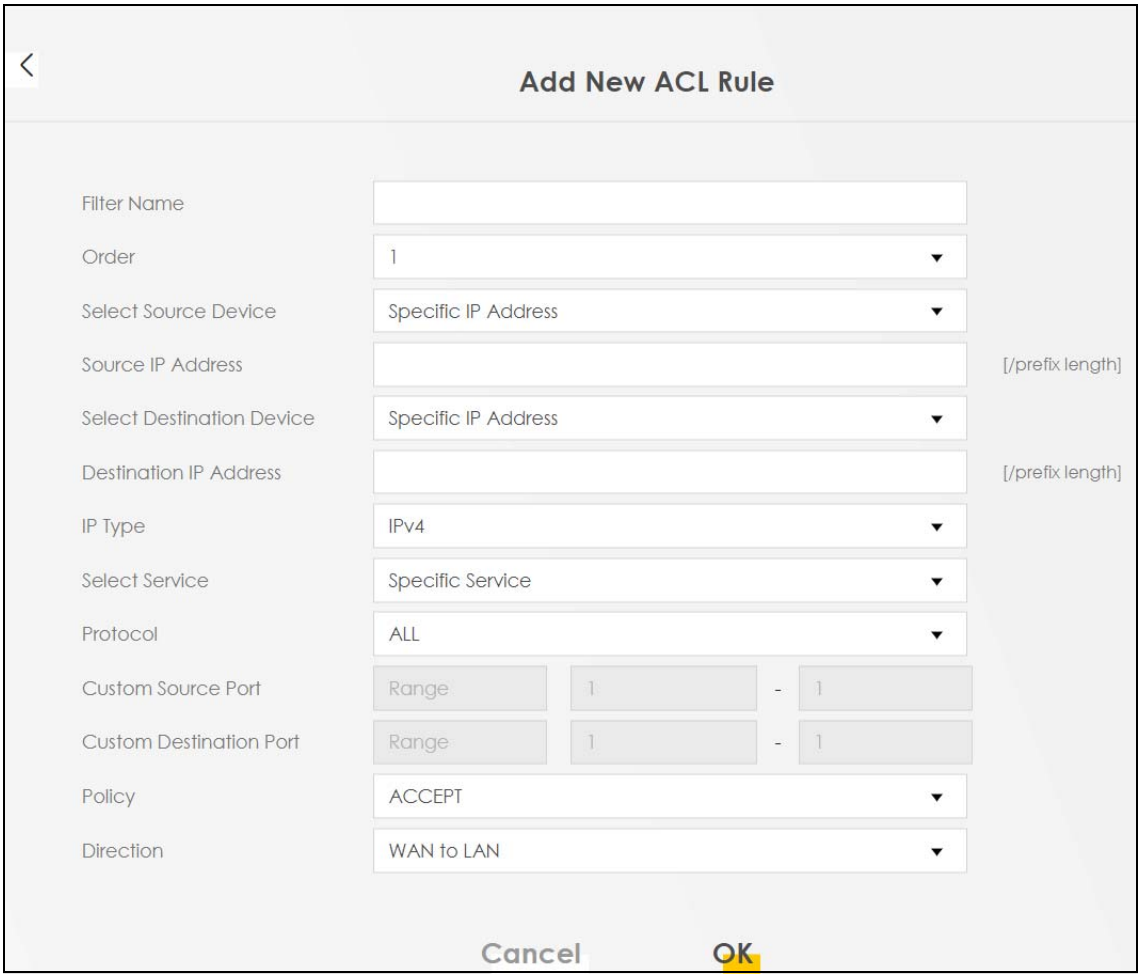
2 Select **IPv4 Firewall**/**IPv6 Firewall** to enable the firewall, and then click **Apply**.




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




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




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

- **Destination IP Address**: Enter the IP address of the computer to which traffic for the application or service is entering.
- **Protocol**: Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP** or **ICMPv6**) used to transport the packets.
- **Policy**: Select whether to (**ACCEPT**, **DROP**, or **REJECT**) the packets.
- **Direction**: Select the direction (**WAN to LAN**, **LAN to WAN**, **WAN to ROUTER**, or **LAN to ROUTER**) of the traffic to which this rule applies.

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

## 5.4.2 Parental Control

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

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

### 5.4.2.1 Configuring Parental Control Schedule and Filter

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

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

Use this feature to:

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

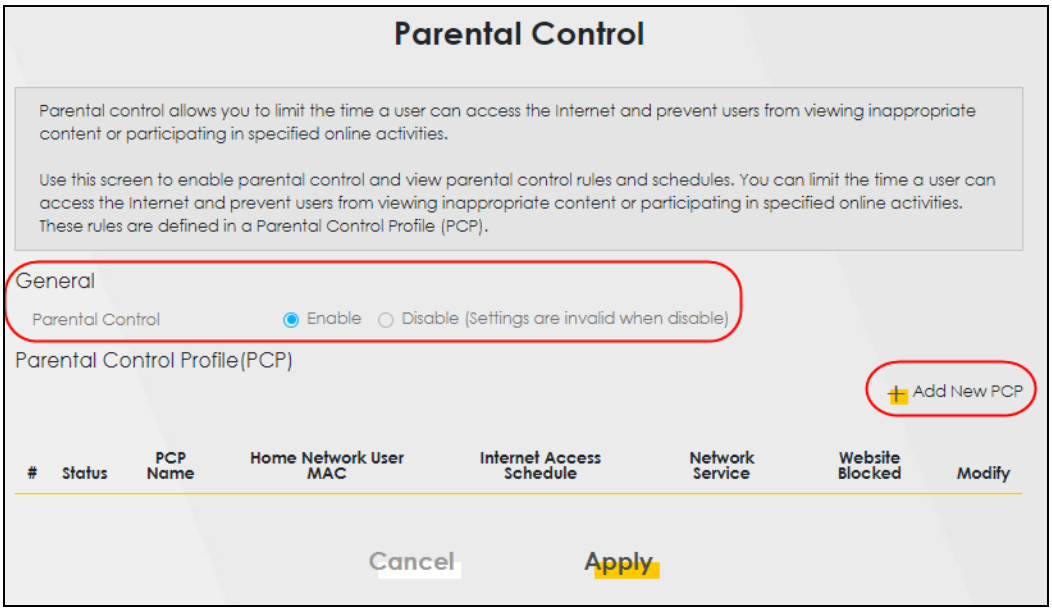
This example shows you how to block a user from accessing the Internet during time for studying. It also shows you how to stop a user from accessing specific websites.

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

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

#### Parental Control Screen

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



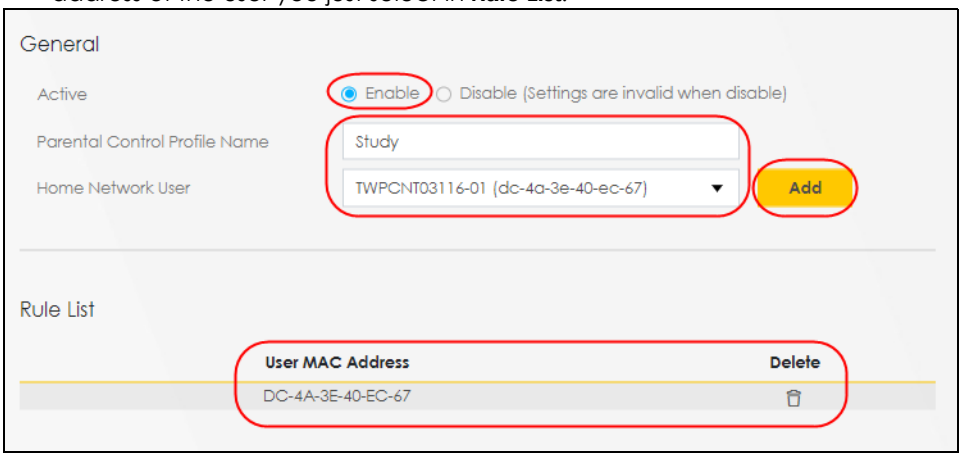

## Add New PCP Screen

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

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

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

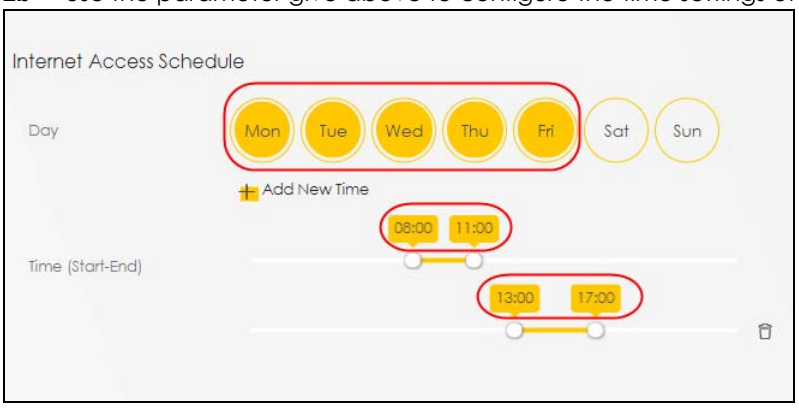
**1c** Select an user this rule applies to in **Home Network User**, then click **Add**. You will see the MAC address of the user you just select in **Rule List**.




2 Under **Internet Access Schedule**:

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

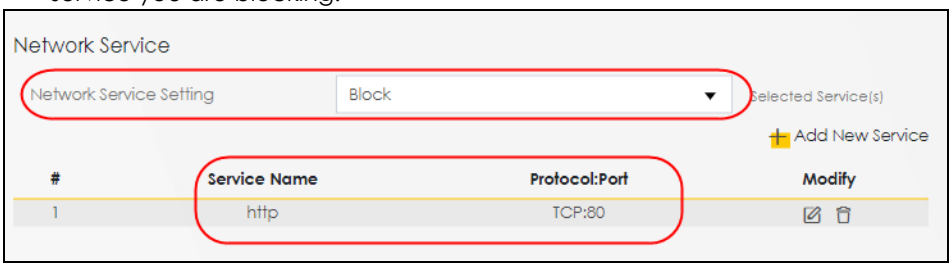
**2b** Use the parameter give above to configure the time settings of your schedule.




**3** Under **Network Service**:

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

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

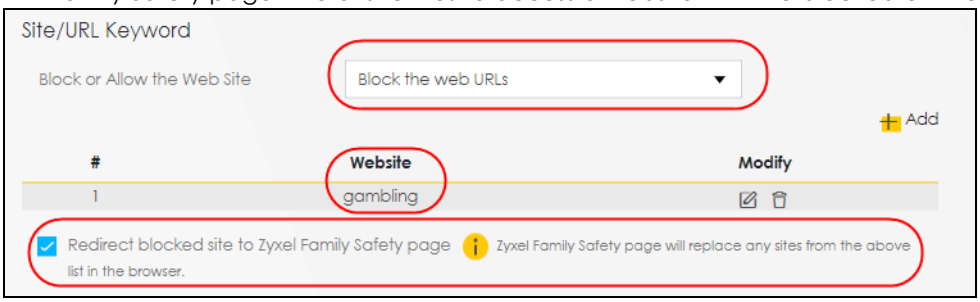


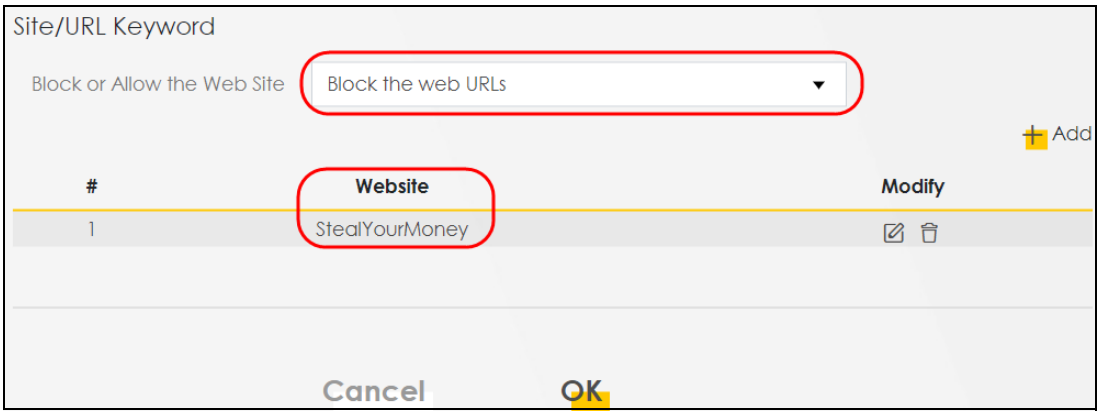

**4** Under **Site / URL Keyword**:

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

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

**4c** Select **Redirect blocked site to Zyxel Family Safety page** to redirect the web browser to the Zyxel Family Safety page if he or she tries to access a website with the blocked URL keyword.






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

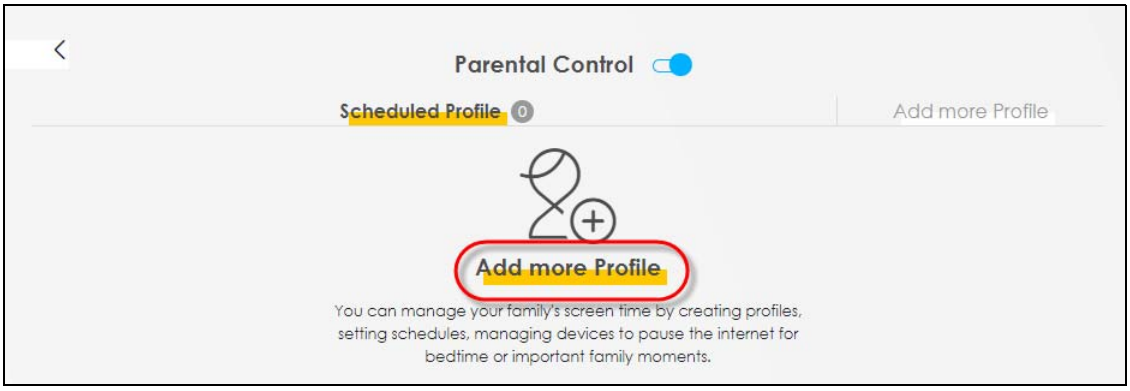
### 5.4.2.2 Configuring a Parental Control Schedule

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

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

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

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

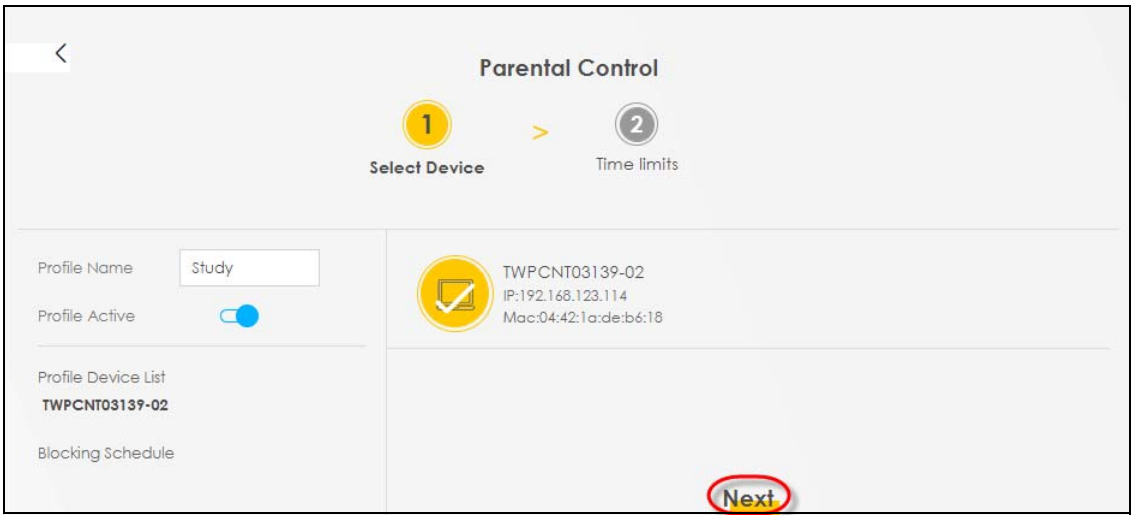



2 Use this screen to add a Parental Control rule.

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

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

2c Select a device, and then click **Next** to proceed.

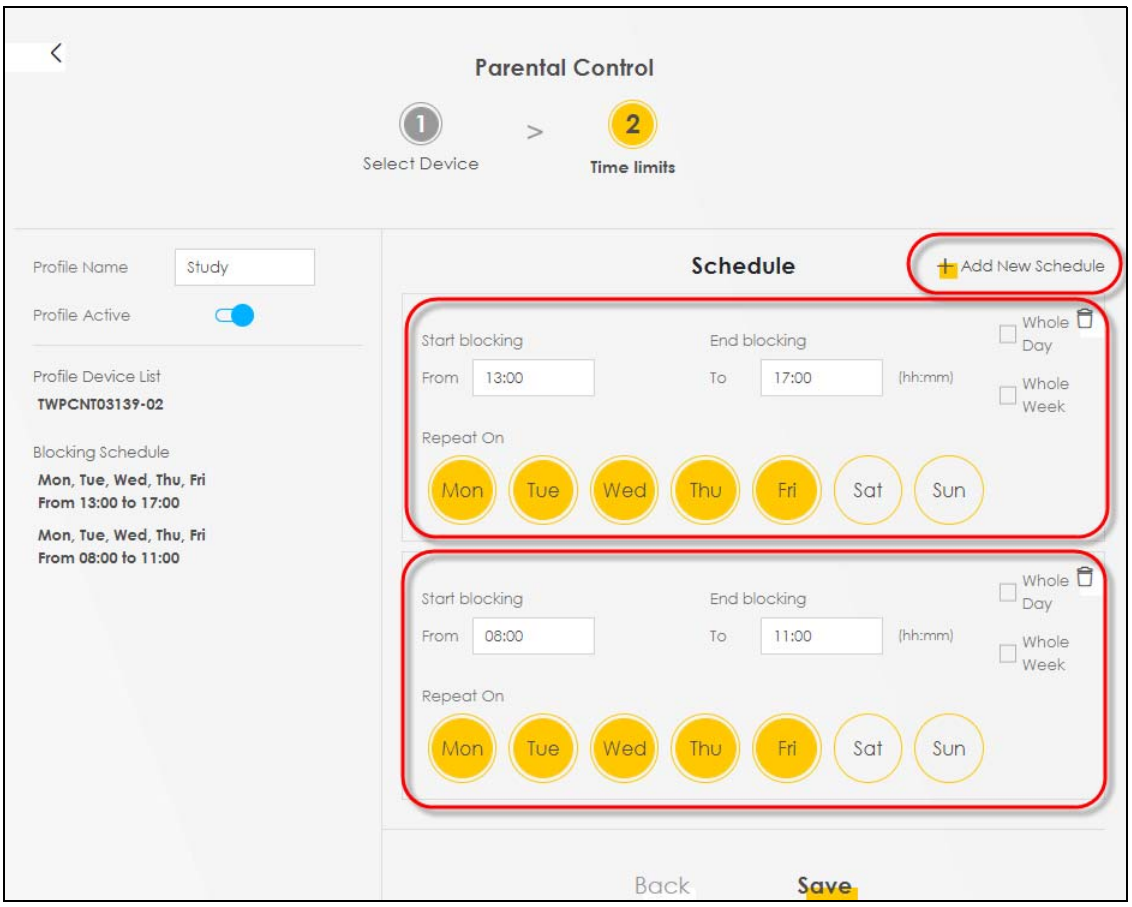



**3** Use this screen to edit the Parental Control schedule.

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

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

**3c** Click **Save** to save the settings.

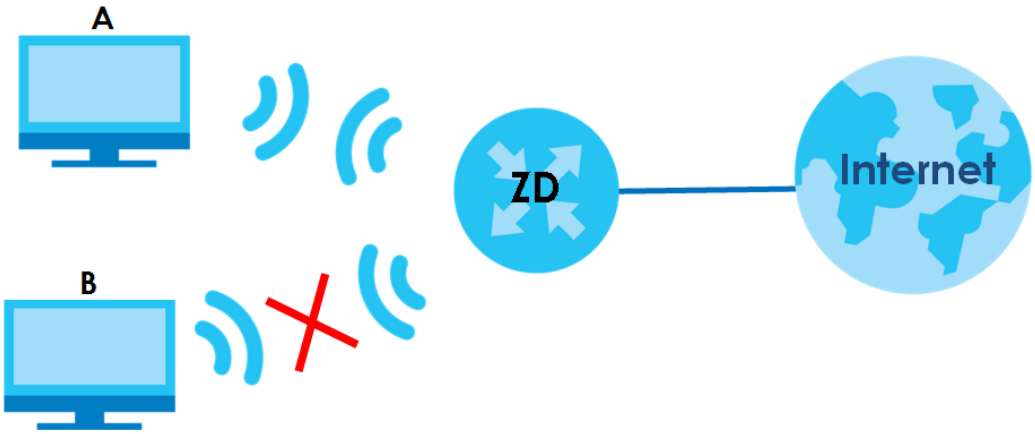


## 5.4.3 Configuring a MAC Address Filter

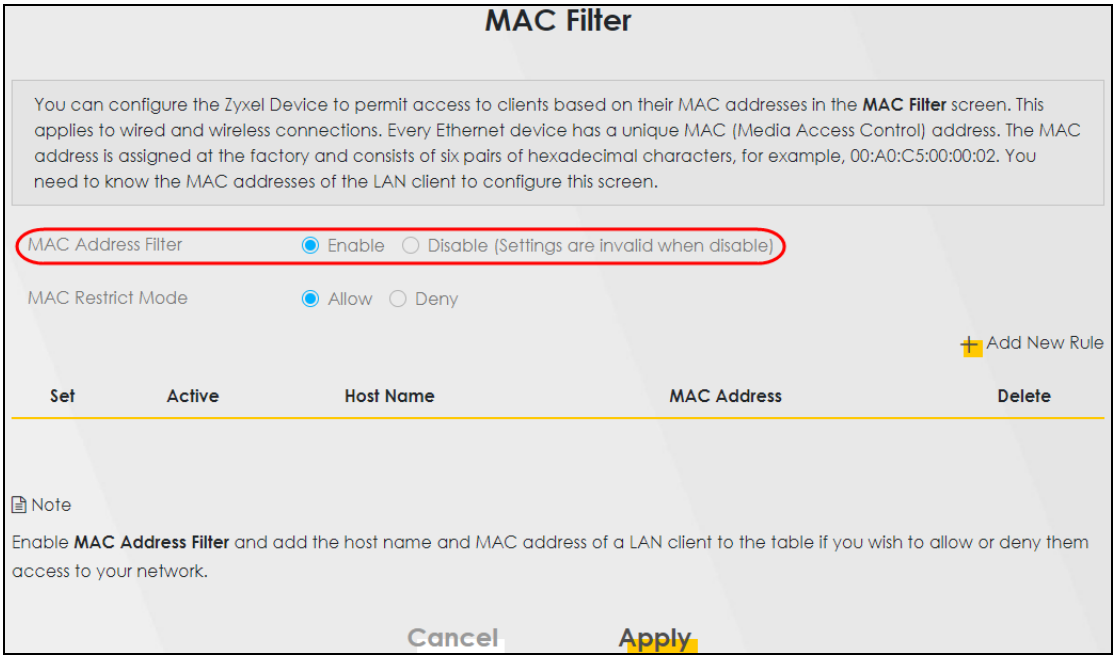
You can use a MAC address filter to exclusively allow or permanently block someone from the WiFi network.

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

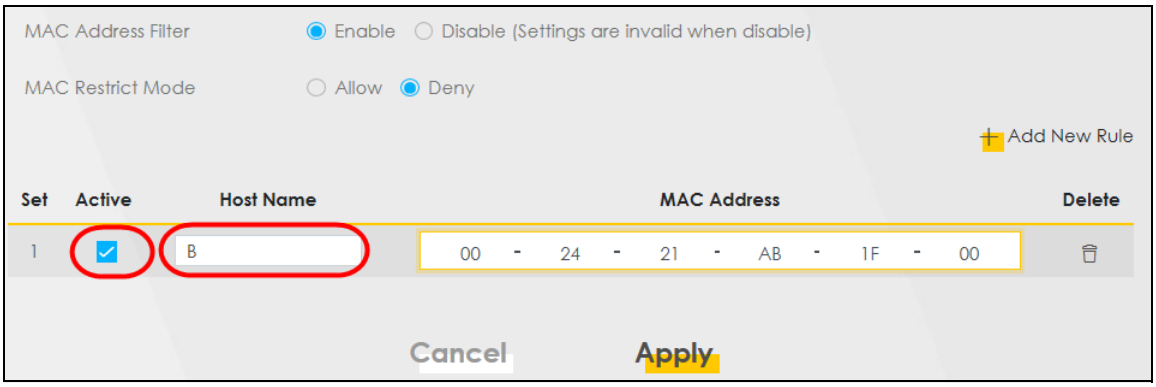
**Figure 38** Configure a MAC Address Filter Example




1 Go to the **Security** > **MAC Filter** > **MAC Filter** screen. Under **MAC Address Filter**, select **Enable**.




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




# 5.5 Device Maintenance

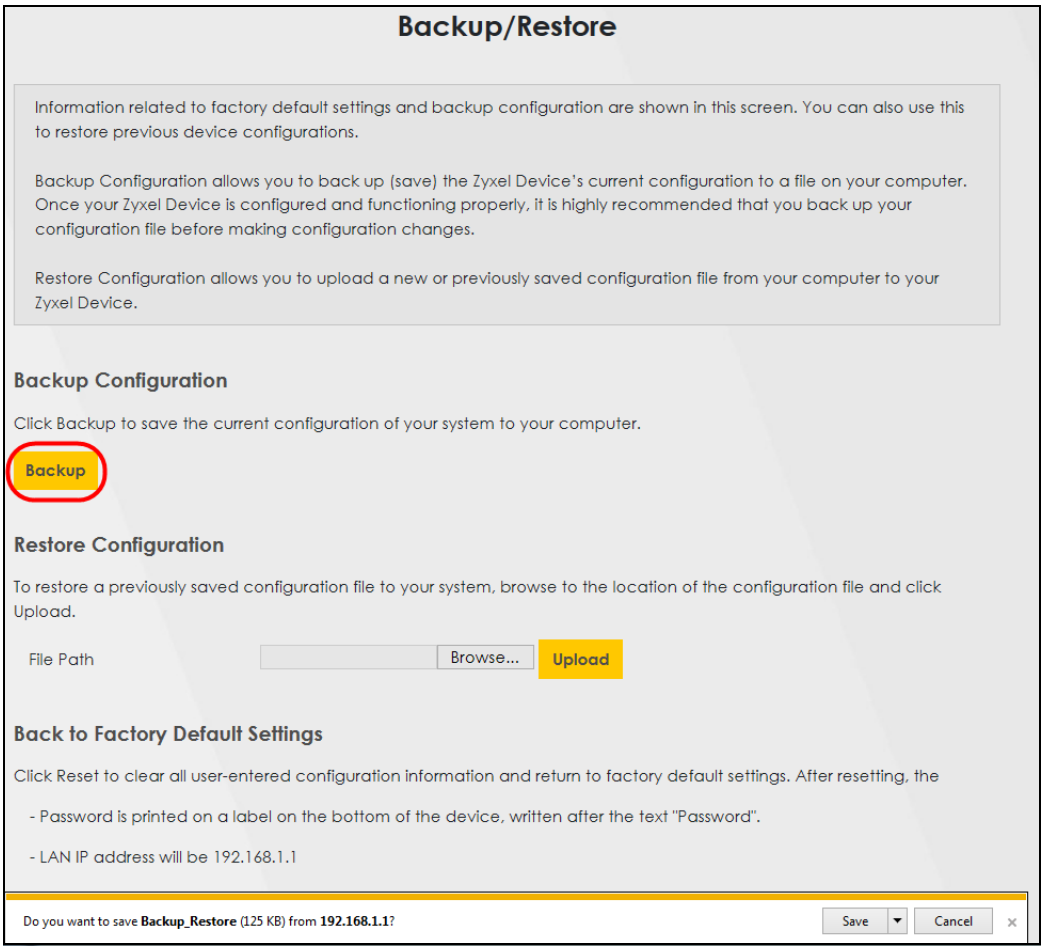
This section shows you how to upgrade device firmware, back up the device configuration and restore the device to its previous or default settings.

## 5.5.1 Backing up the Device Configuration

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

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

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

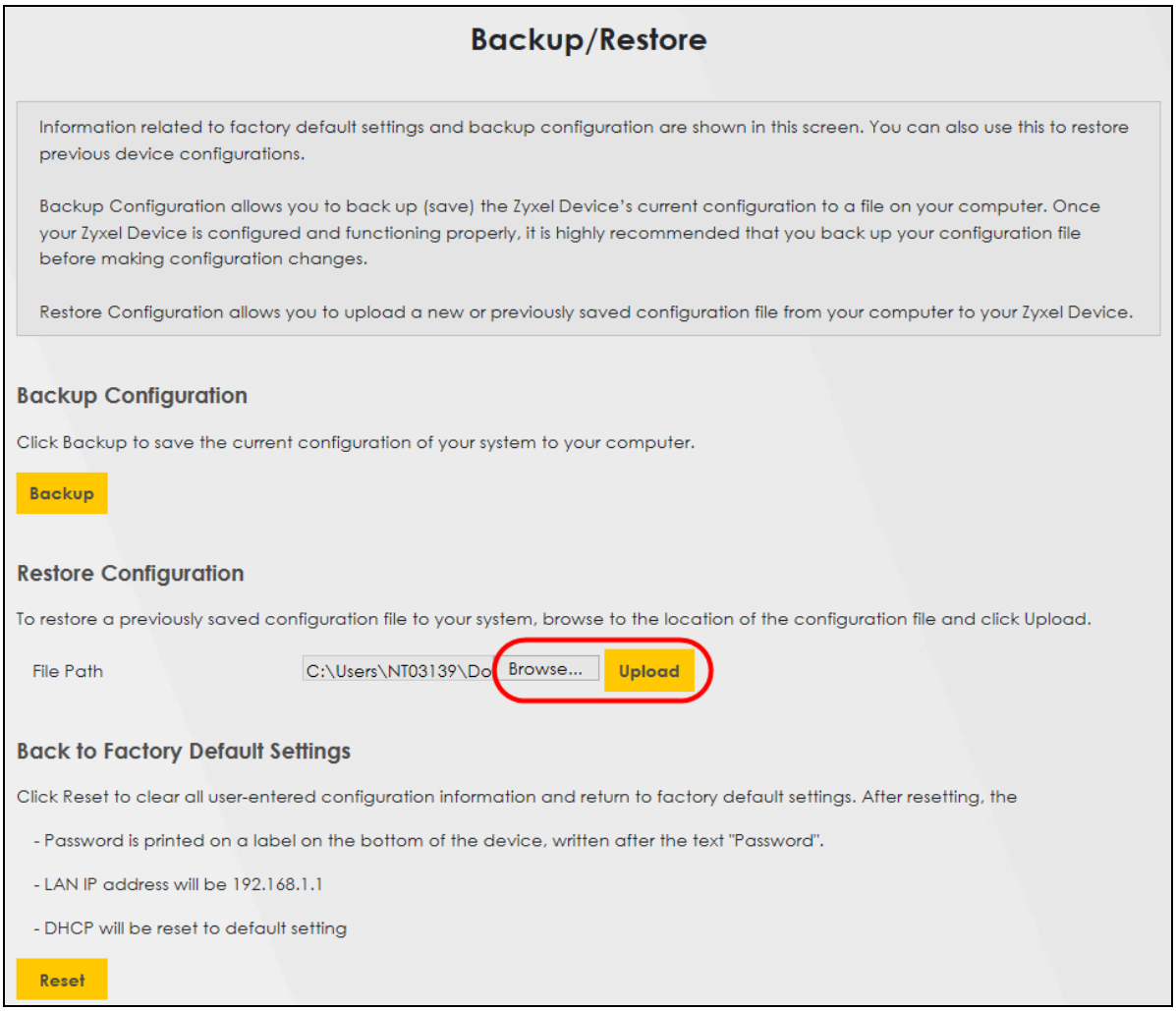



## 5.5.2 Restoring the Device Configuration

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

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

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




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

# CHAPTER 6
# Rover App Tutorials

## 6.1 Overview

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

The table below explains the terms used in this chapter.

Table 9 Tutorial Term Definition

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

## 6.2 What You Can Do

- Set up your Rover Router with a repeater (the WRE6605 Repeater as an example) using a wireless connection; see Section 6.3.1 on page 73.
- Set up your Rover AP with a router (Rover Router as an example) using a wired connection; see Section 6.4.1 on page 74.
- Set up your Rover Router with an access point (the WRE6605AP as an example) using a wired connection; see Section 6.4.2 on page 75.
- Use the **Home** screen to see how many devices are connected to your Zyxel Device; see Section 6.6 on page 77.
- Use the **WiFi Settings** screen to configure your general or guest WiFi network; see Section 6.7 on page 78.
- Use the **Devices** screen to view the information of WiFi clients connected to the Zyxel Device; see Section 6.8 on page 84.
- Use the **Parental Control** screen to configure parental control WiFi schedules to block or allow WiFi client device access to the Internet; see Section 6.9 on page 87.
- Use the **Others** screen to run a speed test, view your app version, or log out of the app; see Section 6.10 on page 89.

## 6.3 WiFi Network Scenario

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

### 6.3.1 Connect the Rover Router to the WRE6605 Repeater

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

Table 10 Device Role

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

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

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

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

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

4 Change the default SSID and WiFi key on the Rover Router for better WiFi security; see Section 6.7.1 on page 79 for more information. After applying changes, you will need to reconnect to the Rover Router again using the new SSID and WiFi key.

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

6 Use the Rover app and the table below to see if the repeater is too far from the Rover Router; see Section 6.8 on page 84 for more information.

Table 11 Link Quality

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

# 6.4 Wired Network Scenarios

- Scenario 1: Connect your Rover AP to a router
- Scenario 2: Connect your Rover Router to an access point

## 6.4.1 Scenario 1: Connect your Rover AP to the Rover Router

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

Table 12 Device Role

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

Note: Make sure you reset the Rover Router and Rover AP to factory defaults before switching to a different mode. Remember to back up your configuration setting before resetting your devices to factory defaults. See Section 2.3 on page 28 for more information.

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

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

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

4 Change the default SSID and WiFi key on the Rover Router for better WiFi security; see Section 6.7.1 on page 79 for more information. After applying changes, you will need to reconnect to Rover Router again using the new SSID and WiFi key.

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

6 Use the Rover app and the table below to see if the access point is securely connected to the Rover Router; see Section 6.8 on page 84 for more information.

Table 13 Link Quality

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

## 6.4.2 Scenario 2: Connect the Rover Router to the WRE6605 AP

Follow the steps below to set up the Rover Router with an access point (the WRE6605AP as an example). Connect the Rover Router to the Internet. The Rover Router must be connected to a modem/router

using an Ethernet cable. Then, connect the LAN port on the WRE6605AP to a LAN port on the Rover Router using another Ethernet cable.

Table 14 Device Role

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

Note: Make sure you reset the Zyxel Device and WRE6605 to factory defaults before switching to a different mode. Remember to back up your configuration setting before resetting your devices to factory defaults. See Section 2.3 on page 28 for more information.

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

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

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

4 Change the default SSID and WiFi key on the Rover Router for better WiFi security; see Section 6.7.1 on page 79 for more information. After applying changes, you will need to reconnect to the Rover Router again using the new SSID and WiFi key.

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

6 Use the Rover app and the table below to see if the access point is securely connected to the Rover Router; see Section 6.8 on page 84 for more information.

Table 15 Link Quality

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

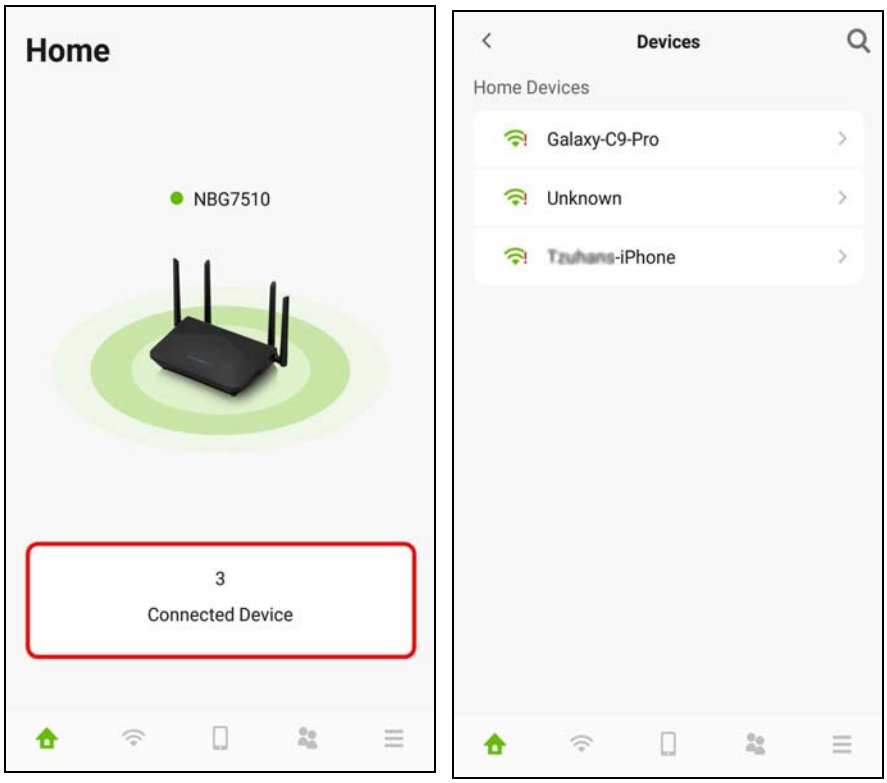
# 6.5 Network Management with the Rover App

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

- Home Settings
- General WiFi and Guest Settings
- Devices Settings
- Parental Control Settings
- Others Settings

# 6.6 Home Settings

Tap on the **Home** icon ( ) in the navigation panel. The **Home** screen displays and shows the number of the devices connected to the Zyxel Device.
You can tap **Connected Device** in the **Home** screen to go to the **Devices** screen. See Section 6.8 on page 84 for more device information.




# 6.7 General WiFi and Guest Settings

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

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

- Employees in Company A will use a general Company WiFi network group.
- Visiting guests will use the Guest WiFi network group, which has a different SSID and password. Visiting guests cannot connect to the company network using guest WiFi.

**Figure 39** General and Guest WiFi Network Example

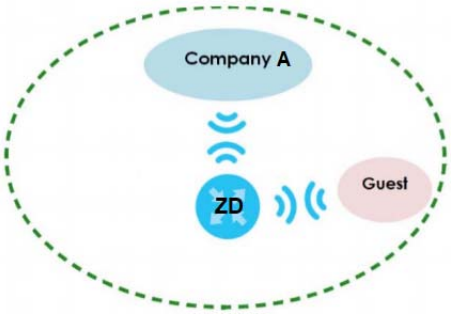
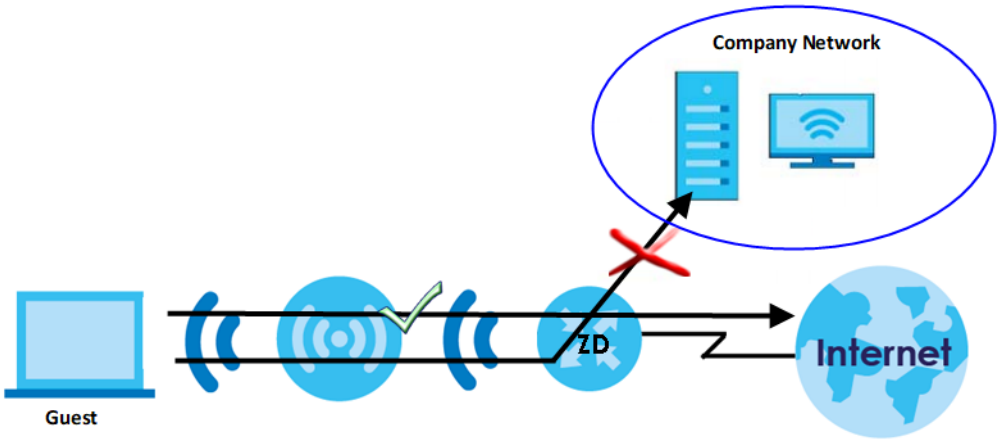


**Figure 40** Visiting Guests Blocked from Company Network



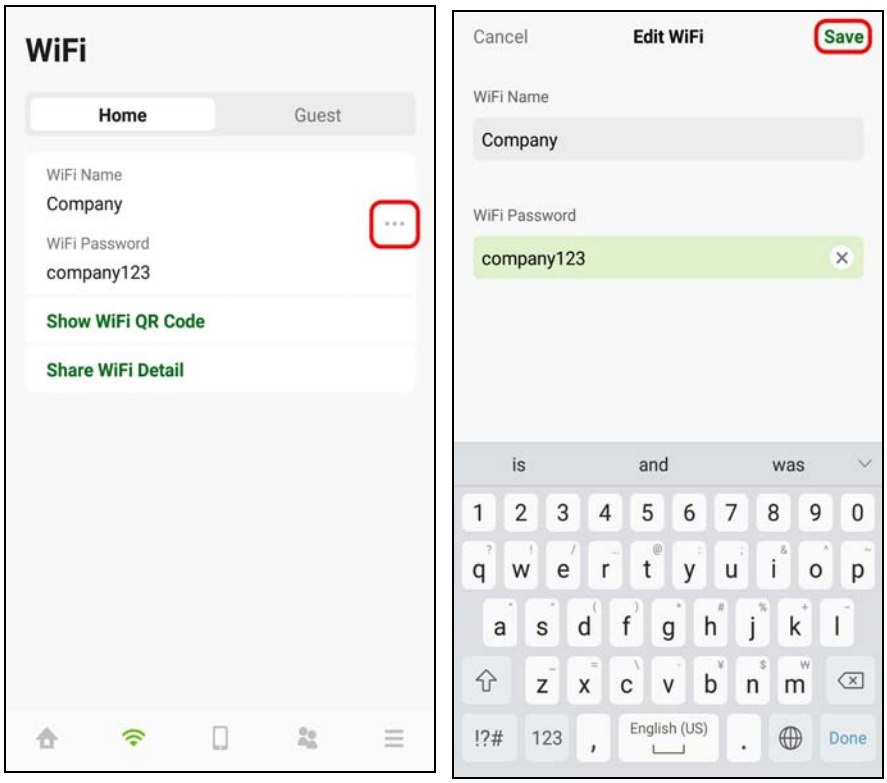

## 6.7.1 Setting Up General WiFi Settings

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

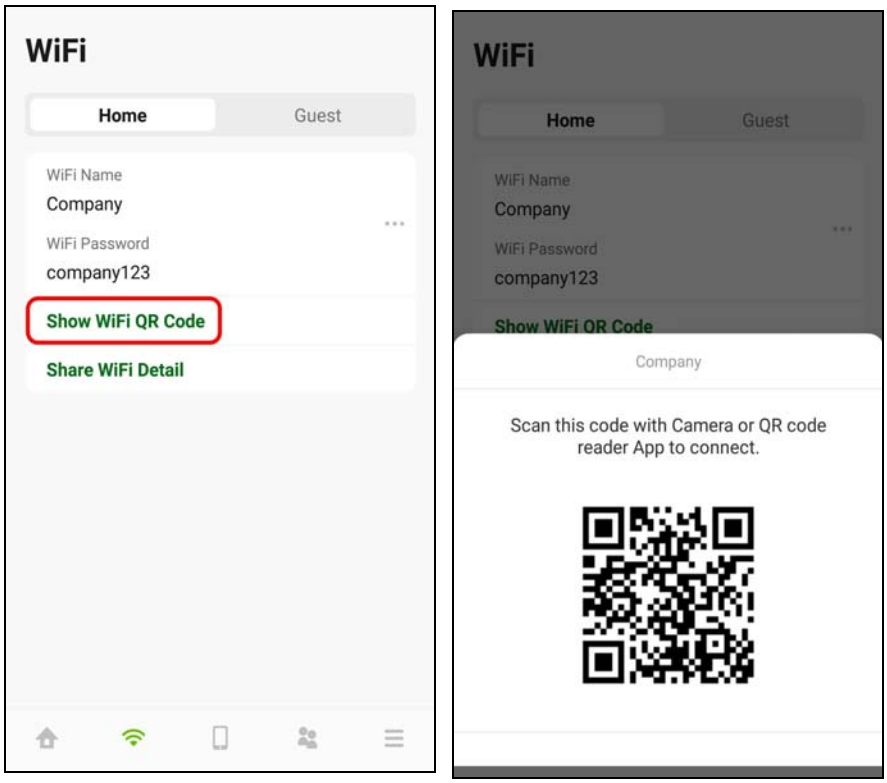
Table 16 The General WiFi Settings Parameters Example

| **GENERAL WIFI** | |
|---|---|
| WiFi Name | Company |
| Password | company123 |

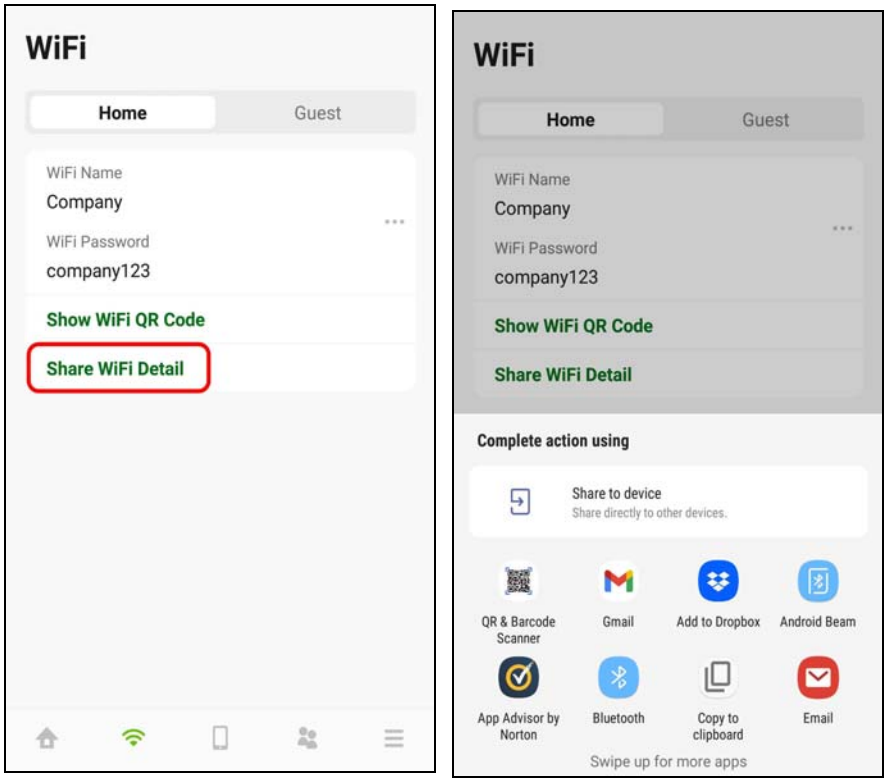
1 Tap on the **WiFi** icon ( ) in the navigation panel. The **WiFi > Home** screen displays. Tap on the ( ) icon to edit your general **WiFi Name** and **WiFi Password**. In this example, enter Company as your general **WiFi Name** and company123 as your general **WiFi Password**. Click **Save** to save the changes.




2 You can use the app to create a QR code with your WiFi network name and password. Tap **Show WiFi QR Code** in the **WiFi > Home** screen, the QR code will display as shown.
Use a smartphone to scan the QR code to join the general WiFi network. By printing and placing the QR code somewhere accessible, you can let your friends or guests scan the QR code and join the WiFi network directly without revealing your actual WiFi password.




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



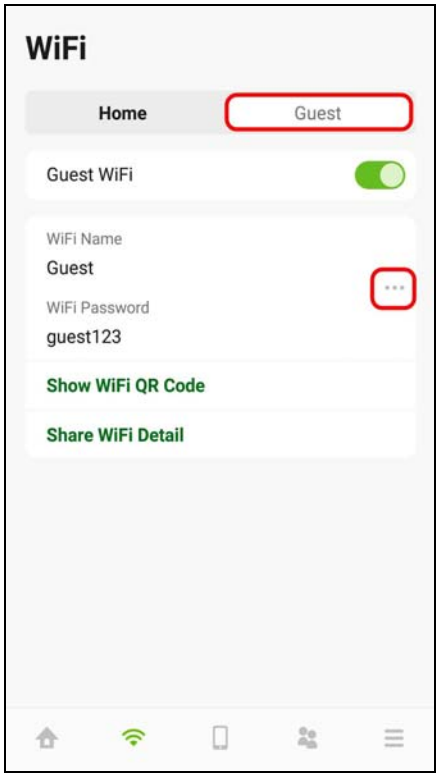
## 6.7.2 Setting Up Guest WiFi Settings

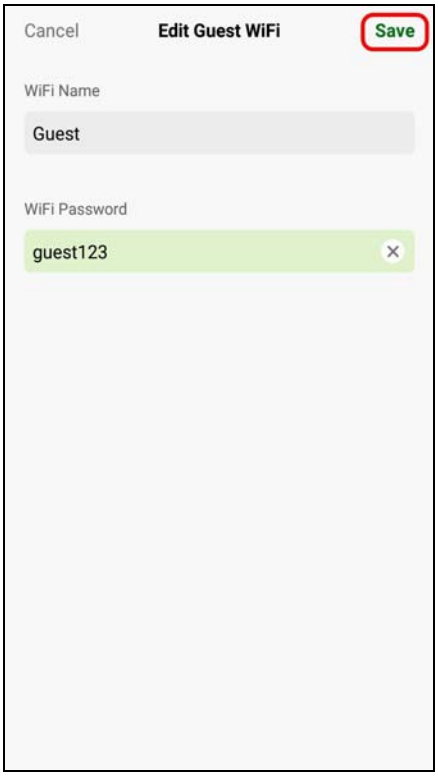
Follow the steps below to configure your guest WiFi settings. Use the parameters in the table below to create a different set of WiFi name and password.

Table 17 The Guest WiFi Settings Parameters Example

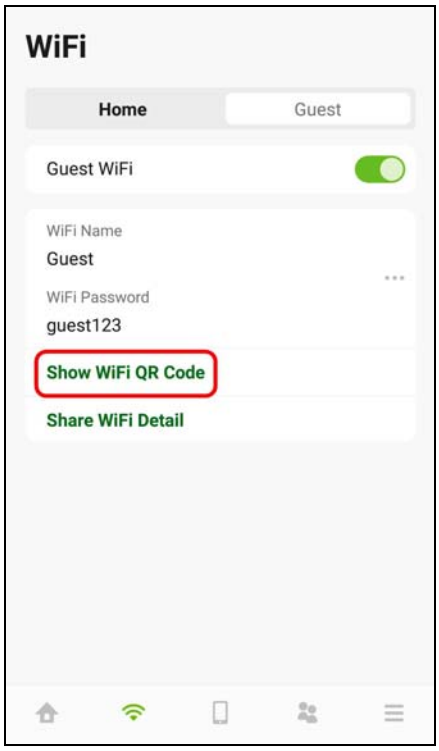
| GUEST WIFI | |
|---|---|
| WiFi Name | Guest |
| WiFi Password | guest123 |

Tap on the **Guest** tab and then the **WiFi > Guest** screen appears. Click the switch to enable **Guest WiFi**. When the switch goes to the right, **Guest WiFi** is enabled. Tap on the ( ... ) icon to edit the guest **WiFi Name** and **WiFi Password**. In this example, enter Guest as your guest **WiFi Name** and guest123 as your guest **WiFi Password**. Click **Save** to save the changes.

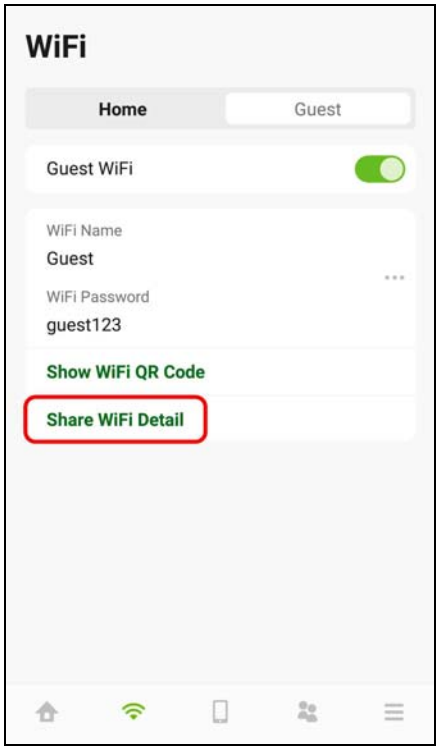


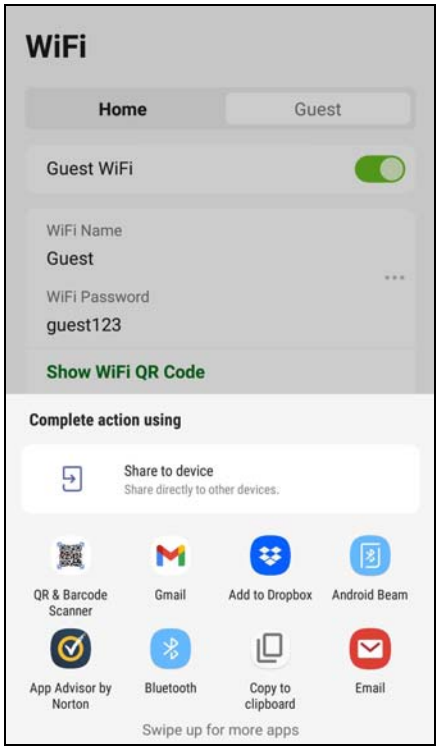




4 You can use the app to create a QR code with your WiFi network name and password. Click **Show WiFi QR Code** in the **WiFi > Guest** screen, the QR code will display as shown.
Use a smartphone to scan the QR code to join the guest WiFi network. By printing and placing the QR code somewhere accessible, you can let your friends or guests scan the QR code and join the WiFi network directly without revealing your actual WiFi password.



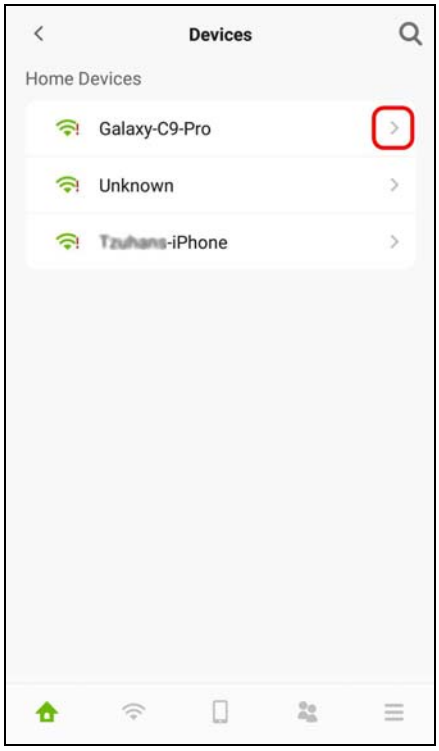
5 Tap **Share WiFi Detail** in the **WiFi > Guest** screen. To share your guest WiFi name and password with your friends, select a media, such as Gmail or Skype, to send connection info to your friends.

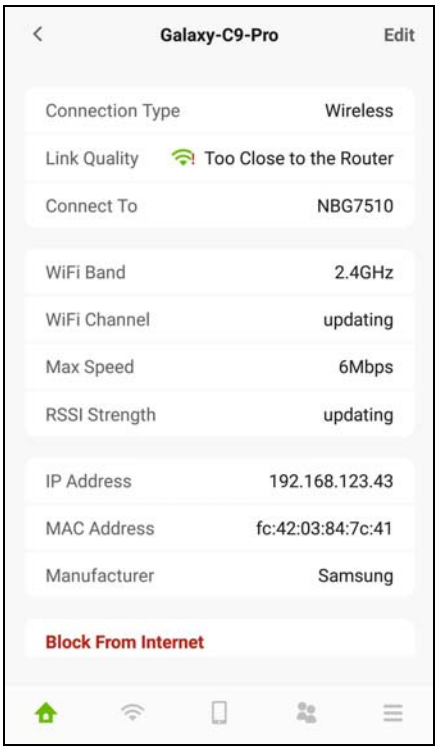


# 6.8 Devices Settings

1 Tap on the **Devices** icon ( ) in the navigation panel. Use the **Devices** screen to view the devices connected to the Zyxel Device. Tap on the Arrow icon ( > ) next the device name you want to see. In this example, tap on the Arrow icon ( > ) next to the **Galaxy-C9-Pro**. The **Galaxy-C9-Pro** screen displays.




2 After you place your access point or repeater connected to the Zyxel Device, use the **Devices** screen and the table below to check WiFi connection status.

Table 18 Link Quality

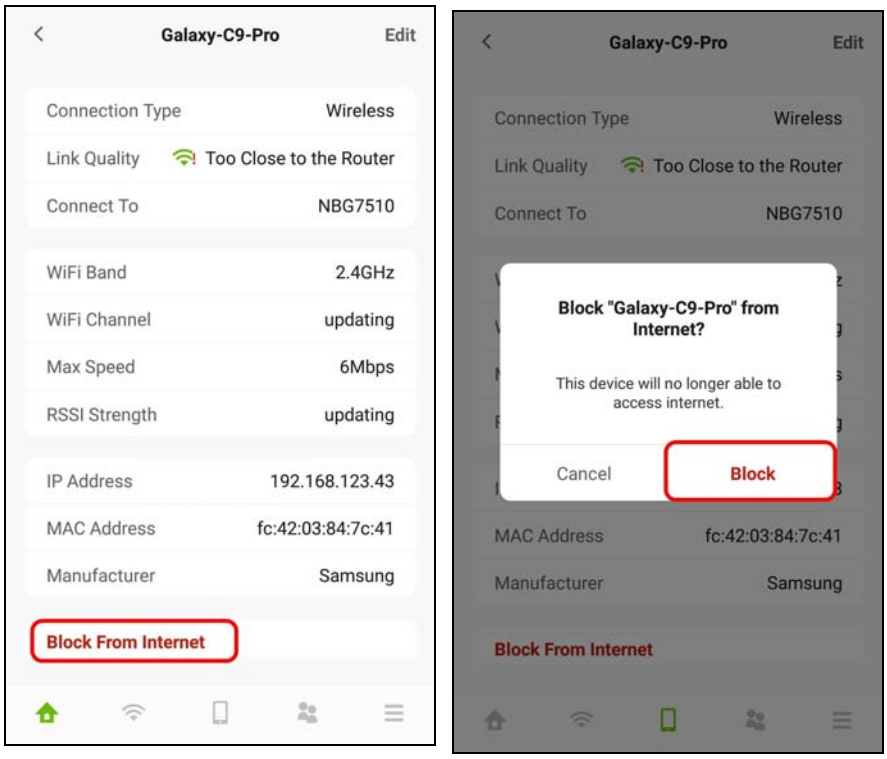
| ICON | CONNECTION TYPE | WIFI STATUS |
|---|---|---|
| | Wired | Wired Connection |
| | Wired | Blocked |
| | Wireless | Good to Go |
| | Wireless | Too Close to the Router |
| | Wireless | Weak WiFi |
| | Wireless | Blocked |

Table 19 WiFi Connection Status

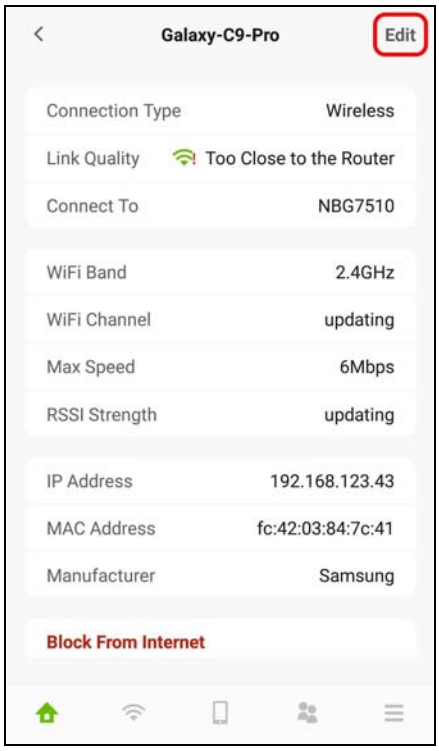
| WIFI CONNECTION STATUS | ACTION |
|---|---|
| Too Close to the Router | Move the client device farther away from the Zyxel Device. |
| Weak WiFi | Move the client device closer to the Zyxel Device. |

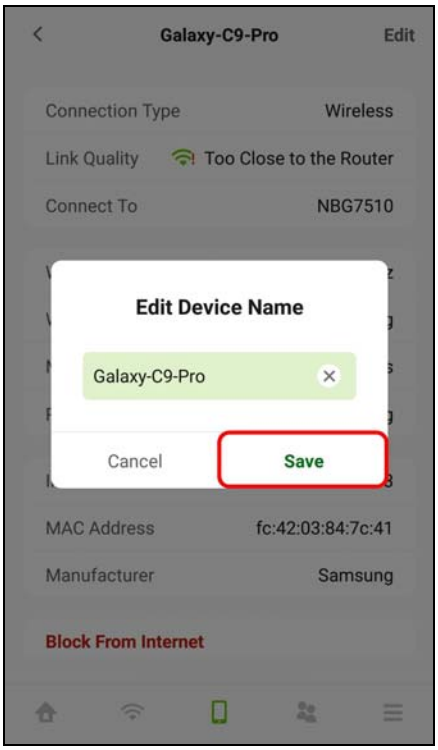
Move your Galaxy-C9-Pro farther away from your Zyxel Device as the WiFi status is **Too Close to the Router.**

3 To quickly block a client device from accessing your WiFi network, click **Block From Internet**. In this example, click **Block from Internet** in the **Galaxy-C9-Pro** screen. Click **Block** to save the changes.

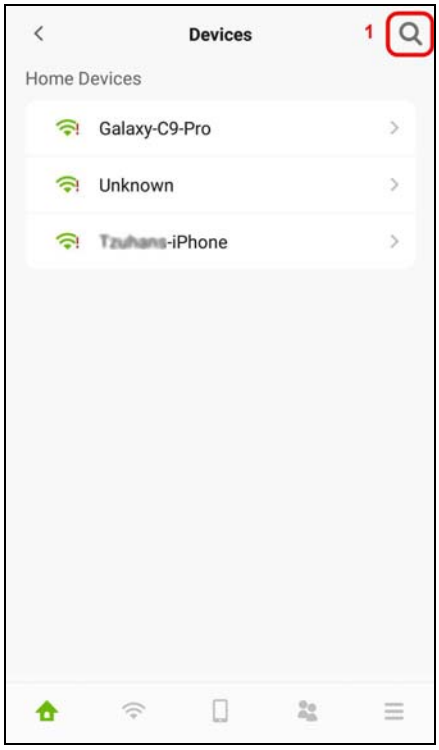


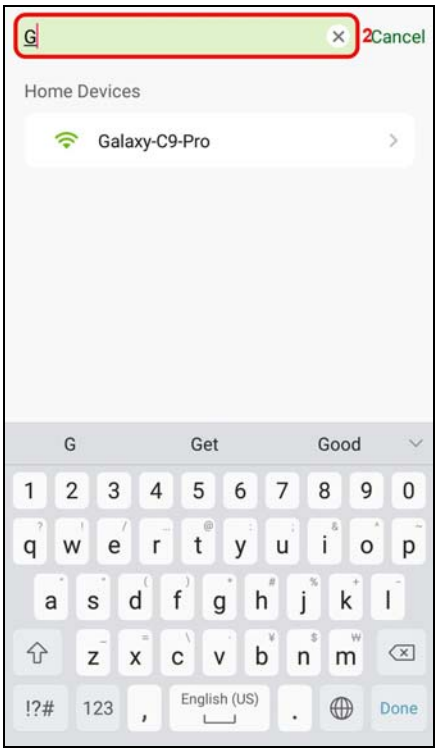

4 Click **Edit** if you want to modify your device name. Enter your device name and then click **Save** to save the changes.




**5** To look for a specific device, tap on the Search icon ( ) in the **Devices** screen. Enter keywords to look for a device. Tap **Cancel** if you want to go back to the previous screen.



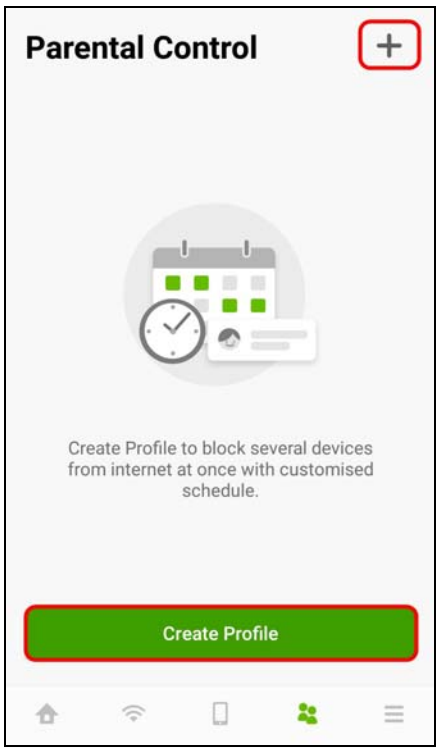
# 6.9 Parental Control Settings

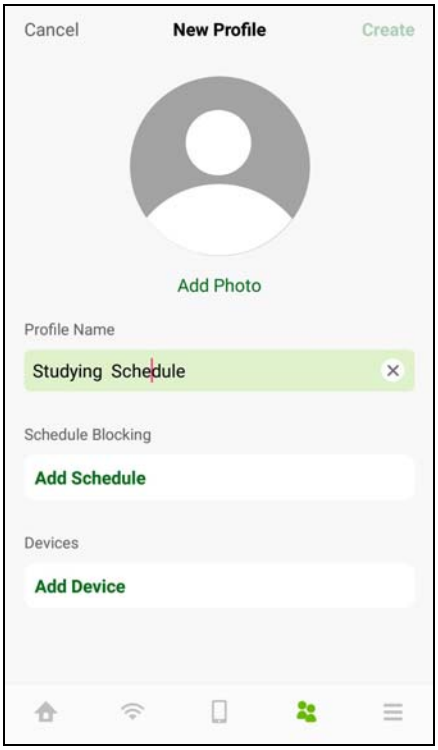
1 Parental Control allows you to create and repeat a weekly schedule to restrict Internet usage for users. Tap on the **Parental Control** icon ( ). The **Parental Control** screen displays. Tap **Create Profile** (only appears at the first time) or the Add icon ( + ) to create a new parental control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

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

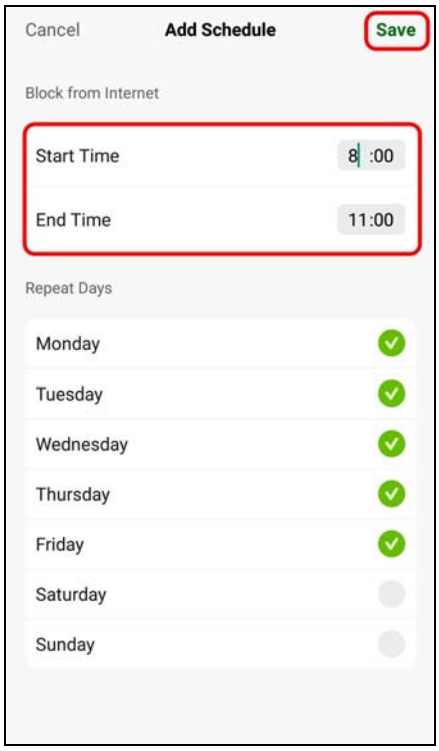
Table 20 Parental Control Settings Parameters Example

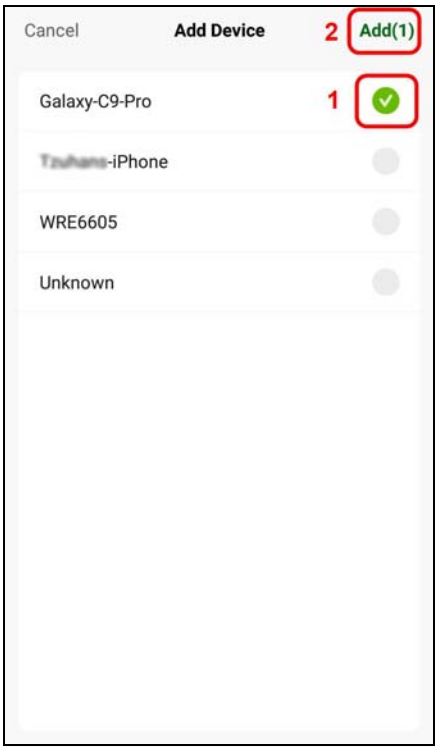
| PROFILE NAME | START TIME | END TIME | REPEAT ON |
|---|---|---|---|
| Studying Schedule | 8:00 am | 11:00 am | from Monday to Friday |



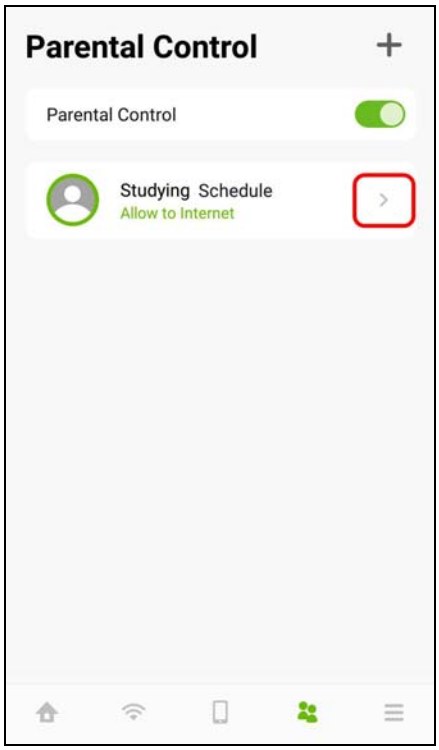



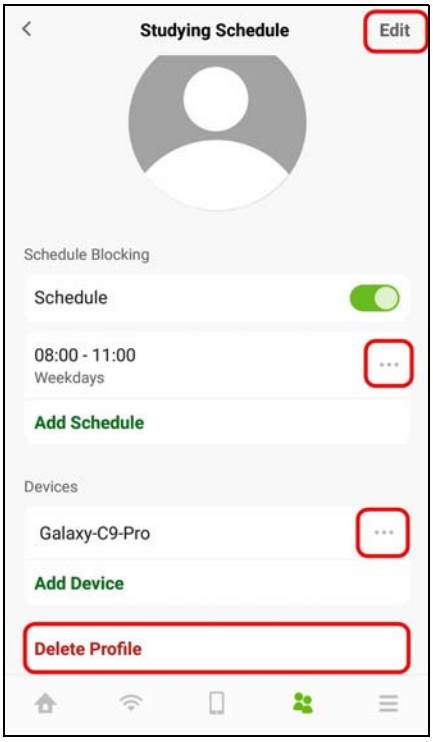

2 Click **Add Schedule** on the **Studying Schedule** screen to create a schedule. The **Add Schedule** screen displays. Select the day(s) of the week to repeat the rule and then enter the **Start Time** and **End Time** in the **Add Schedule** screen. In this example, select from Monday to Friday. Then, enter 8:00 as **Start Time**, and 11:00 as **End Time.**
Click **Add Device** to apply the **Studying Schedule** profile to a device. The **Add Device** screen appears as shown. Select the device you want to add and then click **Add** to save the changes.



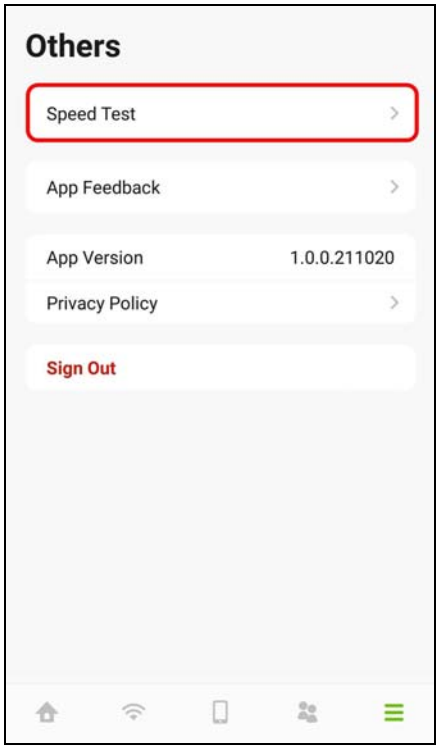

**3** Tap on the Arrow icon ( > ) next to the profile to go back and continue modifying your profile. In this example, click the Arrow icon ( > ) next to Studying Schedule. The **Studying Schedule** screen will appear.
Click **Edit** if you want to modify the name of the profile. Click the switch to enable or disable this WiFi schedule profile. Click the ( ... ) icon if you want to edit the parental control schedule or apply this profile to another device. Click **Delete Profile** to remove this profile.

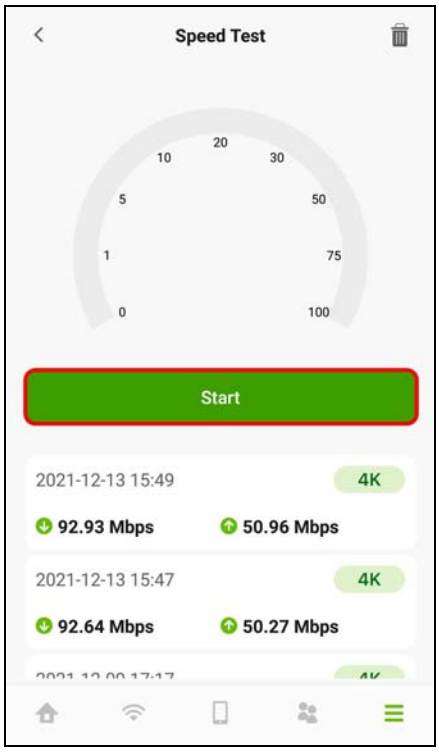


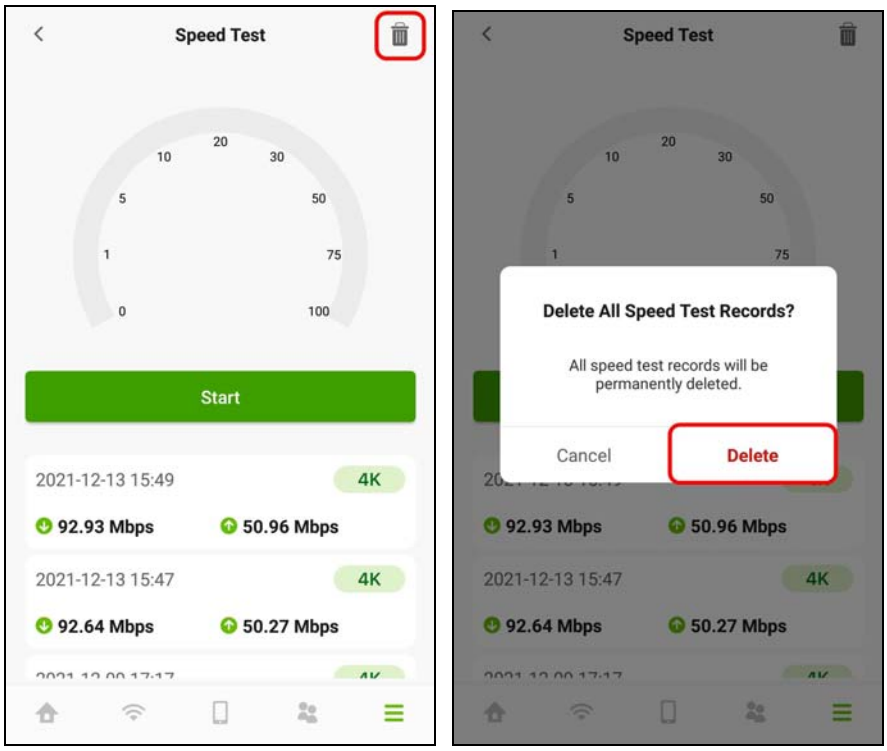
# 6.10 Others Settings

1 Tap on the **Others** icon ( ) in the navigation panel. The **Others** screen appears. Click Speed Test if you want to conduct a speed test for downstream and upstream data rates. The **Speed Test** screen appears. Click **Start** to perform a test.



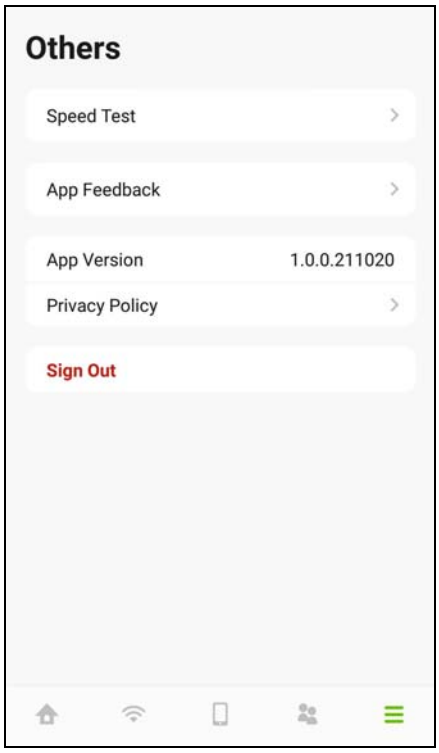



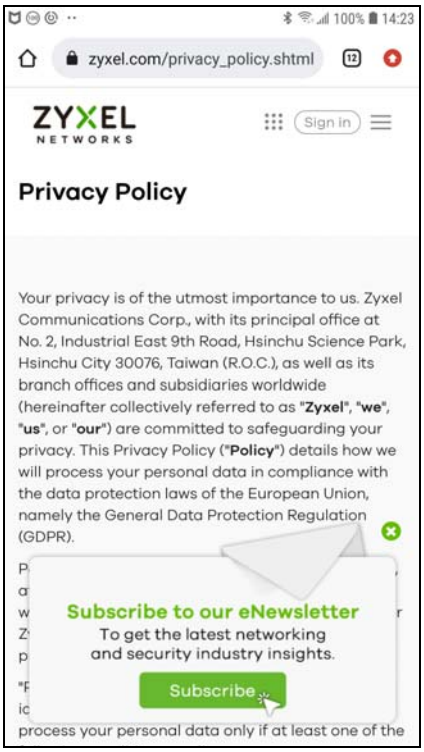

2 Click the Delete icon ( ) if you want to remove all previous test results. Click **Delete** to confirm the changes.




**3** You can also use this screen to do the following:

- Give us feedback.
- View the app version.
- View the privacy policy.
- Log out of the app.


Others
Speed Test
App Feedback
App Version
1.0.0.211020
Privacy Policy
Sign Out


100% 14:23
zyxel.com/privacy_policy.shtml
ZYXEL
NETWORKS
Sign in
Privacy Policy
Your privacy is of the utmost importance to us. Zyxel Communications Corp., with its principal office at No. 2, Industrial East 9th Road, Hsinchu Science Park, Hsinchu City 30076, Taiwan (R.O.C.), as well as its branch offices and subsidiaries worldwide (hereinafter collectively referred to as "Zyxel", "we", "us", or "our") are committed to safeguarding your privacy. This Privacy Policy ("Policy") details how we will process your personal data in compliance with the data protection laws of the European Union, namely the General Data Protection Regulation (GDPR).
Subscribe to our eNewsletter
To get the latest networking and security industry insights.
Subscribe
process your personal data only if at least one of the

# PART II
# Technical Reference

# CHAPTER 7
# Connection Status

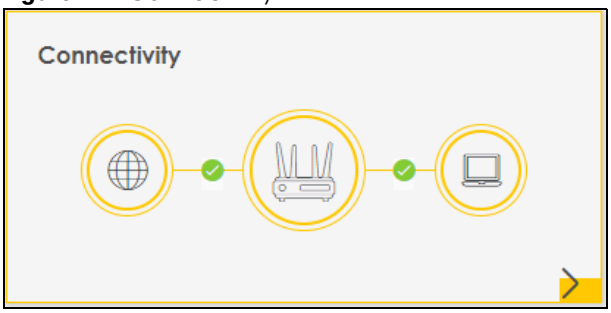
## 7.1 Connection Status Overview

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

### 7.1.1 Connectivity

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

**Figure 41** Connectivity




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

**Figure 42** Connectivity: Connected Devices

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

### 7.1.2 Icon and Device Name

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

( ) **Internet Blocking** (or **Active**) for a connected WiFi client. Click **Save** to save your changes.

**Figure 43** Connectivity: Edit

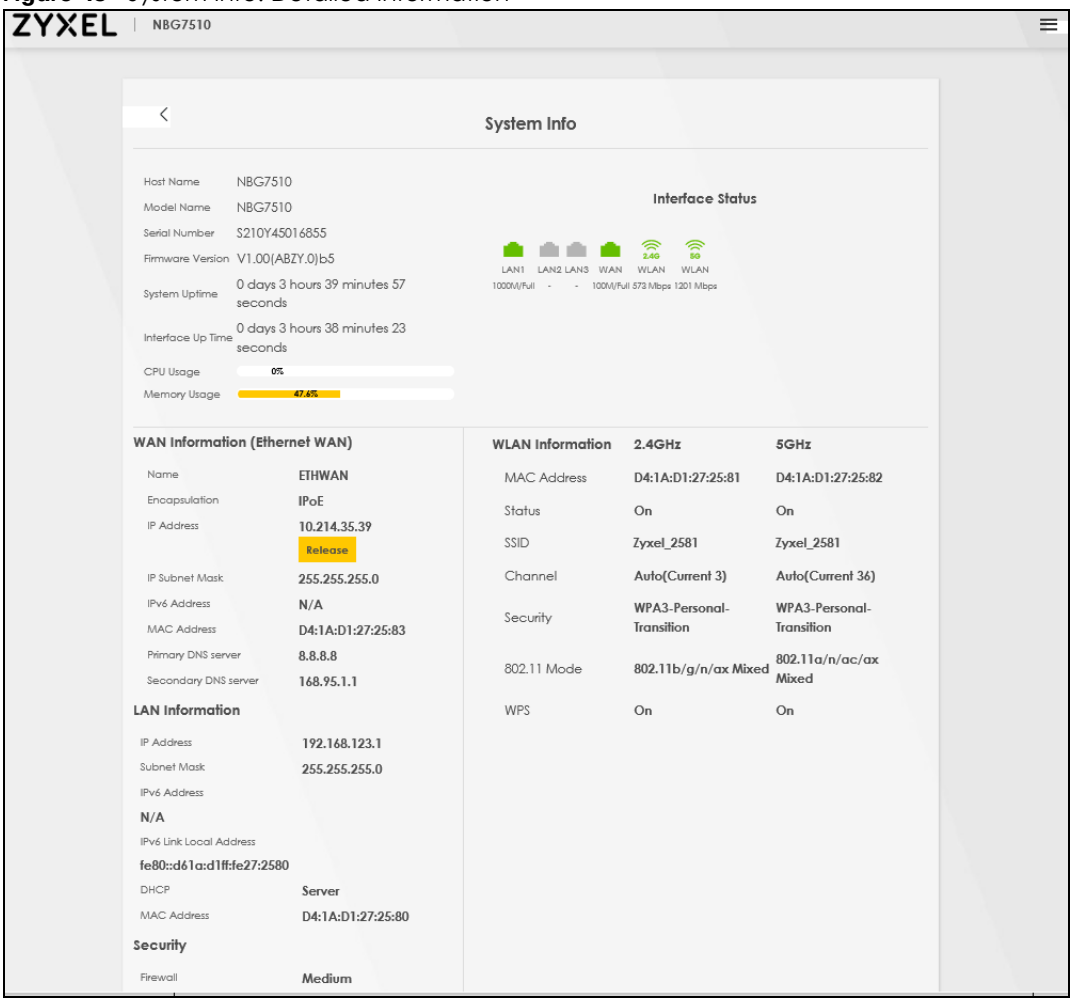
## 7.1.3 System Info

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

**Figure 44** System Info

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

**Figure 45** System Info: Detailed Information




Each field is described in the following table.

Table 21 System Info: Detailed Information

| LABEL | DESCRIPTION |
|---|---|
| Host Name | This field displays the Zyxel Device system name. It is used for identification. |
| Model Name | This shows the model number of your Zyxel Device. |
| Serial Number | This field displays the serial number of the Zyxel Device. |
| Firmware Version | This is the current version of the firmware inside the Zyxel Device. |
| System Uptime | This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (**Maintenance** > **Reboot**), or when you reset it. |
| IP Subnet Mask | This field displays the current subnet mask in the WAN. |
| Primary DNS server | This field displays the first DNS server address assigned by the ISP. |
| Secondary DNS server | This field displays the second DNS server address assigned by the ISP. |
| 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. |

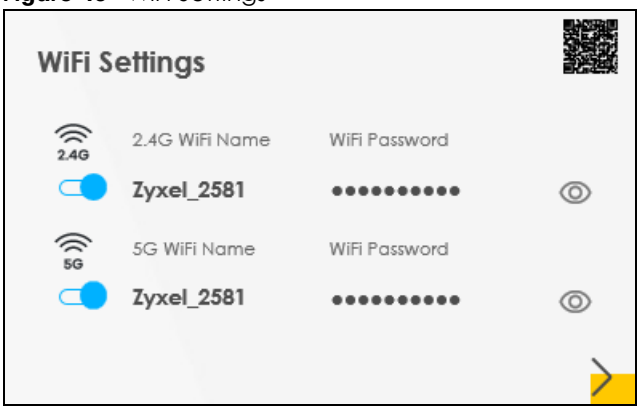
Table 21 System Info: Detailed Information (continued)

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

## 7.1.4 WiFi Settings

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

**Figure 46** WiFi Settings



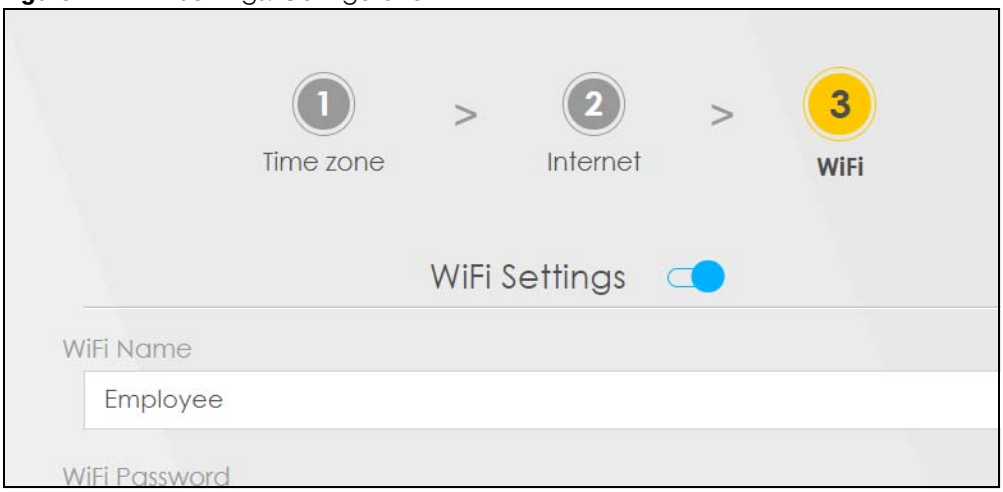

Click the Arrow icon ( ) to configure the SSIDs and/or passwords for your main wireless networks. Click the Eye icon ( ) to display the characters as you enter the WiFi Password.

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

Select **Smart Connect** to use the same SSID for 2.4 GHz and 5 GHz bands.

Note: Note that you have to disable Zyxel MESH in the **Network** > **Wireless** > **Mesh** screen to deselect the **Smart Connect** check box.

**Figure 47** WiFi Settings: Configuration




Each field is described in the following table.

Table 22 WiFi Settings: Configuration

| LABEL | DESCRIPTION |
|---|---|
| Smart Connect | Select this and the 2.4 GHz and 5 GHz wireless networks will use the same SSID.<br>If you deselect this, the screen will change. You need to assign different SSIDs for the 2.4 GHz and 5 GHz wireless networks. |
| 2.4 GHz / 5 GHz WiFi | Click this switch to enable or disable the 2.4G / 5G WiFi network. When the switch turns blue , the function is enabled. |
| WiFi Name | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.<br><br>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |

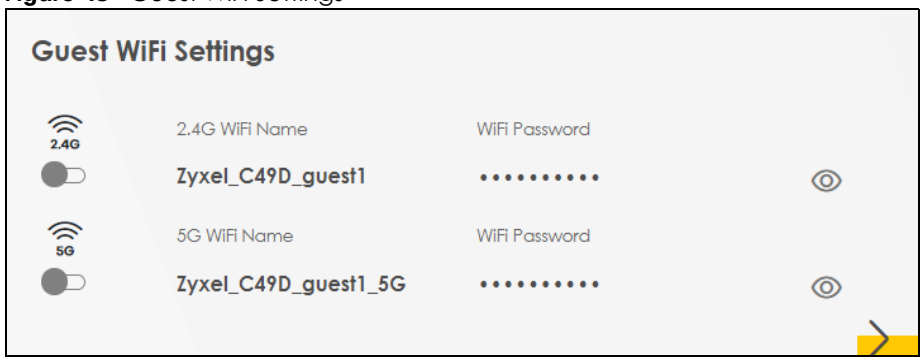
Table 22 WiFi Settings: Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| WiFi Password | If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device.<br><br>If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.<br><br>Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden. |
| Random Password | Select this to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option. |
| Hide WiFi network name | Select this to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.<br><br>Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID. |
| Save | Click **Save** to save your changes. |

# 7.2 Guest WiFi Settings

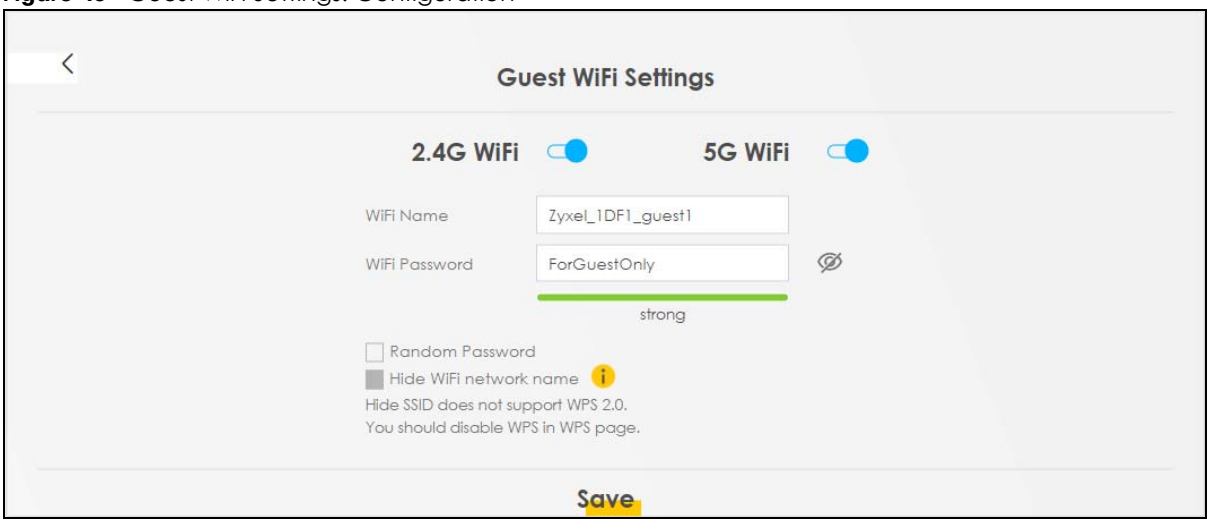
Use this screen to enable or disable the guest 2.4 GHz and/or 5 GHz wireless networks. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click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

**Figure 48** Guest WiFi Settings




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

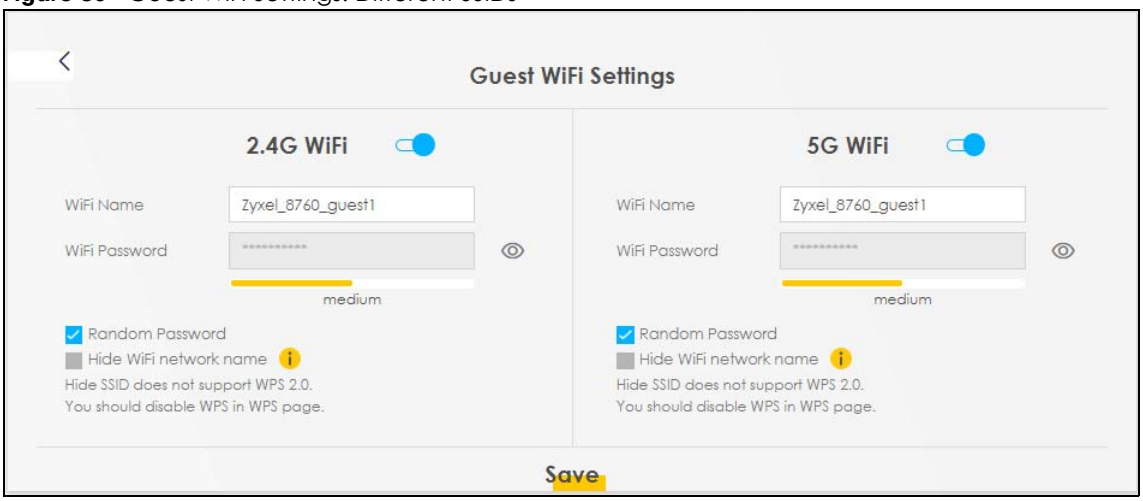
**Figure 49** Guest WiFi Settings: Configuration




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

Note: Note that you have to disable Zyxel MESH in the **Network** > **Wireless** > **Mesh** screen to clear the **Smart Connect** check box.

**Figure 50** Guest WiFi Settings: Different SSIDs




Each field is described in the following table.

Table 23 WiFi Settings: Configuration

| LABEL | DESCRIPTION |
|---|---|
| 2.4G/5G WiFi | Click this switch to enable or disable the 2.4 GHz and/or 5 GHz wireless networks. When the switch goes to the right , the function is enabled. Otherwise, it is not. |
| WiFi Name | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.<br><br>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |

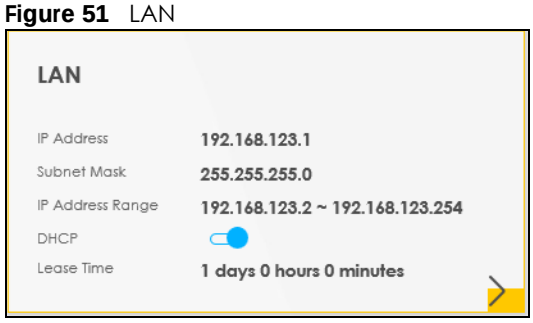
Table 23 WiFi Settings: Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| WiFi Password | If you selected **Random Password**, this field displays a pre-shared key generated by the Zyxel Device.<br><br>If you did not select **Random Password**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. |
| | Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden. |
| Random Password | Select this option to have the Zyxel Device automatically generate a password. The **WiFi Password** field will not be configurable when you select this option. |
| Hide WiFi network name | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.<br><br>Note: Disable WPS in the **Network Setting** > **Wireless** > **WPS** screen to hide the SSID. |
| Save | Click **Save** to save your changes. |

## 7.2.1 LAN

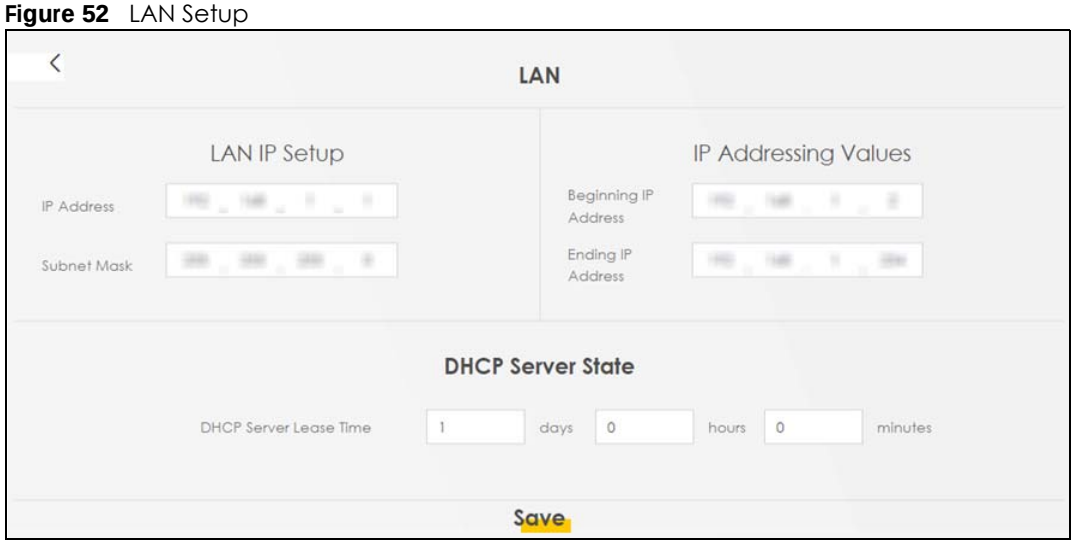
Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device. Click the switch button to turn on/off the DHCP server.

**Figure 51** LAN




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

**Figure 52** LAN Setup



Each field is described in the following table.

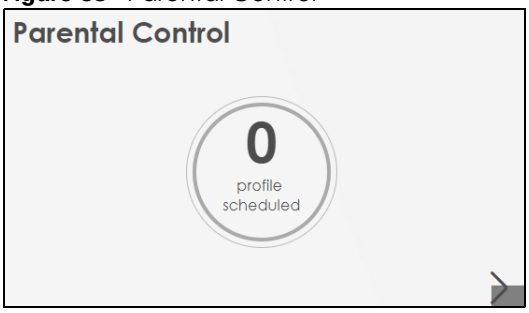
Table 24 LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| LAN IP Setup | |
| IP Address | Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.123.1 (factory default). |
| Subnet Mask | Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so. |
| IP Addressing Values | |
| Beginning IP Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Ending IP Address | This field specifies the last of the contiguous addresses in the IP address pool. |
| DHCP Server State | |
| DHCP Server Lease Time | This is the period of time a DHCP-assigned address is valid, before it expires.<br>When a client connects to the Zyxel Device, DHCP automatically assigns the client an IP addresses from the IP address pool. DHCP leases each addresses for a limited period of time, which means that past addresses are "recycled" and made available for future reassignment to other devices. |
| Days/Hours/ Minutes | Enter the lease time of the DHCP server. |

# 7.3 The Parental Control Screen

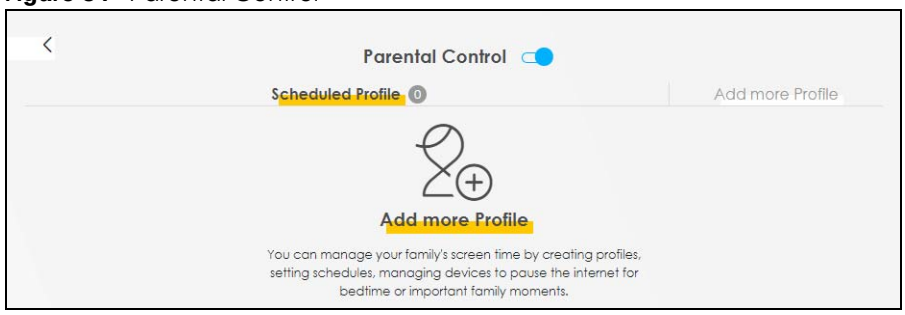
Use this screen to view the number of profiles that were created for parental control.

**Figure 53** Parental Control




Click the yellow Arrow icon to open the following screen. Use this screen to enable parental control and add more profiles..

**Figure 54** Parental Control




Each field is described in the following table.

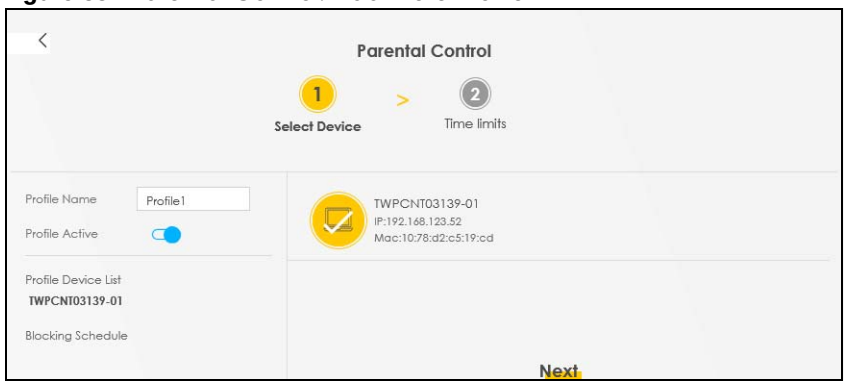
Table 25 Parental Control: Schedule

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

## 7.3.1 Create a Parental Control Profile

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

**Figure 55** Parental Control: Add More Profile




Each field is described in the following table.

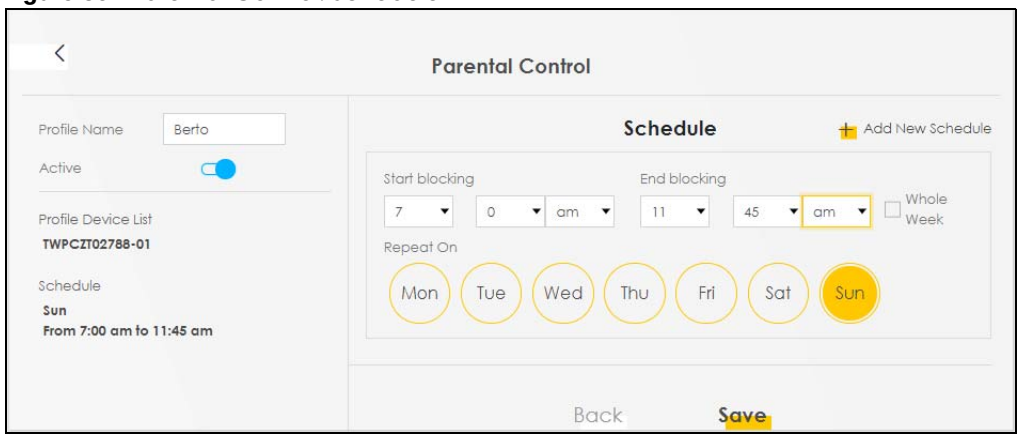
Table 26 Parental Control: Add More Profile

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

## 7.3.2 Define a Schedule

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

**Figure 56** Parental Control: Schedule




Each field is described in the following table.

Table 27 Parental Control: Schedule

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

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

**Figure 57** Parental Control: Edit_Delete

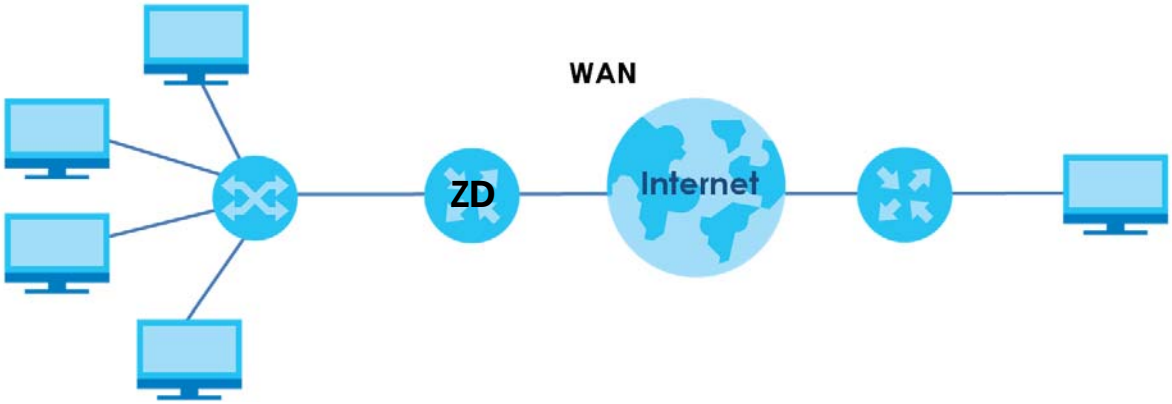
# CHAPTER 8
# Broadband

## 8.1 Overview

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

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

**Figure 58** LAN and WAN




### 8.1.1 What You Can Do in this Chapter

- Use **Broadband** screens to view, remove or add a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access (Section 8.2 on page 108).

Table 28 WAN Setup Overview

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

## 8.1.2 What You Need to Know

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

### WAN IP Address

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

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

### IPv6 Introduction

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

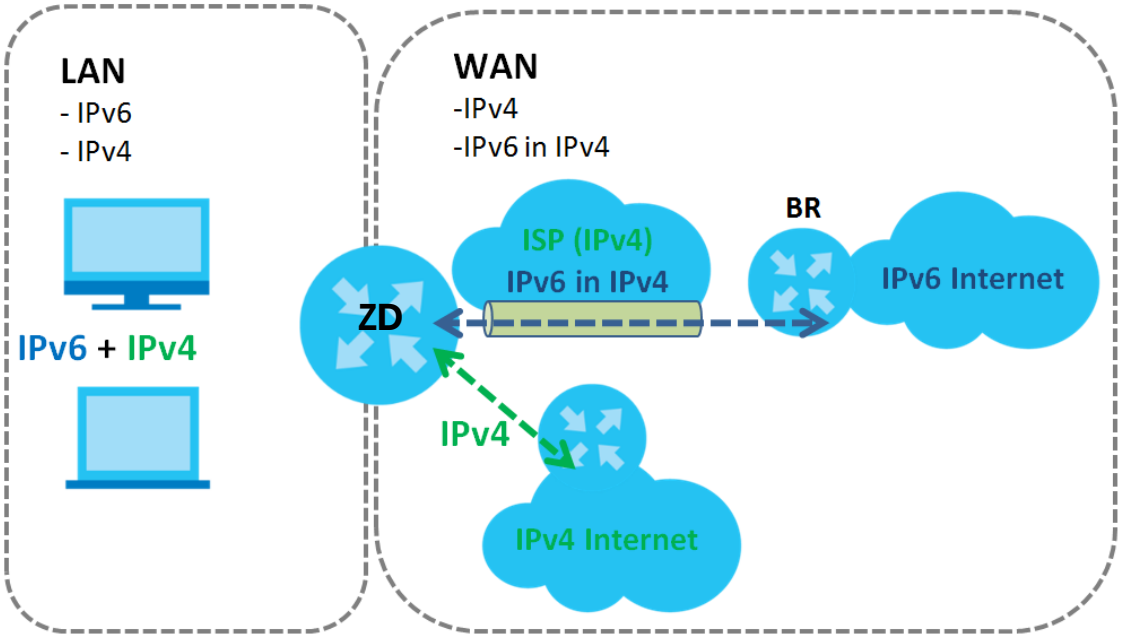
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example, 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 **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

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

**Figure 59** IPv6 Rapid Deployment

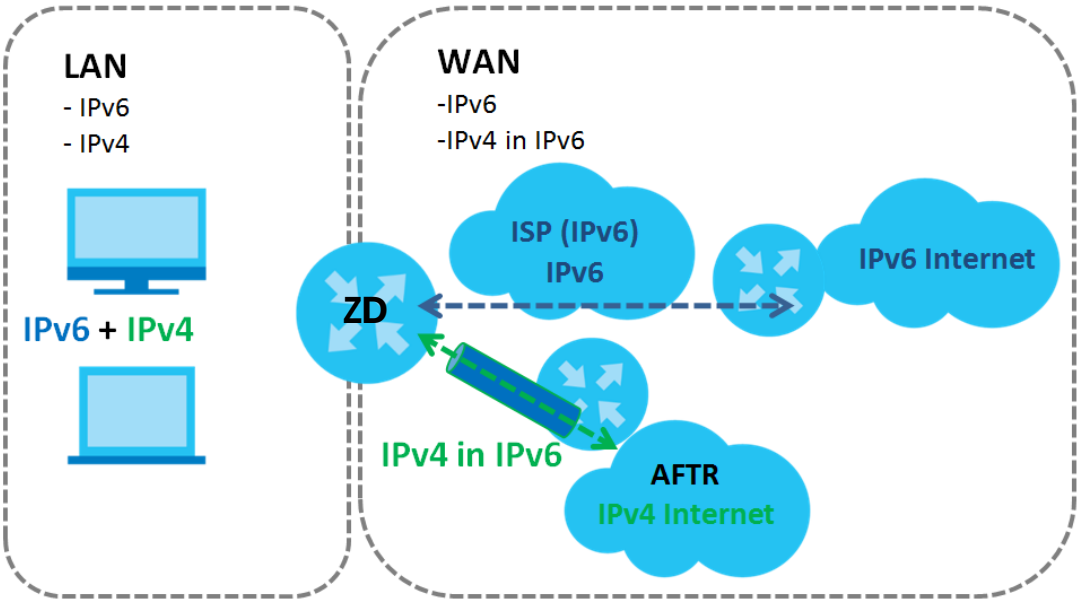



## Dual Stack Lite

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

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

**Figure 60** Dual Stack Lite




### 8.1.3 Before You Begin

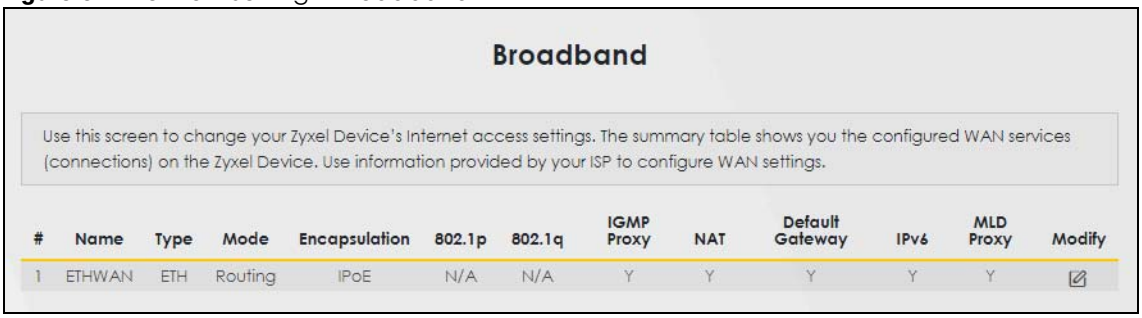
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

## 8.2 Broadband Settings

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

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

**Figure 61** Network Setting > Broadband



The following table describes the labels in this screen.

Table 29 Network Setting > Broadband

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

## 8.2.1 Edit Internet Connection

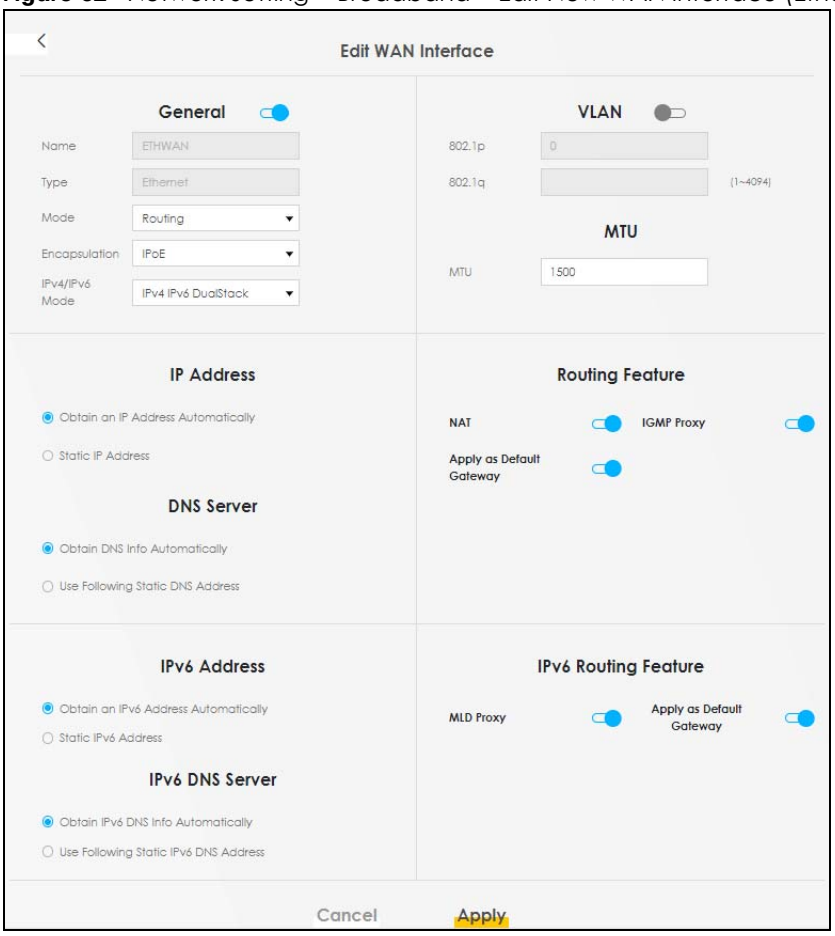
Click the Edit icon in the **Networking** > **Broadband** screen to open the following screen. Use this screen to configure a WAN connection. The screen varies depending on the mode, encapsulation, and IPv6 or IPv4 mode you select.

### Routing Mode

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

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

**Figure 62** Network Setting > Broadband > Edit New WAN Interface (Ethernet)




The following table describes the labels in this screen.

Table 30 Network Setting > Broadband > 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.<br><br>This field is read-only if you are editing the WAN interface. |
| Type | This field shows the types of available connections.<br><br>This field is read-only if you are editing the WAN interface. |
| Mode | Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account. |
| Encapsulation | Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field.<br><br>When you select **Ethernet**, the choices are **PPPoE** and **IPoE.** |

Table 30 Network Setting > Broadband > Edit New WAN Interface (Routing Mode) (continued)

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

Table 30 Network Setting > Broadband > Edit New WAN Interface (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Fullcone NAT Enable | Click this switch to enable or disable full cone NAT on this connection. When the switch goes to the right , the function is enabled. Otherwise, it is not.<br><br>This field is available only when you activate **NAT**.<br><br>In full cone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port. |
| 6RD | The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6/IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 107 for more information.<br><br>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. |
| Automatically configured by DHCPC | The **Automatically configured by DHCPC** option is configurable only when you set the method of encapsulation to **IPoE**. |
| Manually Configured | Select **Manually Configured** if you have the IPv4 address of the relay server. Otherwise, select **Automatically configured by DHCPC** to have the Zyxel Device detect it automatically through DHCP. |
| Service Provider IPv6 Prefix | Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet. |
| IPv4 Mask Length | Enter the subnet mask number (1 – 32) for the IPv4 network. |
| IPv6 Address (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field.) | |
| Obtain an IPv6 Address Automatically | Select **Obtain an IPv6 Address Automatically** if you want to have the Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address. |
| Static IPv6 Address | Select **Static IPv6 Address** if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear. |
| IPv6 Address | Enter an IPv6 IP address that your ISP gave to you for this WAN interface. |
| Prefix Length | Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address. |
| IPv6 Default Gateway | Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interfaces. The gateway helps forward packets to their destinations. |
| IPv6 DNS Server (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. Configure the IPv6 DNS server in the following section.) | |
| Obtain IPv6 DNS Info Automatically | Select **Obtain IPv6 DNS Info Automatically** to have the Zyxel Device get the IPv6 DNS server addresses from the ISP automatically. |
| Use Following Static IPv6 DNS Address | Select **Use Following Static IPv6 DNS Address** to have the Zyxel Device use the IPv6 DNS server addresses you configure manually. |
| Primary DNS Server | Enter the first IPv6 DNS server address assigned by the ISP. |
| Secondary DNS Server | Enter the second IPv6 DNS server address assigned by the ISP. |
| IPv6 Routing Feature (This is available only when you select **IPv4 IPv6 DualStack** or **IPv6 Only** in the **IPv4/IPv6 Mode** field. You can enable IPv6 routing features in the following section.) | |
| MLD Proxy Enable | Select this check box to have the Zyxel Device act as an MLD proxy on this connection. This allows the Zyxel Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly. |

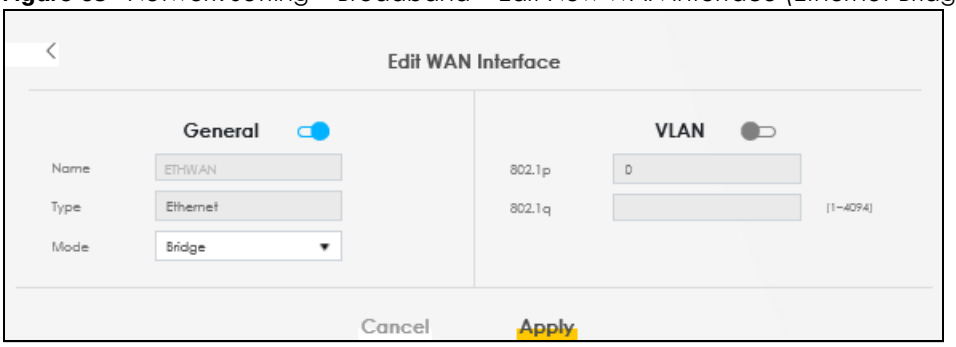
Table 30 Network Setting > Broadband > Edit New WAN Interface (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply as Default Gateway | Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway. |
| DS-Lite | This is available only when you select **IPv6 Only** in the **IPv4/IPv6 Mode** field. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 107 for more information.<br>Click this switch to let local computers use IPv4 through an ISP's IPv6 network. When the switch goes to the right , the function is enabled. Otherwise, it is not. |
| DS-Lite Relay Server IP | Specify the transition router's IPv6 address. |
| Cancel | Click **Cancel** to restore your previously saved settings. |
| Apply | Click **Apply** to save your changes. |

## Bridge Mode

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

**Figure 63** Network Setting > Broadband > Edit New WAN Interface (Ethernet-Bridge Mode)




The following table describes the fields in this screen.

Table 31 Network Setting > Broadband > Edit New WAN Interface (VDSL over PTM or Ethernet-Bridge Mode)

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

Table 31 Network Setting > Broadband > Edit New WAN Interface (VDSL over PTM or Ethernet-Bridge Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| 802.1p | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.<br>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| 802.1q | Type the VLAN ID number (from 0 to 4094) for traffic through this connection. |
| Cancel | Click **Cancel** to exit this screen without saving. |
| Apply | Click **Apply** to save your changes. |

# 8.3 Technical Reference

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

## Encapsulation

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

## IP Address Assignment

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

## Introduction to VLANs

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

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

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

## Introduction to IEEE 802.1Q Tagged VLAN

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

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

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

## Multicast

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

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

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

## DNS Server Address Assignment

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

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

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

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

## IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

## IPv6 Prefix and Prefix Length

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

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

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

# CHAPTER 9
# Wireless

## 9.1 Overview

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

### 9.1.1 What You Can Do in this Chapter

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

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the WiFi security mode (Section 9.2 on page 118)
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device (Section 9.3 on page 122).
- Use the **MAC Authentication** screen to allow or deny WiFi clients based on their MAC addresses from connecting to the Zyxel Device (Section 9.4 on page 126).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 9.5 on page 127).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 9.6 on page 128).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 9.7 on page 129).
- Use the **Channel Status** screen to scan the number of accessing points and view the results (Section 9.8 on page 132).
- Use the **Mesh** screen to enable or disable Mesh on your Zyxel Device (Section 9.9 on page 132).
- Use the **Mesh Topology** screen to view the topology information (Section 9.10 on page 133).

### 9.1.2 What You Need to Know

#### Wireless Basics

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

### WiFi6 / IEEE 802.11ax

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

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

Table 32 WiFI Standards Comparison

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

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

### Finding Out More

See Section 9.11 on page 134 for advanced technical information on WiFi networks.

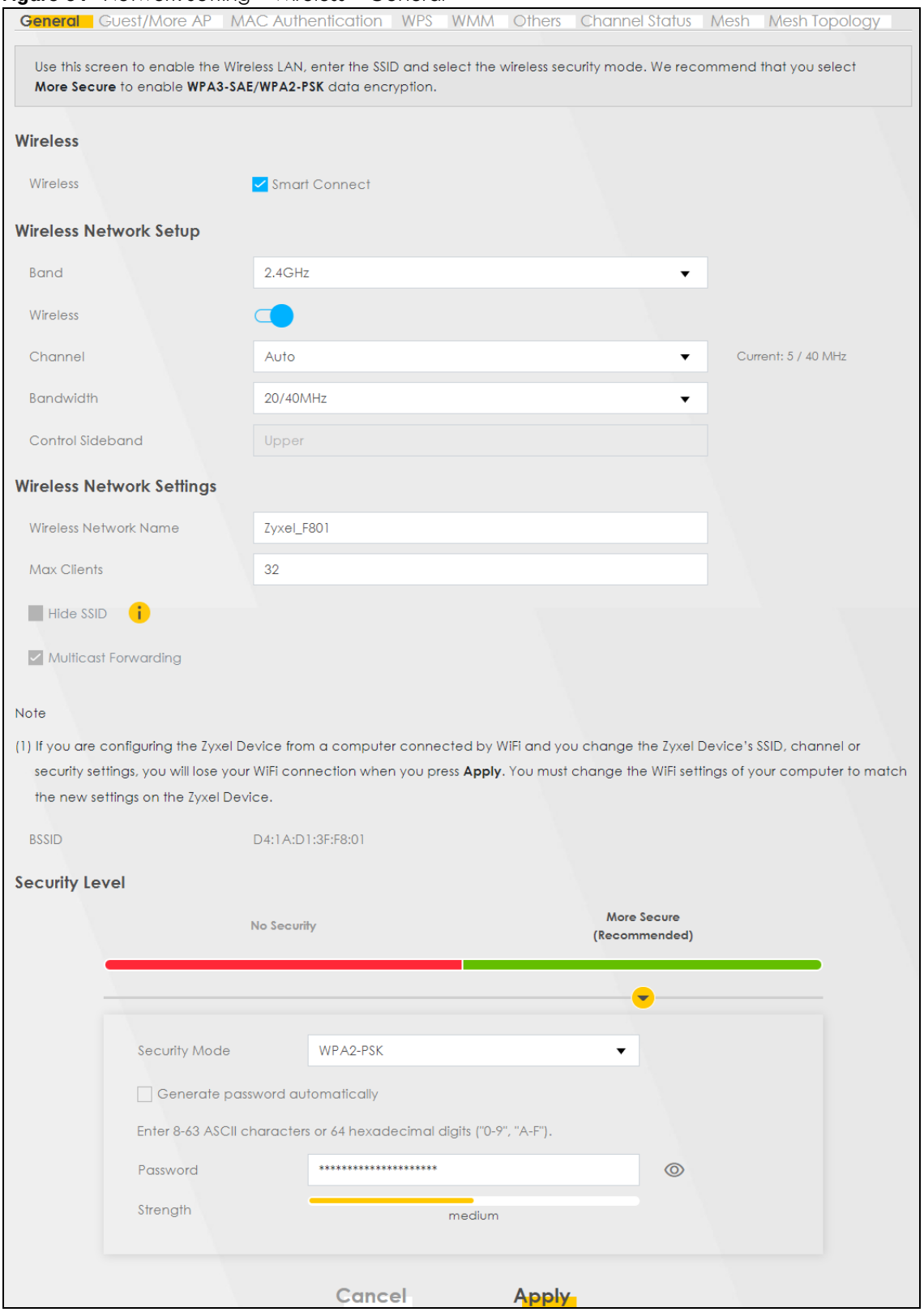
## 9.2 Wireless General Settings

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

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

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

**Figure 64** Network Setting > Wireless > General



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

Table 33 Network Setting > Wireless > General

| LABEL | DESCRIPTION |
|---|---|
| Wireless | |
| Smart Connect | Select **Smart Connect** and the 2.4 GHz and 5 GHz wireless networks will use the same SSID and wireless security settings. |
| Wireless/WiFi Network Setup | |
| Band | This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax WiFi clients while **5GHz** is used by IEEE 802.11a/n/ac/ax WiFi clients. |
| Wireless/WiFi | Click this switch to enable or disable WiFi in this field. When the switch turns blue , the function is enabled. Otherwise, it is not. |
| Channel | Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.<br><br>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**, **20/40MHz**, **20/40/80MHz** or **20/40/80/160MHz**.<br><br>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.<br><br>40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.<br><br>An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher.<br><br>Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the WiFi clients do not support channel bonding.<br><br>Because not all devices support 40 MHz and/or 160 MHz channels, select **20/40MHz** or **20/40/80/160MHz** to allow the Zyxel Device to adjust the channel bandwidth automatically. |
| Control Sideband | This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz** or **20/40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands. |
| Wireless/WiFi Network Settings | |
| Wireless/WiFi Network Name | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.<br><br>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.<br><br>This check box is grayed out if the WPS function is enabled in the **Network Setting** > **Wireless** > **WPS** screen. |
| Multicast Forwarding | Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic. |
| BSSID | This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled. |
| Security Level | |

Table 33 Network Setting > Wireless > General (continued)

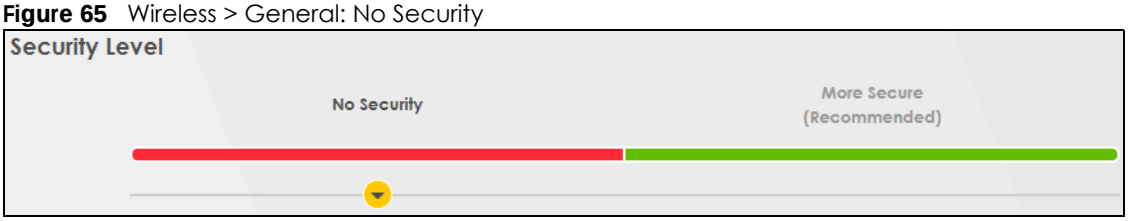
| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Select **More Secure (Recommended)** to add security on this wireless network. The WiFi clients which want to associate to this network must have same wireless security settings as the Zyxel Device. When you select to use a security, additional options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

## 9.2.1 No Security

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

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

**Figure 65** Wireless > General: No Security




The following table describes the labels in this screen.

Table 34 Wireless > General: No Security

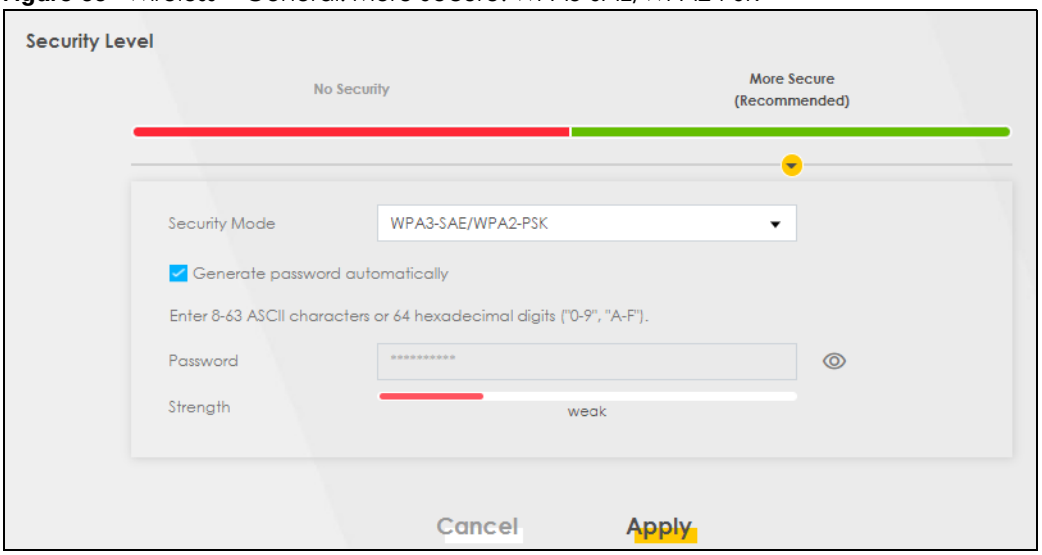
| LABEL | DESCRIPTION |
|---|---|
| Security Level | Choose **No Security** to allow all WiFi connections without data encryption or authentication. |

## 9.2.2 More Secure (Recommended)

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

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

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




The following table describes the labels in this screen.

Table 35 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

| LABEL | DESCRIPTION |
|---|---|
| Security Level | Select **More Secure** to enable data encryption. |
| Security Mode | Select a security mode from the drop-down list box. |
| Generate password automatically | Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option. |
| Password | Select **Generate password automatically** or enter a **Password**.<br><br>The password has two uses.<br><br>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.<br><br>2. WPS. When using WPS, the Zyxel Device sends this password to the client.<br><br>Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden. |

# 9.3 Guest/More AP Screen

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

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

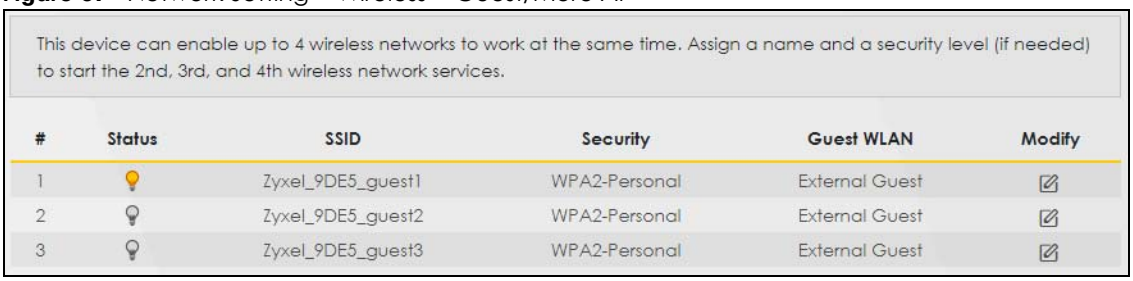
The following table introduces the supported wireless networks.

Table 36 Supported Wireless Networks

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

The following screen displays.

**Figure 67** Network Setting > Wireless > Guest/More AP




The following table describes the labels in this screen.

Table 37 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.<br>This field displays the name of the wireless profile on the network. When a WiFi client scans for an AP to associate with, this is the name that is broadcast and seen in the WiFi client utility. |
| Security | This field indicates the security mode of the SSID profile. |
| Guest WLAN | This displays if the guest WLAN function has been enabled for this WLAN.<br>If **Home Guest** displays, clients can connect to each other directly.<br>If **External Guest** displays, clients are blocked from connecting to each other directly.<br>**N/A** displays if guest WLAN is disabled. |
| Modify | Click the **Edit** icon of an SSID profile to configure the SSID profile. |

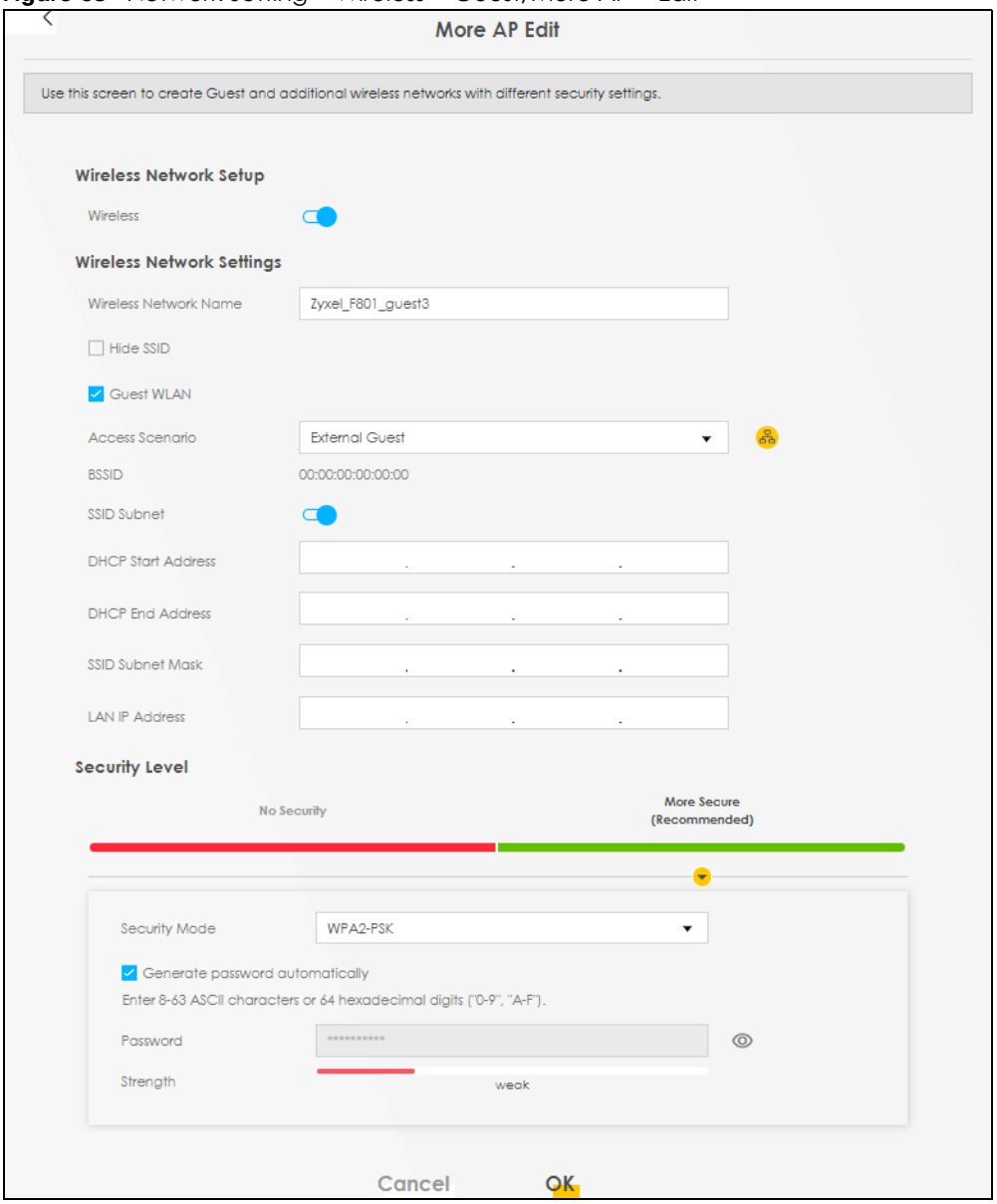
## 9.3.1 The Edit Guest/More AP Screen

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

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

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

**Figure 68** Network Setting > Wireless > Guest/More AP > Edit




The following table describes the fields in this screen.

Table 38 Network Setting > Wireless > Guest/More AP > Edit

| LABEL | DESCRIPTION |
|---|---|
| Wireless Network Setup | |
| Wireless | Click this switch to enable or disable the wireless LAN in this field. When the switch turns blue , the function is enabled; otherwise, it is not. |
| Wireless Network 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.<br><br>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |

Table 38 Network Setting > Wireless > Guest/More AP > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Guest WLAN | Select this to create Guest WLANs for home and external clients. Select the WLAN type in the **Access Scenario** field. |
| Access Scenario | If you select **Home Guest**, clients can connect to each other directly.<br>If you select **External Guest**, clients are blocked from connecting to each other directly. |
| BSSID | This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled. |
| SSID Subnet | Click on this switch to **Enable** this function if you want the wireless network interface to assign DHCP IP addresses to the associated WiFi clients.<br>This option cannot be used if the WPS function is enabled in the **Network** > **Wireless** > **WPS** screen or if the **Smart Connect** check box is selected in **Network** > **Wireless > General**. |
| DHCP Start Address | Specify the first of the contiguous addresses in the DHCP IP address pool.<br>The Zyxel Device assigns IP addresses from this DHCP pool to WiFi clients connecting to the SSID. |
| DHCP End Address | Specify the last of the contiguous addresses in the DHCP IP address pool. |
| SSID Subnet Mask | Specify the subnet mask of the Zyxel Device for the SSID subnet. |
| LAN IP Address | Specify the IP address of the Zyxel Device for the SSID subnet. |
| Security Level | |
| Security Mode | Select **More Secure (Recommended)** to add security on this wireless network. The WiFi 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.<br>Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication.<br>See Section 9.2.1 on page 121 for more details about this field. |
| Generate password automatically | Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option. |
| Password | WPA2-PSK uses a simple common password, instead of user-specific credentials.<br>If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.<br>Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it's hidden. |
| | Click this to show more fields in this section. Click again to hide them. |
| Encryption | Select the encryption type (**AES** or **TKIP+AES**) for data encryption.<br>Select **AES** if your WiFi clients can all use AES.<br>Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. |
| Timer | The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients. |
| Cancel | Click **Cancel** to exit this screen without saving. |
| OK | Click **OK** to save your changes. |

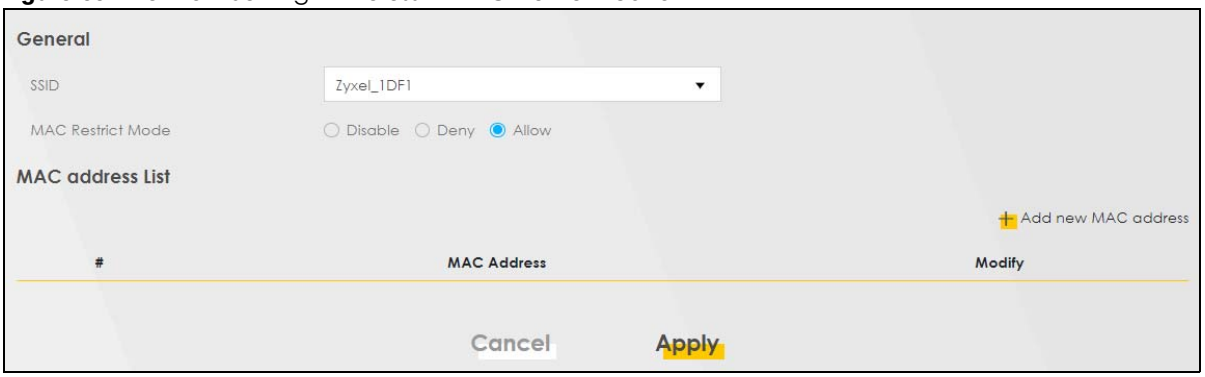
# 9.4 MAC Authentication

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

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

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

**Figure 69** Network Setting> Wireless > MAC Authentication

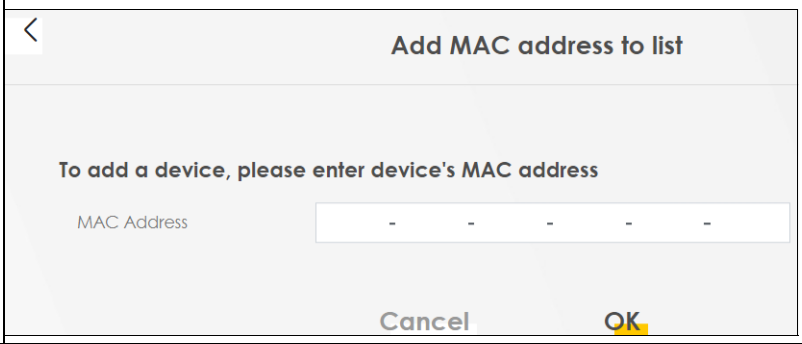



The following table describes the labels in this screen.

Table 39 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.<br>Select **Disable** to turn off MAC filtering.<br>Select **Deny** to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device.<br>Select **Allow** to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device. |
| MAC address List | |

Table 39 Network Setting > Wireless > MAC Authentication (continued)

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

# 9.5 WPS

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

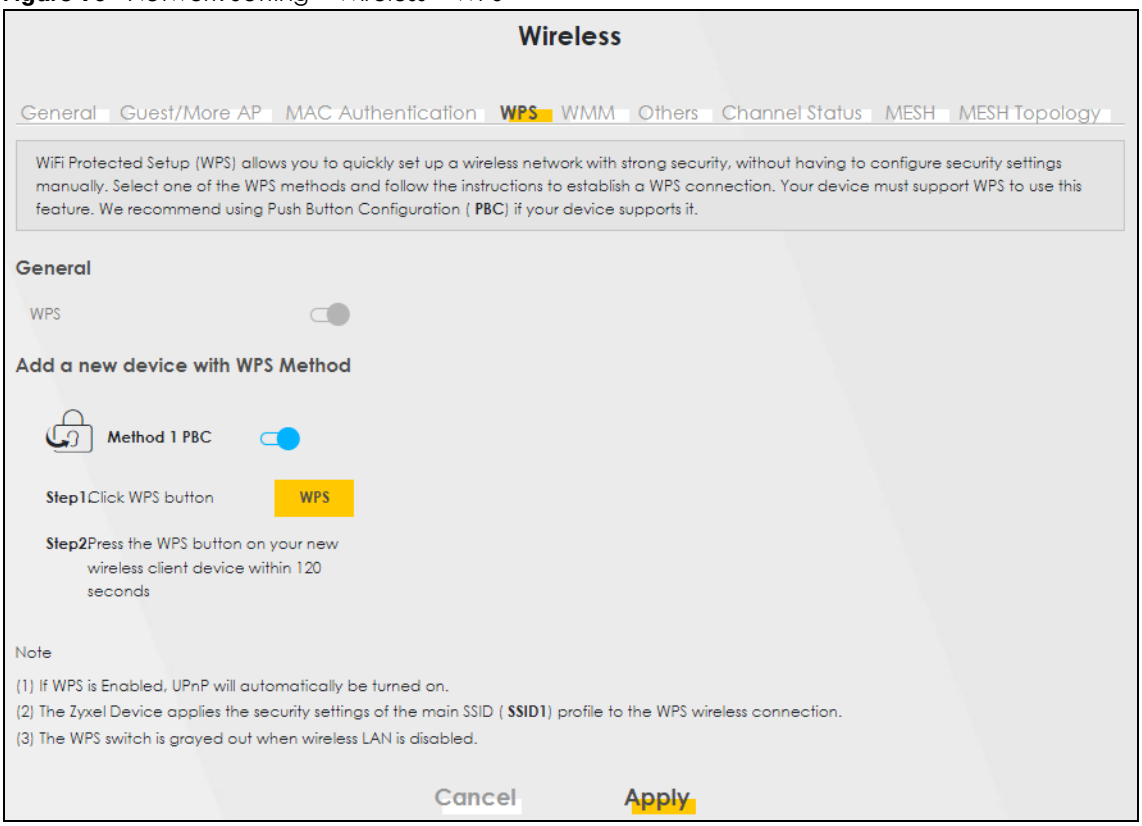
WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection.Your devices must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your device supports it. See Section 9.11.8.1 on page 139 for more information about WPS.

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection (see Section 9.2.2 on page 121).

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

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

**Figure 70** Network Setting > Wireless > WPS




The following table describes the labels in this screen.

Table 40 Network Setting > Wireless > WPS

| LABEL | DESCRIPTION |
|---|---|
| General | |
| WPS | Click to enable ( ) and have the Zyxel Device activate WPS. Otherwise, it is disabled. |
| Add a new device with WPS Method | |
| Method 1 PBC | Use this section to set up a WPS WiFi network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click **Apply** to activate WPS method 1 on the Zyxel Device. |
| WPS | Click this button to add another WPS-enabled WiFi device (within WiFi range of the Zyxel Device) to your WiFi network. This button may either be a physical button on the outside of a device, or a menu button similar to the **WPS button** on this screen.<br><br>Note: You must press the other WiFi device's WPS button within 2 minutes of pressing this button. |
| Cancel | Click **Cancel** to restore your previously saved settings. |
| Apply | Click **Apply** to save your changes. |

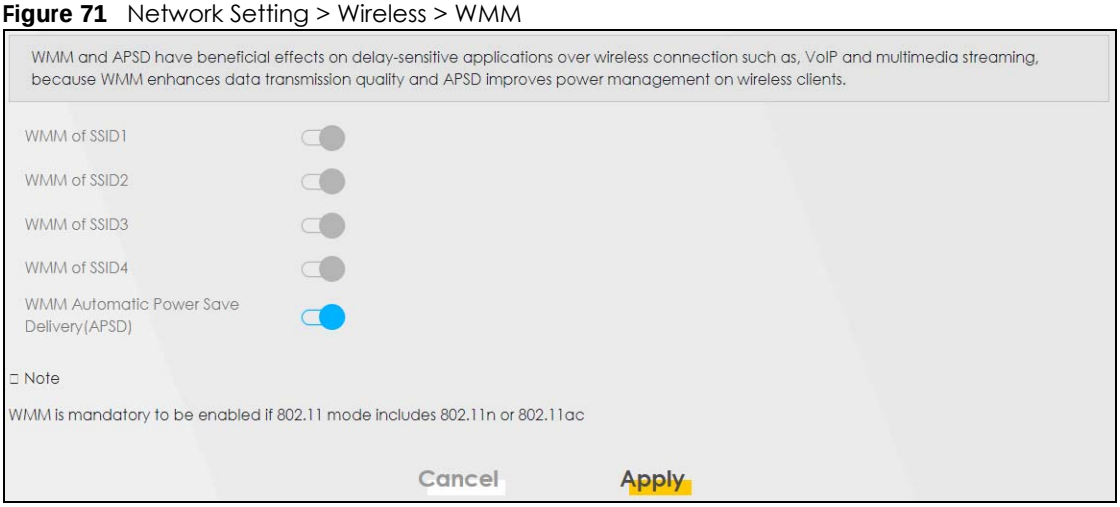
# 9.6 WMM

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

power management of WiFi 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 71** Network Setting > Wireless > WMM




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

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

The following table describes the labels in this screen.

Table 41 Network Setting > Wireless > WMM

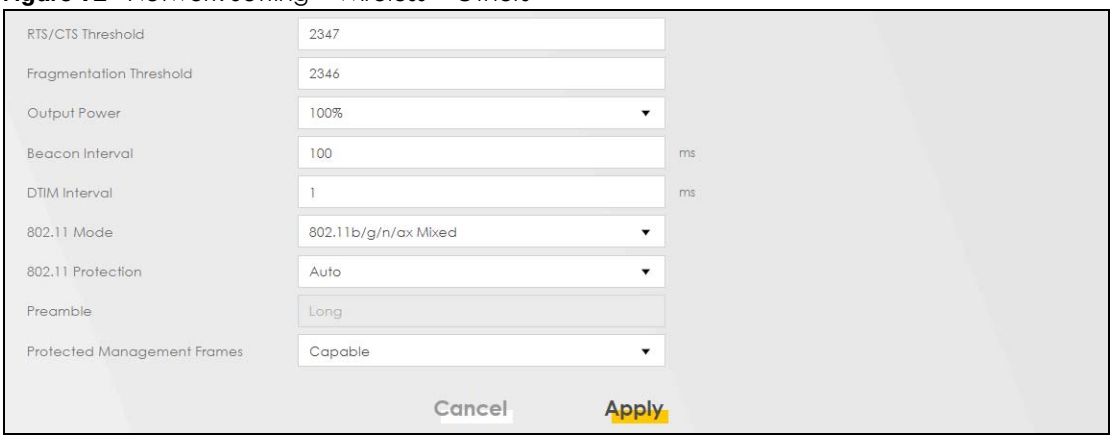
| LABEL | DESCRIPTION |
|---|---|
| WMM of SSID | Select **On** to have the Zyxel Device automatically give the WiFi network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to video, which makes them run more smoothly.<br><br>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.<br><br>Note: This works only if the WiFi device to which the Zyxel Device is connected also supports this feature. |
| Cancel | Click **Cancel** to restore your previously saved settings. |
| Apply | Click **Apply** to save your changes. |

# 9.7 Others Screen

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

See Section 9.11.2 on page 135 for detailed definitions of the terms listed here.

**Figure 72** Network Setting > Wireless > Others




The following table describes the labels in this screen.

Table 42 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.<br><br>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.<br><br>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 42 Network Setting > Wireless > Others (continued)

| LABEL | DESCRIPTION |
|---|---|
| 802.11 Mode | For 2.4 GHz frequency WiFi devices:<br>• Select **802.11b Only** to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device.<br>• Select **802.11g Only** to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device.<br>• Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device.<br>• 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.<br>• 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.<br>• 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.<br>For 5 GHz frequency WiFi devices:<br>• Select **802.11a Only** to allow only IEEE 802.11a compliant WiFi devices to associate with the Zyxel Device.<br>• Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device.<br>• Select **802.11ac Only** to allow only IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device.<br>• 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.<br>• 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.<br>• 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.<br>• 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).<br>Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.<br>Select **Off** to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network.<br>This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**. |
| Preamble | Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 9.11.7 on page 138 for more information.<br>This field is configurable only when you set 802.11 Mode to **802.11b**. |
| Protected Management Frames | WiFi with Protected Management Frames (PMF) provides protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging. Select **Capable** if the WiFi client supports PMF, then the management frames will be encrypted. Select **Required** to force the WiFi client to support PMF; otherwise the authentication cannot be performed by the Zyxel Device. Otherwise, select **Disabled**. |
| Cancel | Click **Cancel** to restore your previously saved settings. |
| Apply | Click **Apply** to save your changes. |

# 9.8 Channel Status

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

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

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

**Figure 73** Network Setting > Wireless > Channel Status

# 9.9 Mesh

Use this screen to enable or disable **Mesh** on the Zyxel Device. Click **Network >Wireless> Mesh** to open the following screen.

**Figure 74** Network > Wireless > Mesh

The following table describes the labels in this screen.

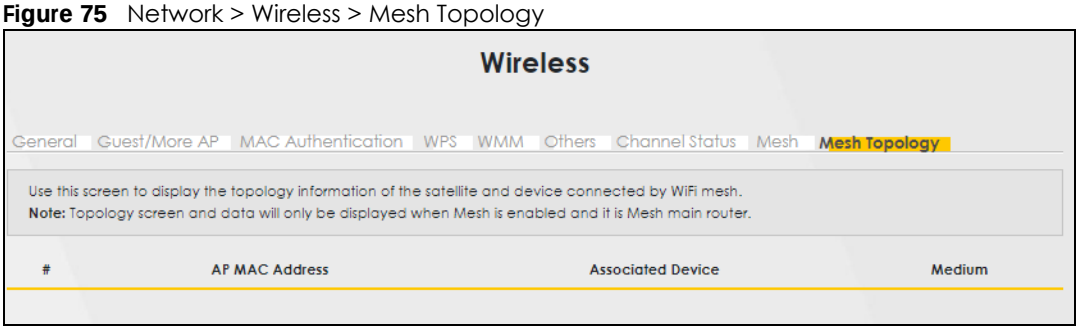
Table 43 Network Setting > Wireless > Mesh

| LABEL | DESCRIPTION |
|---|---|
| Mesh | Slide the switch to the right ( )to enable **Mesh**. |
| OK | Click **OK** to save the changes back to the Zyxel Device. |
| Cancel | Click **Cancel** to close the window with changes unsaved. |

# 9.10 Mesh Topology

Use this screen to configure the MAC address of the extender connected to the Zyxel Device. Click **Network > Wireless> Mesh Topology** to open the following screen.

**Figure 75** Network > Wireless > Mesh Topology




The following table describes the labels in this screen.

Table 44 Network Setting > Wireless > Mesh Topology

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the entry. |
| AP MAC Address | This show the MAC address of the satellites connected to the router. The router functions as a network controller to coordinate and optimize WiFi activity In a Mesh network. The controller collects Channel Availability Check responses and scan reports from the satellites. Then, the controller selects the best channel and the final optimized topology based on the current situation. |
| Associated Device | This shows the MAC address of the client devices connected to the Mesh network. |
| Medium | This shows the WiFi channel through which the WiFi networks can send and receive data. |

# 9.11 Technical Reference

This section discusses wireless LANs in depth.

## 9.11.1 WiFi Network Overview

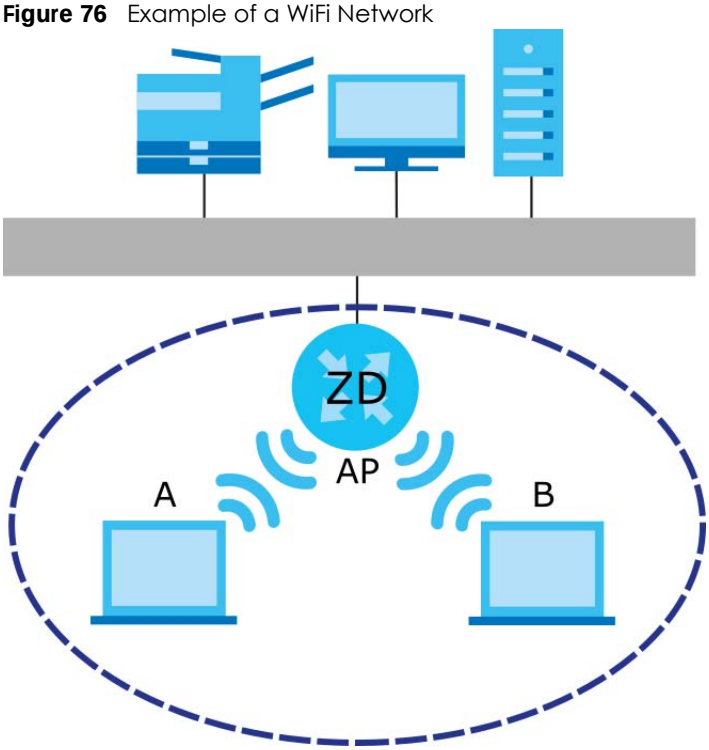
WiFi networks consist of WiFi clients, access points and bridges.

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

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

The following figure provides an example of a WiFi network.

**Figure 76** Example of a WiFi Network




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

Every WiFi network must follow these basic guidelines.

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

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

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

  Like radio stations or television channels, each WiFi network uses a specific channel, or frequency, to send and receive information.
- Every device in the same WiFi network must use security compatible with the AP.

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

## 9.11.2 Additional Wireless Terms

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

Table 45 Additional WiFi Terms

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

## 9.11.3 WiFi Security Overview

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

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

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

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

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

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

#### 9.11.3.1 SSID

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

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

#### 9.11.3.2 MAC Address Filter

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

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

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

#### 9.11.3.3 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 9.11.3.3 on page 136 for information about this.)

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

Table 46 Types of Encryption for Each Type of Authentication

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

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

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

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

## 9.11.4 Signal Problems

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

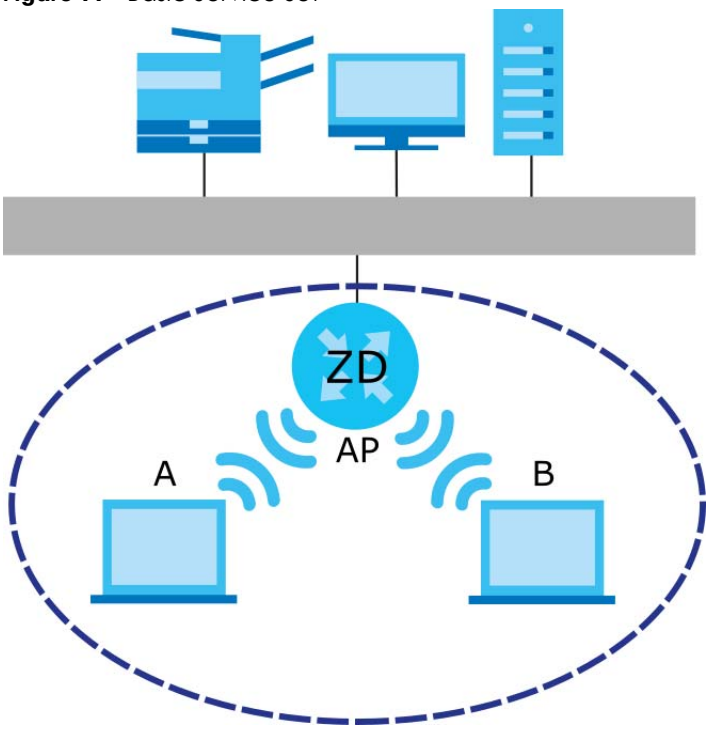
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters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

## 9.11.5 BSS

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

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

**Figure 77** Basic Service Set




## 9.11.6 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.

### 9.11.6.1 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.

## 9.11.7 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 WiFi devices on the network support, and to provide more reliable communications in busy WiFi networks.

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

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

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

## 9.11.8 WiFi Protected Setup (WPS)

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

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

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

### 9.11.8.1 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 9.5 on page 127).
3. Press the button on one of the devices (it doesn't matter which). For the Zyxel Device you must press the **WiFi** button for more than 5 seconds.
4. Within 2 minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

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

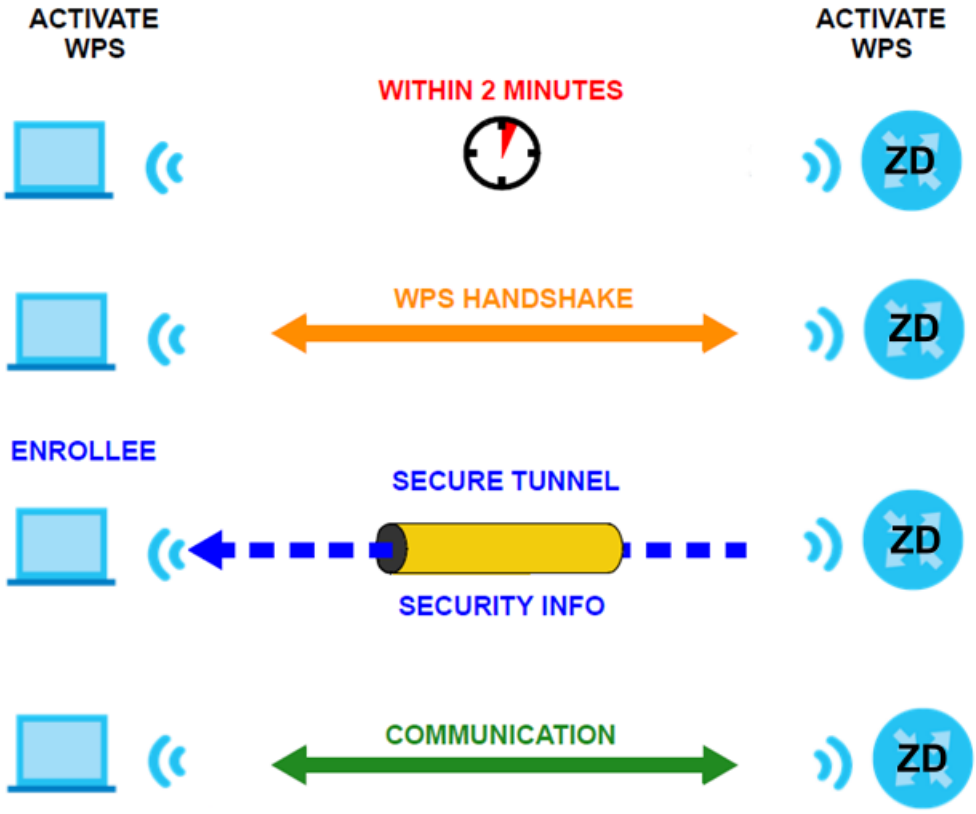
### 9.11.8.2 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or

WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA2-PSK randomly.

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

**Figure 78** How WPS Works




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

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

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

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

### 9.11.8.3 Example WPS Network Setup

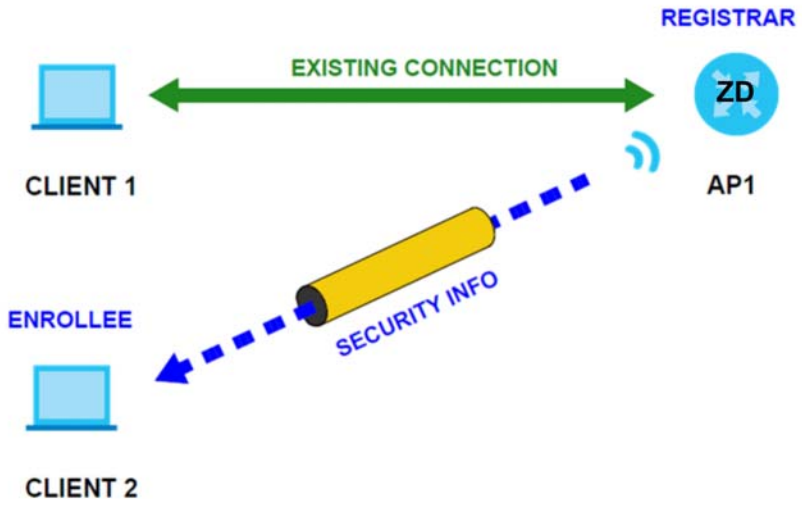
This section shows how security settings are distributed in a sample WPS setup.

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

**Figure 79** WPS: Example Network Step 1

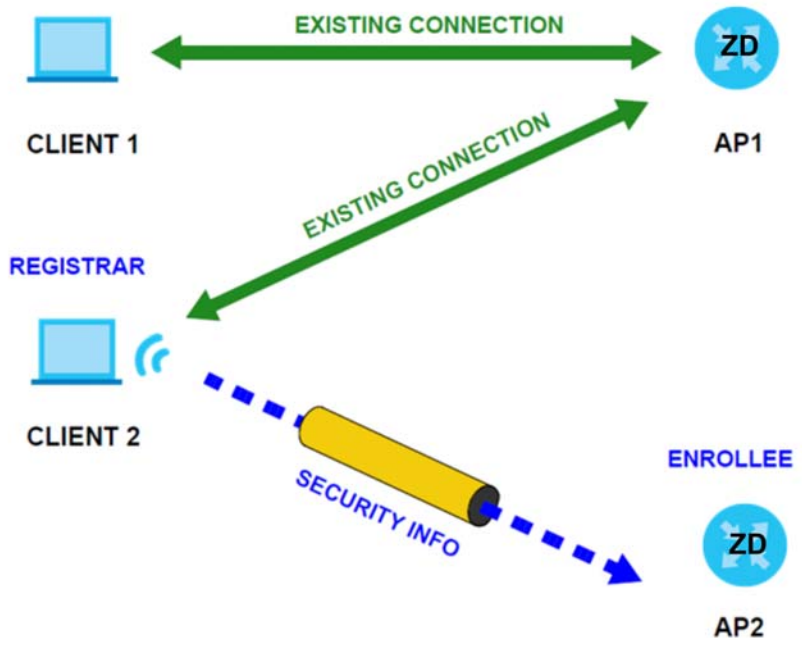
In step **2**, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

**Figure 80** 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 81** WPS: Example Network Step 3




### 9.11.8.4 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

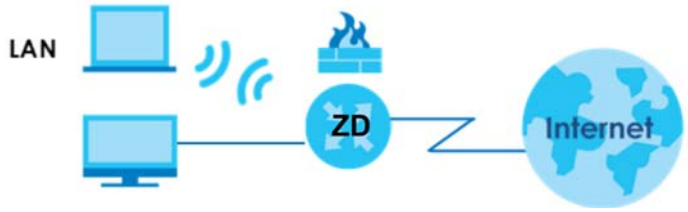
# CHAPTER 10
# Home Networking

## 10.1 Overview

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

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

**Figure 82** Home Networking Example




### 10.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 10.2 on page 145).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 10.3 on page 149).
- Use the **UPnP** screen to enable UPnP (Section 10.4 on page 151).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 10.5 on page 152).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. (Section 10.6 on page 154).
- Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. (Section 10.7 on page 155).

### 10.1.2 What You Need To Know

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

#### 10.1.2.1 About LAN

##### IP Address

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

### Subnet Mask

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

### DHCP

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

### DNS

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

### RADVD (Router Advertisement Daemon)

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

## 10.1.2.2 About UPnP

### How do I know if I am using UPnP?

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

### NAT Traversal

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

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

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

### Cautions with UPnP

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

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

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

### UPnP and Zyxel

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

See Section 10.9 on page 158 for examples on installing and using UPnP.

## 10.1.3 Before You Begin

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

# 10.2 LAN Setup

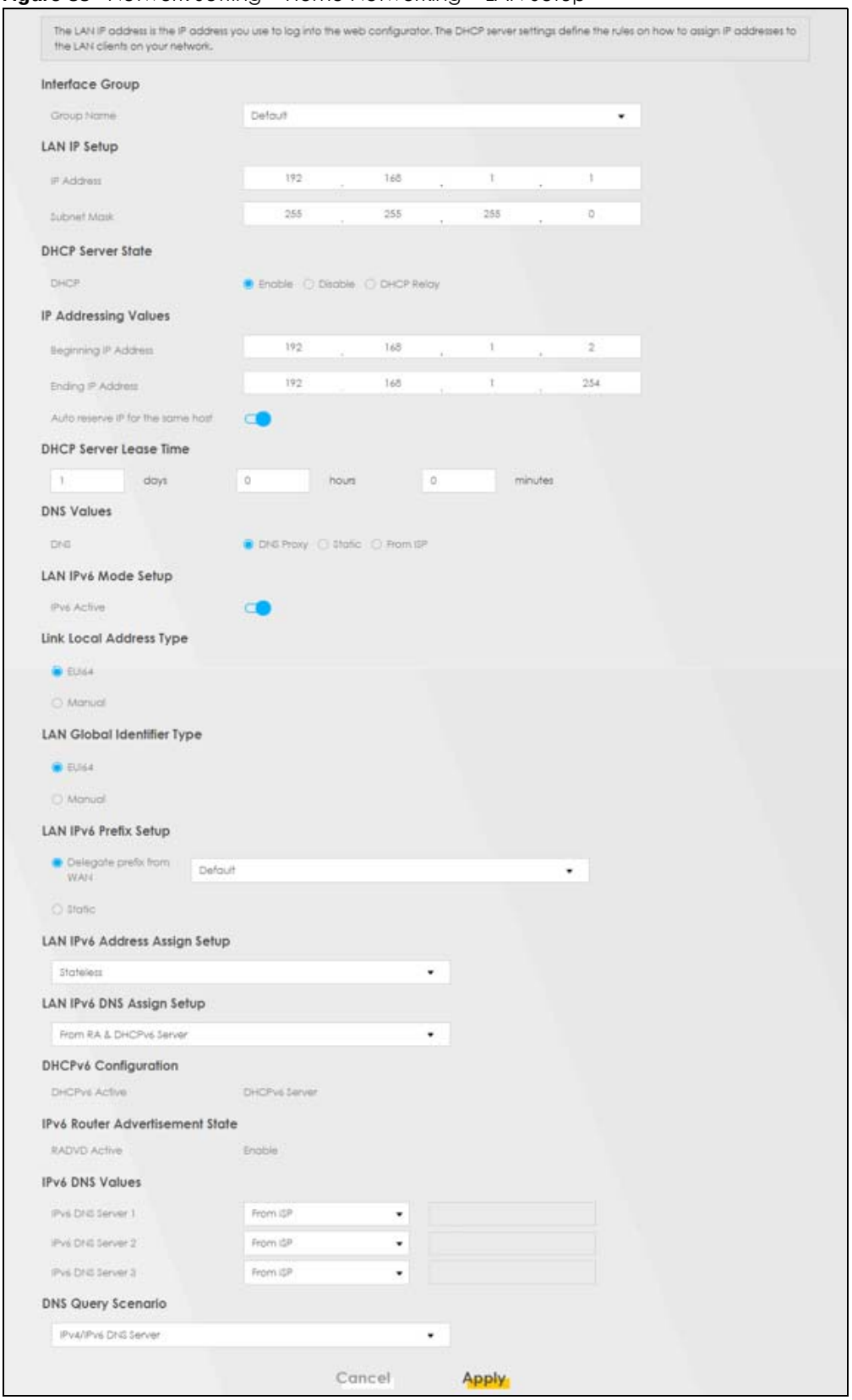
A LAN IP address is the IP address of a networking device in the LAN. You can use the Zyxel Device's LAN IP address to access its Web Configurator from the LAN. The DHCP server settings define the rules on assigning IP addresses to LAN clients on your network.

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

Follow these steps to configure your LAN settings.

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

**Figure 83** Network Setting > Home Networking > LAN Setup



The following table describes the fields in this screen.

Table 47 Network Setting > Home Networking > LAN Setup

| LABEL | DESCRIPTION |
|---|---|
| Interface Group | |
| Group Name | This displays the name of the group that your Zyxel Device belongs to. |
| LAN IP Setup | |
| IP Address | Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.123.1 (factory default). |
| Subnet Mask | Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so. |
| DHCP Server State | |
| DHCP | Select **Enable** to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.<br>If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN.<br>If you select **DHCP Relay**, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.<br>When DHCP is used, the following fields need to be set: |
| IP Addressing Values<br>The **IP Addressing Values** fields appear only when you select **Enable** in the **DHCP** field. | |
| Beginning IP Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Ending IP Address | This field specifies the last of the contiguous addresses in the IP address pool. |
| Auto reserve IP for the same host | Enable this if you want to reserve the IP address for the same host. |
| DHCP Server Lease Time<br>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.<br>This field is only available when you select **Enable** in the **DHCP** field. | |
| Days/Hours/Minutes | DHCP server leases an address to a new device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different device. |
| DNS Values<br>This field appears only when you select **Enable** in the **DHCP** field. | |

Table 47 Network Setting > Home Networking > LAN Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| DNS | The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client.<br><br>Select **DNS Proxy** to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay.<br><br>Select **Static** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.<br><br>Select **From ISP** if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address). |
| LAN IPv6 Mode Setup | |
| IPv6 Active | Use this to enable or disable IPv6 activation on the Zyxel Device.<br><br>When IPv6 activation is used, the following fields need to be set. |
| Link Local Address Type | A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows. Select **EUI64** to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select **Manual**.<br><br>Link-local Unicast Address Format<br>1111 1110 10 \| 0 \| Interface ID<br>10 bits \| 54 bits \| 64 bits |
| EUI64 | Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format. |
| Manual | Select this to manually enter an interface ID for the LAN interface's link-local address. |
| LAN Global Identifier Type | Select **EUI64** to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select **Manual** to manually enter an interface ID for the LAN interface's global IPv6 address. |
| EUI64 | Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. |
| Manual | Select this to manually enter an interface ID for the LAN interface's global IPv6 address. |
| LAN IPv6 Prefix Setup | Select **Delegate prefix from WAN** to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select **Static** to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address. |
| Delegate prefix from WAN | Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router. |
| Static | Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address. |
| LAN IPv6 Address Assign Setup | Select how you want to obtain an IPv6 address:<br><br>**Stateless**: The Zyxel Device uses IPv6 stateless auto-configuration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled.<br><br>**Stateful**: The Zyxel Device uses IPv6 stateful auto-configuration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients. |

Table 47 Network Setting > Home Networking > LAN Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| LAN IPv6 DNS Assign Setup | Select how the Zyxel Device provide DNS server and domain name information to the clients:<br>**From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.<br>**From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6.<br>**From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements. |
| DHCPv6 Configuration | |
| DHCPv6 Active | This shows the status of the DHCPv6. **DHCP Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients. |
| IPv6 Router Advertisement State | |
| RADVD Active | This shows whether RADVD is enabled or not. |
| IPv6 DNS Values | |
| IPv6 DNS Server 1 – 3 | Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.<br>**User Defined** – Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients.<br>**From ISP** – Select this if your ISP dynamically assigns IPv6 DNS server information.<br>**Proxy** – Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.<br>Otherwise, select **None** if you do not want to configure IPv6 DNS servers. |
| DNS Query Scenario | Select how the Zyxel Device handles clients' DNS information requests.<br>**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.<br>**IPv6 DNS Server Only**: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives.<br>**IPv4 DNS Server Only**: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives.<br>**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.<br>**IPv4 DNS Server First**: The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 10.3 Static DHCP

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

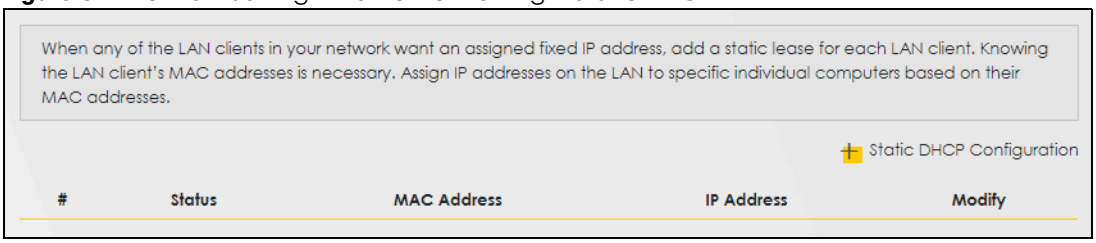
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

## 10.3.1 Before You Begin

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

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

**Figure 84** Network Setting > Home Networking > Static DHCP



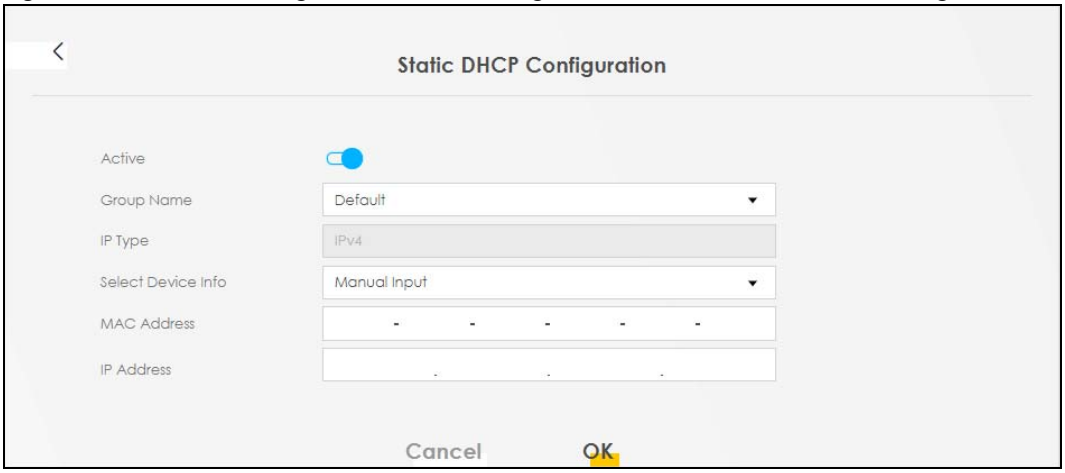

The following table describes the labels in this screen.

Table 48 Network Setting > Home Networking > Static DHCP

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

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

**Figure 85** Network Setting > Home Networking > Static DHCP: Static DHCP Configuration




The following table describes the labels in this screen.

Table 49 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

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

# 10.4 UPnP

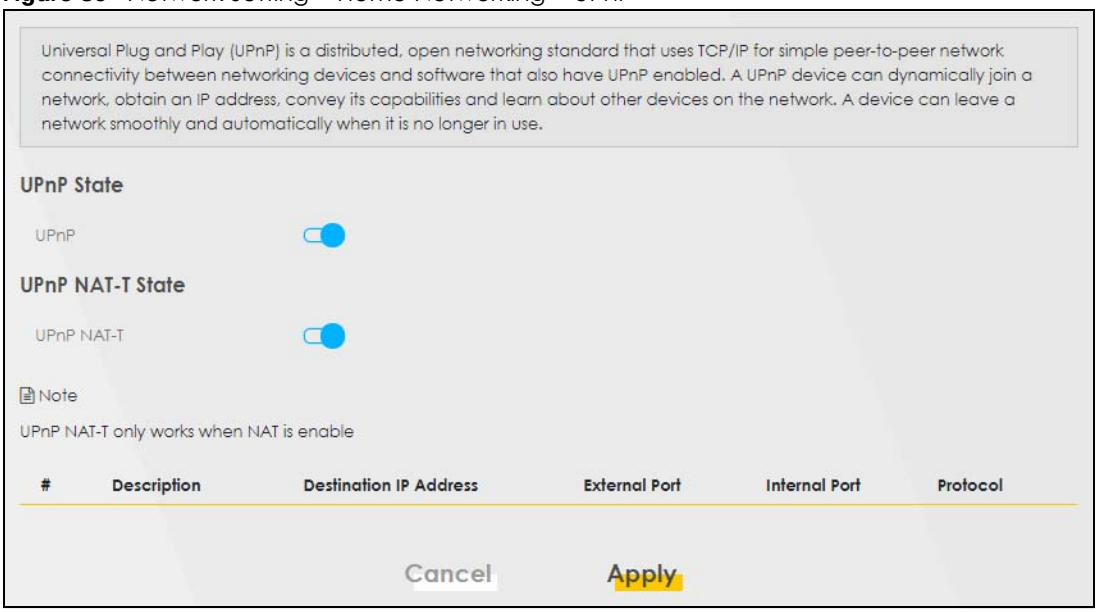
Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn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

See Section 10.9 on page 158 for more information on UPnP.

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

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

**Figure 86** Network Setting > Home Networking > UPnP




The following table describes the labels in this screen.

Table 50 Network Settings > Home Networking > UPnP

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

# 10.5 LAN Additional Subnet

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

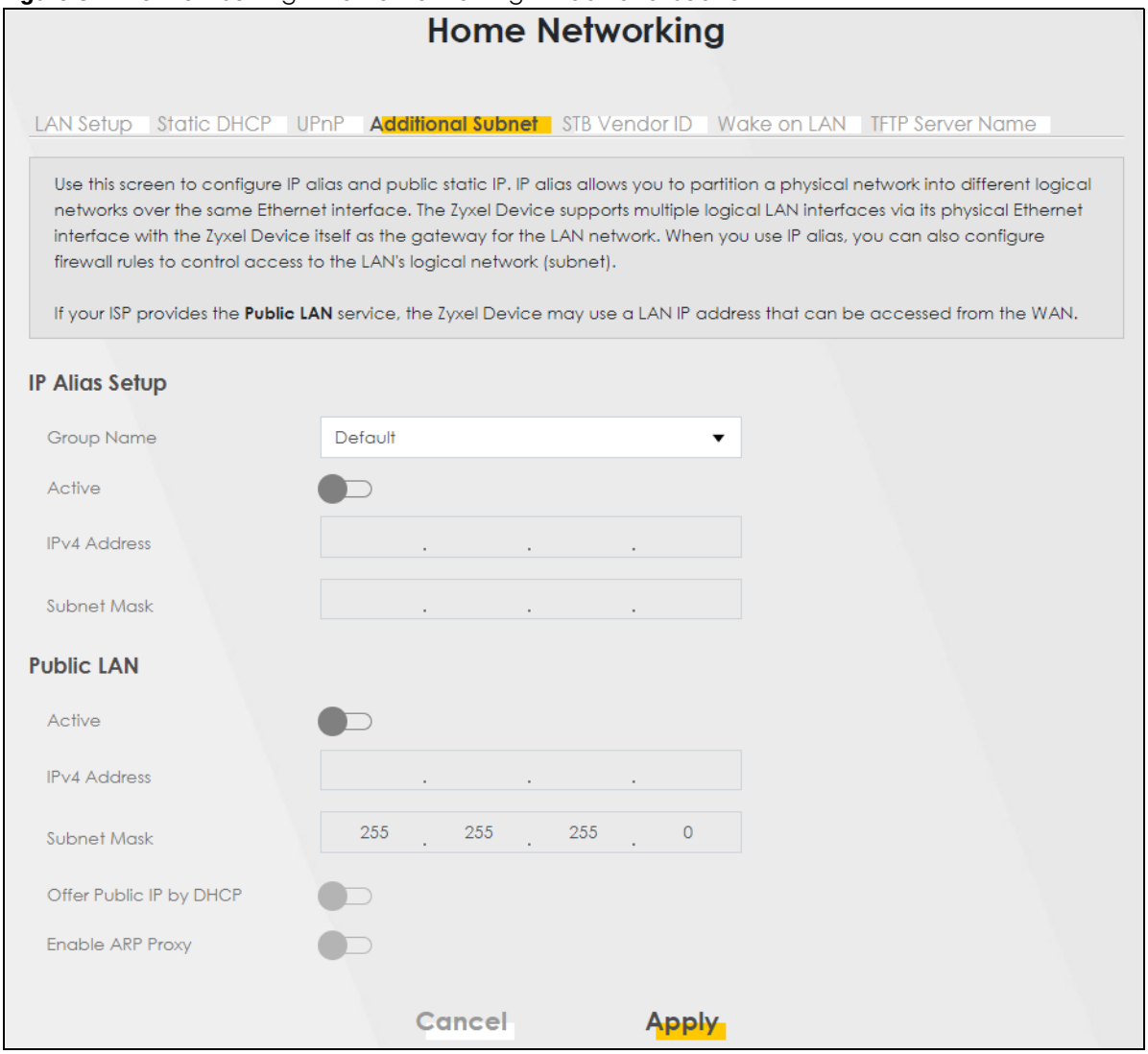
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Zyxel Device supports multiple logical LAN interfaces through its physical Ethernet

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

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

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

**Figure 87** Network Setting > Home Networking > Additional Subnet




The following table describes the labels in this screen.

Table 51 Network Setting > Home Networking > Additional Subnet

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

Table 51 Network Setting > Home Networking > Additional Subnet (continued)

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

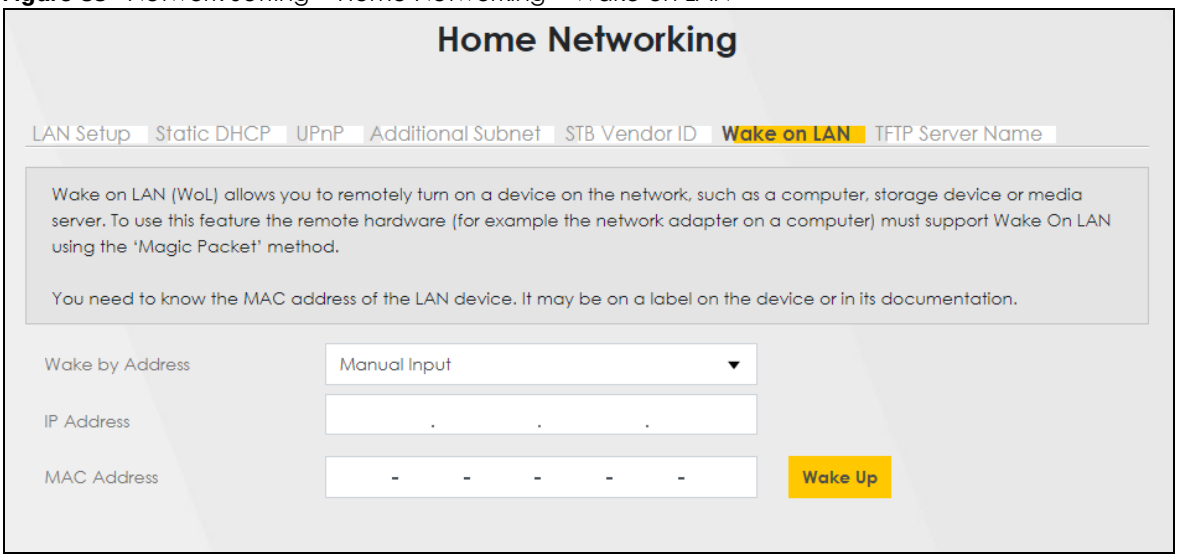
# 10.6 Wake on LAN

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

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

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

**Figure 88** Network Setting > Home Networking > Wake on LAN



The following table describes the labels in this screen.

Table 52 Network Setting > Home Networking > Wake on LAN

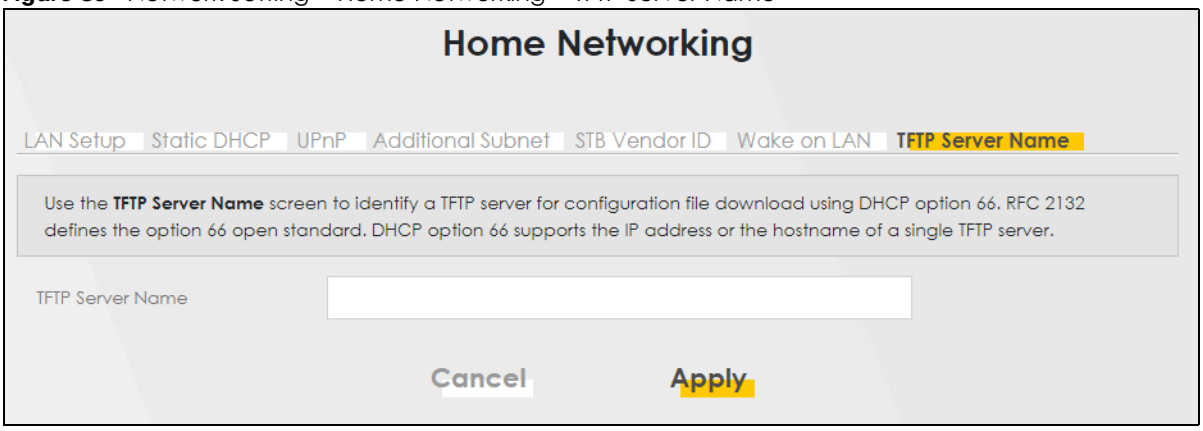
| LABEL | DESCRIPTION |
|---|---|
| Wake by Address | Select **Manual** and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the Zyxel Device's ARP table. If you select an IP address, the MAC address of the device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

# 10.7 TFTP Server Name

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

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

**Figure 89** Network Setting > Home Networking > TFTP Server Name




The following table describes the labels in this screen.

Table 53 Network Setting > Home Networking > TFTP Server Name

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

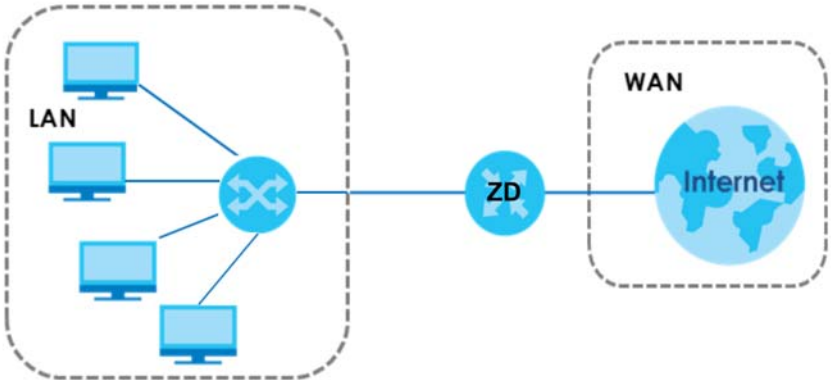
# 10.8 Technical Reference

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

### LANs, WANs and the Zyxel Device

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

**Figure 90** LAN and WAN IP Addresses




## 10.8.1 DHCP Setup

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

### IP Pool Setup

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

## 10.8.2 DNS Server Addresses

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

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

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

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

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

## 10.8.3 LAN TCP/IP

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

### IP Address and Subnet Mask

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

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

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

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

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

### Private IP Addresses

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

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

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

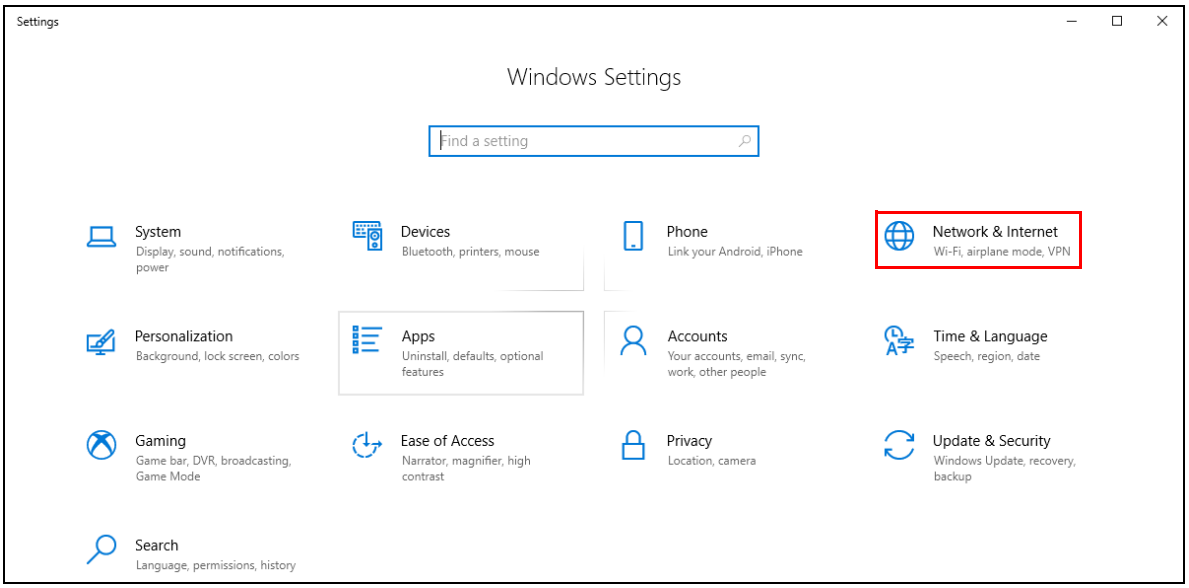
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

# 10.9 Turn on UPnP in Windows 10 Example

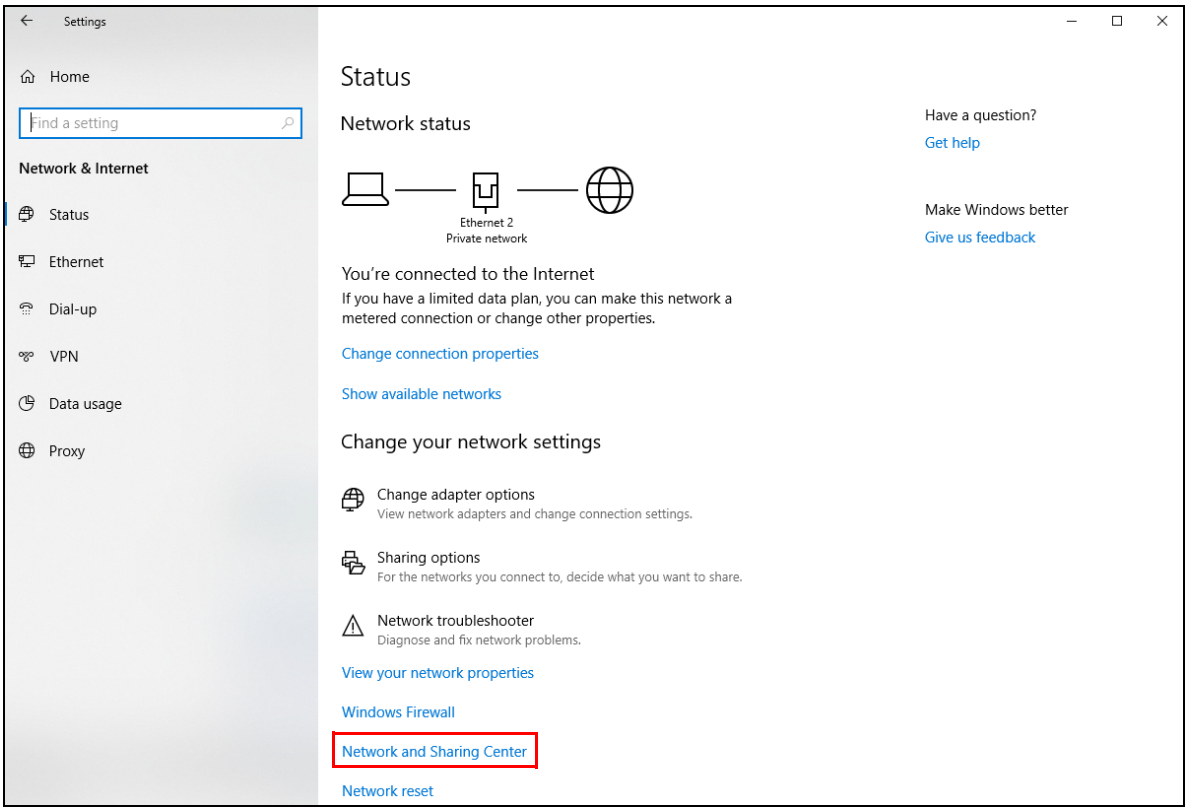
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting** > **Home Networking** > **UPnP**.

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

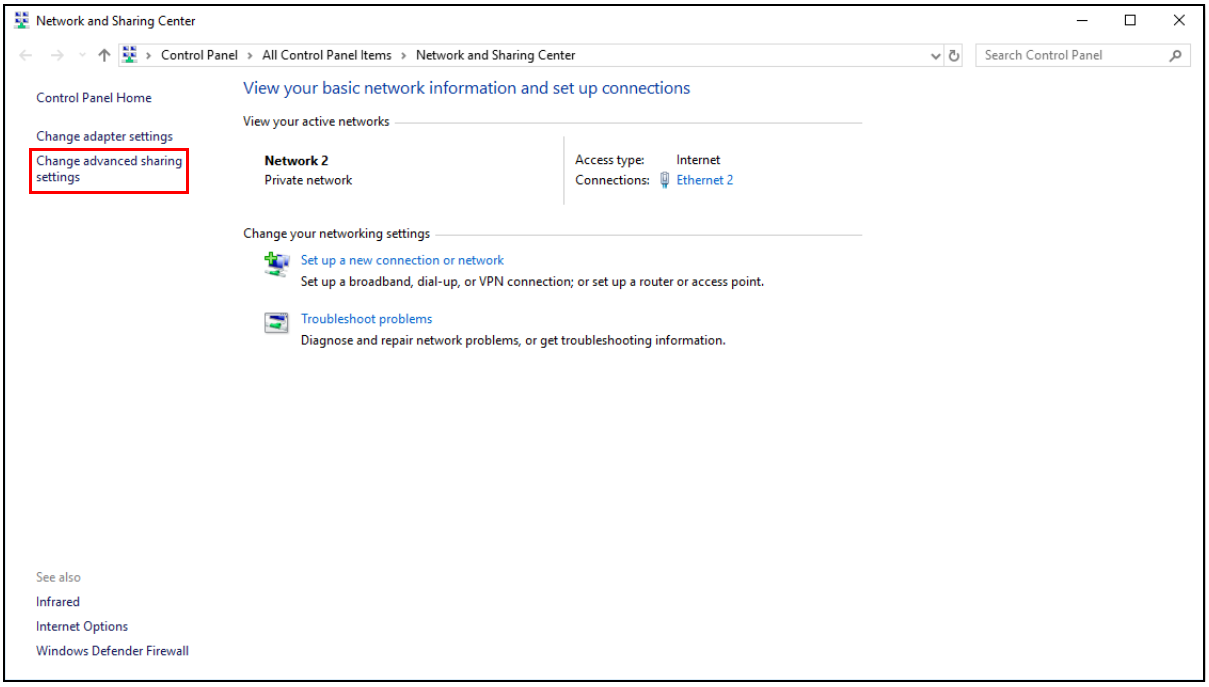
1 Click the start icon, **Settings** and then **Network & Internet**.



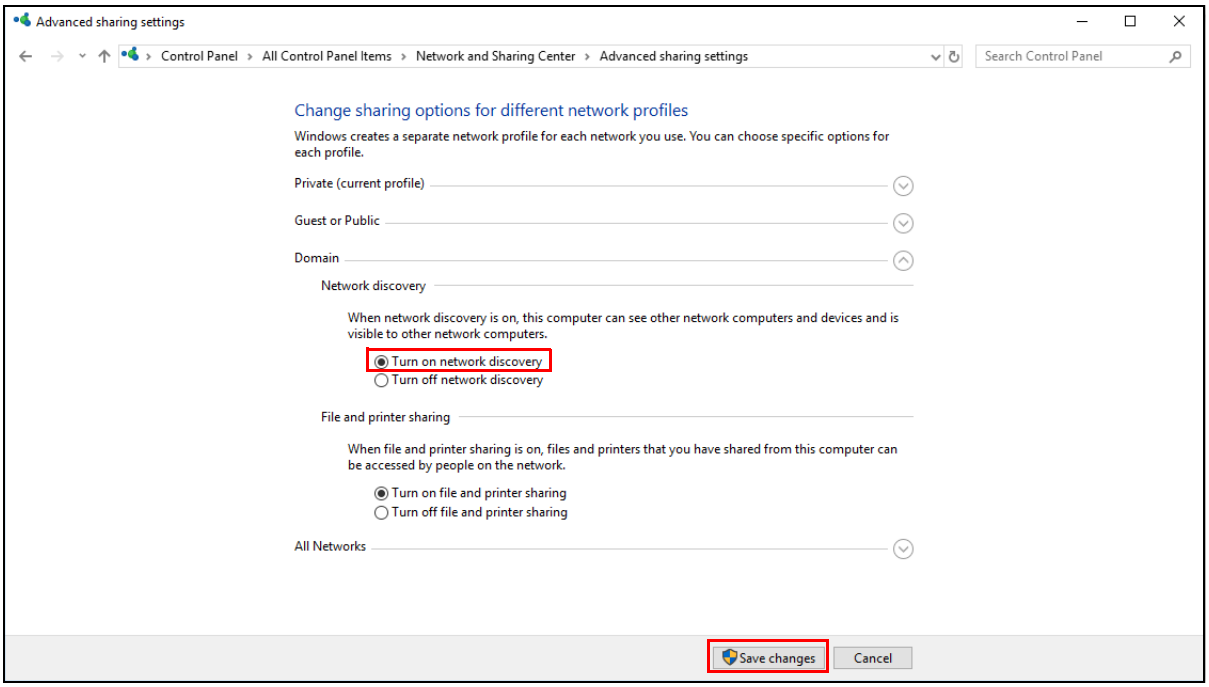

2 Click **Network and Sharing Center**.




3 Click **Change advanced sharing settings**.




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




## 10.9.1 Auto-discover Your UPnP-enabled Network Device

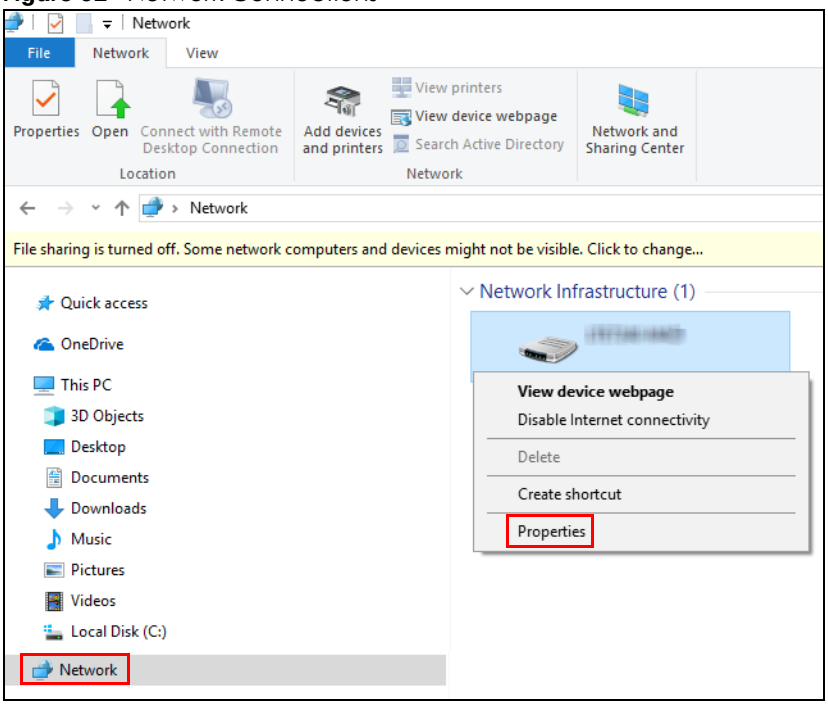
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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

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

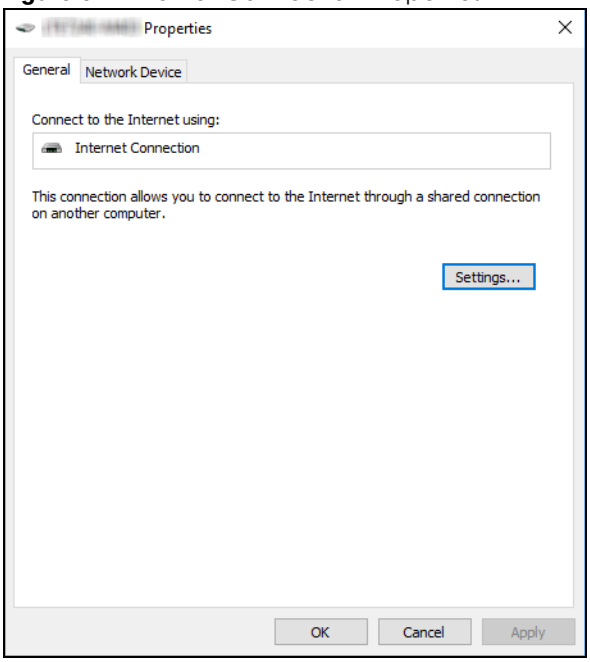
2 Right-click the Zyxel Device icon and select **Properties**.

**Figure 91** Network Connections




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

**Figure 92** Internet Connection Properties




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

**Figure 93** Internet Connection Properties: Advanced Settings

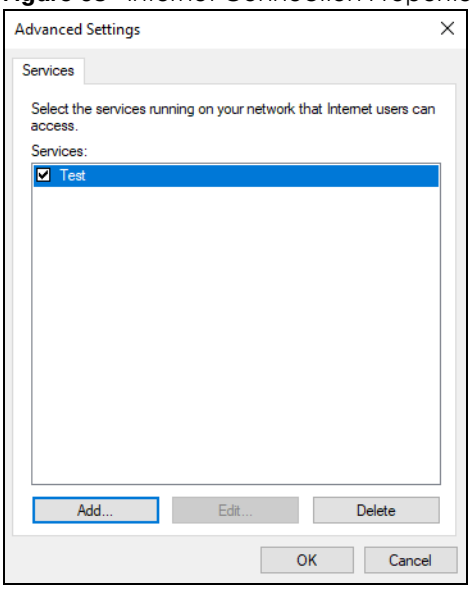
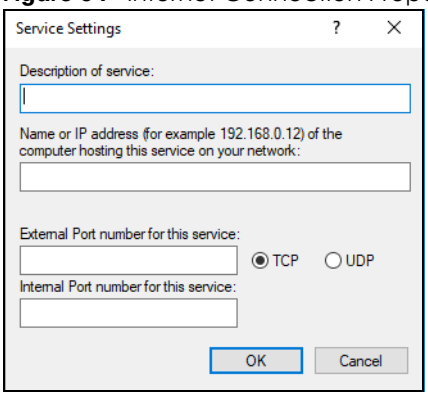


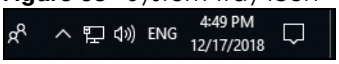

**Figure 94** Internet Connection Properties: Advanced Settings: Add




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

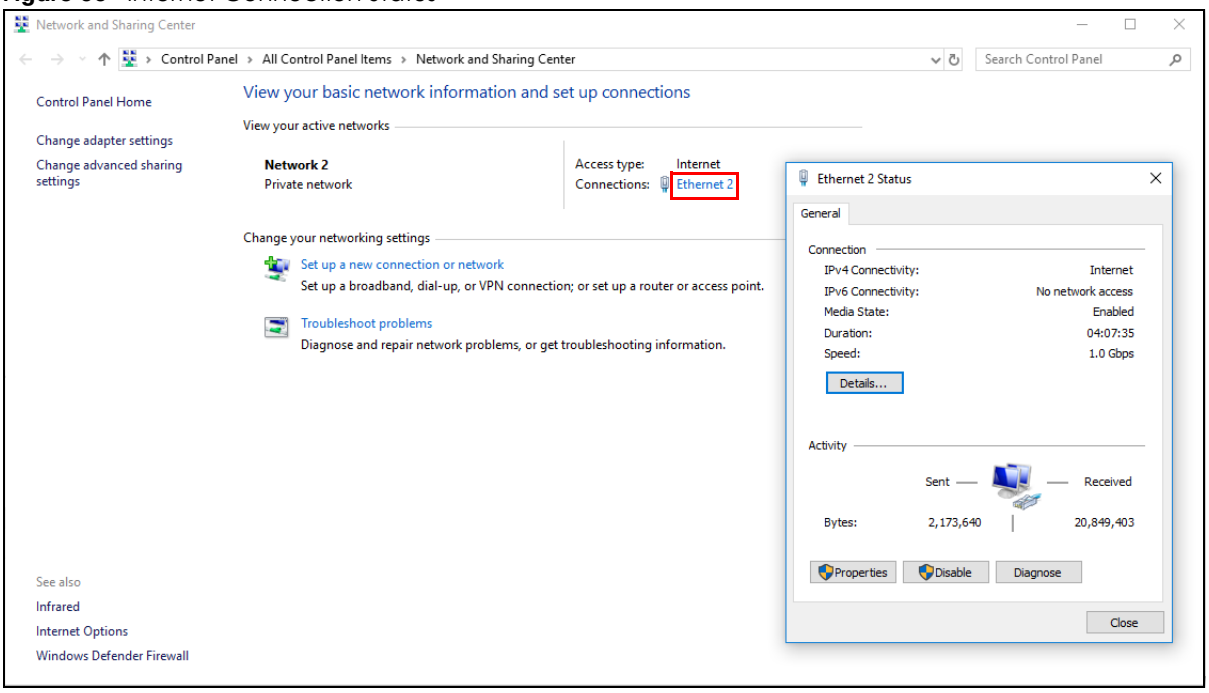
5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

**Figure 95** System Tray Icon




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

**Figure 96** Internet Connection Status



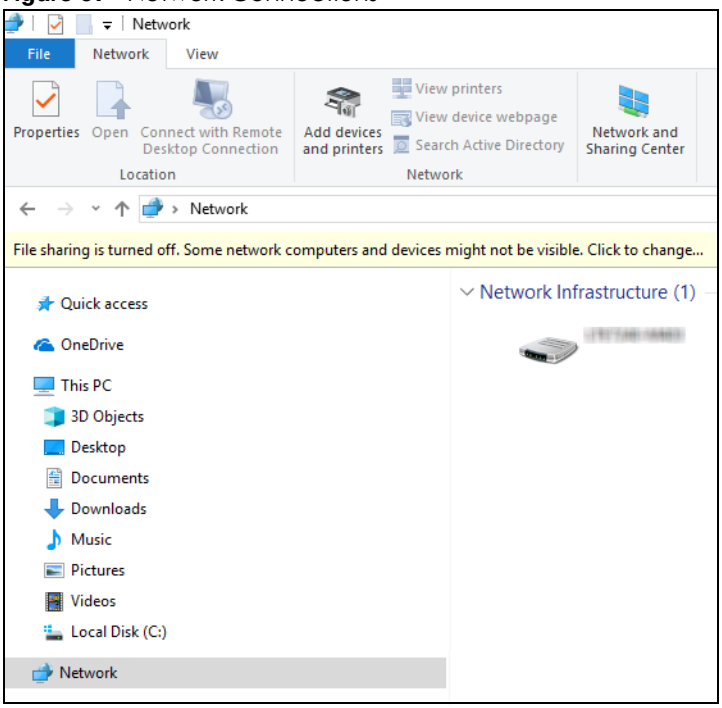

# 10.10 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

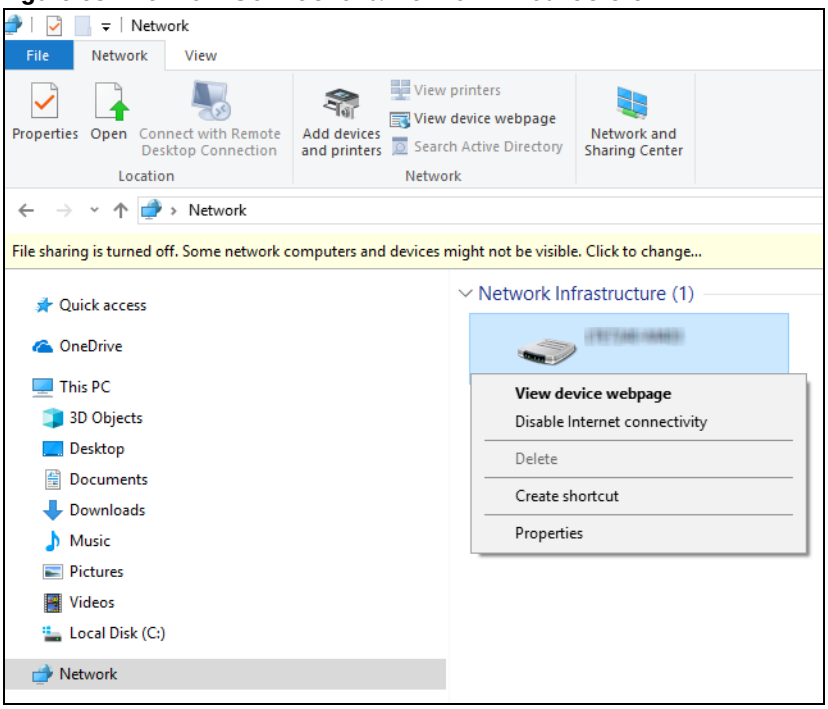
**Figure 97** Network Connections




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

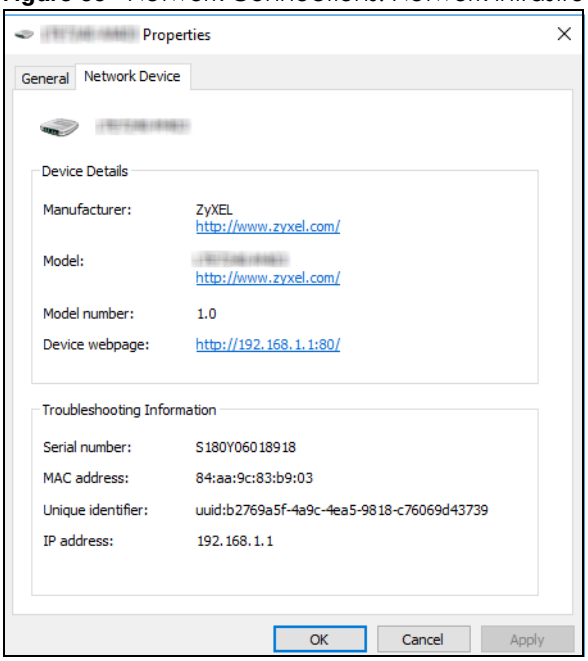
4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

**Figure 98** Network Connections: Network Infrastructure




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

**Figure 99** Network Connections: Network Infrastructure: Properties: Example



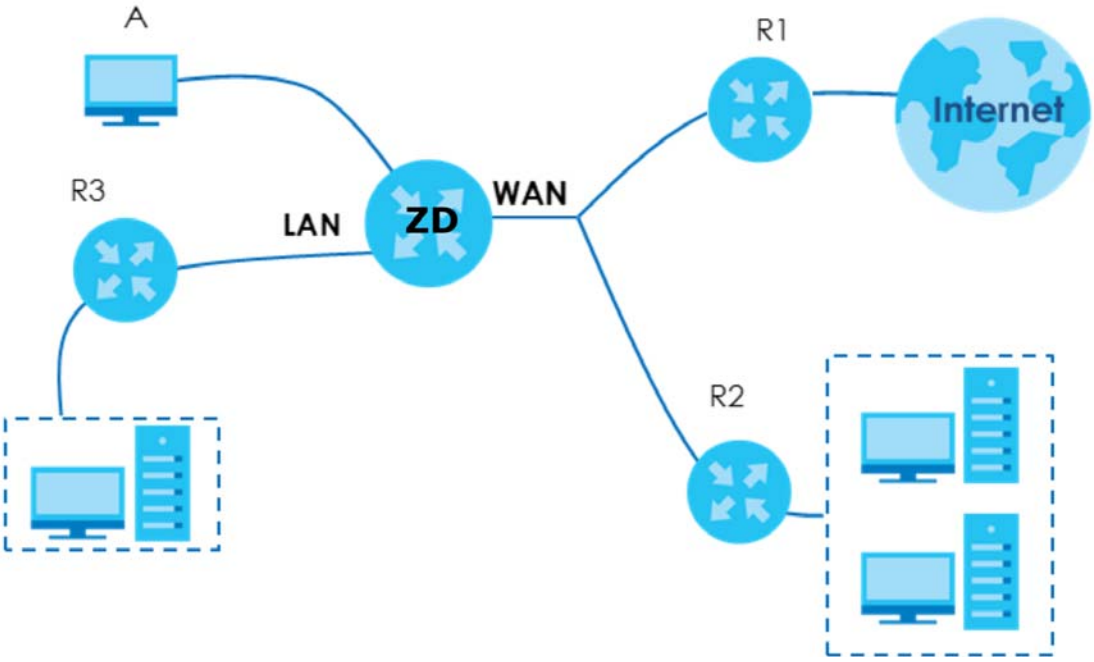
# CHAPTER 11
# Routing

## 11.1 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.

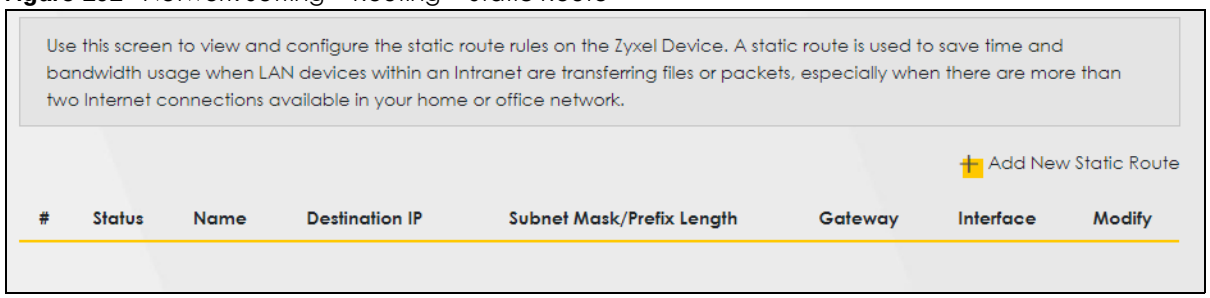
**Figure 100** Example of Static Routing Topology




## 11.2 Configure Static Route

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

**Figure 101** Network Setting > Routing > Static Route




The following table describes the labels in this screen.

Table 54 Network Setting > Routing > Static Route

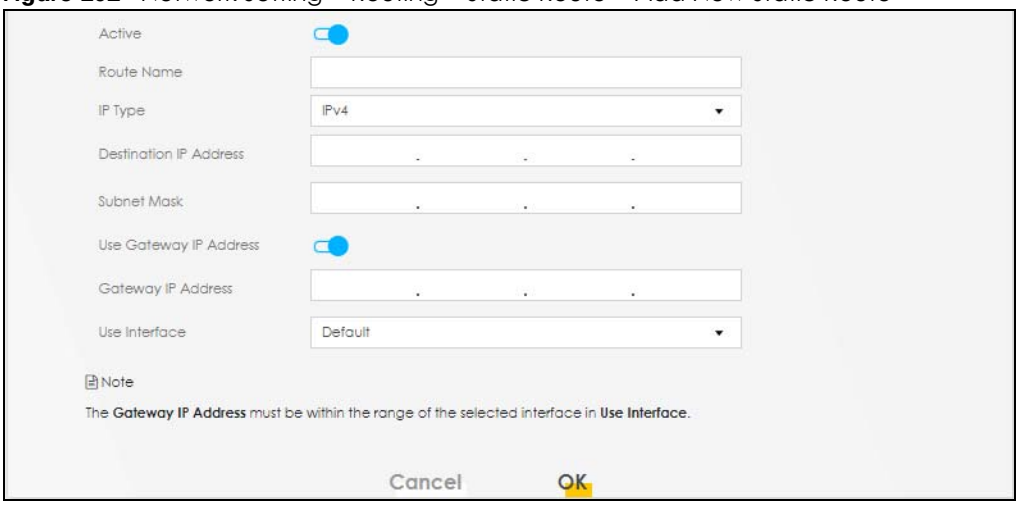
| LABEL | DESCRIPTION |
|---|---|
| Add New Static Route | Click this to set up a new static route on the Zyxel Device. |
| # | This is the number of an individual static route. |
| Status | This field indicates whether the rule is active (yellow bulb) or not (gray bulb). |
| Name | This is the name of the static route. |
| Destination IP | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Subnet Mask/ Prefix Length | This parameter specifies the IP network subnet mask of the final destination. |
| Gateway | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Interface | This is the WAN interface through which the traffic is routed. |
| Modify | Click the **Edit** icon to go to the screen where you can set up a static route on the Zyxel Device.<br>Click the **Delete** icon to remove a static route from the Zyxel Device. |

## 11.2.1 Add or Edit Static Route

Use this screen to add or edit a static route. Click **Add New Static Route** in the **Static Route** screen, the following screen appears. Configure the required information for a static route.

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

**Figure 102** Network Setting > Routing > Static Route > Add New Static Route




The following table describes the labels in this screen.

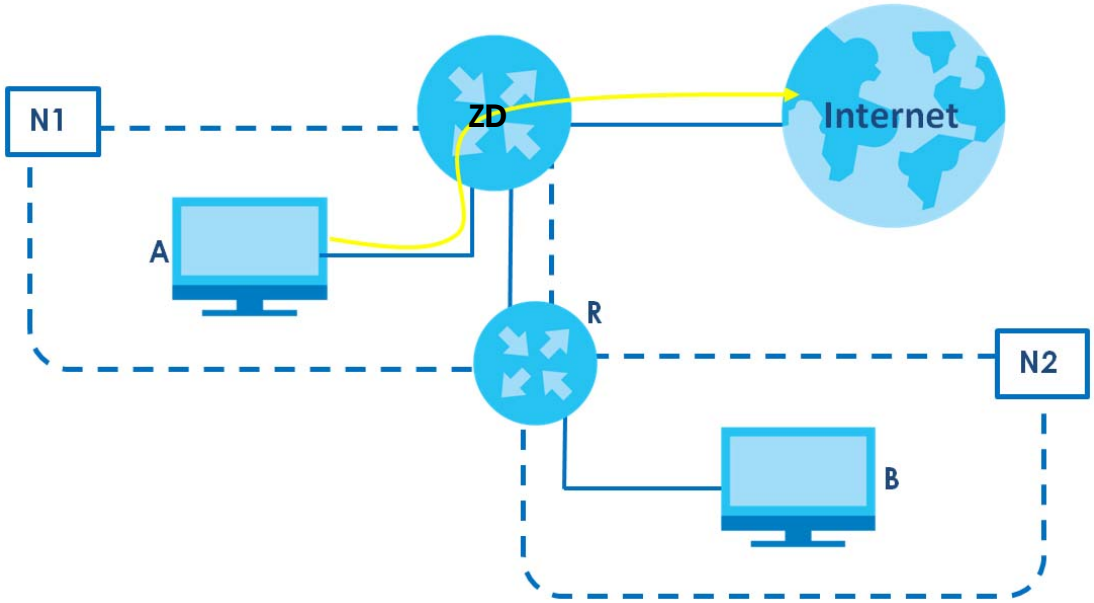
Table 55 Network Setting > Routing > Static Route > Add New Static Route

| LABEL | DESCRIPTION |
|---|---|
| Active | Click to enable ( ) and to activate static route. Otherwise, click to disable. |
| Route Name | Assign a name for your static route (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign ($) vertical bar (\|) ampersand (&) semicolon (;) |
| IP Type | Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4**/**IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD). |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| Subnet Mask | If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here. |
| Use Gateway IP Address | The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.<br>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. |
| User Interface | Select the WAN interface you want to use for this static route. |
| OK | Click this to save your changes. |
| Cancel | Click this to exit this screen without saving. |

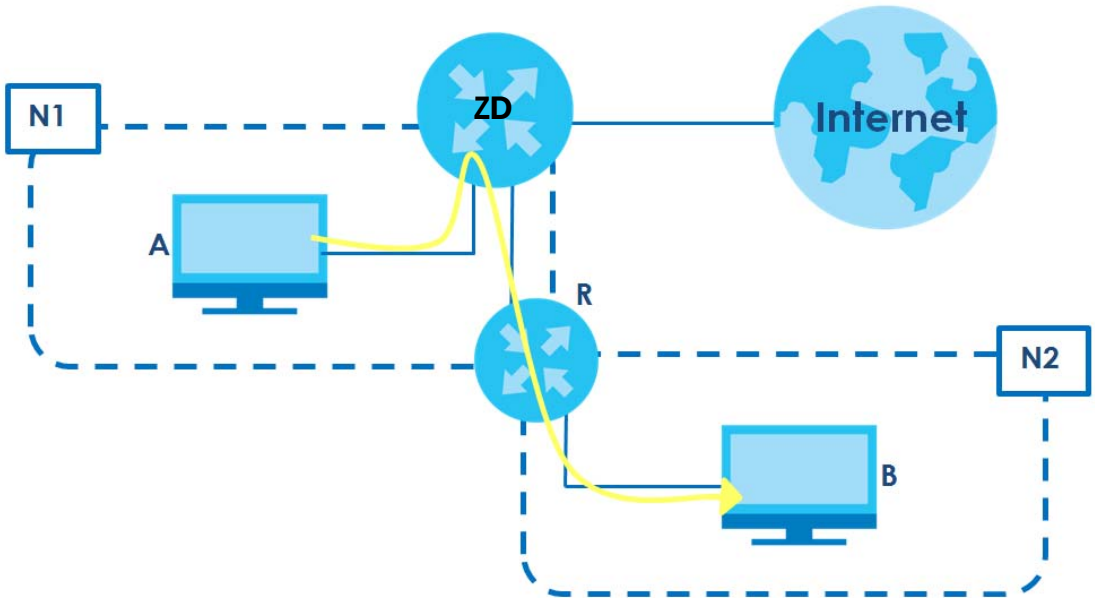
### 11.2.1.1 An Example of Adding a Static Route

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

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




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



This tutorial uses the following example IP settings:

Table 56 IP Settings in this Tutorial

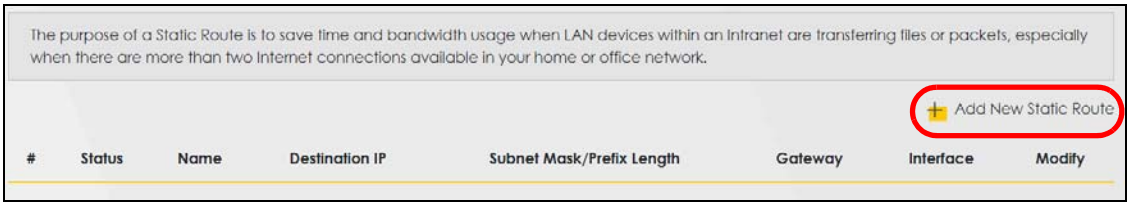
| DEVICE / COMPUTER | IP ADDRESS |
|---|---|
| The Zyxel Device's WAN | 172.16.1.1 |
| The Zyxel Device's LAN | 192.168.123.1 |
| IP Type | IPv4 |
| Use Interface | VDSL |
| **A** | 192.168.1.34 |
| **R**'s N1 | 192.168.1.253 |
| **R**'s N2 | 192.168.10.2 |
| **B** | 192.168.10.33 |

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

1 Log into the Zyxel Device's Web Configurator in advanced mode.

2 Click **Network Setting** > **Routing**.

3 Click **Add new Static Route** in the **Static Route** screen.




4 Configure the **Static Route Setup** screen using the following settings:

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

**4b** Set **IP Type** to **IPv4**.

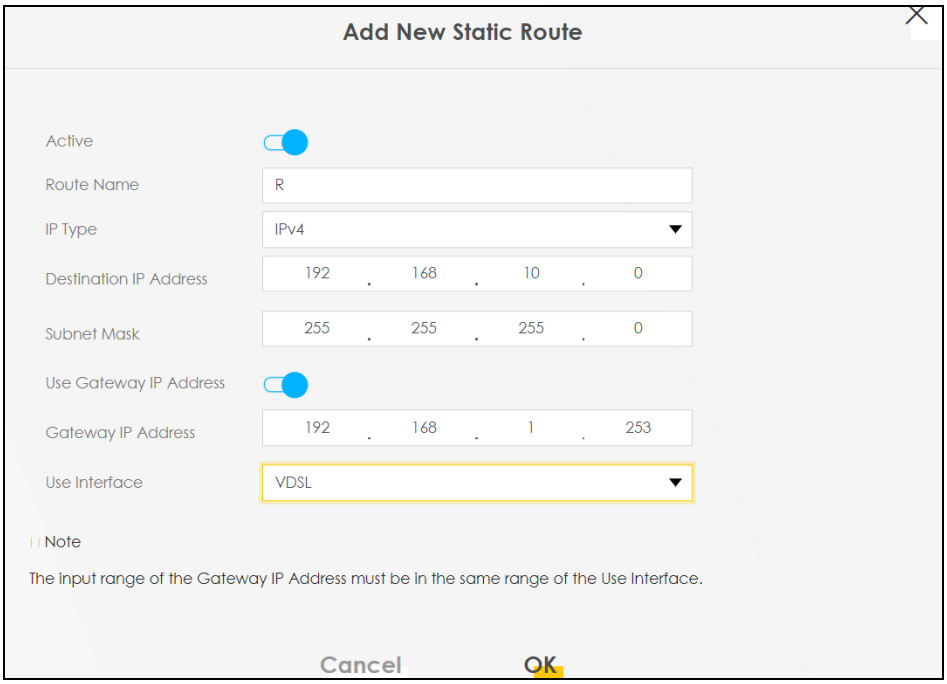
**4c** Type the **Destination IP Address 192.168.10.0** and **IP Subnet Mask 255.255.255.0** for the destination, **N2**.

**4d** Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right ( ), the function is enabled. Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.

**4e** Select **VDSL** as the **Use Interface**.

**4f** Click **OK**.

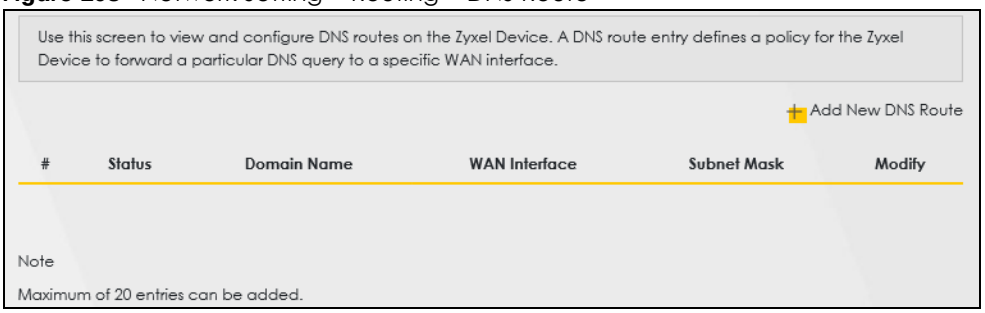
Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.




# 11.3 DNS Route

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface. Click **Network Setting** > **Routing** > **DNS Route** to open the **DNS Route** screen.

**Figure 103** Network Setting > Routing > DNS Route




The following table describes the labels in this screen.

Table 57 Network Setting > Routing > DNS Route

| LABEL | DESCRIPTION |
|---|---|
| Add New DNS Route | Click this to create a new entry. |
| # | This is the number of an individual DNS route. |
| Status | This field indicates whether the rule is active (yellow bulb) or not (gray bulb). |
| Domain Name | This is the domain name to which the DNS route applies. |
| WAN Interface | This is the WAN interface through which the matched DNS request is routed. |

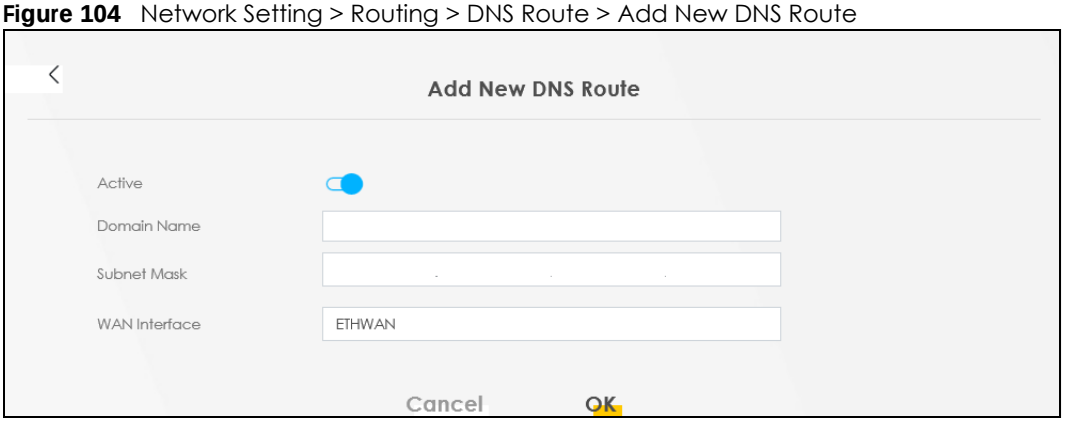
Table 57 Network Setting > Routing > DNS Route (continued)

| LABEL | DESCRIPTION |
|---|---|
| Subnet Mask | This parameter specifies the IP network subnet mask. |
| Modify | Click the **Edit** icon to configure a DNS route on the Zyxel Device.<br>Click the **Delete** icon to remove a DNS route from the Zyxel Device. |

### 11.3.1 Add or Edit DNS Route

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **DNS Route** screen, use this screen to configure the required information for a DNS route.

**Figure 104** Network Setting > Routing > DNS Route > Add New DNS Route




The following table describes the labels in this screen.

Table 58 Network Setting > Routing > DNS Route > Add New DNS Route

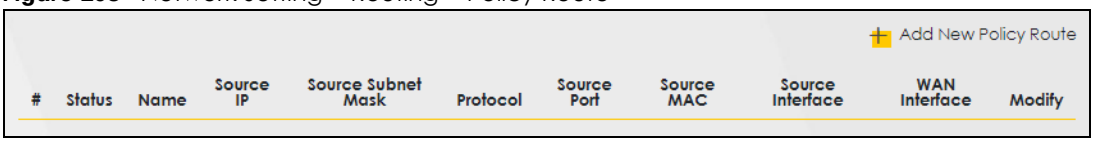
| LABEL | DESCRIPTION |
|---|---|
| Active | Enable DNS route in your Zyxel Device. |
| Domain Name | Enter the domain name you want to resolve.<br>You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Zyxel Device forwards DNS queries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

## 11.4 Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address. For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.

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

**Figure 105** Network Setting > Routing > Policy Route




The following table describes the labels in this screen.

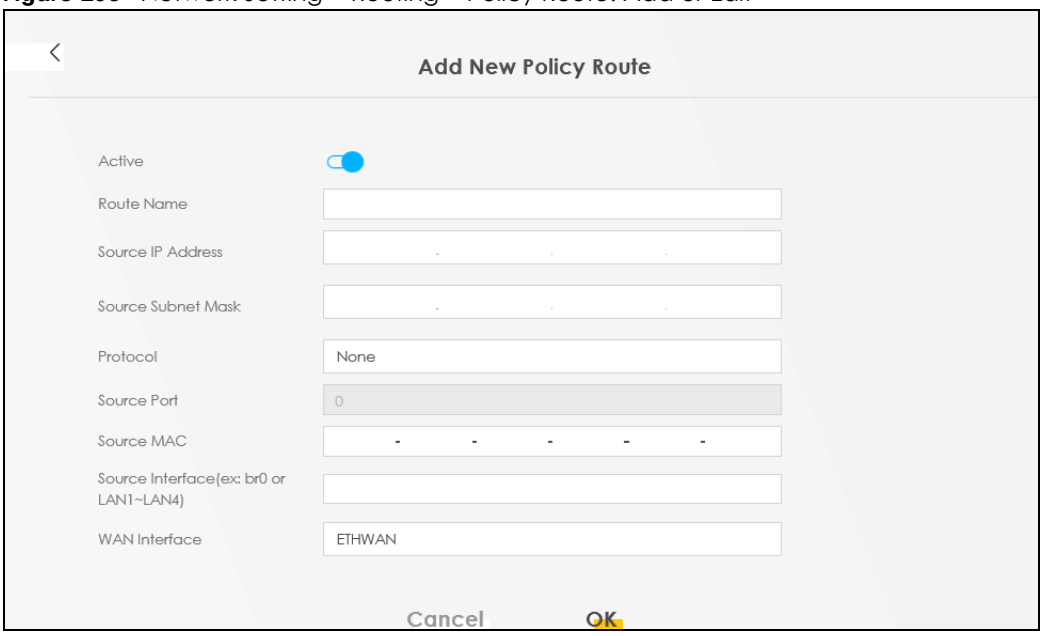
Table 59 Network Setting > Routing > Policy Route

| LABEL | DESCRIPTION |
|---|---|
| Add New Policy Route | Click this to create a new policy forwarding rule. |
| # | This is the index number of the entry. |
| Status | This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active. |
| Name | This is the name of the rule. |
| Source IP | This is the source IP address. |
| Source Subnet Mask | This is the source subnet mask address. |
| Protocol | This is the transport layer protocol. |
| Source Port | This is the source port number. |
| Source MAC | This is the source MAC address. |
| Source Interface | This is the interface from which the matched traffic is sent. |
| WAN Interface | This is the WAN interface through which the traffic is routed. |
| Modify | Click the **Edit** icon to edit this policy.<br>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. |

## 11.4.1 Add or Edit Policy Route

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

**Figure 106** Network Setting > Routing > Policy Route: Add or Edit




The following table describes the labels in this screen.

Table 60 Network Setting > Routing > Policy Route: Add or Edit

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

# CHAPTER 12
# Network Address Translation (NAT)

## 12.1 Overview

NAT (Network Address Translation – NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

### 12.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the servers on your local network (Section 12.2 on page 176).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings (Section 12.3 on page 179).
- Use the **DMZ** screen to configure a default server (Section 12.4 on page 182).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 12.5 on page 183).
- Use the **Address Mapping** screen to enable and disable the NAT Address Mapping in the Zyxel Device (Section 12.6 on page 184).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section 12.7 on page 187).

### 12.1.2 What You Need To Know

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

#### Inside/Outside and Global/Local

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

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

#### NAT

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

### Port Forwarding

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

## 12.2 Port Forwarding

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

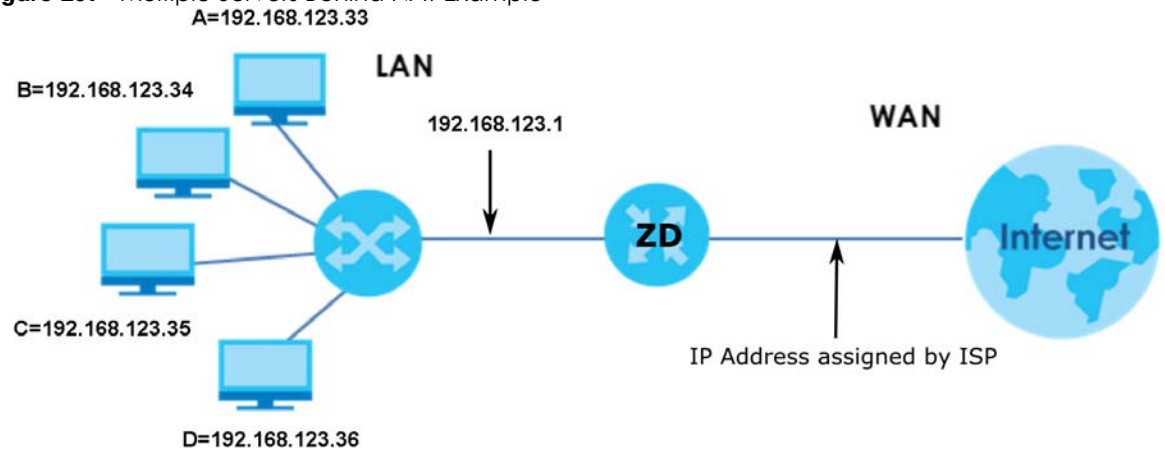
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more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

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

### Configure Servers Behind Port Forwarding (Example)

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

**Figure 107** Multiple Servers Behind NAT Example

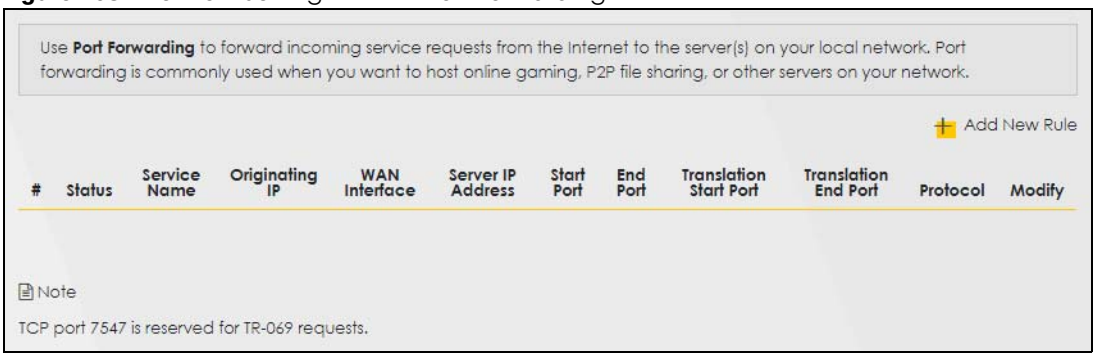



### 12.2.1 Port Forwarding

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

Note: TCP port 7547 is reserved for system use.

**Figure 108** Network Setting > NAT > Port Forwarding




The following table describes the fields in this screen.

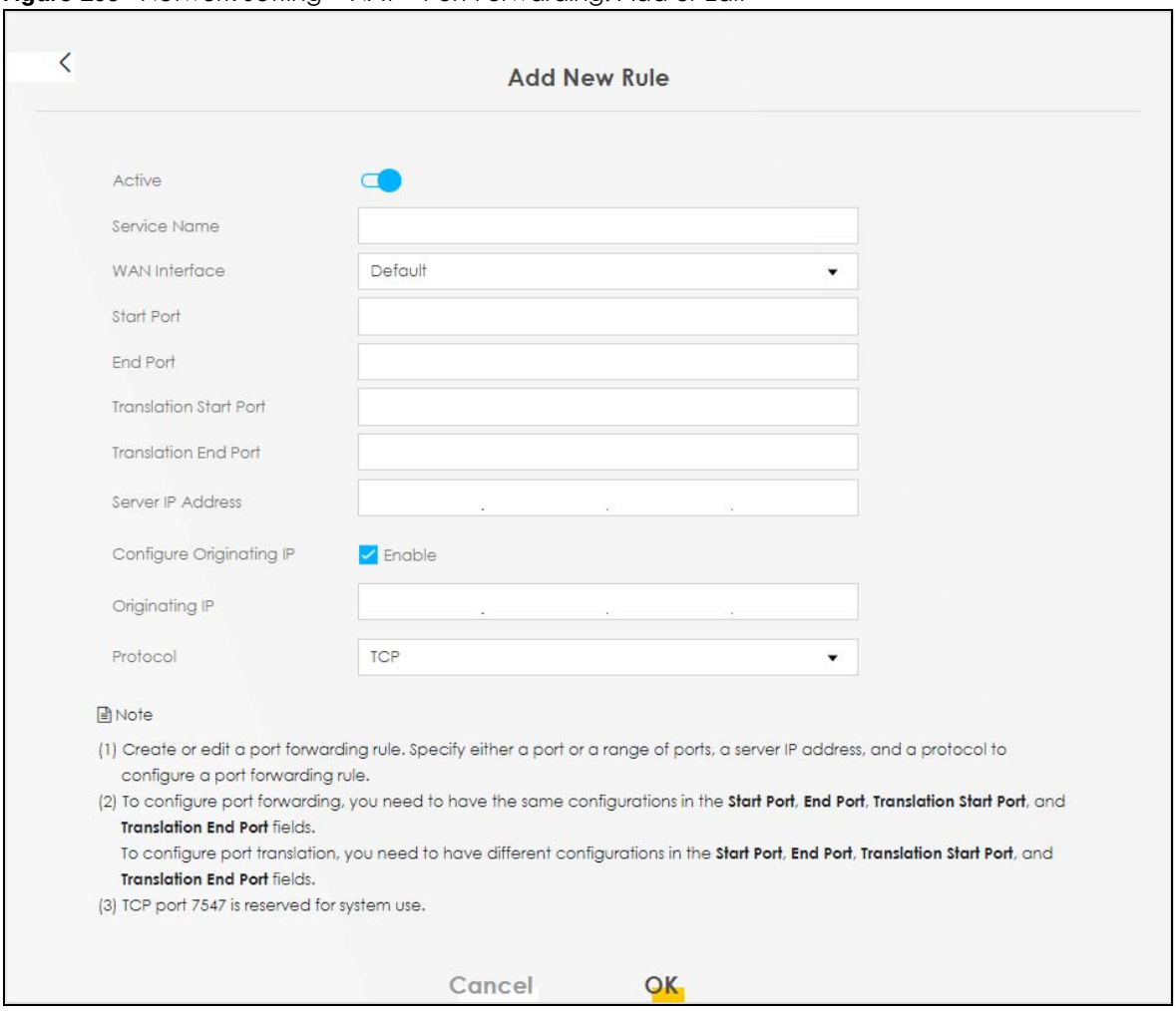
Table 61 Network Setting > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Add New Rule | Click this to add a new port forwarding rule. |
| # | This is the index number of the entry. |
| Status | This field indicates whether the rule is active or not.<br><br>A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. |
| Service Name | This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon. |
| Originating IP | This is the source's IP address. |
| WAN Interface | Select the WAN interface for which to configure NAT port forwarding rules. |
| Server IP Address | This is the server's IP address. |
| Start Port | This is the first external port number that identifies a service. |
| End Port | This is the last external port number that identifies a service. |
| Translation Start Port | This is the first internal port number that identifies a service. |
| Translation End Port | This is the last internal port number that identifies a service. |
| Protocol | This field displays the protocol (TCP, UDP, TCP+UDP) used to transport the packets for which you want to apply the rule. |
| Modify | Click the **Edit** icon to edit the port forwarding rule.<br><br>Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action. |

## 12.2.2 Add or Edit Port Forwarding

Create or edit a port forwarding rule. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule. Click **Add New Rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

**Figure 109** Network Setting > NAT > Port Forwarding: Add or Edit




Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
Here is an example to configure port translation. Configure **Start Port** to 100, **End Port** to 120, **Translation Start Port** to 200, and **Translation End Port** to 220.

Note: TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

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

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

Table 62 Network Setting > NAT > Port Forwarding: Add or Edit (continued)

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

# 12.3 Port Triggering

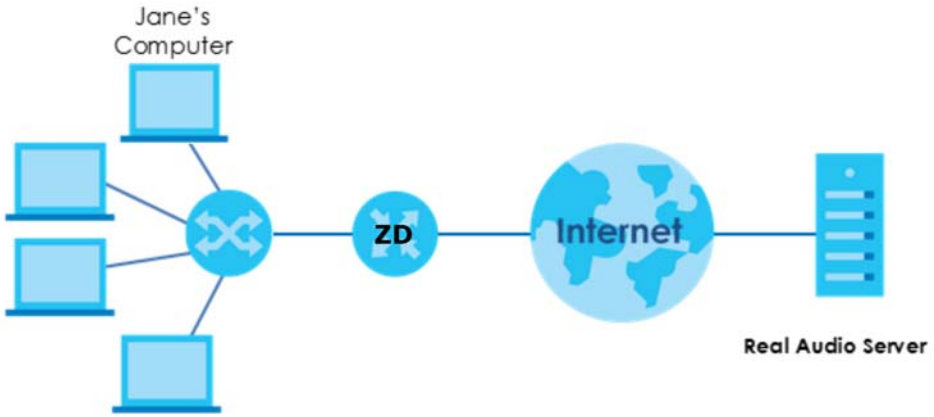
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service.

The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a \"trigger\" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol (\"open\" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

**Figure 110** Trigger Port Forwarding Process: Example




1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970 – 7170.

3 The Real Audio server responds using a port number ranging between 6970 – 7170.

4 The Zyxel Device forwards the traffic to Jane's computer IP address.

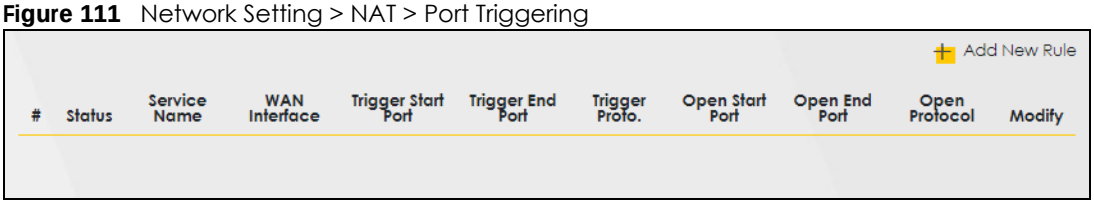
5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in 3 minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

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

Note: TCP port 7547 is reserved for system use.

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

**Figure 111** Network Setting > NAT > Port Triggering




The following table describes the labels in this screen.

Table 63 Network Setting > NAT > Port Triggering

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

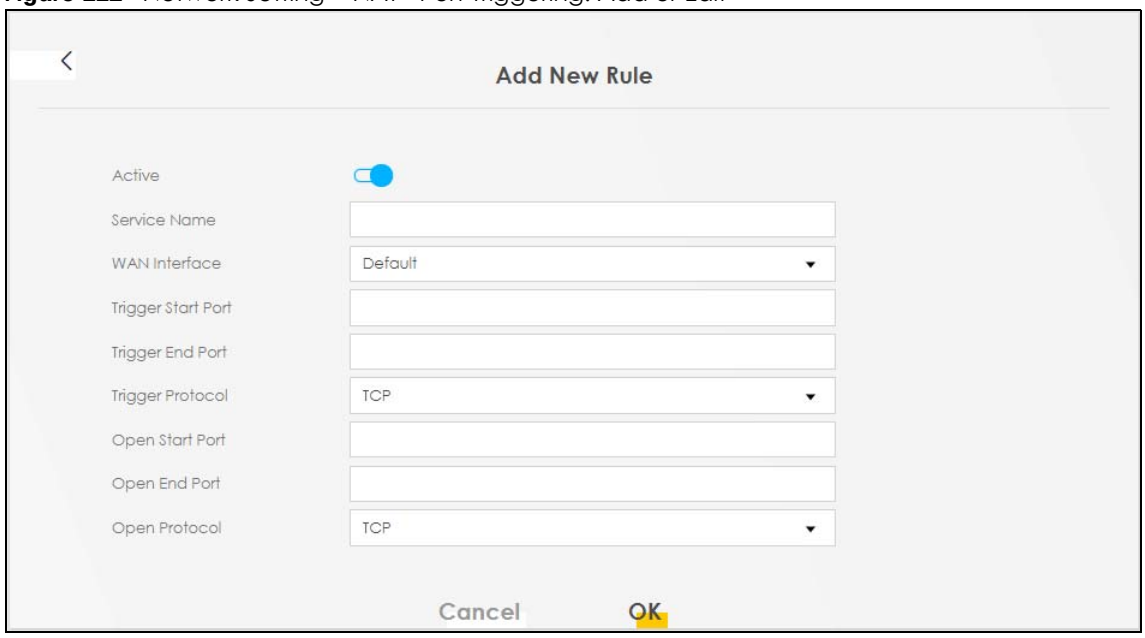
Table 63 Network Setting > NAT > Port Triggering (continued)

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

## 12.3.1 Add or Edit Port Triggering Rule

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

**Figure 112** Network Setting > NAT> Port Triggering: Add or Edit



The following table describes the labels in this screen.

Table 64 Network Setting > NAT > Port Triggering: Add or Edit

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

# 12.4 DMZ

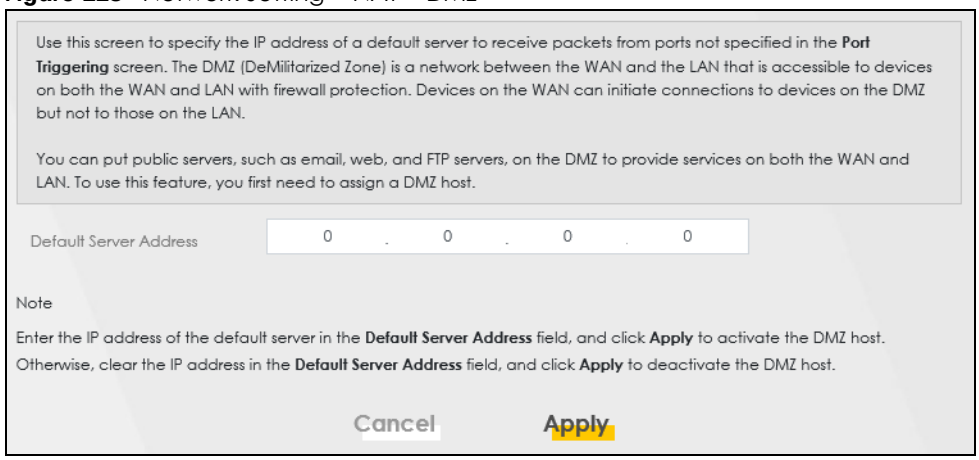
Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (DeMilitarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on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

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

Note: Use an IPv4 address for the DMZ server.

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

**Figure 113** Network Setting > NAT > DMZ




The following table describes the fields in this screen.

Table 65 Network Setting > NAT > DMZ

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

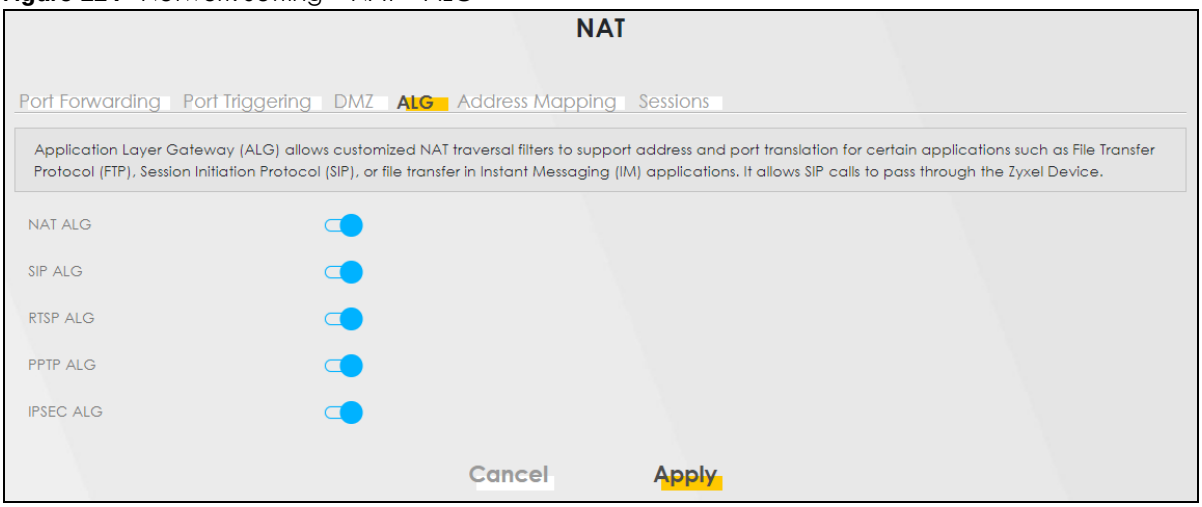
# 12.5 ALG

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

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

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

**Figure 114** Network Setting > NAT > ALG




The following table describes the fields in this screen.

Table 66 Network Setting > NAT > ALG

| LABEL | DESCRIPTION |
|---|---|
| NAT ALG | Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules. |
| SIP ALG | Click this (switch turns blue) to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. Otherwise, click this to turn off (switch turns gray) the SIP ALG. |
| RTSP ALG | Enable this to have the Zyxel Device detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| PPTP ALG | Click this to turn on (switch turns blue) the PPTP ALG on the Zyxel Device to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT. |
| IPSEC ALG | Enable this to turn on the IPsec ALG on the Zyxel Device to detect IPsec traffic and help build IPsec sessions through the Zyxel Device's NAT. |
| Apply | Click **Apply** to save your changes back to the Zyxel Device. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 12.6 Address Mapping

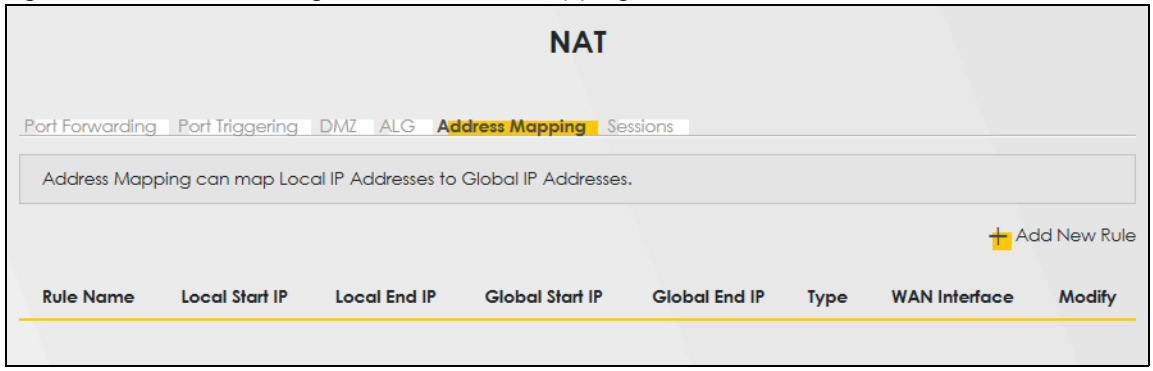
Address mapping can map local IP Addresses to global IP addresses. Ordering your rules is important because the Zyxel Device applies the rules in the order that you specify. When a rule matches the current packet, the Zyxel Device takes the corresponding action and the remaining rules are ignored.

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

## 12.6.1 Address Mapping Screen

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

**Figure 115** Network Setting > NAT > Address Mapping




The following table describes the fields in this screen.

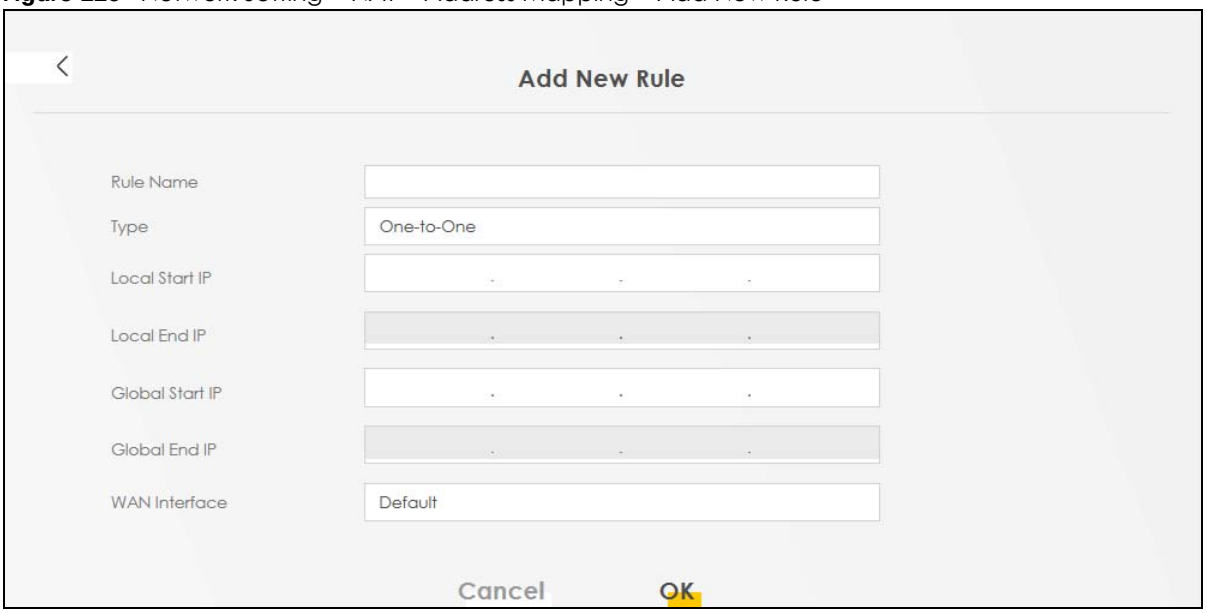
Table 67 Network Setting > NAT > Address Mapping

| LABEL | DESCRIPTION |
|---|---|
| Add New Rule | Click this to create a new rule. |
| Rule Name | This is the name of the rule. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). |
| Local End IP | This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for **One-to-One** mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the **Many-to-One** mapping type. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types. |
| Type | This is the address mapping type.<br><br>**One-to-One**: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type.<br><br>**Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only.<br><br>**Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses. |
| WAN Interface | This is the WAN interface to which the address mapping rule applies. |
| Modify | Click the **Edit** icon to go to the screen where you can edit the address mapping rule.<br><br>Click the **Delete** icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action. |

## 12.6.2 Add New Rule Screen

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

**Figure 116** Network Setting > NAT > Address Mapping > Add New Rule




The following table describes the fields in this screen.

Table 68 Network Setting > NAT > Address Mapping > Add New Rule

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

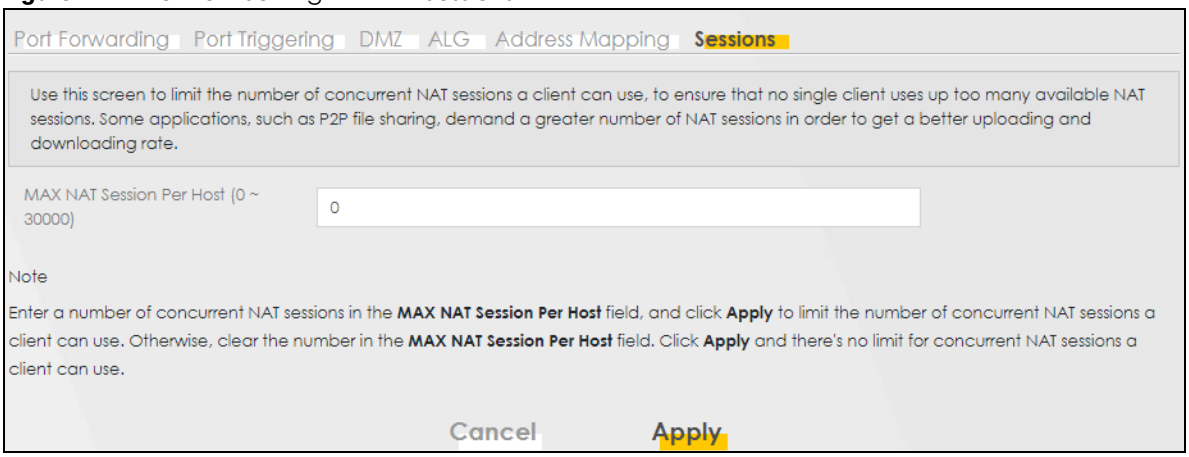
# 12.7 Sessions

Use this screen to limit the number of concurrent NAT sessions a client can use, to ensure that no single client uses up too many available NAT sessions. Some applications, such as P2P file sharing, demand a greater number of NAT sessions in order to get a better uploading and downloading rate. Click **Network Setting** > **NAT** > **Sessions** to display the following screen.

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

Note: Enter a number of concurrent NAT sessions in the **MAX NAT Session Per Host** field, and click **Apply** to limit the number of concurrent NAT sessions a client can use. Otherwise, clear the number in the **MAX NAT Session Per Host** field. Click **Apply** and there is no limit for concurrent NAT sessions a client can use.

**Figure 117** Network Setting > NAT > Sessions




The following table describes the fields in this screen.

Table 69 Network Setting > NAT > Sessions

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

# 12.8 Technical Reference

This part contains more information regarding NAT.

### 12.8.1 NAT Definitions

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

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

Note that inside or outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 70 NAT Definitions

| ITEM | DESCRIPTION |
|---|---|
| Inside | This refers to the host on the LAN. |
| Outside | This refers to the host on the WAN. |
| Local | This refers to the packet address (source or destination) as the packet travels on the LAN. |
| Global | This refers to the packet address (source or destination) as the packet travels on the WAN. |

NAT never changes the IP address (either local or global) of an outside host.

### 12.8.2 What NAT Does

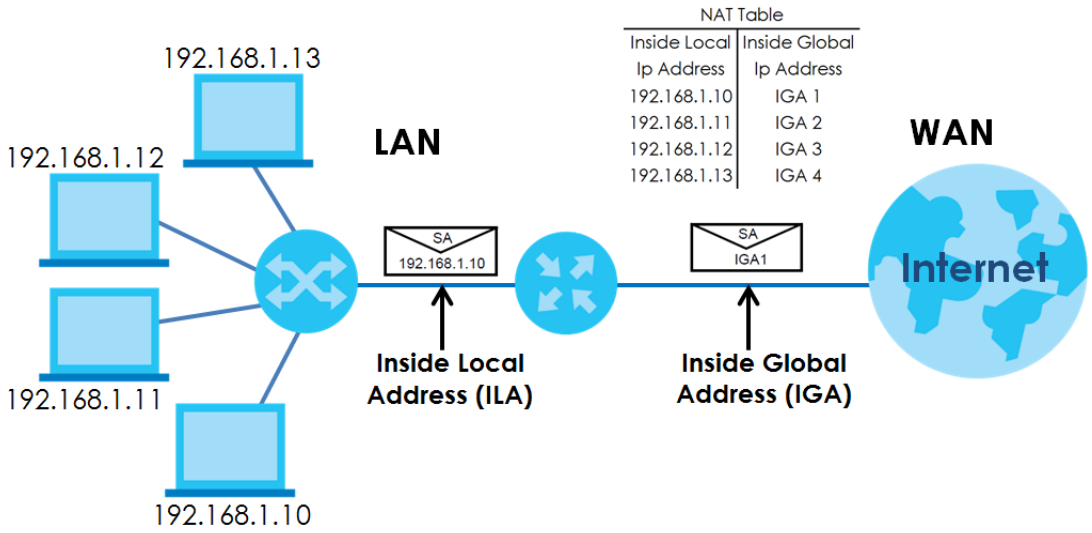
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Zyxel Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## 12.8.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Zyxel Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

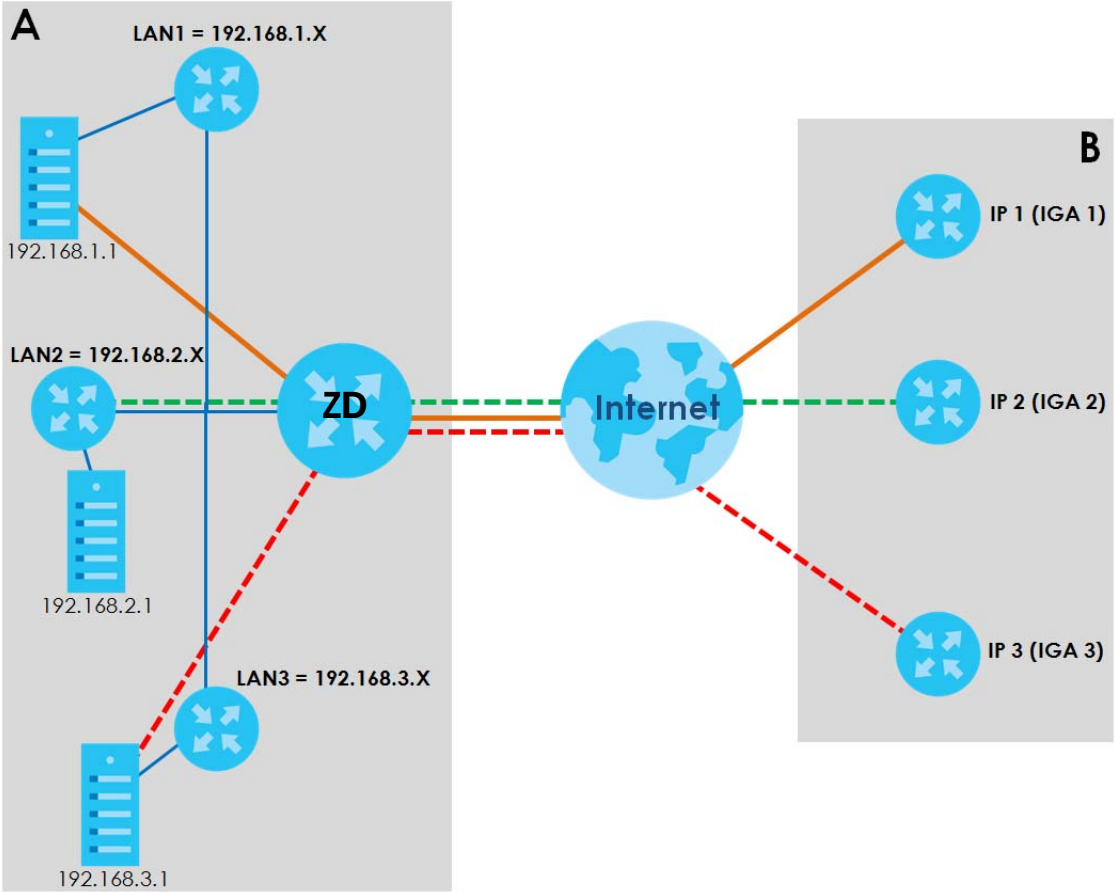
**Figure 118** How NAT Works




## 12.8.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the Zyxel Device can communicate with three distinct WAN networks.

**Figure 119** NAT Application With IP Alias




## Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

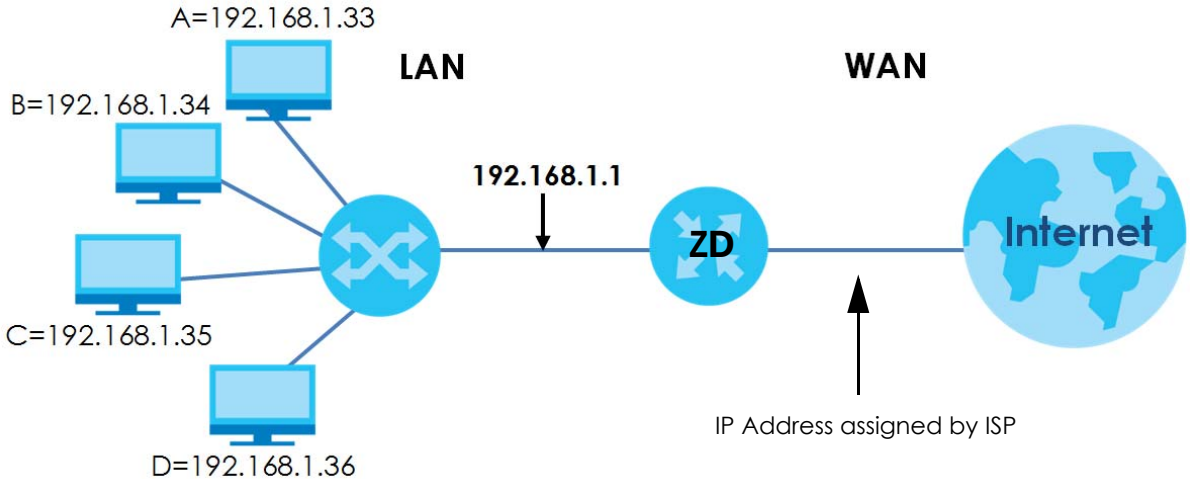
Table 71 Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|---|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer protocol or WWW, Web) | 80 |
| POP3 (Post Office Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

## Port Forwarding Example

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

**Figure 120** Multiple Servers Behind NAT Example



# CHAPTER 13
# DNS

## 13.1 DNS Overview

### DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS servers, each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. The Zyxel Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Zyxel Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Note: For information on configuring DNS route, see Chapter 11 on page 166.

### Dynamic DNS

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

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

### 13.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 13.2 on page 193).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device (Section 13.3 on page 194).

### 13.1.2 What You Need To Know

#### DYNDNS Wildcard

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

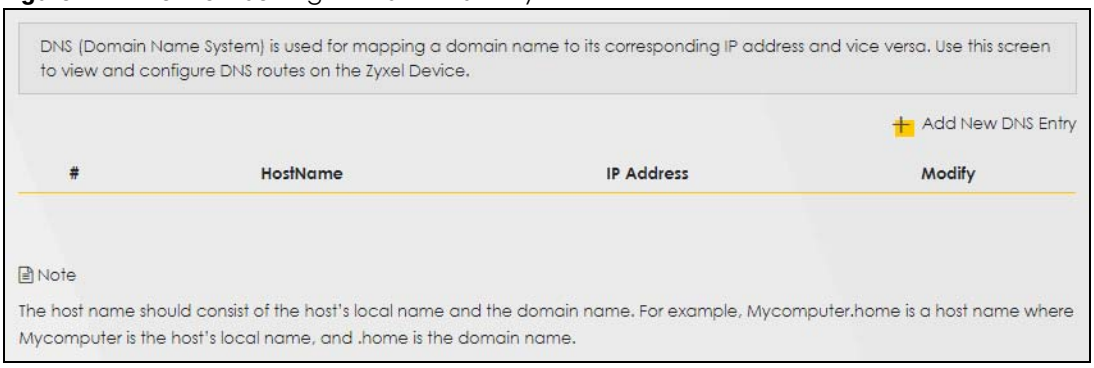
If you have a private WAN IP address, then you cannot use Dynamic DNS.

## 13.2 DNS Entry

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure manual DNS entires on the Zyxel Device. Click **Network Setting** > **DNS** to open the **DNS Entry** screen.

Note: The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.

**Figure 121** Network Setting > DNS > DNS Entry




The following table describes the fields in this screen.

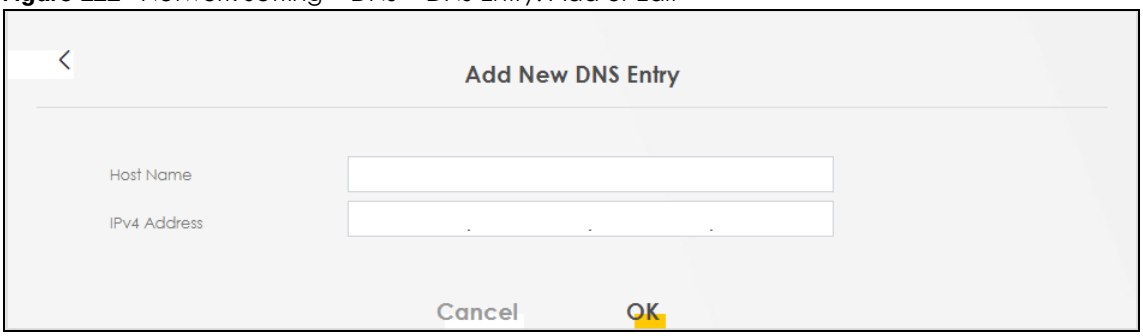
Table 72 Network Setting > DNS > DNS Entry

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

### 13.2.1 Add or Edit DNS Entry

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

**Figure 122** Network Setting > DNS > DNS Entry: Add or Edit




The following table describes the labels in this screen.

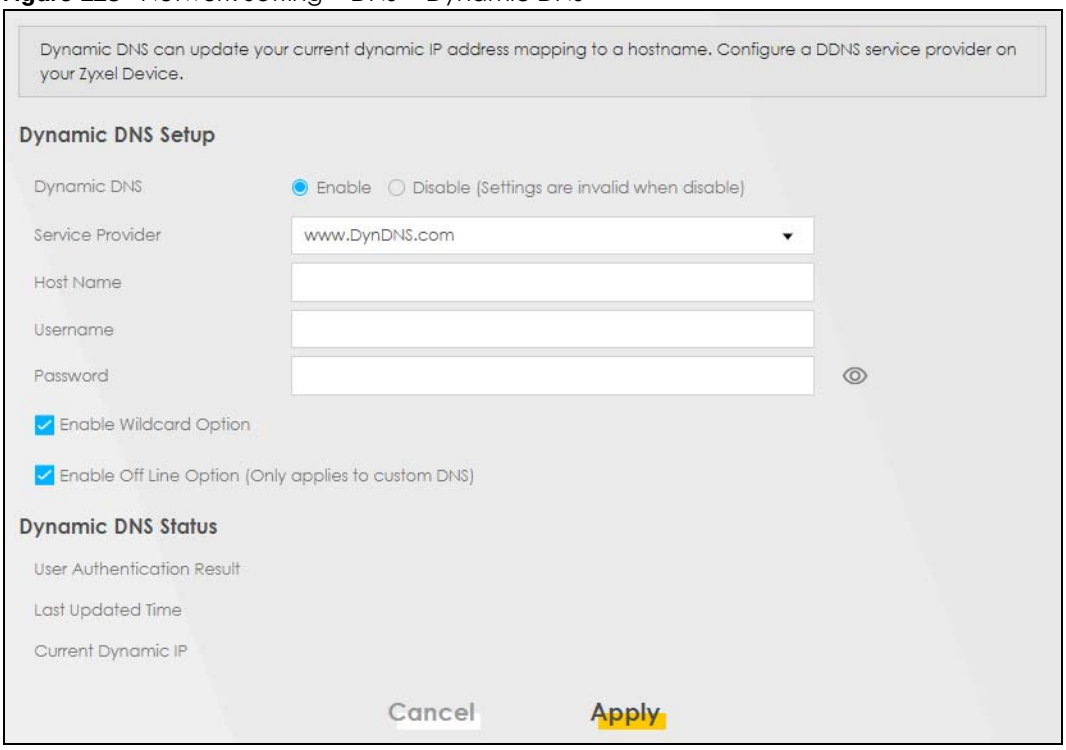
Table 73 Network Setting > DNS > DNS Entry: Add or Edit

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

## 13.3 Dynamic DNS

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

**Figure 123** Network Setting > DNS > Dynamic DNS




The following table describes the fields in this screen.

Table 74 Network Setting > DNS > Dynamic DNS

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

# CHAPTER 14
# Firewall

## 14.1 Overview

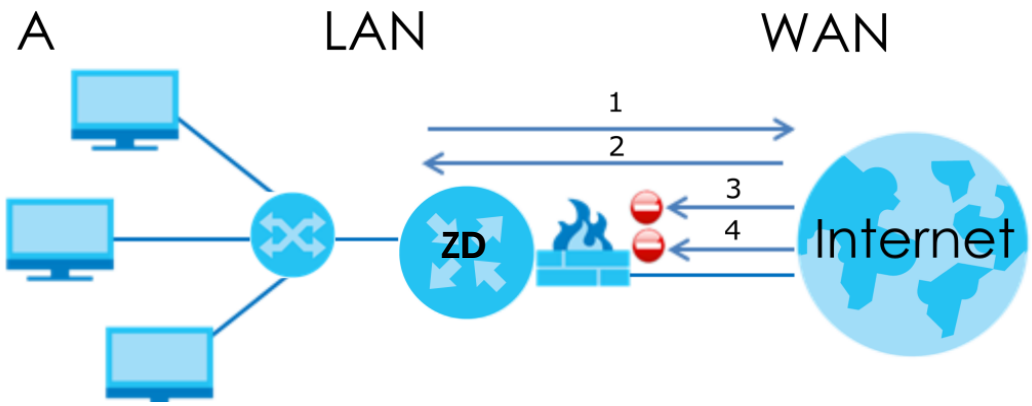
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

By default, the Zyxel Device blocks DoS attacks whether the firewall is enabled or disabled.

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

**Figure 124** Default Firewall Action




### 14.1.1 What You Need to Know About Firewall

#### SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

### DoS

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

### DoS Thresholds

For DoS attacks, the Zyxel Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

### DDoS

A Distributed Denial-of-Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

### ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

### LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

### Ping of Death

Ping of Death uses a 'ping' utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

### SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

## 14.2 Firewall

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it.

### 14.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device (Section 14.3 on page 198).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 14.4 on page 199).
- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules (Section 14.5 on page 200).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 14.6 on page 203).

## 14.3 Firewall General Settings

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

**Figure 125** Security > Firewall > General

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.
When the security level is set to **High**, Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

The following table describes the labels in this screen.

Table 75 Security > Firewall > General

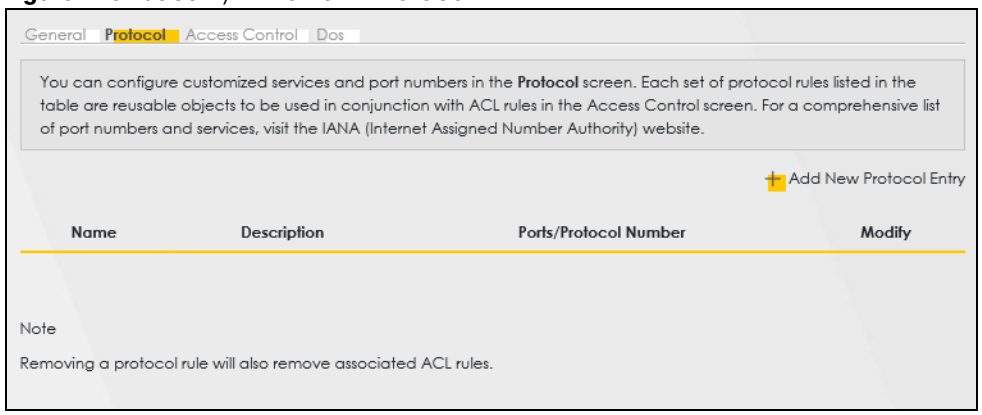
| LABEL | DESCRIPTION |
|---|---|
| IPv4 Firewall | Enable firewall protection when using **IPv4** (Internet Protocol version 4). |
| IPv6 Firewall | Enable firewall protection when using **IPv6** (Internet Protocol version 6). |
| High | This setting blocks all traffic to and from the Internet. Only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

# 14.4 Protocol (Customized Services)

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security** > **Firewall** > **Protocol** to display the following screen.

Note: Removing a protocol rule will also remove associated ACL rules.

**Figure 126** Security > Firewall > Protocol




The following table describes the labels in this screen.

Table 76 Security > Firewall > Protocol

| LABEL | DESCRIPTION |
|---|---|
| Add New Protocol Entry | Click this to configure a customized service. |
| Name | This is the name of your customized service. |
| Description | This is a description of your customized service. |

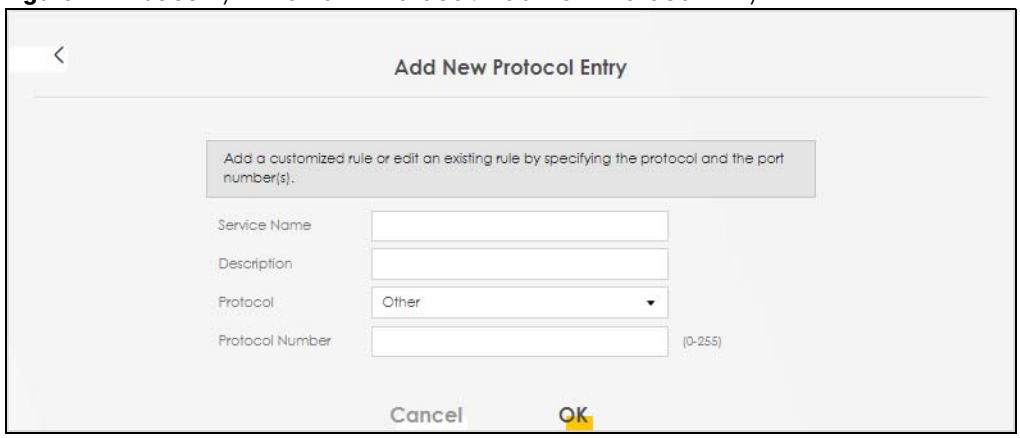
Table 76 Security > Firewall > Protocol (continued)

| LABEL | DESCRIPTION |
|---|---|
| Ports/Protocol Number | This shows the port number or range and the IP protocol (**TCP** or **UDP**) that defines your customized service. |
| Modify | Click this to edit a customized service. |

### 14.4.1 Add Customized Service

Add a customized rule or edit an existing rule by specifying the protocol and the port numbers. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

**Figure 127** Security > Firewall > Protocol: Add New Protocol Entry




The following table describes the labels in this screen.

Table 77 Security > Firewall > Protocol: Add New Protocol Entry

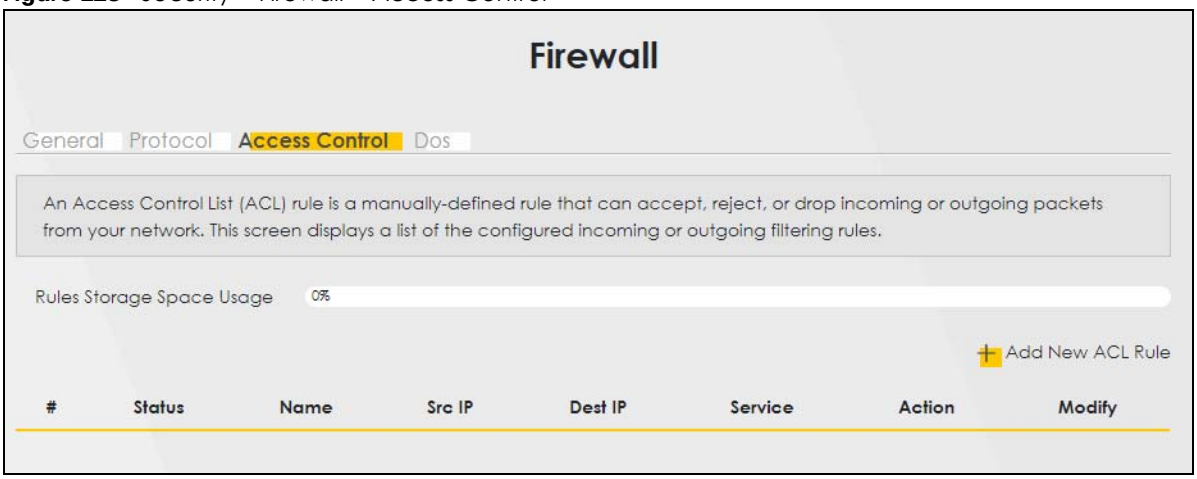
| LABEL | DESCRIPTION |
|---|---|
| Service Name | Type a unique name for your custom port. |
| Description | Enter a description for your custom port. |
| Protocol | Choose the protocol (**TCP**, **UDP**, **ICMP**, **ICMPv6**, or **Other**) that defines your customized port from the drop down list box. |
| Protocol Number | Type a single port number or the range of port numbers (**0** – **255**) that define your customized service. |
| OK | Click this to save your changes. |
| Cancel | Click this to exit this screen without saving. |

## 14.5 Access Control (Rules)

An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed. Click **Security** > **Firewall** > **Access Control** to display the following screen.

Note: The ordering of your rules is very important as rules are applied in turn.

**Figure 128** Security > Firewall > Access Control




The following table describes the labels in this screen.

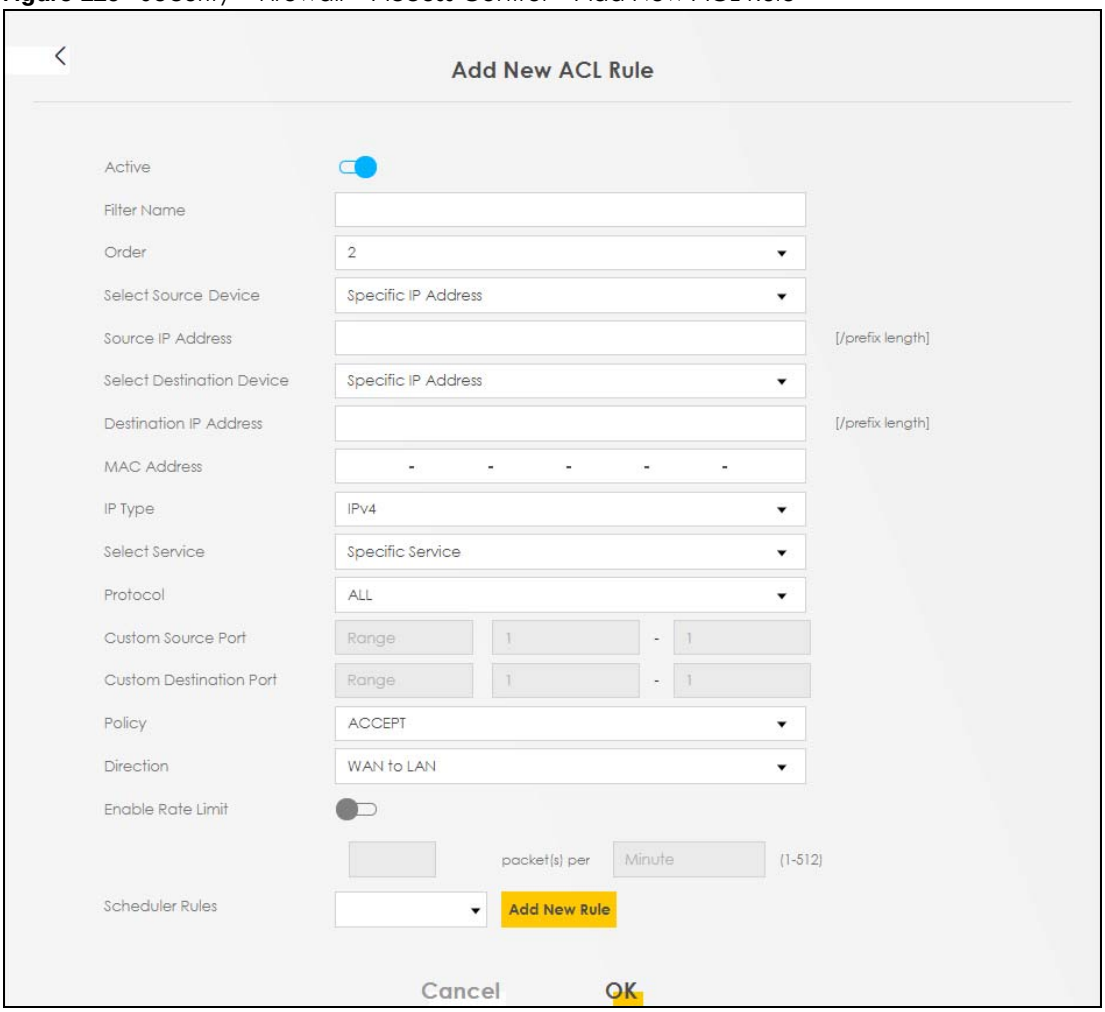
Table 78 Security > Firewall > Access Control

| LABEL | DESCRIPTION |
|---|---|
| Rules Storage Space Usage | This read-only bar shows how much of the Zyxel Device's memory is in use for recording firewall rules. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. |
| Add New ACL Rule | Select an index number and click **Add New ACL Rule** to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8. |
| # | This field displays the rule index number. The ordering of your rules is important as rules are applied in turn. |
| Status | This field displays the status of the ACL rule. A yellow bulb signifies that this ACL rule is active, while a gray bulb signifies that this ACL rule is not active. |
| Name | This field displays the rule name. |
| Src IP | This field displays the source IP addresses to which this rule applies. |
| Dest IP | This field displays the destination IP addresses to which this rule applies. |
| Service | This field displays the protocol (All, TCP, UDP, TCP/UDP, ICMP, ICMPv6, or any) used to transport the packets for which you want to apply the rule. |
| Action | Displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule. |
| Modify | Click the **Edit** icon to edit the firewall rule.<br>Click the **Delete** icon to delete an existing firewall rule. |

## 14.5.1 Add New ACL Rule

Click **Add new ACL** rule or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays. Use this screen to accept, reject, or drop packets based on specified parameters, such as source and destination IP address, IP Type, service, and direction. You can also specify a limit as to how many packets this rule applies to at a certain period of time or specify a schedule for this rule.

**Figure 129** Security > Firewall > Access Control > Add New ACL Rule




The following table describes the labels in this screen.

Table 79 Security > Firewall > Access Control > Add New ACL Rule

| LABEL | DESCRIPTION |
|---|---|
| Active | Click the **Active** button to enable this ACL rule. When the switch goes to the right ( ), the function is enabled. |
| Filter Name | Type a unique name for your filter rule. |
| Order | Assign the order of your rules as rules are applied in turn. |
| Select Source Device | If you want the source to come from a particular (single) IP, select **Specific IP Address**. If not, select from a detected device. |
| Source IP Address | If you selected **Specific IP Address** in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device. |
| Select Destination Device | If you want your rule to apply to packets with a particular (single) IP, select **Specific IP Address**. If not, select a detected device. |
| Destination IP Address | If you selected **Specific IP Address** in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device. |
| MAC Address | Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |

Table 79 Security > Firewall > Access Control > Add New ACL Rule (continued)

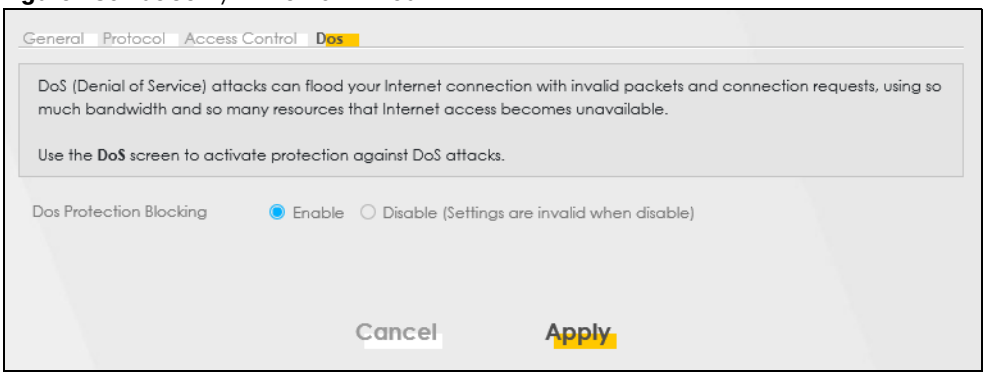
| LABEL | DESCRIPTION |
|---|---|
| IP Type | Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4**/**IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD). |
| Select Service | Select a service from the **Select Service** box. |
| Protocol | Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) used to transport the packets for which you want to apply the rule. |
| Custom Source Port | This is a single port number or the starting port number of a range that defines your rule. |
| Custom Destination Port | This is a single port number or the ending port number of a range that defines your rule. |
| Policy | Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule. |
| Direction | Select **WAN to LAN** to apply the rule to traffic from WAN to LAN. Select **LAN to WAN** to apply the rule to traffic from LAN to WAN. Select **WAN to Router** to apply the rule to traffic from WAN to router. Select **LAN to Router** to apply the rule to traffic from LAN to router. |
| OK | Click this to save your changes. |
| Cancel | Click this to exit this screen without saving. |

# 14.6 DoS

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Use the **DoS** screen to activate protection against DoS attacks.

Click **Security** > **Firewall** > **DoS** to display the following screen.

**Figure 130** Security > Firewall > DoS




The following table describes the labels in this screen.

Table 80 Security > Firewall > DoS

| LABEL | DESCRIPTION |
|---|---|
| DoS Protection Blocking | Enable this to protect against DoS attacks. The Zyxel Device will drop sessions that surpass maximum thresholds. |

Table 80 Security > Firewall > DoS

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click this to save your changes. |
| Cancel | Click this to restore your previously saved settings. |

# 14.7 Firewall Technical Reference

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

## 14.7.1 Firewall Rules Overview

Your customized rules take precedence and override the Zyxel Device's default settings. The Zyxel Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the Zyxel Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to Router
- LAN to WAN
- WAN to LAN
- WAN to Router

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

- LAN to Router

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

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

- LAN to WAN

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

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

- WAN to LAN

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

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

- WAN to Router

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

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

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

For example, you may create rules to:

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

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

### 14.7.2 Guidelines For Security Enhancement With Your Firewall

1. Change the default password through the Web Configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your router.
4. Don't enable any local service (such as telnet or FTP) that you do not use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

### 14.7.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Zyxel Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC (Internet Relay Chat) is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

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

4 Does this rule conflict with any existing rules?

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

# CHAPTER 15
# MAC Filter

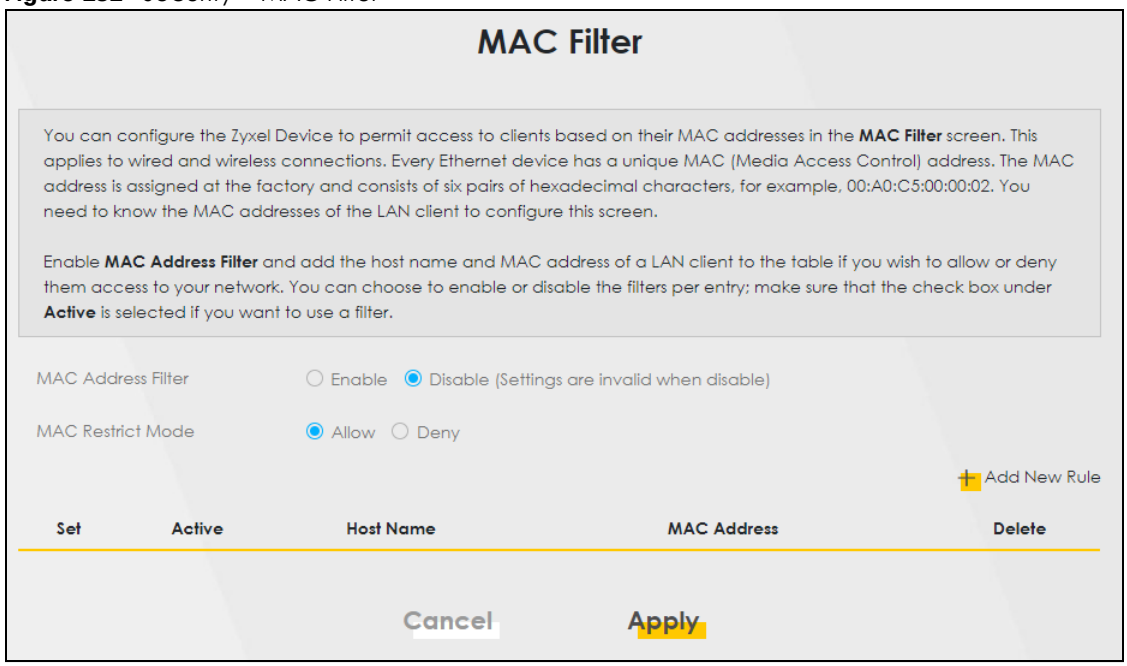
## 15.1 MAC Filter Overview

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

## 15.2 MAC Filter

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

**Figure 131** Security > MAC Filter



The following table describes the labels in this screen.

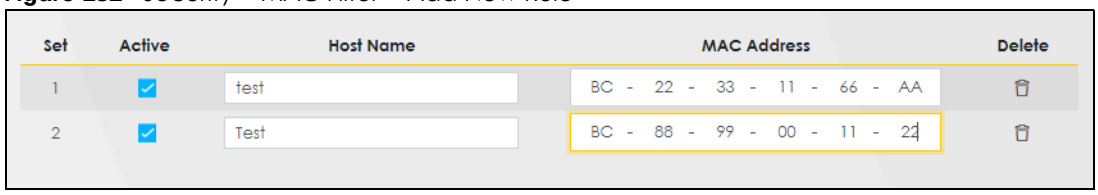
Table 81 Security > MAC Filter

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

## 15.2.1 Add New Rule

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

**Figure 132** Security > MAC Filter > Add New Rule




The following table describes the labels in this screen.

Table 82 Security > MAC Filter > Add New Rule

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

# CHAPTER 16
# Scheduler Rule

## 16.1 Scheduler Rule Overview

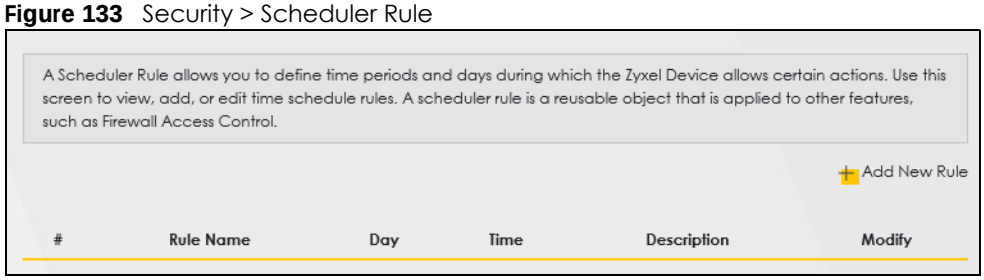
A Scheduler Rule allows you to define time periods and days during which the Zyxel Device allows certain actions.

## 16.2 Scheduler Rule Settings

Use this screen to view, add, or edit time schedule rules. A scheduler rule is a reusable object that is applied to other features, such as Firewall Access Control.

Click **Security** > **Scheduler Rule** to open the following screen.

**Figure 133** Security > Scheduler Rule




The following table describes the fields in this screen.

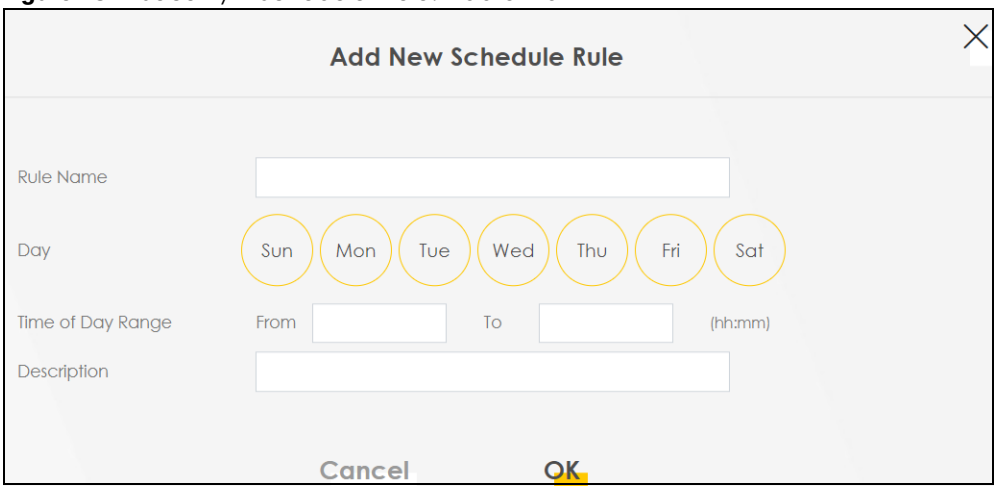
Table 83 Security > Scheduler Rule

| LABEL | DESCRIPTION |
|---|---|
| Add New Rule | Click this to create a new rule. |
| # | This is the index number of the entry. |
| Rule Name | This shows the name of the rule. |
| Day | This shows the days on which this rule is enabled. |
| Time | This shows the period of time on which this rule is enabled. |
| Description | This shows the description of this rule. |
| Modify | Click the **Edit** icon to edit the schedule.<br>Click the **Delete** icon to delete a scheduler rule.<br>Note: You cannot delete a scheduler rule once it is applied to a certain feature. |

### 16.2.1 Add or Edit a Schedule Rule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

**Figure 134** Security > Scheduler Rule: Add or Edit




The following table describes the fields in this screen.

Table 84 Security > Scheduler Rule: Add or Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Name | Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule. |
| Day | Select check boxes for the days that you want the Zyxel Device to perform this scheduler rule. |
| Time of Day Range | Enter the time period of each day, in 24-hour format, during which the rule will be enforced. |
| Description | Enter a description for this scheduler rule. |
| Cancel | Click **Cancel** to exit this screen without saving. |
| OK | Click **OK** to save your changes. |

# CHAPTER 17
# Log

## 17.1 Log Overview

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

### 17.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 17.2 on page 212).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 17.3 on page 213).

### 17.1.2 What You Need To Know

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

#### Alerts and Logs

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

#### Syslog Overview

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

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

Table 85 Syslog Severity Levels

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

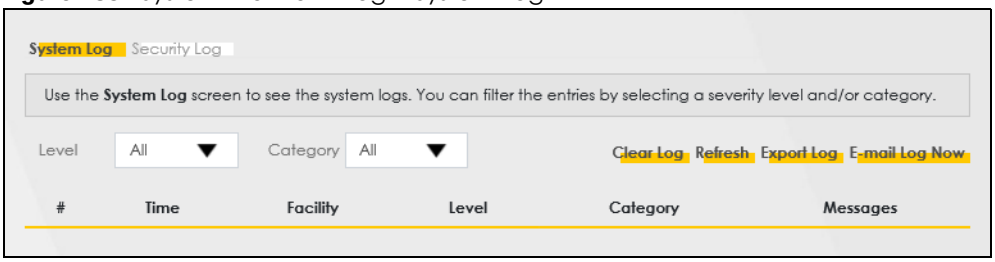
Table 85 Syslog Severity Levels (continued)

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

# 17.2 System Log

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

**Figure 135** System Monitor > Log > System Log




The following table describes the fields in this screen.

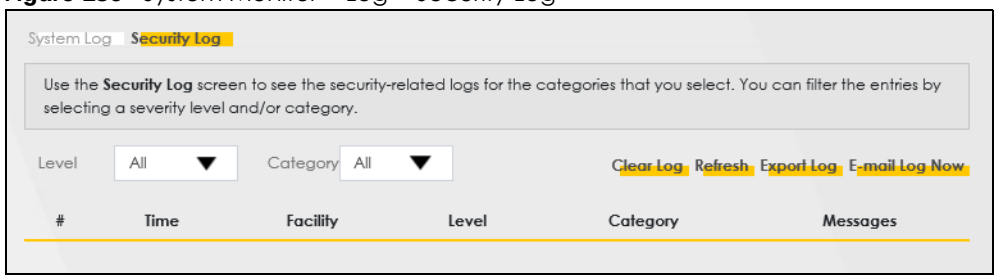
Table 86 System Monitor > Log > System Log

| LABEL | DESCRIPTION |
|---|---|
| Level | Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher. |
| Category | Select the type of logs to display. |
| Clear Log | Click this to delete all the logs. |
| Refresh | Click this to renew the log screen. |
| Export Log | Click this to export the selected logs. |
| E-mail Log Now | Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen. |
| # | This field is a sequential value and is not associated with a specific entry. |
| Time | This field displays the time the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Level | This field displays the severity level of the log that the device is to send to this syslog server. |
| Category | This field displays the type of the log. |
| Messages | This field states the reason for the log. |

# 17.3 Security Log

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

**Figure 136** System Monitor > Log > Security Log




The following table describes the fields in this screen.

Table 87 System Monitor > Log > Security Log

| LABEL | DESCRIPTION |
|---|---|
| Level | Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher. |
| Category | Select the type of logs to display. |
| Clear Log | Click this to delete all the logs. |
| Refresh | Click this to renew the log screen. |
| Export Log | Click this to export the selected logs. |
| E-mail Log Now | Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen. |
| # | This field is a sequential value and is not associated with a specific entry. |
| Time | This field displays the time the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Level | This field displays the severity level of the log that the device is to send to this syslog server. |
| Category | This field displays the type of the log. |
| Messages | This field states the reason for the log. |

# CHAPTER 18
# Traffic Status

## 18.1 Traffic Status Overview

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

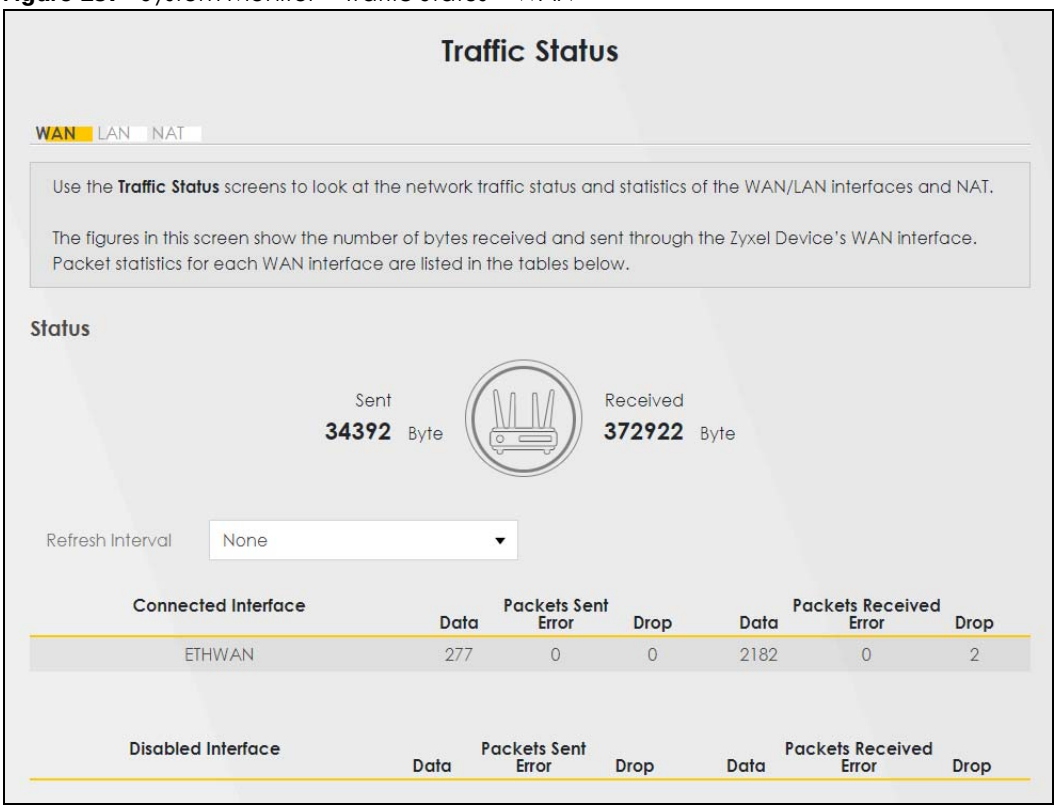
### 18.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 18.2 on page 214).
- Use the **LAN** screen to view the LAN traffic statistics (Section 18.3 on page 216).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's clients (Section 18.4 on page 217).

## 18.2 WAN Status

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

**Figure 137** System Monitor > Traffic Status > WAN




The following table describes the fields in this screen.

Table 88 System Monitor > Traffic Status > WAN

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

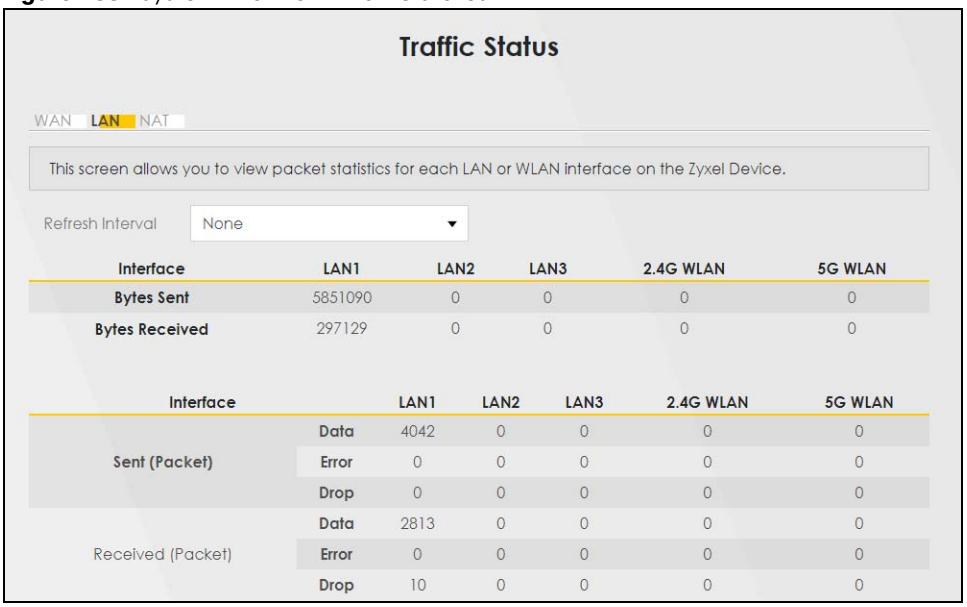
Table 88 System Monitor > Traffic Status > WAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| Error | This indicates the number of frames with errors received on this interface. |
| Drop | This indicates the number of received packets dropped on this interface. |

# 18.3 LAN Status

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

**Figure 138** System Monitor > Traffic Status > LAN




The following table describes the fields in this screen.

Table 89 System Monitor > Traffic Status > LAN

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

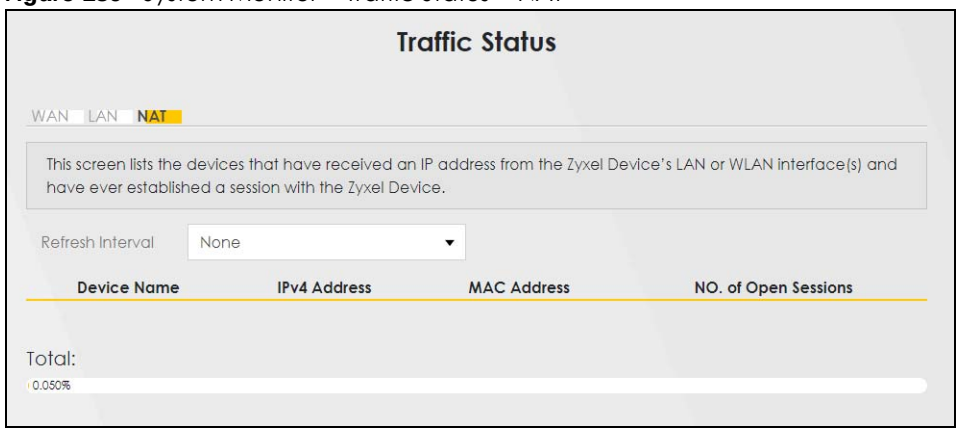
Table 89 System Monitor > Traffic Status > LAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| Error | This indicates the number of frames with errors received on this interface. |
| Drop | This indicates the number of received packets dropped on this interface. |

# 18.4 NAT Status

Click **System Monitor** > **Traffic Status** > **NAT** to open the following screen. This screen lists the devices that have received an IP address from the Zyxel Device LAN or WLAN interfaces and have ever established a session with the Zyxel Device.

**Figure 139** System Monitor > Traffic Status > NAT




The following table describes the fields in this screen.

Table 90 System Monitor > Traffic Status > NAT

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the Zyxel Device to update this screen. |
| Device Name | This displays the name of the connected host. |
| IPv4 Address | This displays the IP address of the connected host. |
| MAC Address | This displays the MAC address of the connected host. |
| No. of Open Session | This displays the number of NAT sessions currently opened for the connected host. |
| Total | This displays what percentage of NAT sessions the Zyxel Device can support is currently being used by all connected hosts. You can also see the number of active NAT sessions and the maximum number of NAT sessions the Zyxel Device can support |

# CHAPTER 19
# ARP Table

## 19.1 ARP Table Overview

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

An IP version 4 address is 32 bits long. MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

### 19.1.1 How ARP Works

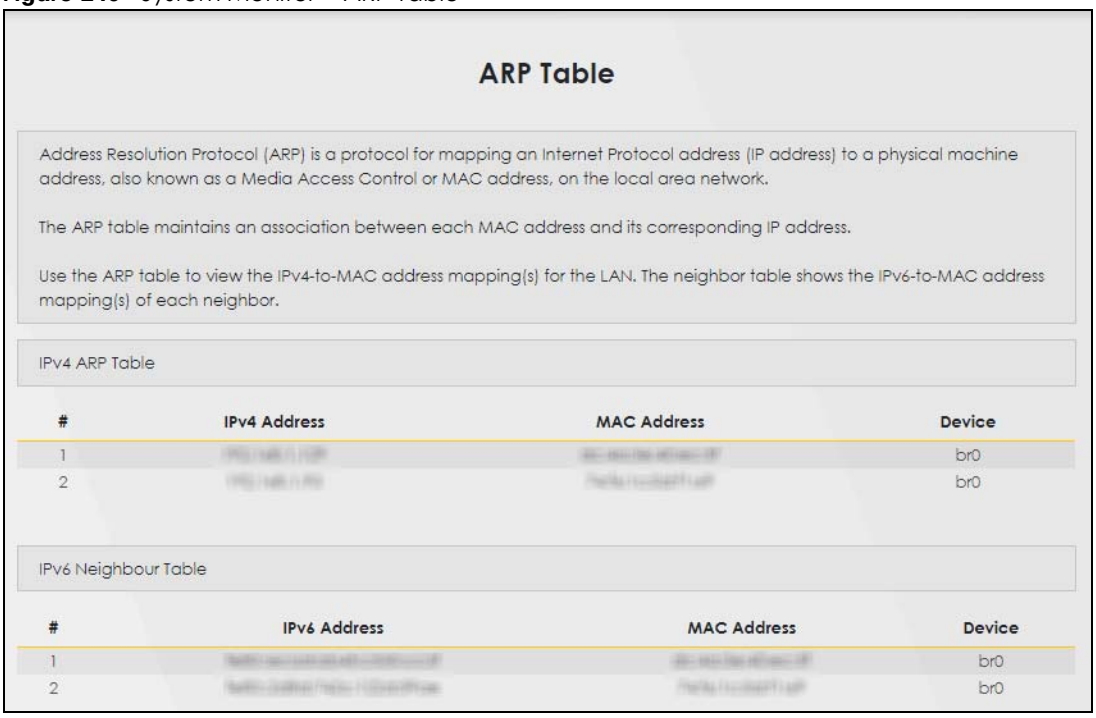
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP table for future reference and then sends the packet to the MAC address that replied.

## 19.2 ARP Table

Use the ARP table to view the IPv4-to-MAC address mappings for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mappings of each IPv6 neighbor. To open this screen, click **System Monitor** > **ARP Table**.

**Figure 140** System Monitor > ARP Table




The following table describes the labels in this screen.

Table 91 System Monitor > ARP Table

| LABEL | DESCRIPTION |
|---|---|
| # | This is the ARP table entry number. |
| IPv4 / IPv6 Address | This is the learned IPv4 or IPv6 IP address of a device connected to a port. |
| MAC Address | This is the MAC address of the device with the listed IP address. |
| Device | This is the type of interface used by the device. You can click the device type to go to its configuration screen. |

# CHAPTER 20
# Routing Table

## 20.1 Routing Table Overview

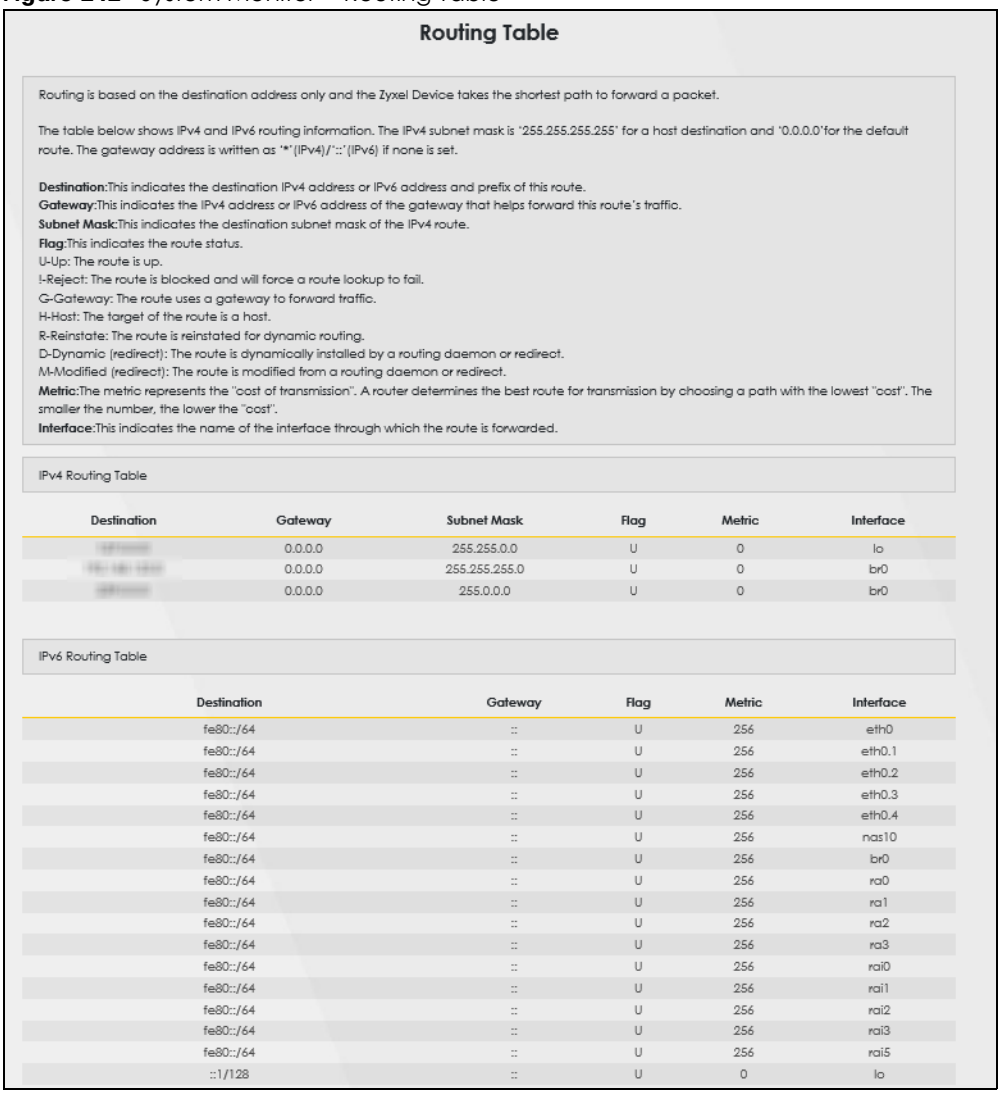
Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

## 20.2 Routing Table

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

Click **System Monitor** > **Routing Table** to open the following screen.

**Figure 141** System Monitor > Routing Table



**Routing Table**

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

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

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

IPv4 Routing Table

| Destination | Gateway | Subnet Mask | Flag | Metric | Interface |
|---|---|---|---|---|---|
| [illegible] | 0.0.0.0 | 255.255.0.0 | U | 0 | lo |
| [illegible] | 0.0.0.0 | 255.255.255.0 | U | 0 | br0 |
| [illegible] | 0.0.0.0 | 255.0.0.0 | U | 0 | br0 |

IPv6 Routing Table

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

The following table describes the labels in this screen.

Table 92 System Monitor > Routing Table

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

Table 92 System Monitor > Routing Table (continued)

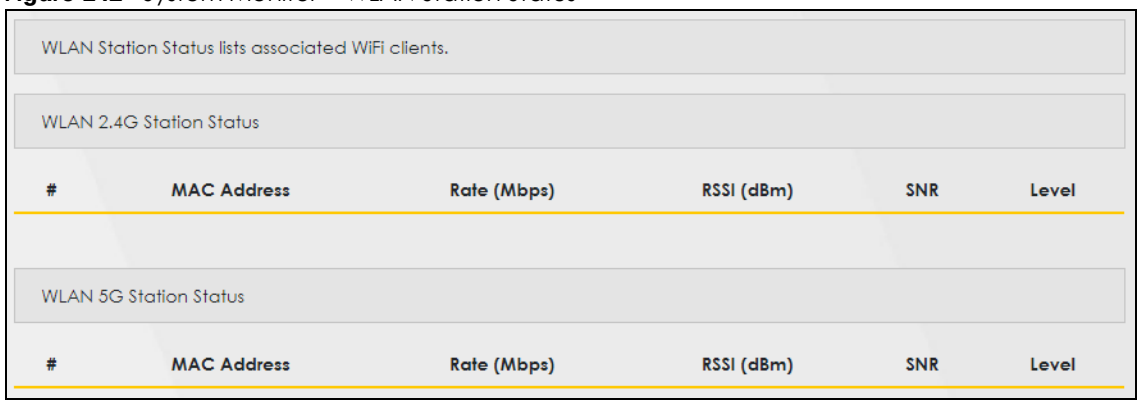
| LABEL | DESCRIPTION |
|---|---|
| Flag | This indicates the route status.<br>**U–Up:** The route is up.<br>**!–Reject:** The route is blocked and will force a route lookup to fail.<br>**G–Gateway:** The route uses a gateway to forward traffic.<br>**H–Host:** The target of the route is a host.<br>**R–Reinstate:**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

# CHAPTER 21
# WLAN Station Status

## 21.1 WLAN Station Status Overview

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

**Figure 142** System Monitor > WLAN Station Status




The following table describes the labels in this screen.

Table 93 System Monitor > WLAN Station Status

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

Table 93 System Monitor > WLAN Station Status (continued)

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

# CHAPTER 22
# Operating Mode

## 22.1 Overview

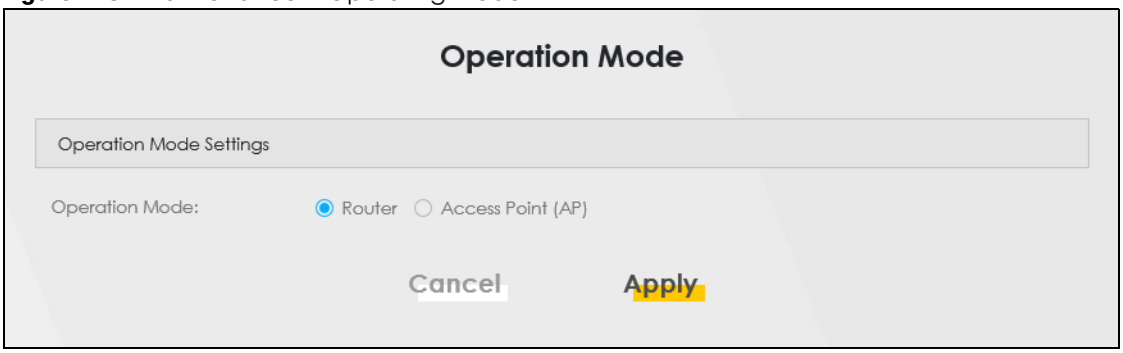
Use this screen to select how you want to use your Zyxel Device. The Operating Mode function lets you configure your Zyxel Device as a router or access point. You can choose between **Router** Mode, and **Access Point (AP)** Mode depending on your network topology and the features you require from your Zyxel Device.

Click **Maintenance > Operating Mode** to show the following screen. The Zyxel Device has the following operating modes:

• **Router**: This is the Zyxel Device's default mode. In this mode, the Zyxel Device routes traffic between a local network and another network such as the Internet.

• **Access Point (AP)**: Use this mode if you already have a router in your network and want to use the Zyxel Device as an access point to bridge a wired network (LAN) and another LAN or wireless LAN (WLAN) in the same subnet.

**Figure 143** Maintenance > Operating Mode




The following table describes the labels in this screen.

Table 94 Maintenance > Operating Mode

| LABEL | DESCRIPTION |
|---|---|
| Operating Mode Settings | |
| Operating Mode | Select **Router** to use the Zyxel Device as a router. Select **Access Point (AP)** to use the Zyxel Device as an access point. |
| Cancel | Click **Cancel** to restore your previously saved settings. |
| Apply | Click **Apply** to save your changes. |

# CHAPTER 23
# System

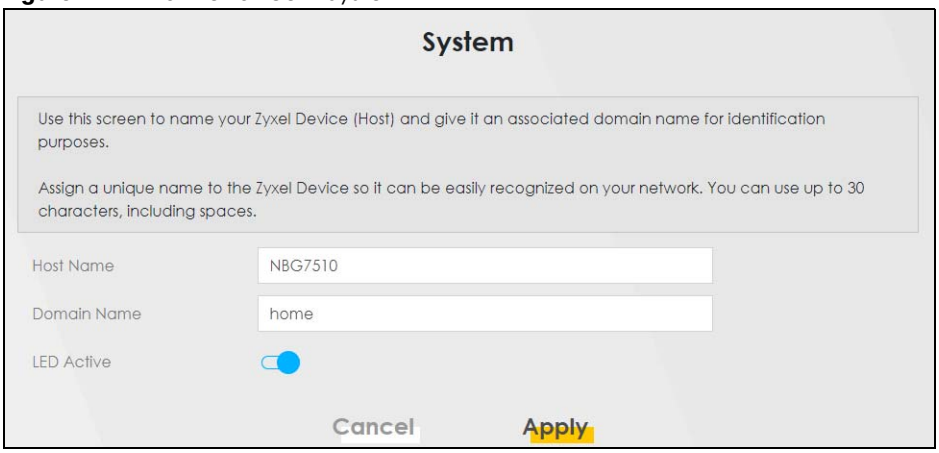
## 23.1 System Overview

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

## 23.2 System

Click **Maintenance** > **System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 alphanumeric characters except [ ? ], [ | ], [ ' ], [ " ] or [ , ].

**Figure 144** Maintenance > System




The following table describes the labels in this screen.

Table 95 Maintenance > System

| LABEL | DESCRIPTION |
|---|---|
| Host Name | Type a host name for your Zyxel Device. Enter a descriptive name of up to 30 alphanumeric characters except [ ? ], [ \| ], [ ' ], [ " ] or [ , ].<br><br>For some models, the supported maximum input length is 16 alphanumeric characters. |
| Domain Name | Type a domain name for your host Zyxel Device. |
| Cancel | Click **Cancel** to abandon this screen without saving. |
| Apply | Click **Apply** to save your changes. |

# CHAPTER 24
# User Account

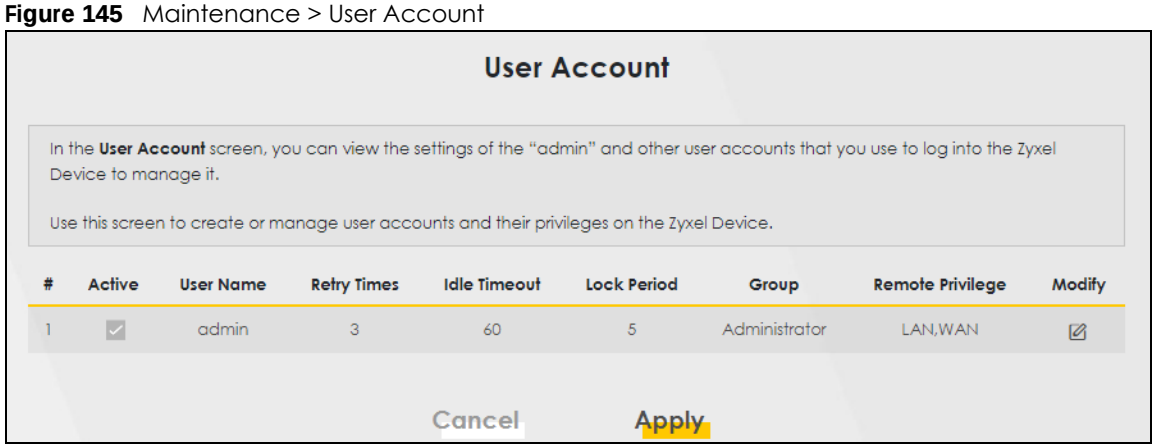
## 24.1 User Account Overview

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

## 24.2 User Account

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

**Figure 145** Maintenance > User Account




The following table describes the labels in this screen.

Table 96 Maintenance > User Account

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number. |
| Active | This indicates whether the user account is active or not.<br><br>The check box is selected when the user account is enabled. It is cleared when it is disabled. |
| User Name | This displays the name of the account used to log into the Zyxel Device Web Configurator. |
| Retry Times | This displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit. |
| Idle Timeout | This displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator. |
| Lock Period | This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**. |
| Group | This field displays whether this user has **Administrator** or **User** privileges. |

Table 96 Maintenance > User Account (continued)

| LABEL | DESCRIPTION |
|---|---|
| Remote Privilege | This field displays whether this user can access the Zyxel Device with HTTP, Telnet or SSH through the **WAN**, **LAN** or **LAN/WAN**. |
| Modify | Click the **Edit** icon to configure the entry. |
| Cancel | Click **Cancel** to restore your previously saved settings. |
| Apply | Click **Apply** to save your changes. |

# CHAPTER 25
# Remote Management

## 25.1 Overview

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

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

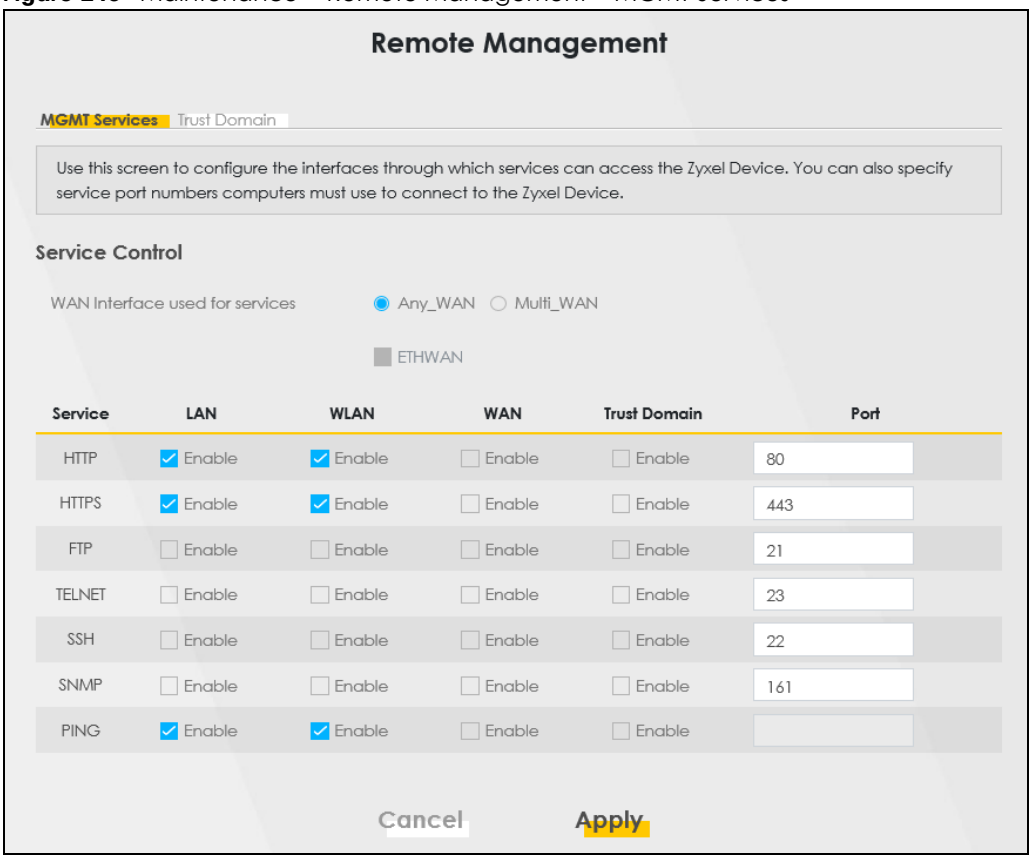
### 25.1.1 What You Can Do in this Chapter

- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 25.2 on page 229).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 25.3 on page 231).

## 25.2 MGMT Services

Use this screen to configure the interfaces through which services can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance** > **Remote Management** > **MGMT Services** to open the following screen.

**Figure 146** Maintenance > Remote Management > MGMT Services




The following table describes the fields in this screen.

Table 97 Maintenance > Remote Management > MGMT Services

| LABEL | DESCRIPTION |
|---|---|
| Service Control | |
| WAN Interface used for services | Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up.<br><br>Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up. |
| ETHWAN | Enable the Ethernet WAN connection configured in **Network Setting** > **Broadband** > **Ethernet WAN** to access the service on the Zyxel Device. |
| Service | This is the service you may use to access the Zyxel Device. |
| LAN | Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN. |
| WLAN | Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the WLAN. |
| WAN | Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections. |
| Trust Domain | Select the **Enable** check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address. |
| Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |

Table 97 Maintenance > Remote Management > MGMT Services

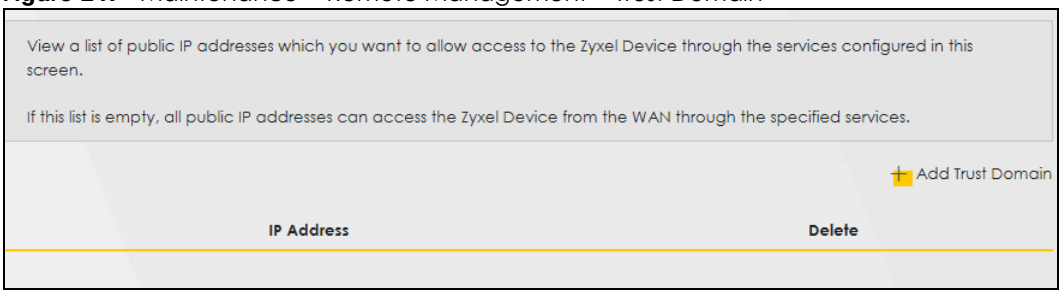
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the Zyxel Device. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

# 25.3 Trust Domain

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

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

**Figure 147** Maintenance > Remote Management > Trust Domain




The following table describes the fields in this screen.

Table 98 Maintenance > Remote Management > Trust Domain

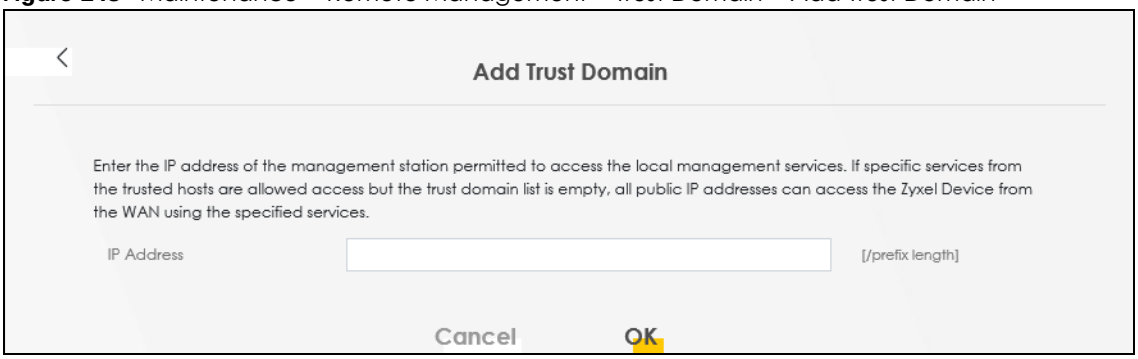
| LABEL | DESCRIPTION |
|---|---|
| Add Trust Domain | Click this to add a trusted host IP address. |
| IP Address | This field shows a trusted host IP address. |
| Delete | Click the **Delete** icon to remove the trusted host IP address. |

# 25.4 Add Trust Domain

Use this screen to add a public IP addresses or a complete domain name of a device which is allowed to access the Zyxel Device. Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted-hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Click the **Add Trust Domain** button in the **Maintenance** > **Remote Management** > **Trust Domain** screen to open the following screen.

**Figure 148** Maintenance > Remote Management > Trust Domain > Add Trust Domain




The following table describes the fields in this screen.

Table 99 Maintenance > Remote Management > Trust Domain > Add Trust Domain

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

# CHAPTER 26
# Time Settings

## 26.1 Time Settings Overview

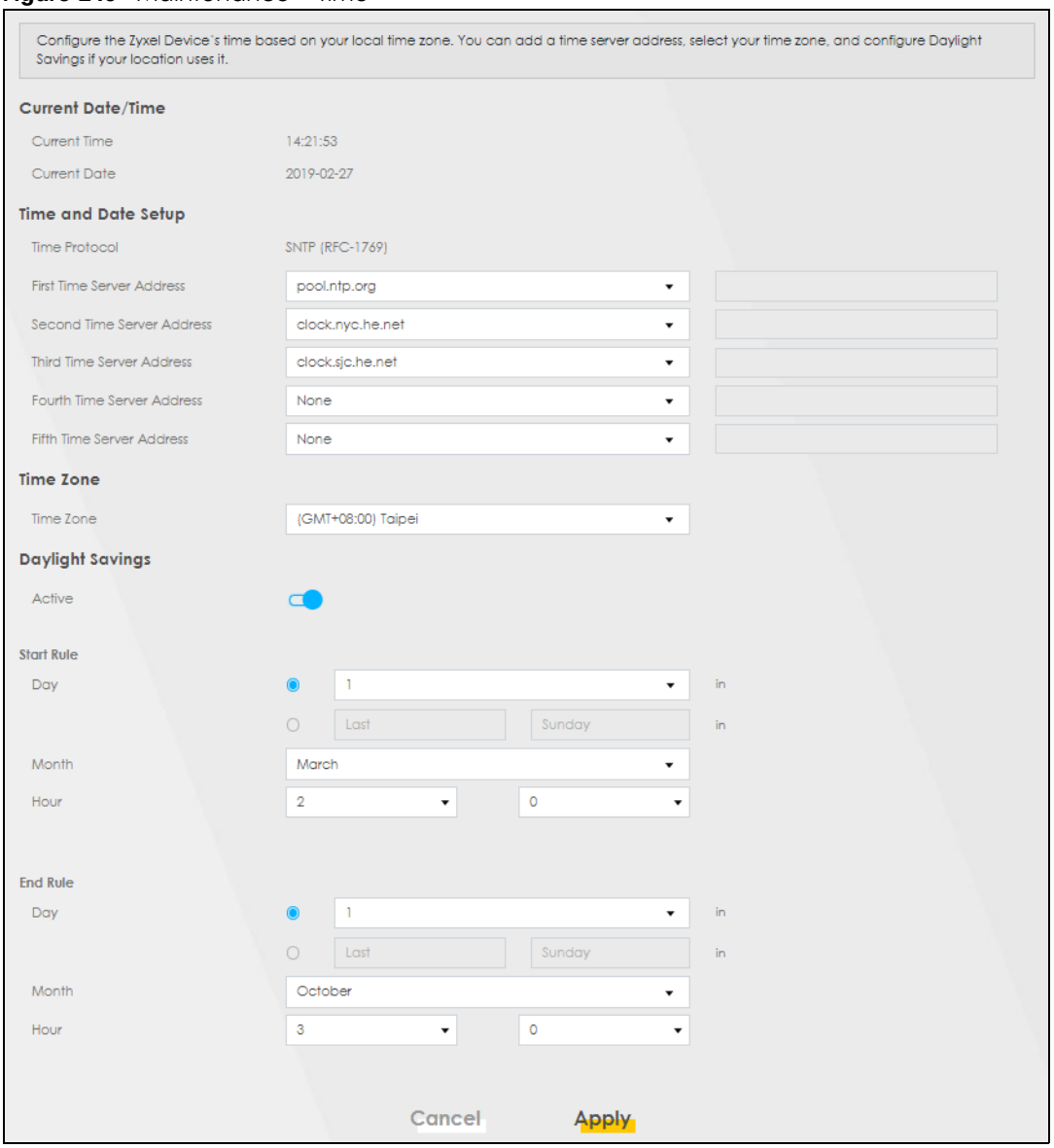
This chapter shows you how to configure system related settings, such as system date and time.

## 26.2 Time

For effective scheduling and logging, the Zyxel Device system time must be accurate. Use this screen to configure the Zyxel Device's time based on your local time zone. You can enter a time server address, select the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings if needed.

To change your Zyxel Device's time and date, click **Maintenance** > **Time**. The screen appears as shown.

**Figure 149** Maintenance > Time




The following table describes the fields in this screen.

Table 100 Maintenance > Time

| LABEL | DESCRIPTION |
|---|---|
| Current Date/Time | |
| Current Time | This displays the time of your Zyxel Device.<br>Each time you reload this screen, the Zyxel Device synchronizes the time with the time server. |
| Current Date | This displays the date of your Zyxel Device.<br>Each time you reload this screen, the Zyxel Device synchronizes the date with the time server. |
| Time and Date Setup | |
| Time Protocol | This displays the time protocol used by your Zyxel Device. |

Table 100 Maintenance > Time (continued)

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

# CHAPTER 27
# Email Notification

## 27.1 Email Notification Overview

A mail server is an application or a computer that can receive, forward and deliver email messages.

To have the Zyxel Device send reports, logs or notifications through email, you must specify an email server and the email addresses of the sender and receiver.

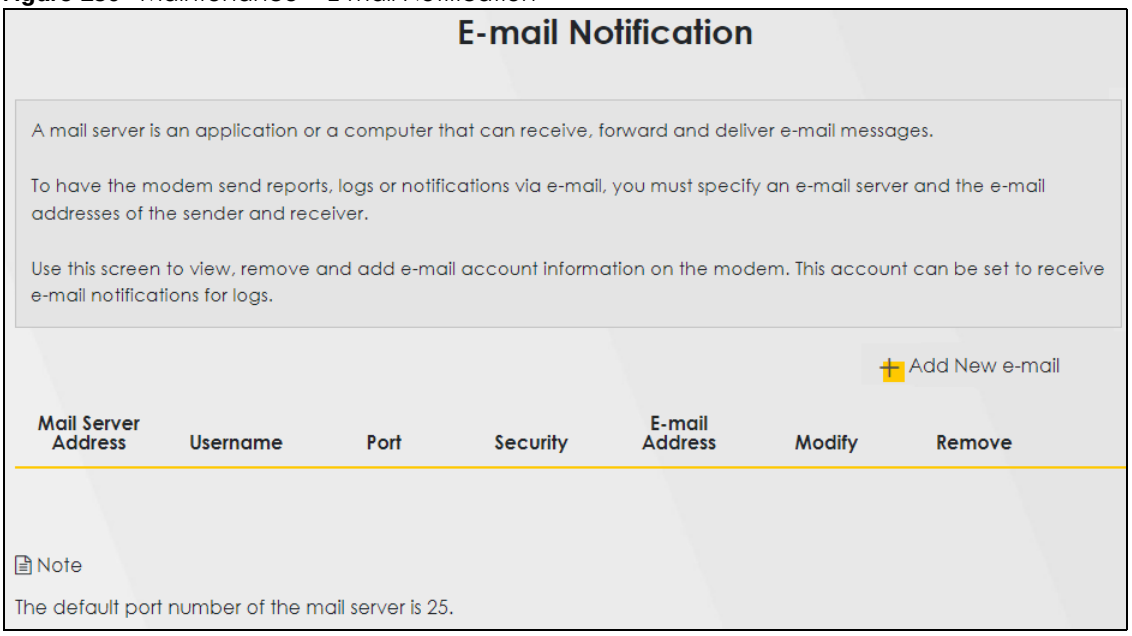
## 27.2 Email Notification

Use this screen to view, remove and add email account information on the Zyxel Device. This account can be set to send email notifications for logs.

Click **Maintenance** > **E-mail Notification** to open the **E-mail Notification** screen.

Note: The default port number of the mail server is 25.

**Figure 150** Maintenance > E-mail Notification



The following table describes the labels in this screen.

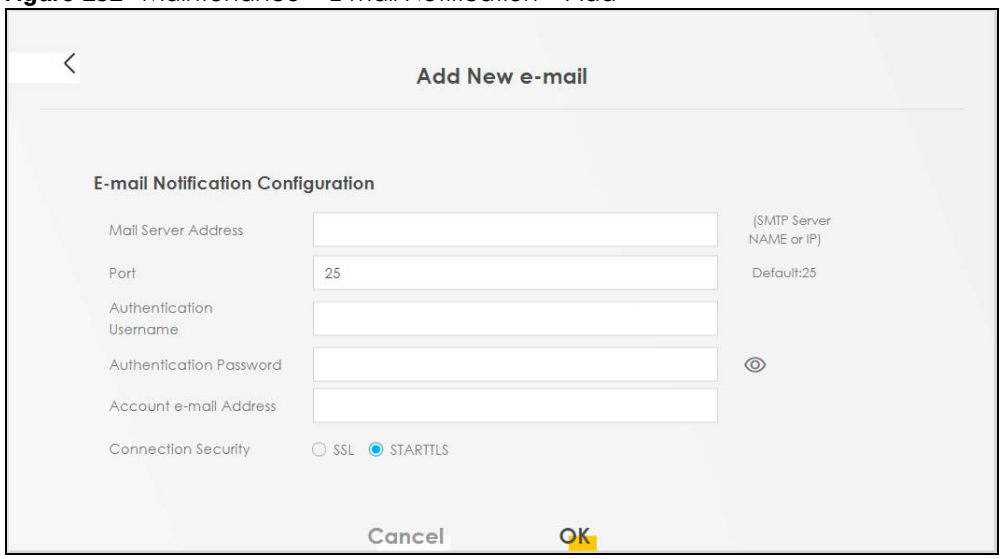
Table 101 Maintenance > E-mail Notification

| LABEL | DESCRIPTION |
|---|---|
| Add New e-mail | Click this button to create a new entry (up to 32 can be created). |
| Mail Server Address | This displays the server name or the IP address of the mail server. |
| Username | This displays the user name of the sender's mail account. |
| Port | This field displays the port number of the mail server. |
| Security | This field displays the protocol used for encryption. |
| E-mail Address | This field displays the email address that you want to be in the from or sender line of the email that the Zyxel Device sends. |
| Modify | Click the **Edit** icon to configure the entry.<br>Click the **Delete** icon to remove the entry. |
| Remove | Click this button to delete the selected entries. |

## 27.2.1 E-mail Notification Edit

Click the **Add** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending email through a mail server.

**Figure 151** Maintenance > E-mail Notification > Add




The following table describes the labels in this screen.

Table 102 Maintenance > E-mail Notification > Add

| LABEL | DESCRIPTION |
|---|---|
| Mail Server Address | Enter the server name or the IP address of the mail server for the email address specified in the **Account e-mail Address** field.<br><br>If this field is left blank, reports, logs or notifications will not be sent through email. |
| Port | Enter the same port number here as is on the mail server for mail traffic. |
| Authentication Username | Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account email Address** field. |

Table 102 Maintenance > E-mail Notification > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Password | Enter the password associated with the user name above. |
| Account e-mail Address | Enter the email address that you want to be in the from or sender line of the email notification that the Zyxel Device sends.<br><br>If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well. |
| Connection Security | Select **SSL** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device.<br><br>Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS. |
| Cancel | Click this button to begin configuring this screen afresh. |
| OK | Click this button to save your changes and return to the previous screen. |

# CHAPTER 28
# Log Setting

## 28.1 Log Setting Overview

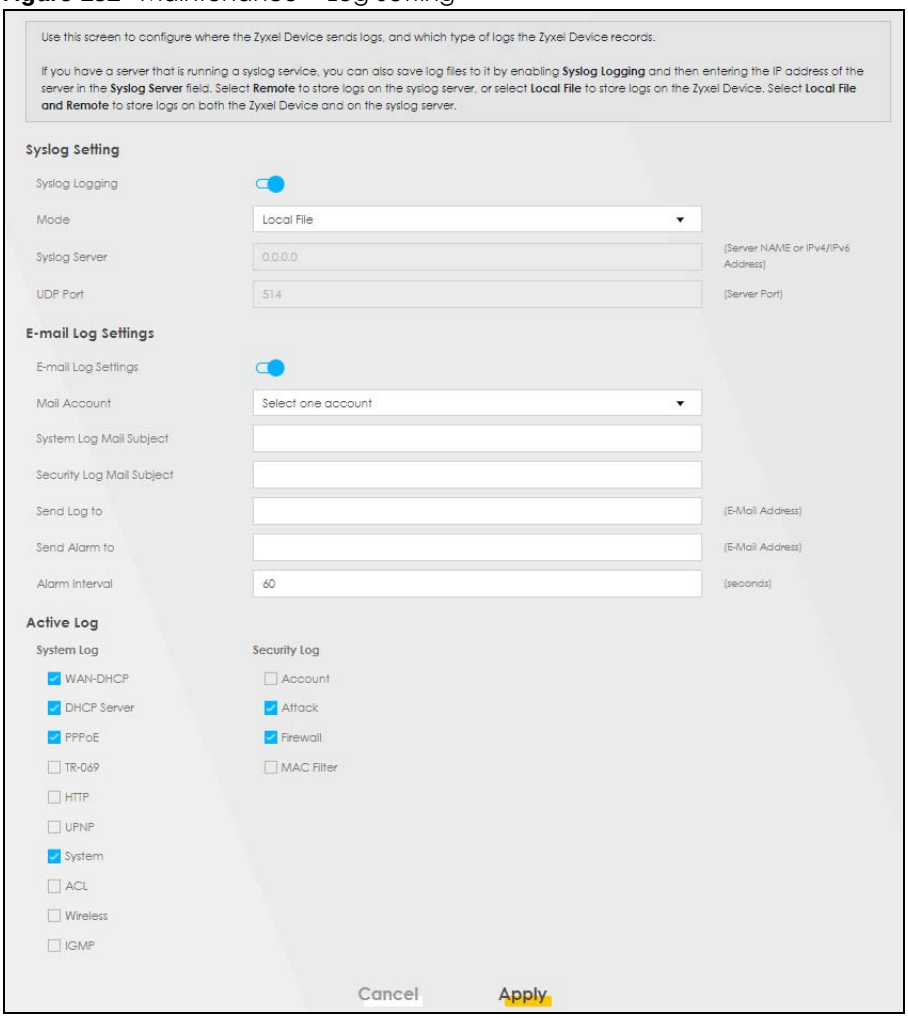
You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the **Logs Setting** screen.

## 28.2 Log Setting

Use this screen to configure where the Zyxel Device sends logs, and which type of logs the Zyxel Device records.

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging**, and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the Zyxel Device. Select **Local File and Remote** to store logs on both the Zyxel Device and the syslog server. To change your Zyxel Device's log settings, click **Maintenance** > **Log Setting**. The screen appears as shown.

**Figure 152** Maintenance > Log Setting




The following table describes the fields in this screen.

Table 103 Maintenance > Log Setting

| LABEL | DESCRIPTION |
|---|---|
| Syslog Settings | |
| Syslog Logging | Click the switch (it will turn blue) to enable syslog logging. |
| Mode | Select **Remote** to have the Zyxel Device send it to an external syslog server.<br>Select **Local File** to have the Zyxel Device save the log file on the Zyxel Device itself.<br>Select **Local File and Remote** to have the Zyxel Device save the log file on the Zyxel Device itself and send it to an external syslog server.<br>Note: A warning appears upon selecting **Remote** or **Local File and Remote**. Just click **OK** to continue. |
| Syslog Server | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| UDP Port | Enter the port number used by the syslog server. |
| E-mail Log Settings | |

Table 103 Maintenance > Log Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| E-mail Log Settings | Click the switch (it will turn blue) to allow the sending through email the system and security logs to the email address specified in **Send Log to**.<br><br>Note: Make sure that the **Mail Server Address** field is not left blank in the **Maintenance** > **E-mail Notifications** screen. |
| Mail Account | Select a server specified in **Maintenance** > **E-mail Notifications** to send the logs to. |
| System Log Mail Subject | This field allows you to enter a descriptive name for the system log email (for example Zyxel System Log). Up to 127 characters are allowed for the **System Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~]. |
| Security Log Mail Subject | This field allows you to enter a descriptive name for the security log email (for example Zyxel Security Log). Up to 127 characters are allowed for the **Security Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~]. |
| Send Log to | This field allows you to enter the log's designated email recipient. The log's format is plain text file sent as an email attachment. |
| Send Alarm to | This field allows you to enter the alarm's designated e-mail recipient. The alarm's format is plain text file sent as an email attachment. |
| Alarm Interval | Select the frequency of showing of the alarm. |
| Active Log | |
| System Log | Select the categories of **System Log**s that you want to record. |
| Security Log | Select the categories of **Security Log**s that you want to record. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to restore your previously saved settings. |

## 28.2.1 Example Email Log

An 'End of Log' message displays for each mail in which a complete log has been sent. The following is an example of a log sent by email.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- '`End of Log`' message shows that a complete log has been sent.

**Figure 153** Email Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……................{snip}……................
……................{snip}……................
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

# CHAPTER 29
# Firmware Upgrade

## 29.1 Overview

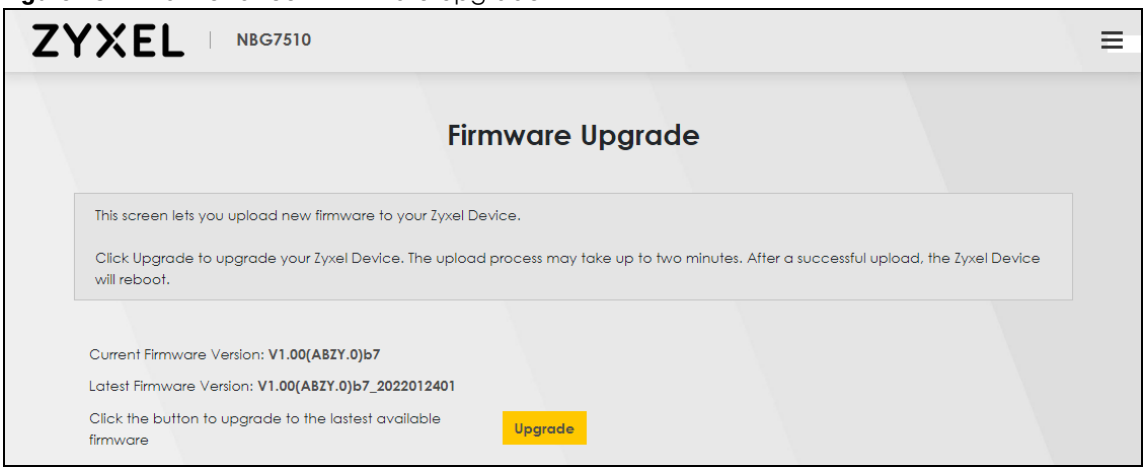
This chapter explains how to upgrade new firmware for your Zyxel Device. You can check and download new firmware online to upgrade your Zyxel Device's performance.

## 29.2 Firmware Upgrade

Click **Maintenance** > **Firmware Upgrade** to open the **following** screen. Click the **Upgrade** button to update to the latest available firmware. The **Upgrade** button is available only when the latest firmware update is available.

**Do NOT turn off the Zyxel Device while firmware upload is in progress!**

**Figure 154** Maintenance > Firmware Upgrade



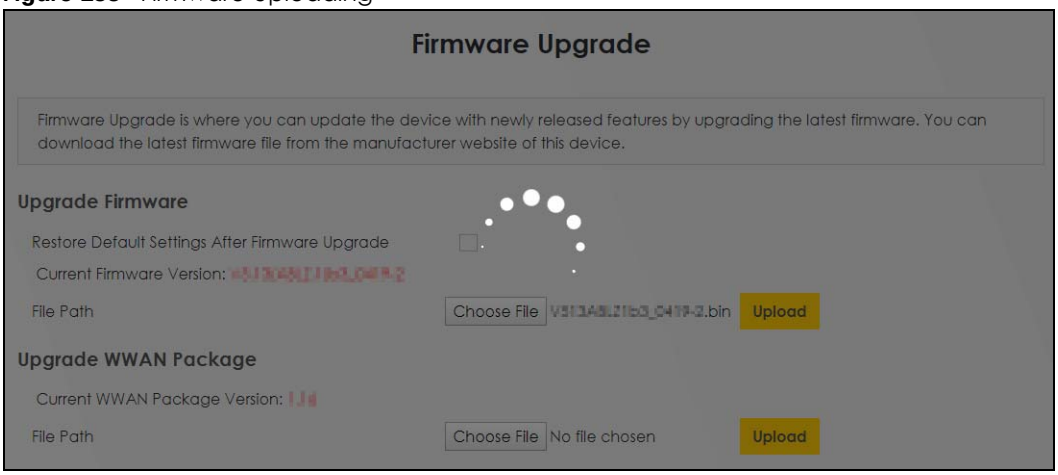

The following table describes the labels in this screen.

Table 104 Maintenance > Firmware Upgrade

| LABEL | DESCRIPTION |
|---|---|
| Upgrade Firmware | |
| Current Firmware Version | This is the current firmware version. |
| Latest Firmware Version | This is the latest firmware version. |

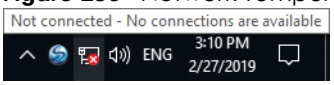
After you see the firmware updating screen, wait a few minutes before logging into the Zyxel Device again.

**Figure 155** Firmware Uploading




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

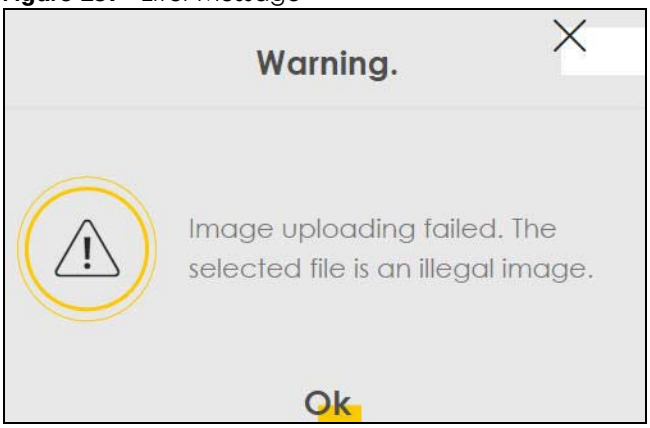
**Figure 156** Network Temporarily Disconnected




After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

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

**Figure 157** Error Message




# 29.3 Module Upgrade

This screen lets you upload new firmware specific to the built-in LTE module in order to improve the LTE module's reliability and performance. The upload process uses HTTP (Hypertext Transfer Protocol) and may take more than 3 minutes. After a successful upload, the Zyxel Device will reboot.

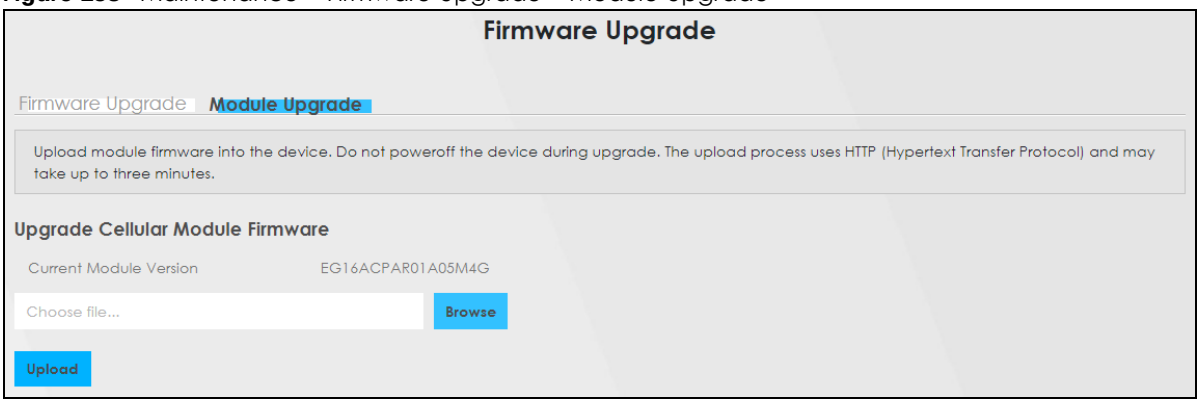
Note: Use this screen to upload LTE module firmware only when you are instructed by Zyxel technical support team and provided with new LTE firmware release.

Note: Available for LTE5388-S905, LTE7480-S905, and LTE7485-S905 models only.

Click **Maintenance** > **Firmware Upgrade** > **Module Upgrade** to open the **following** screen.

**Do NOT turn off the Zyxel Device while module firmware upload is in progress!**

**Figure 158** Maintenance > Firmware Upgrade > Module Upgrade




The following table describes the labels in this screen.

Table 105 Maintenance > Firmware Upgrade > Module Upgrade

| LABEL | DESCRIPTION |
|---|---|
| Upgrade Cellular Module Firmware | |
| Current Module Version | This is the current module firmware version. |
| Choose file... | Enter the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it. |
| Choose File/ Browse | Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click this to begin the upload process. This process may take more than 3 minutes. |

# CHAPTER 30
# Backup/Restore

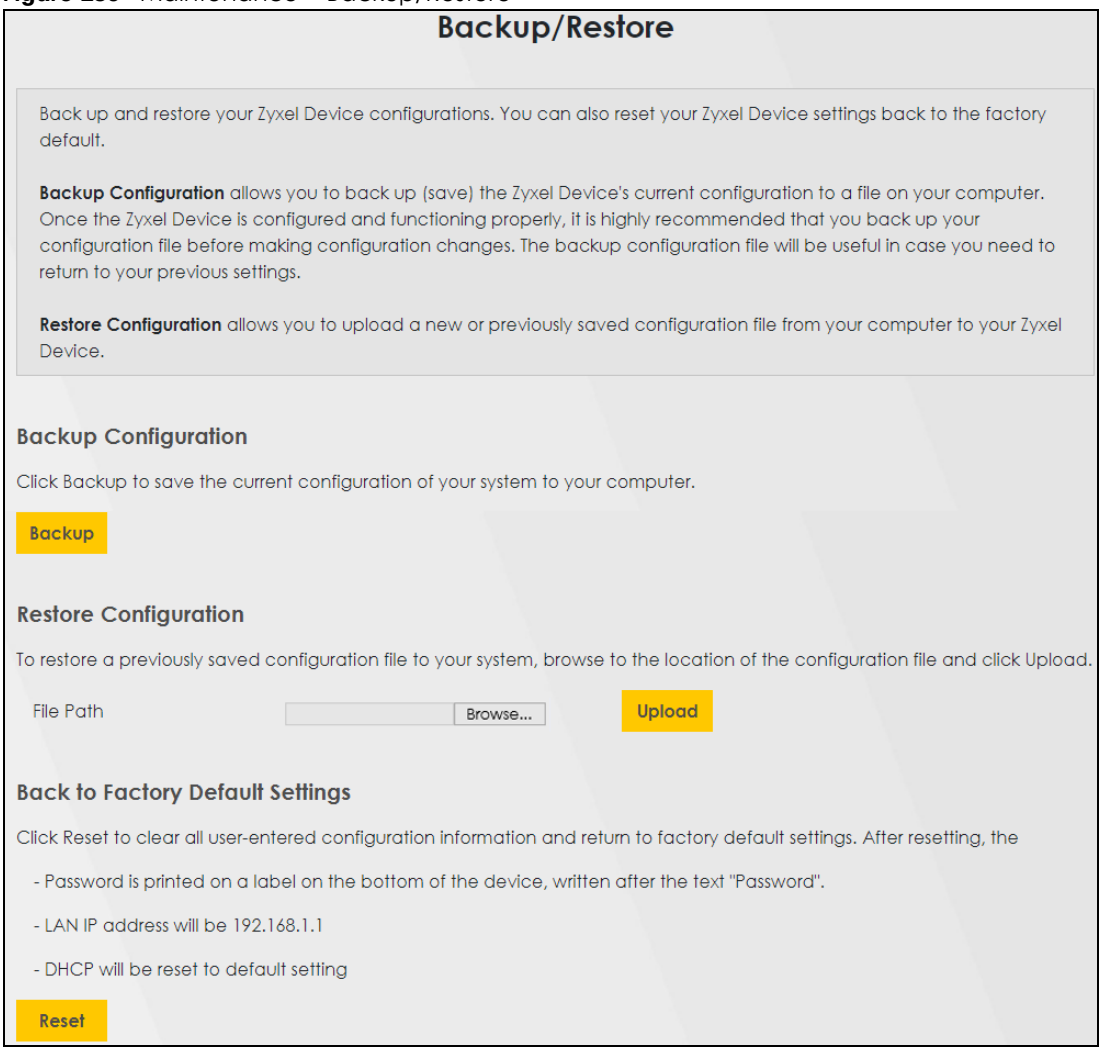
## 30.1 Backup/Restore Overview

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

## 30.2 Backup/Restore

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

**Figure 159** Maintenance > Backup/Restore




## Backup Configuration

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

Click **Backup** to save the Zyxel Device's current configuration to your computer.

## Restore Configuration

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

Table 106 Maintenance > Backup/Restore: Restore Configuration

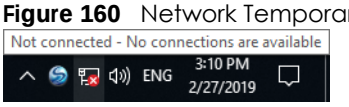
| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Choose File** / **Browse** to find it. |
| Choose File / Browse | Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Upload | Click this to begin the upload process. |
| Reset | Click this to reset your Zyxel Device settings back to the factory default. |

**Do not turn off the Zyxel Device while configuration file upload is in progress.**

After the Zyxel Device configuration has been restored successfully, the login screen appears. Login again to restart the Zyxel Device.

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

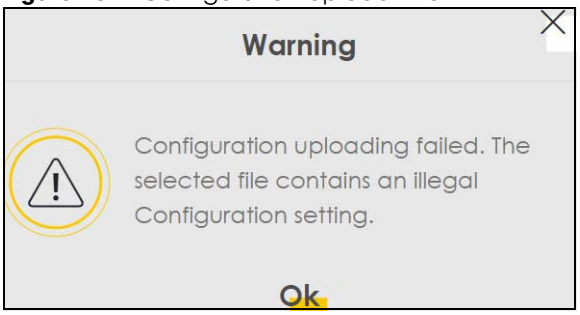
**Figure 160** Network Temporarily Disconnected




If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default Zyxel Device IP address (192.168.1.1192.168.123.1).

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

**Figure 161** Configuration Upload Error




## Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Zyxel Device to its factory defaults. The following warning screen appears.

**Figure 162** Reset Warning Message

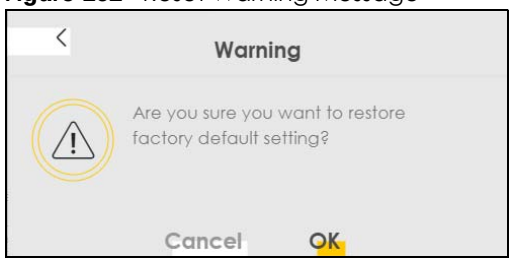
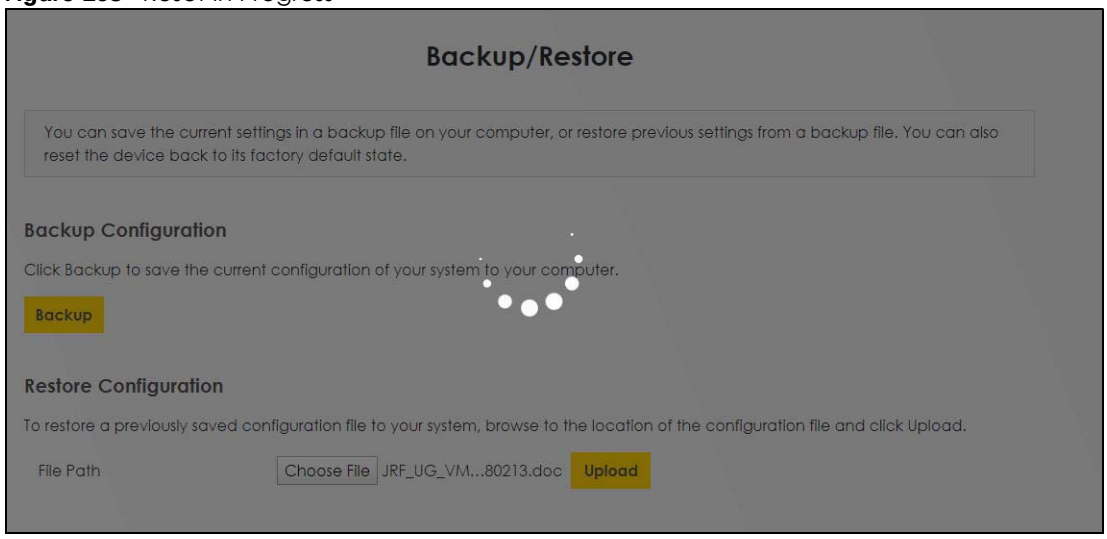



**Figure 163** Reset In Progress



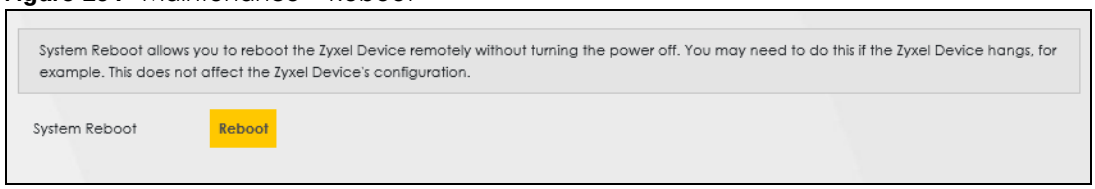

You can also press the **RESET** button on the panel to reset the factory defaults of your Zyxel Device.

# 30.3 Reboot

System **Reboot** allows you to reboot the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example. This does not affect the Zyxel Device's configuration.

Click **Maintenance** > **Reboot**. Click **Reboot** to have the Zyxel Device reboot.

**Figure 164** Maintenance > Reboot



# CHAPTER 31
# Diagnostic

## 31.1 Diagnostic Overview

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

### 31.1.1 What You Can Do in this Chapter

- The **Diagnostic** screen lets you ping an IP address or trace the route packets take to a host (Section 31.2 on page 250).

## 31.2 Diagnostic

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

Click **Maintenance** > **Diagnostic** to open the following screen.

**Figure 165** Maintenance > Diagnostic

The following table describes the fields in this screen.

Table 107 Maintenance > Diagnostic

| LABEL | DESCRIPTION |
|---|---|
| Ping/TraceRoute Test (Diagnostic Test) | The result of tests is shown here in the info area. |
| TCP/IP | |
| Address | Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection. |
| Ping | Click this button to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area. |
| Ping 6 | Click this button to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area. |
| Trace Route | Click this button to perform the IPv4 trace route function. This determines the path a packet takes to the specified host. |
| Trace Route 6 | Click this button to perform the IPv6 trace route function. This determines the path a packet takes to the specified host. |
| Nslookup | Click this button to perform a DNS lookup on the IP address or host name. |

# PART III
# Troubleshooting and Appendices

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

# CHAPTER 32
# Troubleshooting

## 32.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power and Hardware Problems
- Device Access Problems
- Internet Problems
- WiFi Problems
- UPnP Problems

## 32.2 Power and Hardware Problems

### The Zyxel Device does not turn on.

1. Make sure you are using the power adapter included with the Zyxel Device.
2. Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adapter to the Zyxel Device.
4. Make sure you have pressed the **POWER** button to turn on the Zyxel Device.
5. If the problem continues, contact the vendor.

### The LED does not behave as expected.

1. Make sure you understand the normal behavior of the LED.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the Zyxel Device off and on.

5 If the problem continues, contact the vendor.

## 32.3 Device Access Problems

### I do not know the IP address of the Zyxel Device.

1 The default IP address is 192.168.123.1

2 If you changed the IP address, you might be able to find the IP address of the Zyxel Device by looking up the IP address of your computer's default gateway. To do this in Microsoft Windows, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device, depending on your network environment.

3 If this does not work, reset the Zyxel Device to its factory defaults.

### I forgot the admin password.

1 See the Zyxel Device label or this document's cover page for the default admin password.

2 If you changed the password from default and cannot remember the new one, you have to reset the Zyxel Device to its factory default settings.

### I cannot access the Web Configurator login screen.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.123.1.
- If you changed the IP address (Section 10.2 on page 145), use the new IP address.
- If you changed the IP address and have forgotten the new address, see the troubleshooting suggestions for I do not know the IP address of the Zyxel Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance** > **Remote Management**).

5 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

## I cannot log into the Zyxel Device.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These both user name and password are case-sensitive, so make sure [Caps Lock] is not on.

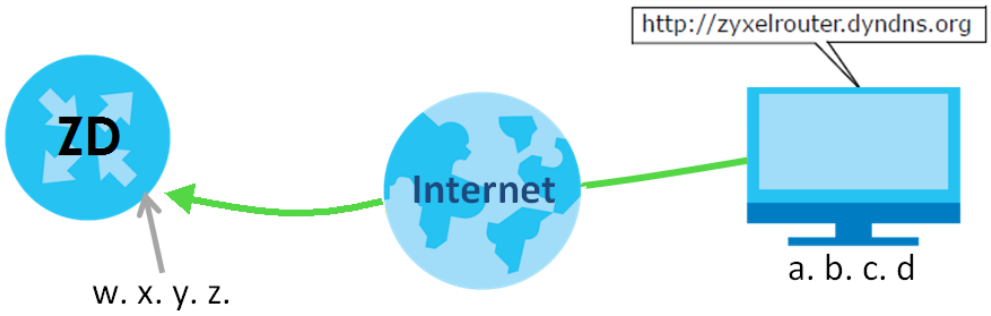
2 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

3 Turn the Zyxel Device off and on.

4 If this does not work, you have to reset the Zyxel Device to its factory default.

## I cannot log into the Zyxel Device using DDNS.

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.




To use this feature, you have to apply for DDNS service at www.dyndns.org.

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

Here are the three steps to use a domain name to log in the Web Configurator:

**Step 1 Register for a DDNS Account on www.dyndns.org**

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

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

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

**Step 2 Configure DDNS on Your Zyxel Device**

Configure the following settings in the **Network Setting** > **DNS** > **Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**). Click **Apply**.

**Step 3 Test the DDNS Setting**

Now you should be able to access the Zyxel Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

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

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

## I cannot connect to the Zyxel Device using FTP, Telnet, SSH, or Ping.

1 See the Remote Management section for details on allowing web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) to access the Zyxel Device.

2 Check the server **Port** number field for the web service in the **Maintenance** > **Remote Management** screen. You must use the same port number in order to use that web service for remote management.

3 Try the troubleshooting suggestions for I cannot access the Web Configurator login screen. Ignore the suggestions about your browser.

# 32.4 Internet Problems

## I cannot access the Internet.

1. Check the hardware connections and make sure the LEDs are behaving as expected. See the **Quick Start Guide**.
2. Make sure you entered your ISP account information correctly on the **Network Setting** > **Broadband** screen. Fields on this screen are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure that you enabled the WiFi in the Zyxel Device and your WiFi client and that the WiFi settings in the WiFi client are the same as the settings in the Zyxel Device.
4. Disconnect all the cables from your device and reconnect them.
5. If the problem continues, contact your ISP.

## I cannot connect to the Internet using an Ethernet connection.

1. Make sure you have the Ethernet WAN port connected to a Modem or Router.
2. Make sure you configured a proper Ethernet WAN interface (**Network Setting** > **Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
3. Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting** > **Interface Group**).
4. If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **Network Setting** > **Home Networking** > **LAN Setup** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

## The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. Look at the LEDs, and check the LED section for more information. If the signal strength is low, try moving the Zyxel Device closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Turn the Zyxel Device off and on.

4 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions in I cannot access the Web Configurator login screen..

## 32.5 WiFi Problems

### The WiFi connection is slow and intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other WiFi devices.

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

- Move your WiFi device closer to the AP if the signal strength is low.
- Reduce WiFi interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the WiFi client.
- Reduce the number of WiFi clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Place the Zyxel Device where there are minimum obstacles (such as walls and ceilings) between the Zyxel Device and the wireless client. Avoid placing the Zyxel Device inside any type of box that might block WiFi signals.

## 32.6 UPnP Problems

### My computer cannot detect UPnP settings from the Zyxel Device.

1 Make sure that UPnP is enabled in your computer. For Windows 10, see Section 10.9 on page 158.

2 On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings** > **Home Networking** > **UPnP** screen. See Section 10.4 on page 151 for details.

3 Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.

4 Reconnect the Ethernet cable.

**5** Restart your computer.

# APPENDIX A
# Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communications offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Networks offices, see *https://www.zyxel.com/index.shtml* for the latest information.

Please have the following information ready when you contact an office.

### Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

## Corporate Headquarters (Worldwide)

### Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com

## Asia

### China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

### India

- Zyxel Technology India Pvt Ltd.
- https://www.zyxel.com/in/en/

### Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

### Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

### Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

### Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

### Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

### Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

### Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

### Thailand

- Zyxel Thailand Co., Ltd.
- https://www.zyxel.com/th/th/

### Vietnam

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

## Europe

### Belarus

- Zyxel BY
- https://www.zyxel.by

### Bulgaria

- Zyxel България
- https://www.zyxel.com/bg/bg/

### Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

### Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

### Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

### France

- Zyxel France
- https://www.zyxel.fr

### Germany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

### Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

### Italy

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

### Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

### Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

### Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

### Romania

- Zyxel Romania

- https://www.zyxel.com/ro/ro

### Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

### Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

### Spain

- Zyxel Communications ES Ltd.
- https://www.zyxel.com/es/es/

### Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

### Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

### Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

### UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

### Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

## South America

### Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

### Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

### Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

### Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

### South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

## Middle East

### Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

## North America

### USA

- Zyxel Communications, Inc. – North America Headquarters
- https://www.zyxel.com/us/en/

# APPENDIX B
# IPv6

## Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x $10^{38}$ IP addresses.

## IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

## Prefix and Prefix Length

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

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

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

## Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 108 Link-local Unicast Address Format

| | | |
|---|---|---|
| 1111 1110 10 | 0 | Interface ID |
| 10 bits | 54 bits | 64 bits |

## Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

## Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

## Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

## Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 109 Predefined Multicast Address

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

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

Table 110 Reserved Multicast Address

| MULTICAST ADDRESS |
|---|
| FF00:0:0:0:0:0:0:0 |
| FF01:0:0:0:0:0:0:0 |
| FF02:0:0:0:0:0:0:0 |
| FF03:0:0:0:0:0:0:0 |
| FF04:0:0:0:0:0:0:0 |
| FF05:0:0:0:0:0:0:0 |
| FF06:0:0:0:0:0:0:0 |
| FF07:0:0:0:0:0:0:0 |
| FF08:0:0:0:0:0:0:0 |
| FF09:0:0:0:0:0:0:0 |
| FF0A:0:0:0:0:0:0:0 |
| FF0B:0:0:0:0:0:0:0 |
| FF0C:0:0:0:0:0:0:0 |
| FF0D:0:0:0:0:0:0:0 |
| FF0E:0:0:0:0:0:0:0 |
| FF0F:0:0:0:0:0:0:0 |

## Subnet Masking

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

## Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

## EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

**Table 111**

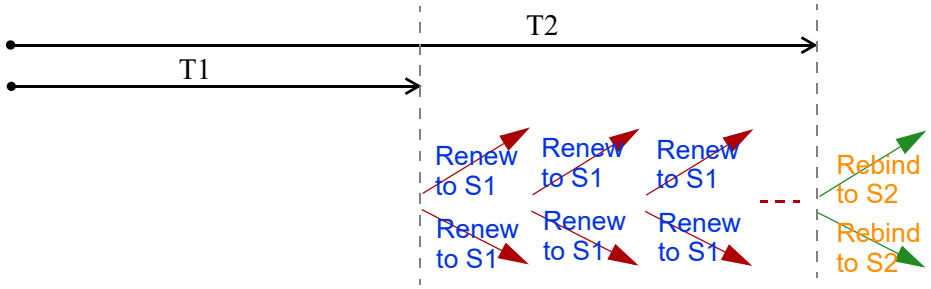
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **MAC** | 00 | : | 13 | : | 49 | : | 12 | : | 34 | : | 56 |

**Table 112**

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **EUI-64** | 02 | : | 13 | : | 49 | : | FF | : | FE | : | 12 | : | 34 | : | 56 |

## Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



## DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

## Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

## ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

## Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

## IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device

receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

## Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

## MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

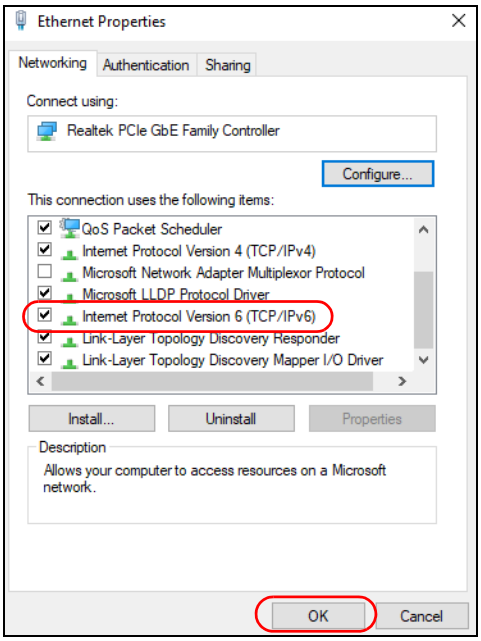
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected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

## Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 10 computer.

To enable IPv6 in Windows 10:

1. Click the start icon, **Settings** and then **Network & Internet**.
2. Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
3. Click **OK** to save the change.




4 Click the Search icon ( ) and then type "cmd" in the search box..

5 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:f
```

# APPENDIX C
# Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 113 Examples of Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM | TCP | 5190 | AOL's Internet Messenger service. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP/UDP<br>TCP/UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP | TCP<br>TCP | 20<br>21 | File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by email. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IMAP4 | TCP | 143 | The Internet Message Access Protocol is used for email. |
| IMAP4S | TCP | 993 | This is a more secure version of IMAP4 that runs over SSL. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NetBIOS | TCP/UDP<br>TCP/UDP<br>TCP/UDP<br>TCP/UDP | 137<br>138<br>139<br>445 | The Network Basic Input/Output System is used for communication between computers in a LAN. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |

Table 113 Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| NFS | UDP | 2049 | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get email from a POP3 server through a temporary connection (TCP/IP or other). |
| POP3S | TCP | 995 | This is a more secure version of POP3 that runs over SSL. |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| ROADRUNNER | TCP/UDP | 1026 | This is an ISP that provides services mainly for cable modems. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | The Simple File Transfer Protocol is an old way of transferring files between computers. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another. |
| SMTPS | TCP | 465 | This is a more secure version of SMTP that runs over SSL. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSDP | UDP | 1900 | The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP). |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |

Table 113 Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| VDOLIVE | TCP<br>UDP | 7000<br>user-defined | A videoconferencing solution. The UDP port number is specified in the application. |

# APPENDIX D
# Legal Information

## Copyright

Copyright © 2022 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates..

Published by Zyxel and/or its affiliates. All rights reserved.

## Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## Regulatory Notice and Statement

### UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

#### FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

#### FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

### EUROPEAN UNION and UNITED KINGDOM

The following information applies if you use the product within the European Union and United Kingdom.

## Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Regulation

- Compliance information forwireless products relevant to the EU, United Kingdom. and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU, United Kingdom, and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.
- The maximum RF power operating for each band as follows:
  - the band 2,400 to 2,483.5 MHz is 98.17 mW,
  - the bands 5,150 MHz to 5,350 MHz is194.54 mW,
  - the 5,470 MHz to 5,725 MHz is 977.24 mW.

| | |
|---|---|
| Български (Bulgarian) | С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.<br>**National Restrictions**<br>• The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.<br>• Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.<br>• Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails. |
| Español (Spanish) | Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.. |
| Čeština (Czech) | Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. |
| Dansk (Danish) | Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.<br>**National Restrictions**<br>• In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.<br>• I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs. |
| Deutsch (German) | Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet. |
| Eesti keel (Estonian) | Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| Ελληνικά (Greek) | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU. |
| English | Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. |
| Français (French) | Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU. |
| Hrvatski (Croatian) | Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU. |
| Íslenska (Icelandic) | Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU. |
| Italiano (Italian) | Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.<br>**National Restrictions**<br>• This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.<br>• Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli. |
| Latviešu valoda (Latvian) | Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.<br>**National Restrictions**<br>• The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.<br>• 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv. |
| Lietuvių kalba (Lithuanian) | Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas. |

| | |
|---|---|
| Magyar (Hungarian) | Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak. |
| Malti (Maltese) | Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU. |
| Nederlands (Dutch) | Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. |
| Polski (Polish) | Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU. |
| Português (Portuguese) | Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU. |
| Română (Romanian) | Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/EU. |
| Slovenčina (Slovak) | Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU. |
| Slovenščina (Slovene) | Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. |
| Suomi (Finnish) | Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| Svenska (Swedish) | Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. |
| Norsk (Norwegian) | Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU. |

**Notes:**

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

### List of national codes

| COUNTRY | ISO 3166 2 LETTER CODE | COUNTRY | ISO 3166 2 LETTER CODE |
|---|---|---|---|
| Austria | AT | Liechtenstein | LI |
| Belgium | BE | Lithuania | LT |
| Bulgaria | BG | Luxembourg | LU |
| Croatia | HR | Malta | MT |
| Cyprus | CY | Netherlands | NL |
| Czech Republic | CZ | Norway | NO |
| Denmark | DK | Poland | PL |
| Estonia | EE | Portugal | PT |
| Finland | FI | Romania | RO |
| France | FR | Serbia | RS |
| Germany | DE | Slovakia | SK |
| Greece | GR | Slovenia | SI |
| Hungary | HU | Spain | ES |
| Iceland | IS | Switzerland | CH |
| Ireland | IE | Sweden | SE |
| Italy | IT | Turkey | TR |
| Latvia | LV | United Kingdom | GB |

## Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.

- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not obstruct the device ventilation slots, as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

## Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.

## Environment Statement

### ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called

as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

Network standby power consumption < 8W, and/or

Off mode power consumption < 0.5W, and/or

Standby mode power consumption < 0.5W.

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

### Disposal and Recycling Information

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

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

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

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

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

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

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
- 前述合法通信，指依電信管理法規定作業之無線電通信低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 使用無線產品時，應避免影響附近雷達系統之操作。高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

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

安全警告 - 為了您的安全，請先閱讀以下警告及指示 :

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

## About the Symbols

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

### Explanation of the Symbols

| SYMBOL | EXPLANATION |
|---|---|
| | Alternating current (AC):<br>AC is an electric current in which the flow of electric charge periodically reverses direction. |
| | Direct current (DC):<br>DC if the unidirectional flow or movement of electric charge carriers. |
| | Earth; ground:<br>A wiring terminal intended for connection of a Protective Earthing Conductor. |
| | Class II equipment:<br>The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation. |

## Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

## Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

## Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information

## Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: https://www.zyxel.com/form/gpl_oss_software_notice.shtml

# Index

## Numbers

6rd
IPv6 107

## A

access
troubleshooting 254
Access Control (Rules) screen 200
access point
coverage area 19
activation
firewalls 198
SSID 123
Address Resolution Protocol 218
Any_WAN
Remote Management 230
Application Layer Gateway (ALG) 183
applications
Internet access 16
applications, NAT 189
ARP Table 218, 220, 225
authentication 135

## B

backup
configuration 247
backup configuration 247
Backup/Restore screen 246
Basic Service Set, see BSS
Bridge mode 113
bridge mode 23
bridge mode example 23
broadband 105
Broadband screen
overview 105
broadcast 115
BSS 137
example 138
button
reset 27

## C

Canonical Format Indicator See CFI
certifications 277
viewing 280
CFI 115
client list 149
configuration
backup 247
firewalls 198
restoring 248
static route 194
contact information 260
controller
network 18
copyright 275
coverage area
access point 19
repeater 19
CTS threshold 130, 135
customer support 260
customized service 199
add 200
customized services 200

## D

daisy chain
form 21
data fragment threshold 130, 135
DDoS 197

Denials of Service, see DoS
DHCP 144, 156
DHCP Server Lease Time 147
DHCP Server State 147
diagnostic 250
diagnostic screens 250
disclaimer 275
DMZ screen 182
DNS 144, 156
DNS server address assignment 115
DNS Values 147
Domain Name 190
domain name system, see DNS
DoS 197
  thresholds 197
DoS protection blocking
  enable 203
Dual Stack Lite 107
dual-band application 17, 20
dual-band gateway 16
dual-band WiFi 19
dynamic DNS 192
  wildcard 193
Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard 193

## E

ECHO 190
email
  log example 241
  log setting 241
Encapsulation 114
encapsulation method
  technical reference 114
Ethernet port 27
Extended Service Set IDentification 120, 124

## F

factory defaults
  reset 248
factory-default configuration
  reload 28
filters
  MAC address 126, 136
Finger services 190
firewall
  enhancing security 205
  LAND attack 197
  security considerations 205
  traffic rule direction 203
Firewall DoS screen 203
Firewall General screen 198
firewall rules
  direction of travel 204
firewalls 196, 198
  actions 203
  configuration 198
  customized service 199
  customized services 200
  DDoS 197
  DoS 197
    thresholds 197
  ICMP 197
  Ping of Death 197
  rules 204
  security 205
  SYN attack 196
firmware
  version 95
Firmware Upgrade screen 243, 245
firmware upload 243, 245
firmware version
  check 243, 245
fragmentation threshold 130, 135
FTP 24, 176, 190
  unusable 256

## G

General wireless LAN screen 118
guest WiFi 17

## H

HTTP 190

## I

ICMP 197
IEEE 802.11a/b/g/n/ac/ax 19
IEEE 802.11ax 118
IEEE 802.1Q 115
IGA 188
IGMP 115
  version 115
ILA 188
Inside Global Address, see IGA
Inside Local Address, see ILA
Internet
  no access 257
  wizard setup 40
Internet access
  wizard setup 40
Internet access application
  Ethernet WAN 16
Internet Blocking 93
Internet connection
  add or edit 109
  slow or erratic 257
Internet Control Message Protocol, see ICMP
Internet Protocol version 6 106
Internet Protocol version 6, see IPv6
IP address 157
  private 157
  WAN 106
IP address assignment 114
IP alias
  NAT applications 190
IP packet
  transmission method 115
IPv4 firewall 199
IPv6 106, 265
  addressing 106, 116, 265
  EUI-64 267
  global address 265
  interface ID 267
  link-local address 265
  Neighbor Discovery Protocol 265
  ping 265
  prefix 106, 116, 265
  prefix and length 106
  prefix delegation 108
  prefix length 106, 116, 265
  subnet mask 106
  unspecified address 266
IPv6 address
  abbreviation method 116
IPv6 firewall 199
IPv6 rapid deployment 107

## L

LAN 143
  client list 149
  DHCP 156
  DNS 156
  IP address 157
  MAC address 150
  status 96, 101
  subnet mask 145, 157
LAN IP address 147
LAN IPv6 Mode Setup 148
LAN Setup screen 145
LAN subnet mask 147
LAND attack 197
limitations
  wireless LAN 137
  WPS 142
Local Area Network, see LAN
Log Setting screen 239
login 31
  password 31
Login screen
  no access 254
logs 211, 214, 239

## M

MAC address 127, 150
  filter 126, 136

LAN 150
MAC Authentication screen 126
MAC Filter 207
managing the device
good habits 24
MBSSID 138
Mesh application 19
MGMT Services screen 229
module firmware 244
MTU (Multi-Tenant Unit) 114
Multi_WAN
Remote Management 230
multicast 115
multi-gigabit 16
Multiple BSS, see MBSSID


## N


NAT 188
applications 189
IP alias 190
default server 182
DMZ host 182
example 189
global 188
IGA 188
ILA 188
inside 188
local 188
multiple server example 176
outside 188
port number 190
services 190
NAT ALG screen 183, 184, 187
NAT example 191
Network Address Translation, see NAT
network disconnect
temporary 244
network map 93
NNTP 190
Nslookup test 251


## O


Others screen 129


## P


password 31
admin 254
lost 254
user 254
PBC 139
Ping of Death 197
Ping test 251
Ping/TraceRoute/Nslookup screen 250
Point-to-Point Tunneling Protocol, see PPTP
POP3 190
port
LAN 27
WAN 27
port forwarding rule
add/edit 177
Port Forwarding screen 176, 177
Port Triggering
add new rule 181
Port Triggering screen 179
POWER button 27
PPTP 190
preamble 131, 135
preamble mode 138
prefix delegation 108
private IP address 157
problem
troubleshooting 253
Protocol (Customized Services) screen 199
Protocol Entry
add 200
Push Button Configuration, see PBC
push button, WPS 139


## R


Reboot screen 249

reset 28
RESET button 27
reset to factory defaults 248
restart system 249
restoring configuration 248
RFC 1631 175
RFC 3164 211
router controller 19
RTS threshold 130, 135

## S

security
  network 205
  wireless LAN 135
Security Log 213
Security Parameter Index, see SPI
service access control 231
Service Set 120, 124
services
  port forwarding 190
setup
  firewalls 198
  static route 194
SMTP 190
SPI 197
SSH
  unusable 256
SSID 136
  activation 123
  MBSSID 138
standard (router) mode 22
standard mode example 23
static DHCP 149
  configuration 151
Static DHCP screen 150
static route 166
  configuration 194
status 93
  firmware version 95
  LAN 96, 101
  wireless LAN 96
subnet mask 157
SYN attack 196
syslog
  protocol 211
  severity levels 211
syslog logging
  enable 240
syslog server
  name or IP address 240
system
  firmware
    version 95
  module firmware 244
  password 31
  reset 28
  status 93
    LAN 96, 101
    wireless LAN 96
  time 233

## T

Telnet
  unusable 256
thresholds
  data fragment 130, 135
  DoS 197
  RTS/CTS 130, 135
time 233
top panel
  LED indicators 25
TPID 115
Trace Route test 251
troubleshooting 253
Trust Domain
  add 231
Trust Domain screen 231
TWT (Target Wakeup Time) 118

## U

unicast 115
Universal Plug and Play, see UPnP
upgrading module firmware 244
uplink connection
  WiFi 21

wired 21
UPnP 151
forum 145
NAT traversal 144
security issues 145
state 152
usage confirmation 144
UPnP screen 151
UPnP-enabled Network Device
auto-discover 160


## V


Virtual Local Area Network See VLAN
VLAN 114
Introduction 114
VLAN ID 115
VLAN tag 115


## W


Wake on LAN 154
WAN
Wide Area Network, see WAN 105
WAN IP address 106
warranty 280
note 280
Web Configurator
login 31
password 31
WEP 121
WEP Encryption 122
WiFi
MBSSID 138
WiFi standards
comparison table 118
WiFi6 introduction 118
Wireless General screen 118
wireless LAN 117
authentication 135
BSS 137
example 138
example 134
fragmentation threshold 130, 135
limitations 137
MAC address filter 126, 136
preamble 131, 135
RTS/CTS threshold 130, 135
security 135
SSID 136
activation 123
status 96
WPS 139
example 141
limitations 142
push button 139
Wireless tutorial 49
wizard setup
Internet 40
WMM screen 129
WPA 121
WPA2 121
WPA2-PSK 121
WPA3-SAE (Simultaneous Authentication of Equals handshake) 121
WPA-PSK (WiFi Protected Access-Pre-Shared Key) 121
WPS 139
activate 28
example 141
limitations 142
push button 139
WPS button 27
using 28
WPS screen 127


## Z


Zyxel Device
managing 23