

User's Guide

WE Series

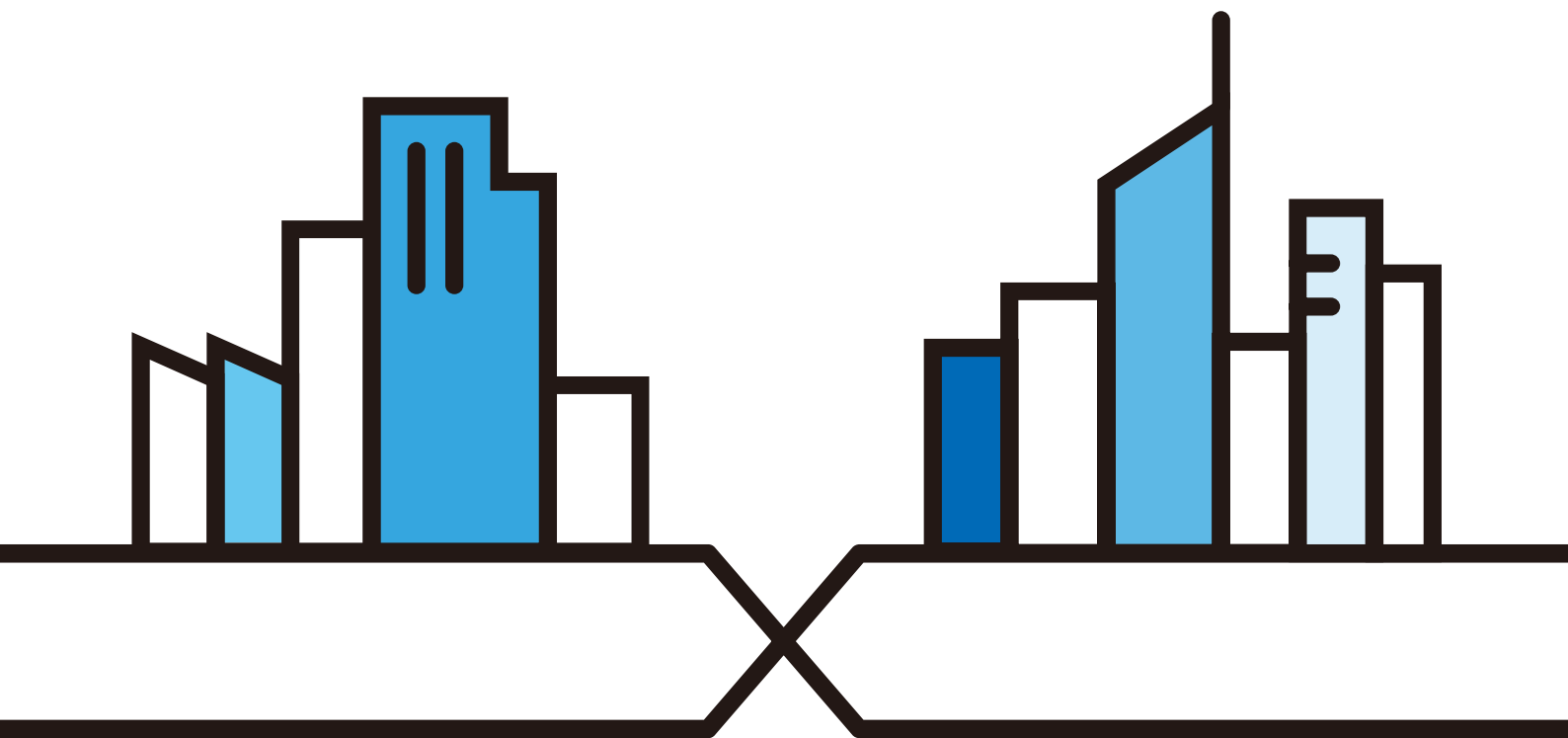
Dual-Band Wireless Extender

DRAFT

Default Login Details

LAN IP Address	http://192.168.1.2
Login	admin
Password	See the device label

Version 5.70-6.70 Ed 1, 07/2025



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 WE Device.

- Zyxel One app

Download the Zyxel One app from Google Play or Apple Store to manage the WE Device using a smartphone or tablet. To view Zyxel One app tutorials, please go to <https://service-provider.zyxel.com/app-help/ZyxelOne/FLA/LAN>

- More Information

Go to <https://service-provider.zyxel.com/global/en/tech-support> to find other information on the WE Device.



Document Conventions

Warnings and Notes

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

Warnings tell you about things that could harm you or your device.

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

Syntax Conventions

- The device in this user's guide may be referred to as the "WE Device" in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting > Wireless > MAC Authentication** means you first click **Network Setting** in the navigation panel, then the **Wireless** sub menu and finally the **MAC Authentication** tab to get to that screen.

Icons Used in Figures

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

WE Device 	Generic Router 	Laptop Computer 
Switch 	Firewall 	Server 
Desktop 	User 	Smartphone 

Accessibility and Compatibility

Introduction

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

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

Accessibility Feature – Screen Reader Support

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

To use the screen reader, do the following:

- 1 Open your screen reader software.
- 2 Navigate to this User's Guide; the screen reader should automatically start reading the contents.
- 3 Use the keyboard shortcuts to navigate through this User's Guide (refer to the screen reader documentation).

Accessibility Feature – Keyboard Navigation

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

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

How to Get Support

If you are an Internet Service Provider (ISP), please contact your Zyxel sales or service representative for direct support.

If you obtained your WE Device from an ISP, please contact your ISP's support team directly, as the WE Devices may have custom configurations.

Contents Overview

User's Guide	16
Introduction	17
Hardware	28
Web Configurator	42
Technical Reference	53
Connection Status	54
Web Tutorials	66
Broadband	85
Wireless	103
Home Networking	138
Routing	163
Network Address Translation (NAT)	174
DNS	189
IGMP/MLD	194
Firewall	197
MAC Filter	208
Home Security	211
Parental Control	213
Certificates	217
Log	226
Traffic Status	229
ARP Table	233
Routing Table	235
Multicast Status	238
WLAN Station Status	240
Operation Mode	242
System	243
User Account	244
Remote Management	247
Power Monitor	249
Time Settings	250
Email Notification	253
Log Setting	256
Firmware Upgrade	260
Backup/Restore	263
Diagnostic	268

Troubleshooting and Appendices 270

 Troubleshooting 271

Table of Contents

Document Conventions	3
Accessibility and Compatibility	4
Contents Overview	5
Table of Contents	7
 Part I: User's Guide	 16
Chapter 1	
Introduction	17
1.1 Overview	17
1.1.1 Introduction	17
1.1.2 Multi-Gigabit	19
1.2 Mesh	20
1.2.1 AP Steering and Band Steering	20
1.2.2 Network Controller	22
1.3 Dual-Band WiFi	23
1.4 Triple-Band WiFi	23
1.5 Daisy Chain	26
1.6 Ways to Manage the WE Device	27
1.7 Good Habits for Managing the WE Device	27
 Chapter 2	
Hardware	28
2.1 LED Indicators Panel	28
2.2 Ports Panel	36
2.3 Wall Mounting	40
2.4 WPS Button	40
2.4.1 Using the WPS Button	40
2.5 RESET Button	41
2.5.1 Using the RESET Button	41
 Chapter 3	
Web Configurator.....	42
3.1 Overview	42
3.2 Accessing the Web Configurator	42
3.2.1 When the WE Device is connected to a modem/router	42

3.2.2 When the WE Device is not connected to a modem/router	43
3.3 Logging into the Web Configurator	43
3.4 Web Configurator Layout	45
3.4.1 Navigation Panel	45

Part II: Technical Reference..... 53

Chapter 4 Connection Status..... 54

4.1 Overview	54
4.1.1 Widget Icon	54
4.1.2 Connectivity	55
4.1.3 System Info	57
4.2 WiFi Settings	60
4.3 Guest WiFi Settings	63
4.4 LAN Settings	65

Chapter 5 Web Tutorials 66

5.1 Overview	66
5.2 What You Can Do	66
5.3 Device Settings	66
5.3.1 How to Change an Interface IP	66
5.3.2 How to Rename Your Device	68
5.3.3 How to Change the Admin Password	68
5.4 WiFi Network Setup	69
5.4.1 Setting Up a WiFi Network	70
5.4.2 How to Set Up a WiFi Network Using WPS	72
5.4.3 How to Set Up a WiFi Network Without WPS	73
5.4.4 How to Set Up Different WiFi Networks Including a Guest Network	73
5.5 Traffic Usage	78
5.5.1 How to View the Interface Status	78
5.5.2 How to View the WLAN Station Status	78
5.6 Device Maintenance	79
5.6.1 How to Upgrade the Firmware	79
5.6.2 How to Back up the Device Configuration	79
5.6.3 How to Restore the Device Configuration	80
5.6.4 How to Reset the Device to the Factory Defaults	80
5.7 System Log	80
5.7.1 How to View Logs	81
5.7.2 How to Send the System Log through E-mail	81

Chapter 6	
Broadband.....	85
6.1 Broadband Overview	85
6.1.1 What You Can Do in this Chapter	85
6.1.2 What You Need to Know	86
6.1.3 Before You Begin	88
6.2 Broadband Settings for Ethernet Routers	88
6.2.1 Add or Edit Internet Connection	90
6.3 Technical Reference	97
Chapter 7	
Wireless.....	103
7.1 Wireless Overview	103
7.1.1 What You Can Do in this Chapter	103
7.1.2 What You Need to Know	103
7.2 Wireless General Settings	104
7.2.1 No Security	108
7.2.2 More Secure (Recommended)	109
7.3 Guest/More AP	110
7.3.1 Edit Guest/More AP Settings	111
7.4 MAC Authentication	113
7.4.1 Add/Edit MAC Addresses	115
7.5 WPS Settings	115
7.6 Channel Status Settings	117
7.7 Mesh	118
7.8 Operating Modes Settings	119
7.9 AP List Screen	122
7.10 Technical Reference	125
7.10.1 WiFi Network Overview	125
7.10.2 Additional WiFi Terms	127
7.10.3 WiFi Security Overview	127
7.10.4 Signal Problems	129
7.10.5 BSS	129
7.10.6 MBSSID	130
7.10.7 Preamble Type	130
7.10.8 WiFi Protected Setup (WPS)	131
Chapter 8	
Home Networking.....	138
8.1 Home Networking Overview	138
8.1.1 What You Can Do in this Chapter	138
8.1.2 What You Need To Know	138
8.1.3 Before You Begin	140

8.2 Home Networking	140
8.3 LAN Setup	142
8.4 Static DHCP	147
8.4.1 Before You Begin	148
8.5 UPnP	149
8.6 LAN Additional Subnet	151
8.7 STB Vendor ID	152
8.8 Technical Reference	153
8.8.1 DHCP Setup	154
8.8.2 DNS Server Addresses	154
8.8.3 LAN TCP/IP	155
8.9 Turn on UPnP in Windows 10 Example	156
8.9.1 Auto-discover Your UPnP-enabled Network Device	158
8.10 Web Configurator Access with UPnP in Windows 10	160

Chapter 9

Routing.....163

9.1 Routing Overview	163
9.2 Configure Static Route	163
9.2.1 Add or Edit Static Route	164
9.3 DNS Route	168
9.3.1 Add or Edit DNS Route	169
9.4 Policy Route	170
9.4.1 Add or Edit Policy Route	171
9.5 RIP Overview	173
9.5.1 RIP	173

Chapter 10

Network Address Translation (NAT).....174

10.1 NAT Overview	174
10.1.1 What You Can Do in this Chapter	174
10.1.2 What You Need To Know	174
10.2 Port Forwarding	175
10.2.1 Port Forwarding	175
10.2.2 Add or Edit Port Forwarding	177
10.3 Port Triggering	178
10.3.1 Add or Edit Port Triggering Rule	181
10.4 DMZ	182
10.5 ALG	183
10.6 Sessions	184
10.7 Technical Reference	185
10.7.1 NAT Definitions	185
10.7.2 What NAT Does	185

10.7.3 How NAT Works	186
10.7.4 NAT Application	186
Chapter 11	
DNS	189
11.1 DNS Overview	189
11.1.1 What You Can Do in this Chapter	189
11.1.2 What You Need To Know	189
11.2 DNS Entry (DNS)	190
11.2.1 Add or Edit DNS Entry	190
11.3 Dynamic DNS	191
Chapter 12	
IGMP/MLD	194
12.1 IGMP/MLD Overview	194
12.1.1 What You Need To Know	194
12.2 The IGMP/MLD Screen	194
Chapter 13	
Firewall	197
13.1 Firewall Overview	197
13.1.1 What You Need to Know About Firewall	197
13.2 Firewall	198
13.2.1 What You Can Do in this Chapter	198
13.3 General	199
13.4 Protocol	200
13.4.1 Add New Protocol Entry	201
13.5 Access Control (Rules)	202
13.5.1 Add New ACL Rule	203
13.6 DoS	205
13.7 Firewall Technical Reference	205
13.7.1 Firewall Rules Overview	206
13.7.2 Guidelines For Security Enhancement With Your Firewall	207
13.7.3 Security Considerations	207
Chapter 14	
MAC Filter	208
14.1 MAC Filter Overview	208
14.2 MAC Filter	208
14.2.1 Add New Rule	209
Chapter 15	
Home Security	211

15.1 Home Security Overview	211
15.2 Home Security	211
Chapter 16	
Parental Control	213
16.1 Parental Control Overview	213
16.2 Parental Control Schedule	213
16.2.1 Add or Edit a Parental Control Profile	214
16.2.2 Define a Schedule	214
16.2.3 Parental Control Scheduled Profile	215
Chapter 17	
Certificates	217
17.1 Certificates Overview	217
17.1.1 What You Can Do in this Chapter	217
17.2 What You Need to Know	217
17.3 Local Certificates	217
17.3.1 Create Certificate Request	219
17.3.2 View Certificate Request	219
17.4 Trusted CA	221
17.5 Import Trusted CA Certificate	222
17.6 View Trusted CA Certificate	222
17.7 Certificates Technical Reference	223
17.7.1 Verify a Certificate	224
Chapter 18	
Log	226
18.1 Log Overview	226
18.1.1 What You Can Do in this Chapter	226
18.1.2 What You Need To Know	226
18.2 System Log Settings	227
18.3 Security Log	228
Chapter 19	
Traffic Status	229
19.1 Traffic Status Overview	229
19.1.1 What You Can Do in this Chapter	229
19.2 WAN Status	229
19.3 LAN Status	231
19.4 NAT Status	232
Chapter 20	
ARP Table	233

20.1 ARP Table Overview	233
20.1.1 How ARP Works	233
20.2 ARP Table	233
Chapter 21	
Routing Table.....	235
21.1 Routing Table Overview	235
21.2 Routing Table	235
Chapter 22	
Multicast Status	238
22.1 Multicast Status Overview	238
22.2 The IGMP Status Screen	238
22.3 The MLD Status Screen	239
Chapter 23	
WLAN Station Status	240
23.1 WLAN Station Status Overview	240
Chapter 24	
Operation Mode	242
24.1 Operation Mode Overview	242
24.2 Operation Mode Settings	242
Chapter 25	
System.....	243
25.1 System Overview	243
25.2 System Settings	243
Chapter 26	
User Account.....	244
26.1 User Account Overview	244
26.2 User Account Settings	244
26.2.1 User Account Add/Edit	245
Chapter 27	
Remote Management	247
27.1 Remote Management Overview	247
27.1.1 What You Can Do in this Chapter	247
27.2 Management Services	247
Chapter 28	
Power Monitor	249

28.1 Power Monitor Overview	249
Chapter 29	
Time Settings.....	250
29.1 Time Settings Overview	250
29.2 Time	250
Chapter 30	
Email Notification.....	253
30.1 Email Notification Overview	253
30.2 Email Notification	253
30.2.1 Add New e-mail	254
Chapter 31	
Log Setting	256
31.1 Log Setting Overview	256
31.2 Log Setting	256
31.2.1 Example Email Log	258
Chapter 32	
Firmware Upgrade	260
32.1 Firmware Upgrade Overview	260
32.2 Firmware Upgrade Settings	260
Chapter 33	
Backup/Restore	263
33.1 Backup/Restore Overview	263
33.2 Backup/Restore Settings	263
33.3 Reboot	266
Chapter 34	
Diagnostic.....	268
34.1 Diagnostic Overview	268
34.1.1 What You Can Do in this Chapter	268
34.2 What You Need to Know	268
34.3 Diagnostic Test	269
 Part III: Troubleshooting and Appendices	 270
Chapter 35	
Troubleshooting.....	271

35.1 Accessibility and Compatibility Problems	271
35.2 Power and Hardware Problems	271
35.3 Device Access Problems	272
35.4 Internet Problems	274
35.5 WiFi Problems	274
35.6 Resetting the WE Device to Its Factory Defaults	275
35.7 Zyxel One App Problems	276
35.8 Daisy Chain Problems	276
Appendix A Customer Support	277
Appendix B IPv6.....	282
Appendix C Services.....	288
Appendix D Legal Information	292
Index	303

PART I

User's Guide

CHAPTER 1

Introduction

1.1 Overview

The WE Device refers to the following models.

- WE3300-00
- WE4600-00

1.1.1 Introduction

The WE Device is a dual-band / tri-band WiFi extender that can extend WiFi coverage from a router/modem with Internet access. The WE Device can act as the controller in either Router mode or Access Point (AP) mode. In Router mode, the WE Device acts as the controller in router mode. In AP mode, the WE Device acts as either mesh controller or mesh agent in bridge mode. To see how to select Router or AP mode in the web configurator, please refer to [Chapter 24 on page 242](#) for more details. The WE Device's uplink connection determines the mode: Router, Access Point (AP) or Repeater (RP).

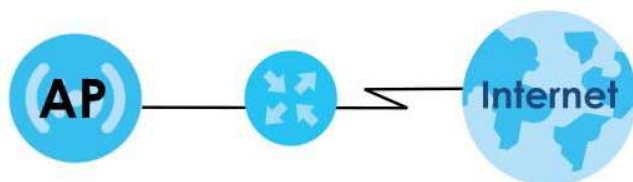
In a Mesh network, a controller manages the extenders. See [Section 1.2 on page 20](#) for more information about Mesh.

Table 1 WE Device Feature Table

FEATURES	WE3300-00	WE4600-00
WiFi 7 Wireless Standard	BE7200	BE19000
Supported Frequency Bands	2.4 GHz / 5 GHz	2.4 GHz / 5 GHz / 6 GHz
Supported Transmission Speed	100M / 1G / 2.5G	100M / 1G / 2.5G
MU-MIMO	2.4 GHz: 4x4 5 GHz: 4x4	2.4 GHz: 4x4 5 GHz: 4x4 6 GHz: 4x5
Antenna	Internal	Internal
Gigabit Ethernet LAN Port	Two 2.5 GbE	Two 2.5 GbE
Mesh	YES	YES
Operation Modes	Router mode Access Point (AP) mode	Router mode Access Point (AP) mode
Wall Mount	YES	YES
WPS	YES	YES
Management App	Zyxel One	Zyxel One

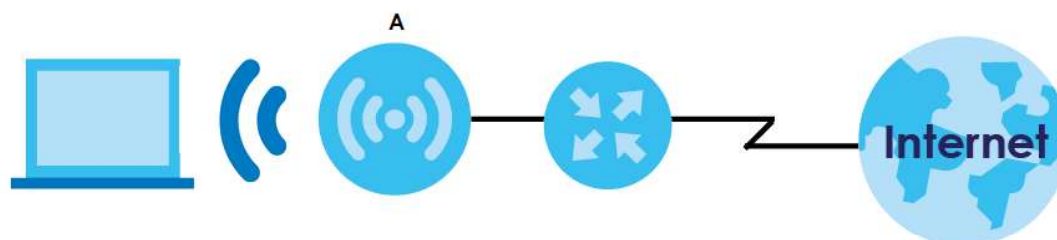
Access Point (AP) mode

If the WE Device has a wired connection to the Mesh router to get the IP address, it is in AP mode.

Figure 1 AP mode

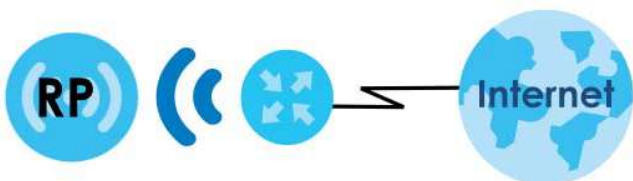
Set your WE Device to Access Point (AP) mode if you already have a Mesh router in your network and you want to bridge a wired network (LAN) and another LAN or wireless LAN (WLAN) in the same subnet. In this mode, the WE Device can act as an access point for the WiFi client to use.

In the following figure, the WE Device (**A**) is in Access Point (AP) mode, and is bridging a wired network and a wired LAN in the same subnet.

Figure 2 Device Operation Mode Example: AP Mode

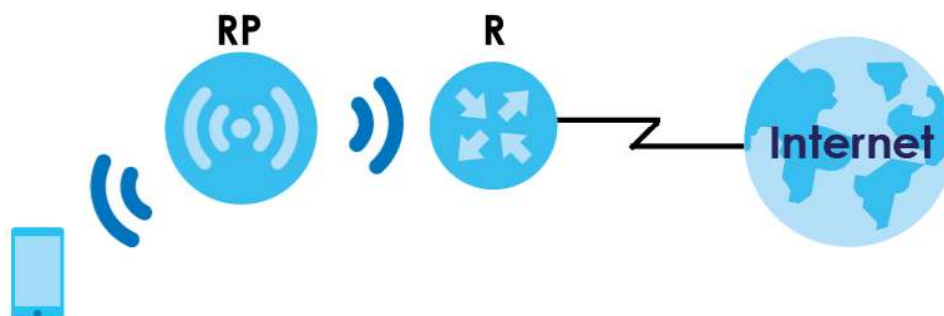
Repeater Mode

If the WE Device has a WiFi connection to the Mesh router to get the IP address, it is in Repeater mode. Repeater mode refers to the WE Device acting as a WiFi Repeater or extender.

Figure 3 Repeater Mode

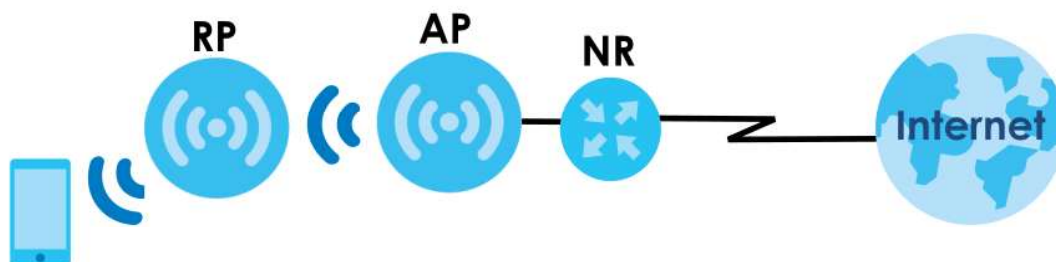
Set your WE Device to Repeater mode, if you want to extend an existing WiFi network from another Access Point and also provide network connection to WiFi clients. In this mode, the WE Device can be an access point and a WiFi client at the same time.

In the following figure, the WE Device is in Repeater (**RP**) mode and is letting a WiFi client connect to the network wirelessly through a Mesh router (**R**). This helps you expand WiFi coverage when you already have an access point or WiFi router in your network.

Figure 4 Device Operation Mode Example: Repeater Mode

Kit mode

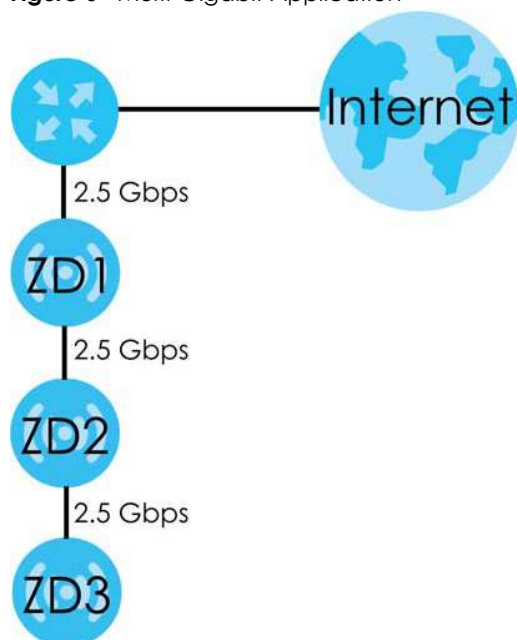
At the time of writing, the WE Device supports Kit mode. Kit mode refers to one non-Mesh Router (**NR**) connecting to two WE Devices. In the figure below, one WE Device acts as the controller in AP mode (**AP**) and the other acts as the repeater (**RP**) in Repeater mode.

Figure 5 Device Operation Mode Example: Kit Mode

1.1.2 Multi-Gigabit

A 2.5 Multi-Gigabit (IEEE 802.3bz) port supports 2.5 Gigabit Ethernet connections over Cat 5e and higher Ethernet cables. A Multi-Gigabit port may use a 100 Mbps or a 1 Gigabit connection if the connected device does not support 2.5 Gigabit or the connected cable is less than Cat 5e.

Multi-Gigabit (IEEE 802.3bz) solves these problems by additionally supporting 2.5 Gigabit Ethernet connections over Cat 5e and higher Ethernet cables. Multi-Gigabit ports are also backward compatible with 100 Mbps and 1 Gigabit ports.

Figure 6 Multi-Gigabit Application

See the following table for the cables required and distance limitation to attain the corresponding speed. Please check [Table 1 on page 17](#) for the transmission speeds supported by the WE Device.

Table 2 Ethernet Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100M	100 m	100 MHz
Category 5e or better	1G / 2.5G / 5G*	100 m	100 MHz
Category 6	5G / 10G	100 m / 55m	250 MHz
Category 6a	10G	100 m	500 MHz
Category 7	10G	100 m	600 MHz
* A high quality Category 5e cable can support 5 Gbps and up to 100 m with no electromagnetic interference.			

1.2 Mesh

The WE Device supports Mesh that lets a controller manage your WiFi network. A controller can automatically configure WiFi settings on extenders in the network as well as optimize bandwidth usage. The controller optimizes bandwidth usage by directing WiFi clients to an extender (AP steering) or 2.4 GHz / 5 GHz band (band steering) that is less busy.

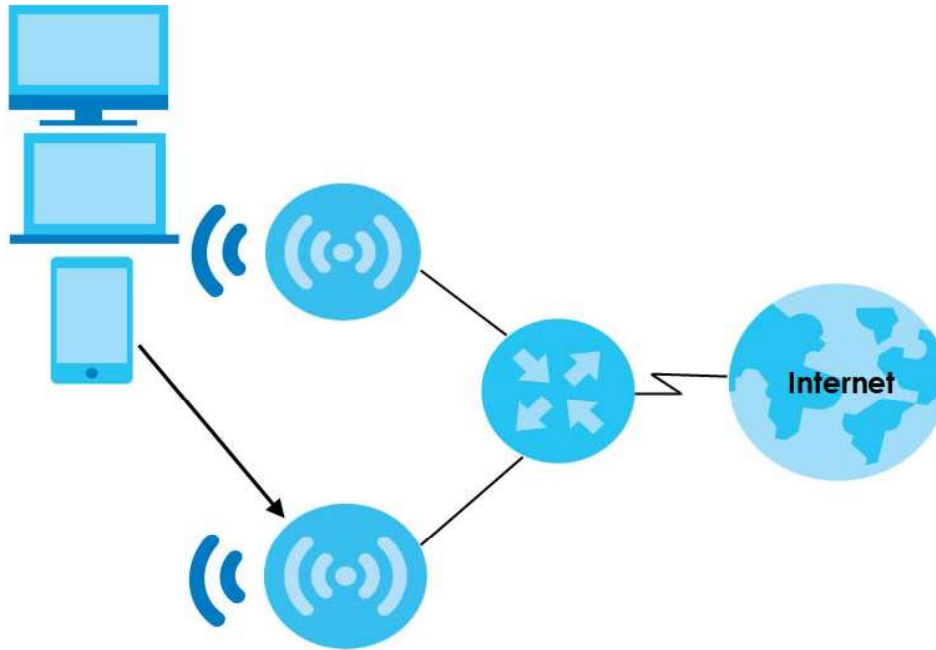
- If the router/modem is a Mesh Router/Modem, then the router/modem is the controller.
- If the router/modem is not a Mesh Router/Modem, then the WE Device is the controller.

1.2.1 AP Steering and Band Steering

Mesh supports AP steering and Band steering.

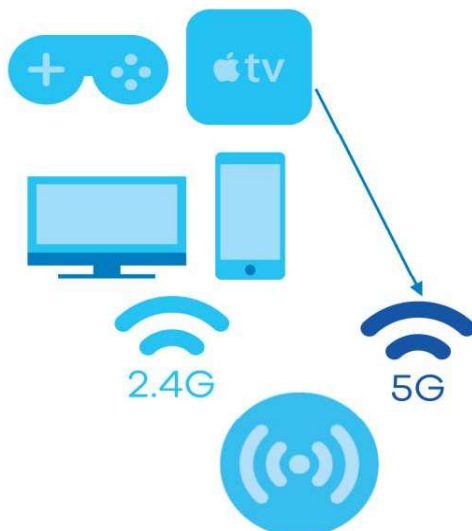
- AP steering allows WiFi clients to roam seamlessly between Mesh supported devices in your Mesh network by using the same SSID and WiFi password. Also, AP steering helps monitor WiFi clients and drop their connections to optimize the WE Device bandwidth when the clients are idle or have a low signal. When a WiFi client is dropped, it has the opportunity to reconnect to a Mesh AP with a strong signal.

Figure 7 AP Steering Application



- Band steering allows 2.4 GHz / 5 GHz dual-band WiFi clients to move from one band to another. For example, if the 2.4 GHz channel is congested, WiFi clients that support 5 GHz can move to the 5 GHz band.

Figure 8 Band Steering Application



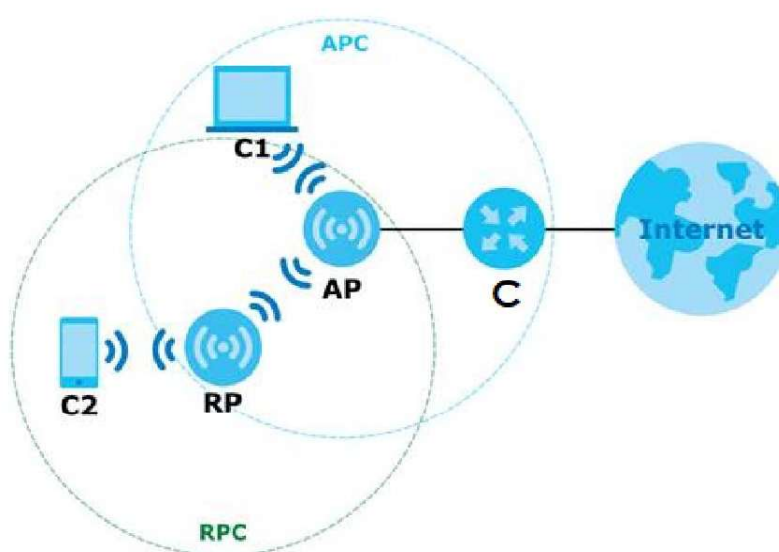
1.2.2 Network Controller

To set up a Mesh network, you need a router or an AP that can function as a controller. A controller manages and coordinates WiFi activity in a network.

A controller also manages the SSIDs and passwords on all APs in a network (auto-configuration). For example, if you change the SSID on the controller, the SSID of each AP in the network will also change.

Note: For AP steering and band steering to work, the controller and all the APs in the network need to have the same SSID and password. Therefore, we recommend using the controller to change the SSID and password.

Figure 9 Mesh Application



The following table describes the icons used in the figure.

Table 3 Icons Used in Mesh Application

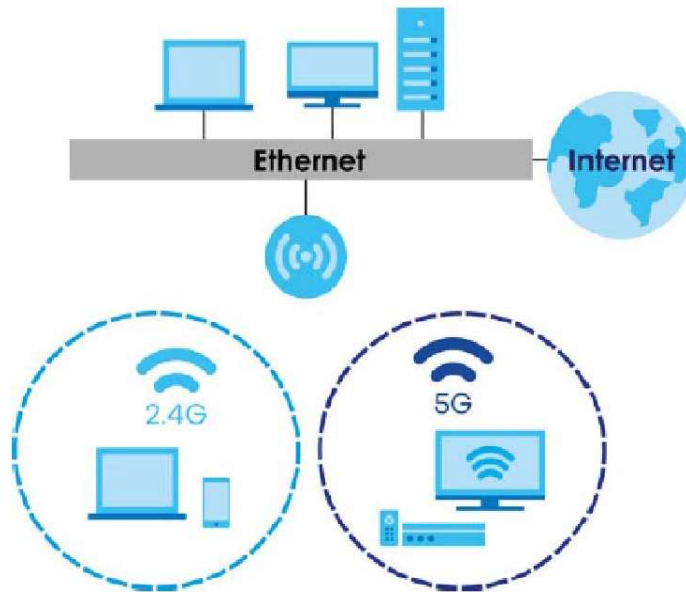
ICON	DESCRIPTION
C	Router Controller or AP controller (please refer to the link of the Zyxel One app tutorial in Section 1.6 on page 27)
AP	Access Point
RP	Repeater
C1	Client1
C2	Client2
APC	Access Point coverage area
RPC	Repeater coverage area

Note: Your router must have an Internet connection whether it supports Mesh or not.

1.3 Dual-Band WiFi

The WE 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 WE 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 10 Dual-Band Application



1.4 Triple-Band WiFi

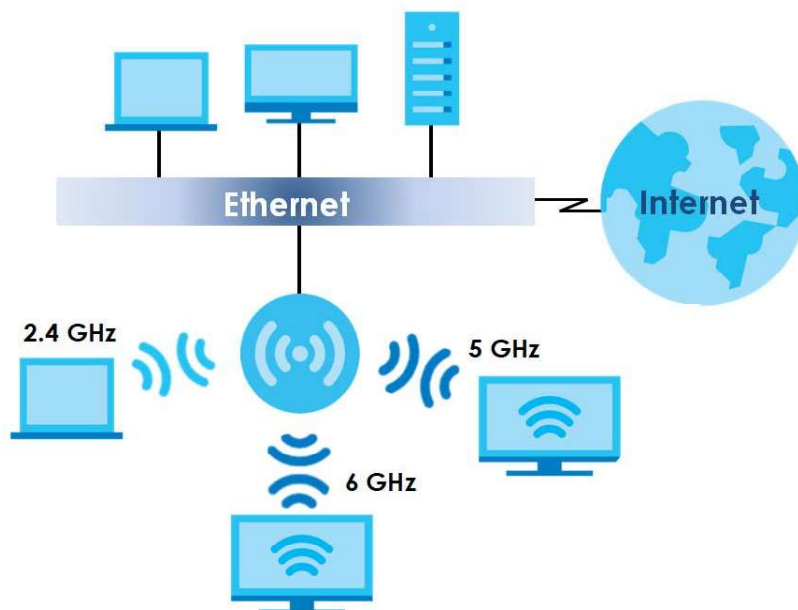
Note: Check [Section 1.1 on page 17](#) to see if your WE Device supports triple-band WiFi.

With triple-band, the WE Device can use 2.4 GHz / 5 GHz / 6 GHz bands to operate simultaneously.

The 6 GHz band provides less coverage but has the highest amount of channels among the three frequency bands. Use the 6GHz band for the most congestion-free transmission for tri-band clients.

Note: Due to each country's regulations on frequency band usage, the available bands (2.4 GHz, 5 GHz, and 6 GHz) may differ by countries or markets the WE Device products are sold to.

You can leverage concurrent tri-band connectivity across 2.4 GHz, 5 GHz, and 6 GHz bands. This allows IoT devices and various clients to simultaneously maintain connections for basic tasks with 2.4 GHz. At the same time, 5 GHz and 6 GHz handle time-sensitive traffic, and high-bandwidth applications like high-definition video, music, and gaming.

Figure 11 Triple-Band Application

WiFi 7 (IEEE802.11be)

WiFi 7 (802.11be) is backwards compatible with WiFi 6 and WiFi 6E. WiFi 7 is a WiFi standard that supports 2.4 GHz, 5 GHz and 6 GHz frequency bands with the following improvements over WiFi 6 and WiFi 6E.

Table 4 WiFi 6, WiFi 6E and WiFi 7 Comparison

FEATURES		WiFi 6	WiFi 6E	WiFi 7
Theoretical Maximum Speed (Up-to)		9.6 Gbps		46 Gbps
Supported Frequency Bands		2.4 GHz/5 GHz	2.4 GHz/5 GHz/6 GHz	2.4 GHz/5 GHz/6 GHz
Supported Channel Bandwidth		20/40/80/160 MHz	20/40/80/160 MHz	20/40/80/160/320 MHz
Total Spectrum (Up-to)	2.4 GHz	80 MHz		80 MHz
	5 GHz	500 MHz		500 MHz
	6 GHz	Not supported.	1200 MHz	1200 MHz
Other Features (OFDMA/BSS Coloring/TWT/Two-Way MU-MIMO/Beamforming/1024-QAM)		WiFi 6E inherits all the features from WiFi 6.		WiFi 7 inherits all the features from WiFi 6 and WiFi 6E, with the addition of multi-link operation and preamble puncturing.

Faster Data Transmission

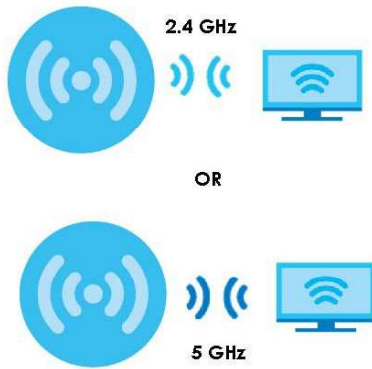
WiFi 7 allows faster data transmission using:

- 4096 QAM (Quadrature Amplitude Modulation) – enhances the amount of data transmitted over the available bandwidth.
- 320 MHz Channel Bandwidth – enlarges the supported channel bandwidth to 320 MHz, allowing higher data throughput.
- Multiple Resource Units (RUs) – allows an AP to allocate multiple RUs to a WiFi client.

Multi-Link Operation (MLO)

An AP can support multiple frequency bands, but a WiFi client can only connect to the AP using one of these frequency bands. The other frequency bands are unused. The client's data transmission speed depends on the frequency band they are connected to.

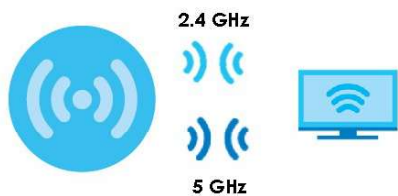
Figure 12 Without Multi-Link Operation



WiFi 7 MLO allows a WiFi client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games.

To use MLO, both the AP and the WiFi client have to support MLO.

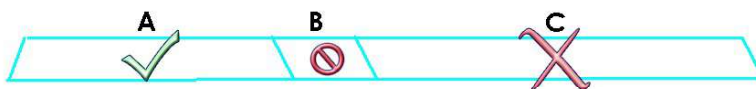
Figure 13 Multi-Link Operation Example



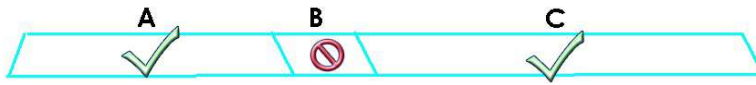
Preamble Puncturing

In WiFi 6 and earlier, any interference would cause the entire WiFi channel to become unavailable. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) becomes unavailable.

Figure 14 Without Preamble Puncturing



WiFi 7 preamble puncturing allows you to block the specific portion of the channel that is experiencing interference while continuing to use the rest of the WiFi channel. In the figure below, if part of the WiFi channel (**B**) experiences interference, the rest of the WiFi channel (**C**) is still available.

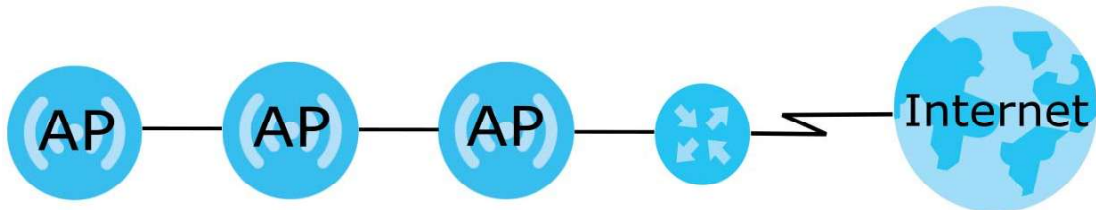
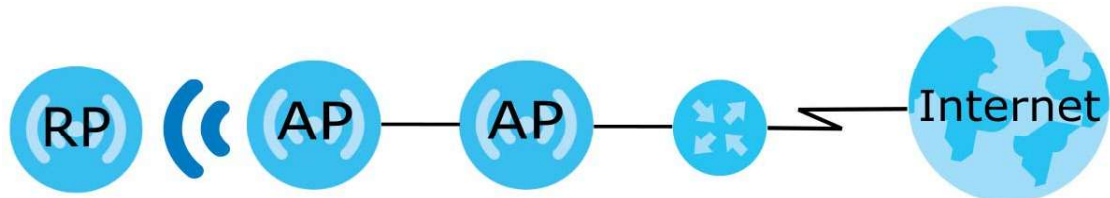
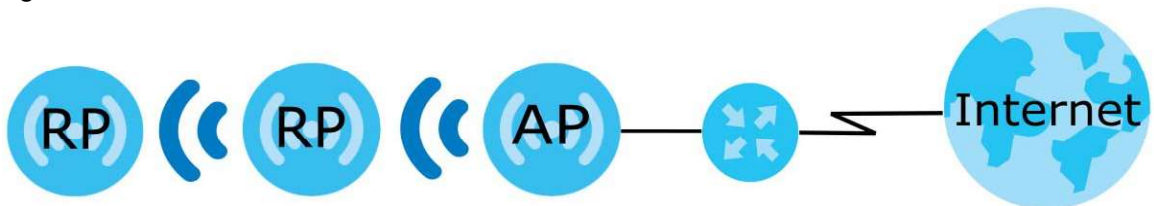
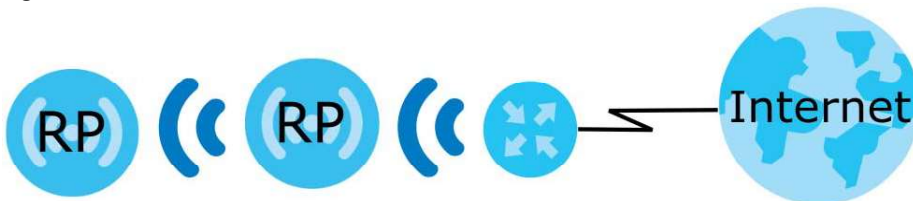
Figure 15 Preamble Puncturing Example

1.5 Daisy Chain

You can add up to three WE Devices to your network to form a daisy chain. Daisy chain refers to the connection from the first WE Device to up to three other WE Devices to extend the WiFi connection from the router to the client. The WE Device uplink connection determines the mode: Access Point (AP) or Repeater (RP).

- If the WE Device has a wired uplink connection to the router, it is in AP mode.
- If the WE Device has a WiFi uplink connection to the router, it is in RP mode.

Here are some example scenarios for the WE Device's daisy chain connection:

Figure 16 Scenario 1: Three APs**Figure 17** Scenario 2: Two APs and one RP**Figure 18** Scenario 3: One AP and two RPs**Figure 19** Scenario 4: Two RPs

Note: Set up your network as in Scenarios 1-3 if you are using non-Mesh Router. Scenario 4 is only for Mesh Routers.

Note: We do not recommend connecting more than three WE Devices in your daisy chain network. If you already have two WE Devices in RP mode, we do not recommend adding another WE Device as a repeater.

1.6 Ways to Manage the WE Device

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

- Web Configurator. Use the Web Configurator for management of the WE Device using a supported web browser.
- Zyxel One app. Download the Zyxel One app from Google Play or Apple Store to manage the WE Device using a smartphone or tablet. To view Zyxel One app tutorials, please go to <https://service-provider.zyxel.com/app-help/ZyxelOne/FLA/LAN>

1.7 Good Habits for Managing the WE Device

Do the following things regularly to make the WE Device more secure and to manage the WE 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 WE Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WE Device. You could simply restore your last configuration.

CHAPTER 2

Hardware

This section describes the front and back panel of the WE Device. Refer to the Quick Start Guides to see how to make the hardware connections.

2.1 LED Indicators Panel

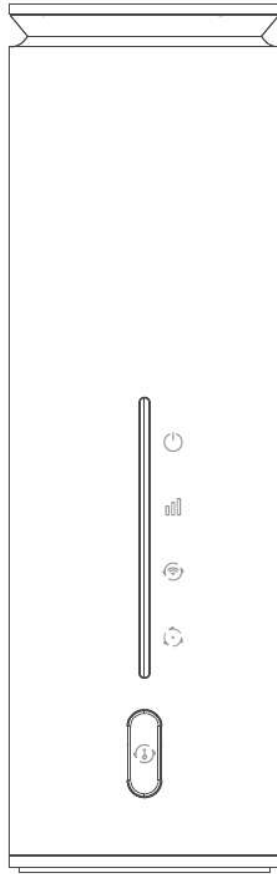
The following shows the LED indicator panel and the LED behaviors of the WE Device. Use the LEDs to determine if the WE Device is behaving normally or if there are problems on your network. None of the LEDs are on if the WE Device is not receiving power. The table below uses WE Device-1 to indicate the LED of the WE Device in AP mode. WE Device-2 is to indicate the LED of the WE Device in RP mode. For details on AP mode and RP mode, please refer to [Section 1.1.1 on page 17](#).

Dual-Band Wireless BE7200 2.5G Extender

- [WE3300-00](#)

Tri-Band Wireless BE19000 2.5G Extender

- [WE4600-00 \(Type 1\)](#)
- [WE4600-00 \(Type 2\)](#)

WE3300-00**Figure 20** LED Indicators (WE3300-00)**Table 5** LED Descriptions (for WE Device-1)

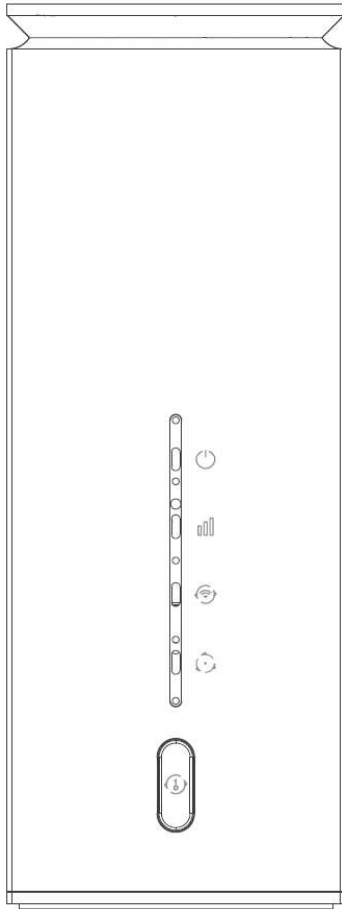
LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Power is on or the Mesh pairing is done.
		Blinking	The WE Device is starting up or under the Mesh pairing process.
	Red	On	The WE Device detects a system error.
		Blinking	Blinking Fast - The WE Device is upgrading firmware. Blinking Slow - The Mesh process has failed.
Link (With a WiFi connection) 	Green	On	The WiFi connection to the Mesh Router is good.
	Red	On	The signal is too weak. Move the WE Device closer to the Mesh Router.
Link (With a wired connection) 	Green	On	The Ethernet cable is connected to the WE Device 2.5G LAN port.

Table 5 LED Descriptions (for WE Device-1) (continued)

LED	COLOR	STATUS	DESCRIPTION
	Green	On	WiFi is ready.
		Blinking	The WE Device is transmitting/receiving WiFi data.
	Amber	Blinking	The WPS is in process.
	Off		WiFi is disabled.
	Green	On	The WE Device in Router mode has a successful Ethernet connection on the WAN, and has an IP address (either static or assigned by a DHCP server). PPP negotiation was successful (if used).
	Amber	On	The WE Device in Router mode has Ethernet WAN enabled and default gateway is in IPv4/IPv6 dual stack mode but failed to get a WAN IP address. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		The WE Device is in Extender mode, or the WE Device does not have an Ethernet connection with the WAN.

Table 6 LED Table (for WE Device-2)

LED	COLOR	STATUS	DESCRIPTION
	Green	On	Power is on or Mesh pairing is done.
		Blinking	The WE Device-2 is starting up or the Mesh pairing is in process.
	Red	On	The WE Device-2 detects a system error.
		Blinking	Blinking Fast - The WE Device-2 is upgrading firmware. Blinking Slow - The Mesh pairing has failed.
	Green	On	The WiFi connection to the WE Device-1 is good.
	Red	On	The signal is too weak. Move the WE Device-2 closer to the WE Device-1.
		Off	There is no Mesh pairing.
	Green	On	The Ethernet cable is connected to the LAN port on the WE Device-2.
		Off	There is no Mesh pairing.
	Green	On	WiFi is ready.
		Blinking	The WE Device-2 is transmitting/receiving WiFi data.
	Amber	Blinking	The WPS is in process.
	Off		WiFi is disabled.
	Green	On	The WE Device-2 in Router mode has a successful Ethernet connection on the WAN, and has an IP address (either static or assigned by a DHCP server). PPP negotiation was successful (if used).
	Amber	On	The WE Device-2 in Router mode has Ethernet WAN enabled and default gateway is in IPv4/IPv6 dual stack mode but failed to get a WAN IP address. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		The WE Device-2 is in Extender mode, or the WE Device-2 does not have an Ethernet connection with the WAN.

WE4600-00 (Type 1)**Figure 21** LED Indicators (WE4600-00)

Note: If your WE Device is an EU model, refer to the LED tables below.

The LED table below is for the WE Device type 1 in Router and AP modes.

Table 7 LED Descriptions (for WE Device-1)

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Power is on or the Mesh pairing is done.
		Blinking	The WE Device is starting up or under the Mesh pairing process.
	Red	On	The WE Device detects a system error.
		Blinking	Blinking Fast - The WE Device is upgrading firmware. Blinking Slow - The Mesh process has failed.
Link (With a WiFi connection) 	Green	On	The WiFi connection to the Mesh Router is good.
	Red	On	The signal is too weak. Move the WE Device closer to the Mesh Router.

Table 7 LED Descriptions (for WE Device-1) (continued)

LED	COLOR	STATUS	DESCRIPTION
Link (With a wired connection) 	Green	On	The Ethernet cable is connected to the WE Device 2.5G LAN port.
		Off	No mesh pairing is in progress.
WiFi or WPS 	Green	On	Either the 2.4 Ghz, 5 Ghz, or 6 Ghz interface is enabled based on the Wi-Fi configuration.
		Blinking	The WE Device is transmitting/receiving data.
	Amber	Blinking	The WPS is in process.
	Off		Either the 2.4 Ghz, 5 Ghz, or 6 Ghz interface is disabled based on the Wi-Fi configuration. The WPS process has either expired or completed successfully.
Mode 	Green	On	The WE Device is configured as a Router in the Operation Mode screen, and has an IP address (either static or assigned by a DHCP server). PPP negotiation was successful (if used).
	Amber	On	The WE Device is configured as an Extender in the Operation Mode screen (AP or Repeater). The WE Device acts as a mesh controller.
		Blinking	The WE Device is configured as a Router in the Operation Mode screen, but failed to get a WAN IP address. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		The WE Device is configured as an Extender in the Operation Mode screen (AP or Repeater), and the WE Device acts as a mesh agent or has the mesh function disabled.

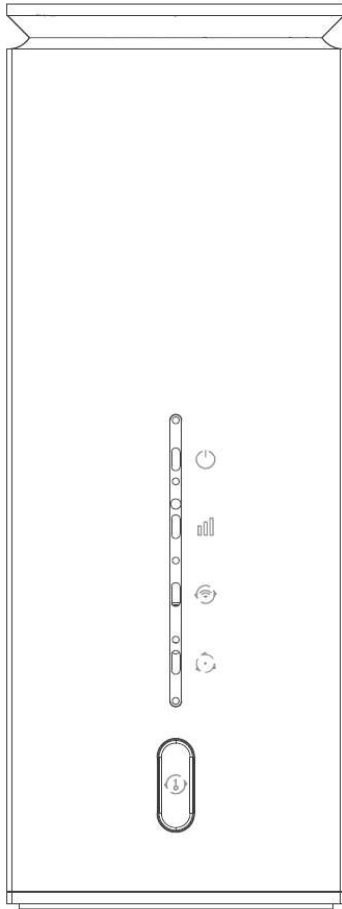
The LED table below is for the WE Device type 1 in Repeater mode.

Table 8 LED Table (for WE Device-2)

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Power is on or Mesh pairing is done.
		Blinking	The WE Device-2 is starting up or the Mesh pairing is in process.
	Red	On	The WE Device-2 detects a system error.
		Blinking	Blinking Fast - The WE Device-2 is upgrading firmware. Blinking Slow - The Mesh pairing has failed.
Link (with a WiFi connection) 	Green	On	The WiFi connection to the WE Device-1 is good.
	Red	On	The signal is too weak. Move the WE Device-2 closer to the WE Device-1.
		Off	There is no Mesh pairing.
Link (with a wired connection) 	Green	On	The Ethernet cable is connected to the LAN port on the WE Device-2.
		Off	There is no Mesh pairing.

Table 8 LED Table (for WE Device-2) (continued)

LED	COLOR	STATUS	DESCRIPTION
WiFi or WPS 	Green	On	Either the 2.4 Ghz, 5 Ghz, or 6 Ghz interface is enabled based on the Wi-Fi configuration.
		Blinking	The WE Device-2 is transmitting/receiving WiFi data.
	Amber	Blinking	The WPS is in process.
	Off		Either the 2.4 Ghz, 5 Ghz, or 6 Ghz interface is disabled based on the Wi-Fi configuration. The WPS process has either expired or completed successfully.
Mode 	Green	On	The WE Device is configured as a Router in the Operation Mode screen, and has an IP address (either static or assigned by a DHCP server). PPP negotiation was successful (if used).
	Amber	On	The WE Device is configured as an Extender in the Operation Mode screen (AP or Repeater). The WE Device acts as a mesh controller.
		Blinking	The WE Device is configured as a Router in the Operation Mode screen, but failed to get a WAN IP address. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
	Off		The WE Device is configured as an Extender in the Operation Mode screen (AP or Repeater), and the WE Device acts as a mesh agent or has the mesh function disabled.

WE4600-00 (Type 2)**Figure 22** LED Indicators (WE4600-00)

Note: If your WE Device is a US model, refer to the LED tables below.

The LED table below is for the WE Device in Router and AP modes.

Table 9 LED Descriptions (for WE Device-1)

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Power is on or the Mesh pairing is done.
		Blinking	The WE Device is starting up or under the Mesh pairing process.
	Red	On	The WE Device detects a system error.
		Blinking	Blinking Fast - The WE Device is upgrading firmware. Blinking Slow - The Mesh process has failed.
Link (With a WiFi connection) 	Green	On	The WiFi connection to the Mesh Router is good.
	Red	On	The signal is too weak. Move the WE Device closer to the Mesh Router.

Table 9 LED Descriptions (for WE Device-1) (continued)

LED	COLOR	STATUS	DESCRIPTION
Link (With a wired connection) 	Green	On	The Ethernet cable is connected to the WE Device 2.5G LAN port.
WiFi or WPS 	Green	On	the WiFi network is ready.
		Blinking	The WE Device is transmitting/receiving WiFi data.
	Amber	Blinking	The WPS is in process.
	Off		Either the 2.4 Ghz, 5 Ghz, or 6 Ghz interface is disabled based on the Wi-Fi configuration. The WPS process has either expired or completed successfully.
Mode 	Off		The WE Device is in Extender mode, or the WE Device does not have an Ethernet connection with the WAN.

The LED table below is for the WE Device in Repeater mode.

Table 10 LED Table (for WE Device-2)

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Power is on or Mesh pairing is done.
		Blinking	The WE Device-2 is starting up or the Mesh pairing is in process.
	Red	On	The WE Device-2 detects a system error.
		Blinking	Blinking Fast - The WE Device-2 is upgrading firmware. Blinking Slow - The Mesh pairing has failed.
Link (with a WiFi connection) 	Green	On	The WiFi connection to the WE Device-1 is good.
	Red	On	The signal is too weak. Move the WE Device-2 closer to the WE Device-1.
		Off	There is no Mesh pairing.
Link (with a wired connection) 	Green	On	The Ethernet cable is connected to the LAN port on the WE Device-2.
		Off	There is no Mesh pairing.
WiFi or WPS 	Green	On	The WiFi network is ready.
		Blinking	The WE Device-2 is transmitting/receiving WiFi data.
	Amber	Blinking	The WPS is in process.
	Off		Either the 2.4 Ghz, 5 Ghz, or 6 Ghz interface is disabled based on the Wi-Fi configuration. The WPS process has either expired or completed successfully.
Mode 	Off		The WE Device-2 is in Extender mode, or the WE Device-2 does not have an Ethernet connection with the WAN.

2.2 Ports Panel

Dual-Band Wireless BE7200 2.5G Extender

- [WE3300-00](#)

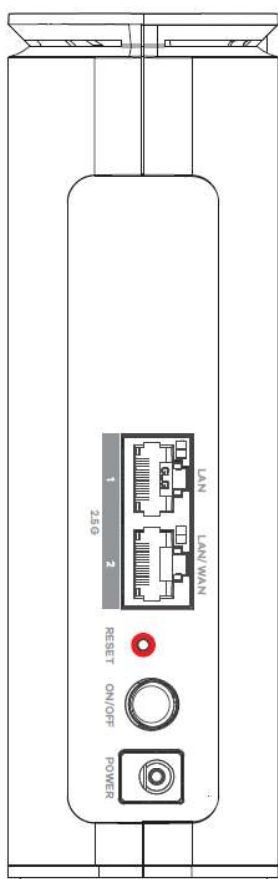
Tri-Band Wireless BE19000 2.5G Extender

- [WE4600-00 \(Type 1\)](#)
- [WE4600-00 \(Type 2\)](#)

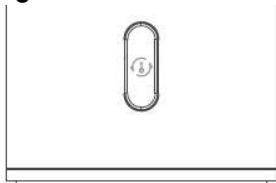
WE3300-00

Place the WE Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 23 Rear Panel (WE3300-00)



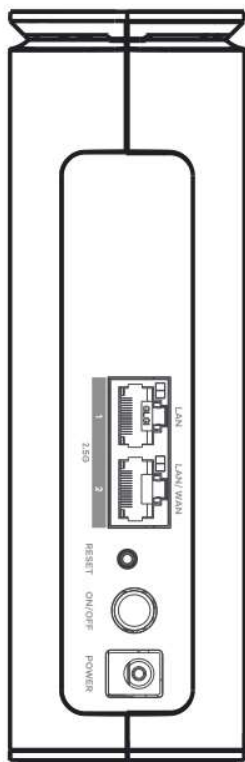
The WPS button is on the front panel of the WE Device closer to the bottom.

Figure 24 WPS button on the Front Side of the WE Device (WE3300-00)**Table 11** Panel Ports and Buttons

LABEL	DESCRIPTION
2.5G LAN	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
2.5G LAN or WAN	The LAN/WAN port can act as a LAN port or a WAN port. This port act as a LAN port to connect computers or other Ethernet devices for Internet access. This port can also act as a WAN port to connect to a router/modem for Internet connection.
RESET	Press the button for more than 5 seconds to return the WE Device to the factory defaults.
POWER ON/OFF and DC input jack	Connect the power adapter and then press the ON/OFF button to start the device.
WPS	Press the WPS button once for 1 to 3 seconds to enable the AP/Repeater mode. (See Section 2.4.1 on page 40 for more information)

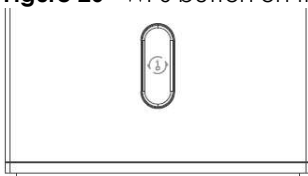
WE4600-00 (Type 1)

Place the WE Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 25 Rear Panel (WE4600-00)

The WPS button is on the front panel of the WE Device closer to the bottom.

Figure 26 WPS button on the Front Side of the WE Device (WE4600-00)



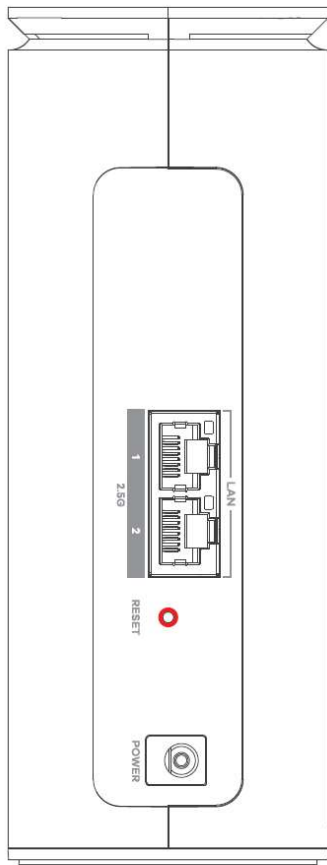
Note: If your WE Device is a EU model, refer to the table below.

Table 12 Panel Ports and Buttons

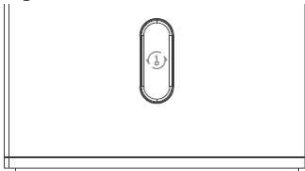
LABEL	DESCRIPTION
2.5G LAN	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
2.5G LAN or WAN	The LAN/WAN port can act as a LAN port or a WAN port. This port act as a LAN port to connect computers or other Ethernet devices for Internet access. This port can also act as a WAN port to connect to a router/modem for Internet connection.
RESET	Press the button for more than 5 seconds to return the WE Device to the factory defaults.
WPS	Press the WPS button once for 1 to 3 seconds to enable the AP/Repeater mode. (See Section 2.4.1 on page 40 for more information)
POWER ON/OFF and DC input jack	Connect the power adapter and then press the ON/OFF button to start the device.

WE4600-00 (Type 2)

Place the WE Device with the ports and buttons facing you and the Zyxel logo on the top.

Figure 27 Rear Panel (WE4600-00)

The WPS button is on the front panel of the WE Device closer to the bottom.

Figure 28 WPS button on the Front Side of the WE Device (WE4600-00)

Note: If your WE Device is a US model, refer to the table below.

Table 13 Panel Ports and Buttons

LABEL	DESCRIPTION
2.5G LAN 1 or 2	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
RESET	Press the button for more than 5 seconds to return the WE Device to the factory defaults.
DC input jack	Connect the power adapter to start the device.
WPS	Press the WPS button once for 1 to 3 seconds to enable the AP/Repeater mode. (See Section 2.4.1 on page 40 for more information)

2.3 Wall Mounting

Please refer to the WE Device's Quick Start Guide for the details of wall mounting.

2.4 WPS Button

Your WE 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 (recommended) on the device itself, or in its Web Configurator. 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.

2.4.1 Using the WPS Button

- 1 Make sure the power LED is on (not blinking).
- 2 Modes
 - APC (AP Controller) mode
 1. Press the WE Device **WPS** button just once for 1 to 3 seconds. The WPS LED should start blinking.
 2. Press the WPS button on the client within 2 minutes.
 - AP Mode (Downlink Daisy Chain for Mesh)
 1. Press the first WE Device **WPS** button just once for 1 to 3 seconds.
 2. Press the **WPS** button once on the downlink WE Device within 2 minutes.
 - Repeater mode (modem/router to the WE Device)
 1. Press the WPS button on the modem/router. Release it when the WPS LED blinks.
 2. Press the WE Device **WPS** button just once for 1 to 3 seconds within 2 minutes to copy the WiFi settings from your modem/router to the WE Device.
 3. The Link LED lights up when the process is finished.
 - Repeater mode (the WE Device to the WiFi client)
 1. Press the WE Device **WPS** button just once for 1 to 3 seconds to copy the WiFi settings from the WE Device to a WiFi client, such as your laptop.
 2. Wait until the WPS LED blinks.
 3. Press the WPS button on the client within 2 minutes.
 - Repeater mode (Downlink Daisy Chain for Mesh)
 1. Press the first WE Device **WPS** button just once for 1 to 3 seconds.
 2. Press the **WPS** button once on the downlink WE Device within 2 minutes.

Note: You must activate WPS in the WE Device and in another WiFi device within 2 minutes of each other. Repeat this procedure separately for each WiFi client.

Note: With WPS, WiFi clients will only connect to the first WiFi network (SSID) in either a 2.4 GHz or 5 GHz WiFi network.

2.5 RESET Button

If you forget your password or you cannot access the Web Configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to the default key on the device label.

2.5.1 Using the RESET Button

- 1 Make sure the power LED is on (not blinking).
- 2 Press the **RESET** button for longer than 5 seconds to set the WE Device back to its factory-default configurations.

CHAPTER 3

Web Configurator

3.1 Overview

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

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

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

3.2 Accessing the Web Configurator

3.2.1 When the WE Device is connected to a modem/router

When your WE Device is in the AP mode:

- 1 Connect your computer to the LAN port of the WE Device using an Ethernet cable.
- 2 Connect the WE Device to a LAN port of the router. Log into the router to check the IP address the router assigned to your WE Device.
- 3 Open a web browser such as Microsoft Edge and enter "https:// (DHCP-assigned IP)" as the web address in your web browser.
- 4 The **Login** screen appears.

When your WE Device is in the Repeater mode:

- 1 Connect a modem/router to the first WE Device wirelessly.
- 2 Connect your computer to a LAN port of the router. Log into the router to check the IP address the router assigned to your WE Device.
- 3 Open a web browser such as Microsoft Edge and enter "https:// (DHCP-assigned IP)" as the web address in your web browser.
- 4 The **Login** screen appears.

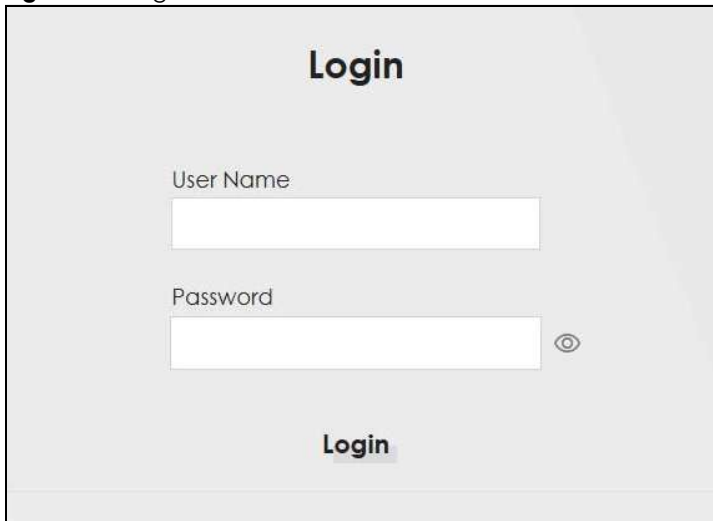
3.2.2 When the WE Device is not connected to a modem/router

- 1 Connect your computer to the LAN port of the WE Device using an Ethernet cable.
- 2 Give your computer a fixed IP address in the range between 192.168.1.3 and 192.168.1.254.
- 3 After you have set your computer's IP address, open a web browser such as Microsoft Edge and enter "https://192.168.1.2" as the web address in your web browser.
- 4 The **Login** screen appears.

3.3 Logging into the Web Configurator

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

Figure 29 Login Screen



Note: The default allowable times that you can enter the **Password** is 3. If you entered the wrong password for the fourth time, by default the Web Configurator will lock itself for 5 minutes before you can try entering the correct **Password** again. You can change these settings at **Maintenance > User Account > Add New Account / Edit** icon (see [Section 26.2.1 on page 245](#)).

- 2 The following screen displays when you log into the Web Configurator for the first time. Enter a new password, re-enter it to confirm, and click **Change password**.

Figure 30 Change Password Screen (WE3300-00)

Password Reset

New Password

Password

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

Change password

- 3 The **Connection Status** page appears. Use this screen to configure basic Internet access and WiFi settings (see [Section 4.1 on page 54](#) for details).

Figure 31 Connection Status

ZYXEL | WE3300-00
☰

Connectivity

System Info

Model Name	WE3300-00
Firmware Version	V5.70(ACKA.0)b4
System Uptime	0 days 0 hours 50 minutes 48 seconds
Host Name	WE3300-72754

WiFi Settings

2.4G	2.4GHz WiFi Name	WiFi Password	
☒	Zyxel_2754		👁
5G	5GHz WiFi Name	WiFi Password	
☒	Zyxel_2754		👁

Guest WiFi Settings

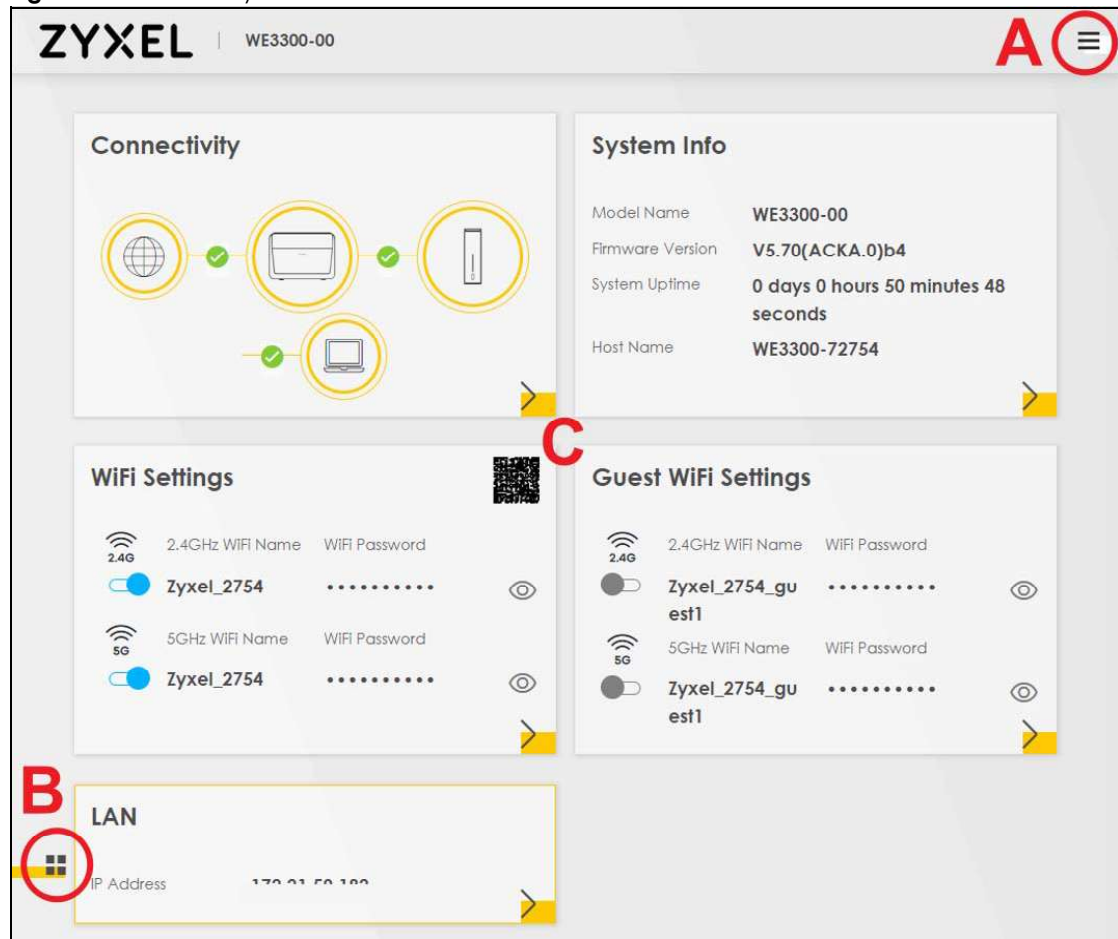
2.4G	2.4GHz WiFi Name	WiFi Password	
☐	Zyxel_2754_guest1		👁
5G	5GHz WiFi Name	WiFi Password	
☐	Zyxel_2754_guest1		👁

LAN

IP Address	172.31.50.100
------------	---------------

3.4 Web Configurator Layout

Figure 32 Screen Layout

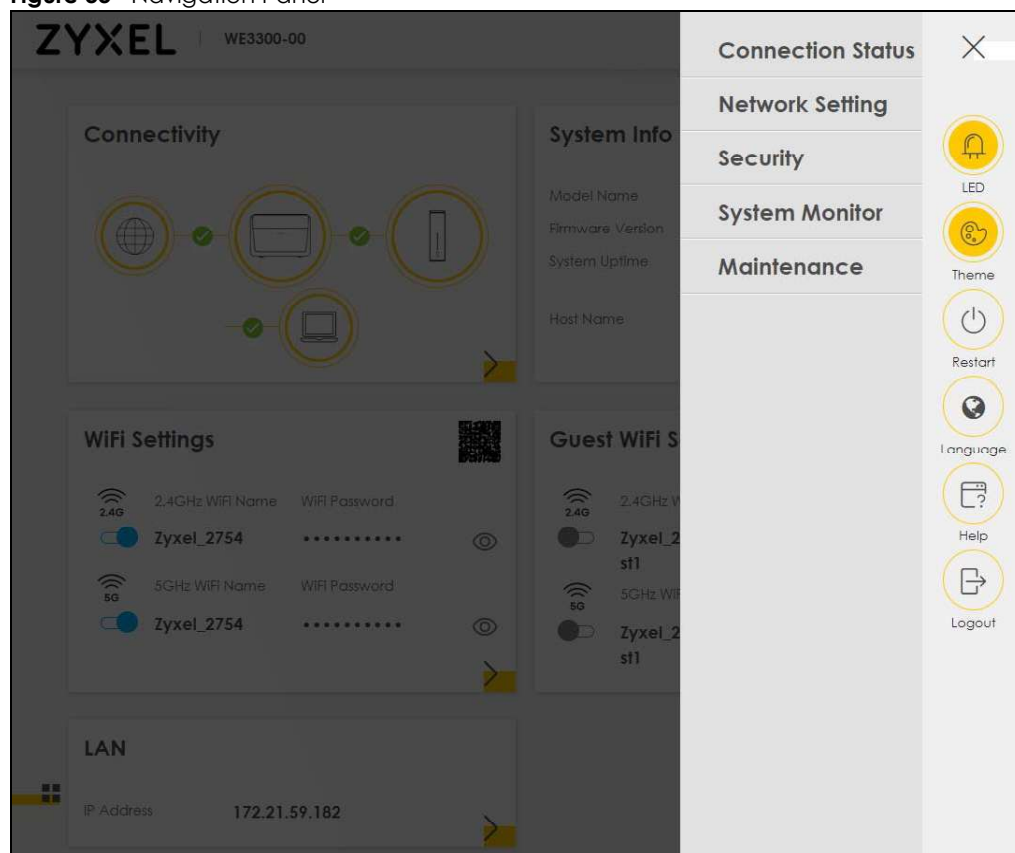


As illustrated above, the main screen is divided into these parts:

- **A** – Navigation Panel
- **B** – Layout Icon
- **C** – Main Window

3.4.1 Navigation Panel

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

Figure 33 Navigation Panel

3.4.1.1 Configuration Menus

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

Table 14 Configuration Menus Summary (WE3300-00)

LINK	TAB	FUNCTION
Connection Status		Use this screen to configure basic Internet access and WiFi settings. This screen also shows the network status of the WE Device and computers/devices connected to it.
Network Setting		
Wireless	General	Use this screen to configure the WiFi settings and WiFi authentication/security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the WE Device.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	Channel Status	Use this screen to scan WiFi channel noises and view the results.
	Operating Modes	In non-mesh extender mode, use this screen to configure upper link wireless network.
	AP List	Use this screen to scan for available wireless networks while under repeater mode. This screen is available only when WE Device is in RP mode.

Table 14 Configuration Menus Summary (WE3300-00) (continued)

LINK	TAB	FUNCTION
Home Networking	Home Networking	Use this screen to configure DHCP/Static IP settings, and other advanced properties.
Security		
Certificates	Local Certificates	Use this screen to view a summary list of certificates, manage certificates, and certify requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	Log	Use this screen to view the status of events that occurred to the WE Device. You can export or email the logs.
WLAN Station Status	WLAN Station Status	Use this screen to view the WiFi stations that are currently associated with the WE Device.
Maintenance		
System	System	Use this screen to set Device name.
User Account	User Account	Use this screen to change user password on the WE Device.
Remote Management	Remote Management	Use this screen to enable specific traffic directions for network services.
Power Monitor	Power Monitor	Use this screen to view the current and past amount of power consumed by the WE Device.
Time	Time	Use this screen to change your WE Device's time and date.
Email Notification	Email Notification	Use this screen to configure up to two mail servers and sender addresses on the WE Device.
Log Setting	Log Setting	Use this screen to change your WE Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your WE Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your WE Device's configuration (settings) or reset the factory default settings or reset devices.
Reboot	Reboot	Use this screen to reboot the WE Device without turning the power off.
Diagnostic	Ping&Traceroute	Use this screen to identify problems with the WE Device. You can use Ping or TraceRoute to help you identify problems.

Table 15 Configuration Menus Summary (WE4600-00)

LINK	TAB	FUNCTION
Connection Status		Use this screen to configure basic Internet access and WiFi settings. This screen also shows the network status of the WE Device and computers/devices connected to it.
Network Setting		
Wireless	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. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	General	Use this screen to configure the WiFi settings and WiFi authentication/security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the WE Device.
	MAC Authentication	Use this screen to block or allow WiFi traffic from WiFi devices of certain SSIDs and MAC addresses to the WE Device.

Table 15 Configuration Menus Summary (WE4600-00) (continued)

LINK	TAB	FUNCTION
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	Channel Status	Use this screen to scan WiFi channel noises and view the results.
	Mesh	Use this screen to enable or disable Mesh.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Additional Subnet	Use this screen to configure IP alias and public static IP. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	STB Vendor ID	Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the WE Device automatically create static DHCP entries for the STB devices when they request IP addresses. This screen is available only when WE Device is in Router and Access Point (AP) mode.
Routing	Static Route	Use this screen to view and set up static routes on the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Policy Route	Use this screen to configure policy routing on the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers. This screen is available only when WE Device is in Router and Access Point (AP) mode.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Port Triggering	Use this screen to change your WE Device's port triggering settings. This screen is available only when WE Device is in Router and Access Point (AP) mode.

Table 15 Configuration Menus Summary (WE4600-00) (continued)

LINK	TAB	FUNCTION
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	ALG	Use this screen to enable the ALGs (Application Layer Gateways) in the WE Device to allow applications to operate through NAT. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
DNS	DNS Entry	Use this screen to view and configure DNS routes. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address. This screen is available only when WE Device is in Router and Access Point (AP) mode.
IGMP/MLD	IGMP/MLD	Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN. This screen is available only when WE Device is in Router and Access Point (AP) mode.
Security		
Firewall	General	Use this screen to configure the security level of your firewall. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Protocol	Use this screen to add Internet services and configure firewall rules. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	Access Control	Use this screen to enable specific traffic directions for network services. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks. This screen is available only when WE Device is in Router and Access Point (AP) mode.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
Home Security	Connected Home Security	Use this screen to set up a URL filter that blocks users on your network from accessing certain websites. This screen is available only when WE Device is in Router and Access Point (AP) mode.

Table 15 Configuration Menus Summary (WE4600-00) (continued)

LINK	TAB	FUNCTION
Parental Control	Parental Control	Use this screen to define time periods and days during which the WE Device performs parental control and/or block web sites with the specific URL. This screen is available only when WE Device is in Router and Access Point (AP) mode.
Certificates	Local Certificates	Use this screen to view a summary list of certificates, manage certificates, and certify requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the WE Device. You can export or email the logs..
	Security Log	Use this screen to view all security related events. You can select the level and category of the security events in their proper drop-down list window. Levels include: - Emergency - Alert - Critical - Error - Warning - Notice - Informational - Debugging Categories include: - Account - Attack - Firewall - MAC Filter
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	NAT	Use this screen to view NAT statistics for connected hosts. This screen is available only when WE Device is in Router and Access Point (AP) mode.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection. This screen is available only when WE Device is in Router and Access Point (AP) mode.
Routing Table	Routing Table	Use this screen to view the routing table on the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.

Table 15 Configuration Menus Summary (WE4600-00) (continued)

LINK	TAB	FUNCTION
Multicast Status	IGMP Status	Use this screen to view the status of all IGMP settings on the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
	MLD Status	Use this screen to view the status of all MLD settings on the WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
WLAN Station Status	WLAN Station Status	Use this screen to view the WiFi stations that are currently associated with the WE Device.
Maintenance		
Operation Mode	Operation Mode	Use this screen to set the WE Device to Router or AP mode. In non-mesh extender mode, use this screen to configure upper link wireless network.
System	System	Use this screen to set Device name.
User Account	User Account	Use this screen to change user password on the WE Device.
Remote Management	Remote Management	Use this screen to enable specific traffic directions for network services.
Time	Time	Use this screen to change your WE 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 WE Device. This screen is available only when WE Device is in Router and Access Point (AP) mode.
Log Setting	Log Setting	Use this screen to change your WE Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your WE Device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your WE Device's configuration (settings) or reset the factory default settings or reset devices.
Reboot	Reboot	Use this screen to reboot the WE Device without turning the power off.
Diagnostic	Diagnostic	Use this screen to identify problems with the Internet connection. You can use Ping, Ping 6, TraceRoute, TraceRoute 6, or Nslookup to help you identify problems.

3.4.1.2 Icons

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

Figure 34 Icons of Navigation Panel (WE3300-00)

The icons provide the following functions.

Table 16 Web Configurator Icons

ICON	DESCRIPTION
	LED: Click this icon to turn off/on the WE Device's panel LEDs.
	Theme: Click this icon to select a color that you prefer and apply it to the Web Configurator. 
	Restart: Click this icon to reboot the WE Device without turning the power off.
	Language: Select the language you prefer.
	Help: Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.
	Logout: Click this icon to log out of the Web Configurator.

PART II

Technical Reference

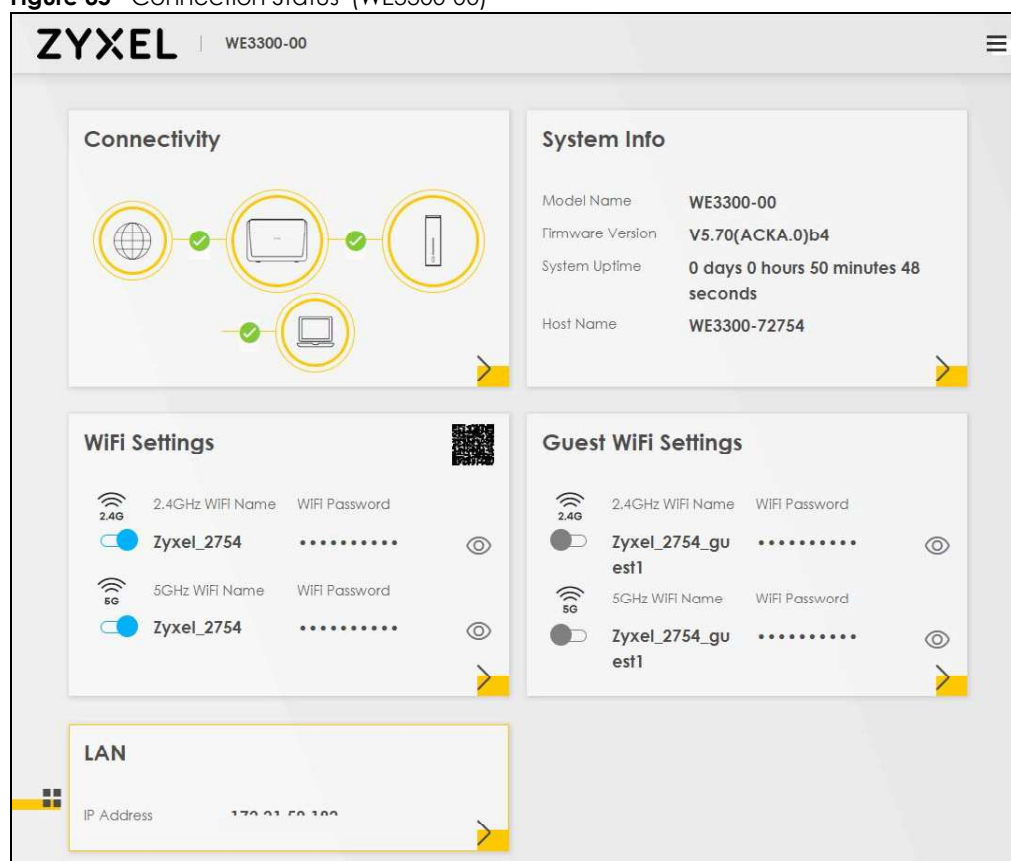
CHAPTER 4

Connection Status

4.1 Overview

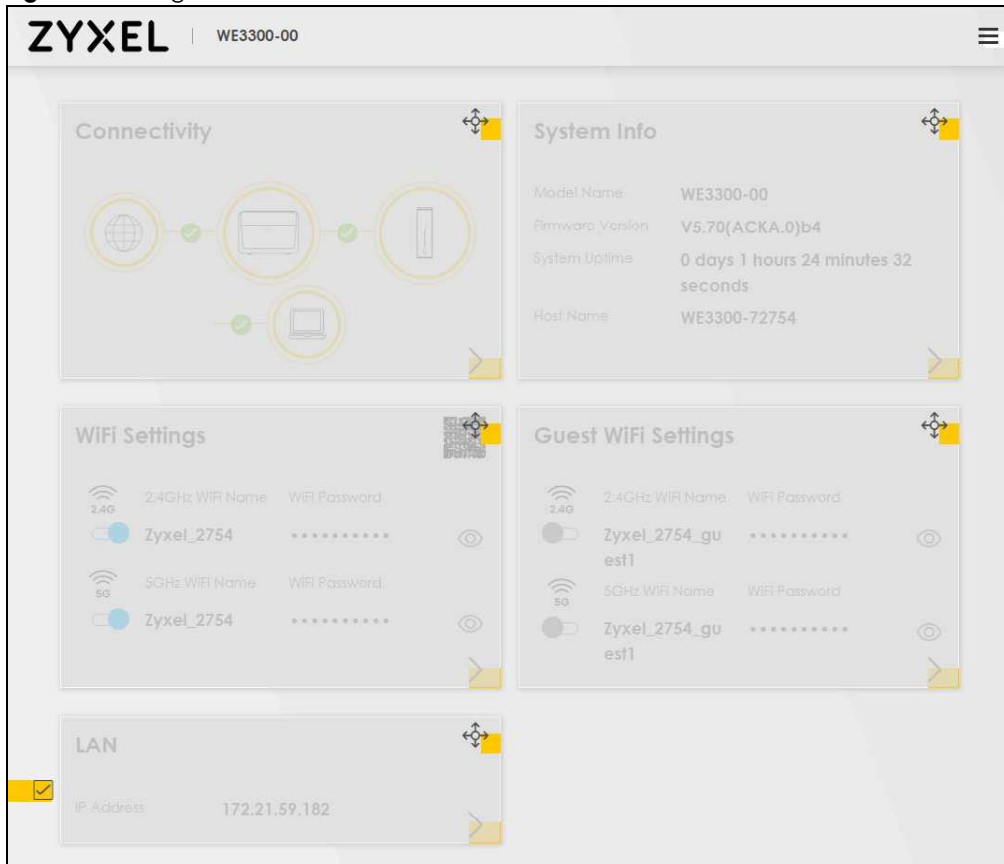
After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access and WiFi settings in this screen. It also shows the network status of the WE Device and computers/devices connected to it.

Figure 35 Connection Status (WE3300-00)



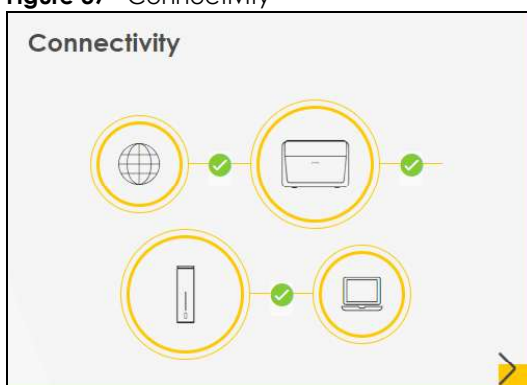
4.1.1 Widget Icon

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

Figure 36 Widget Icon

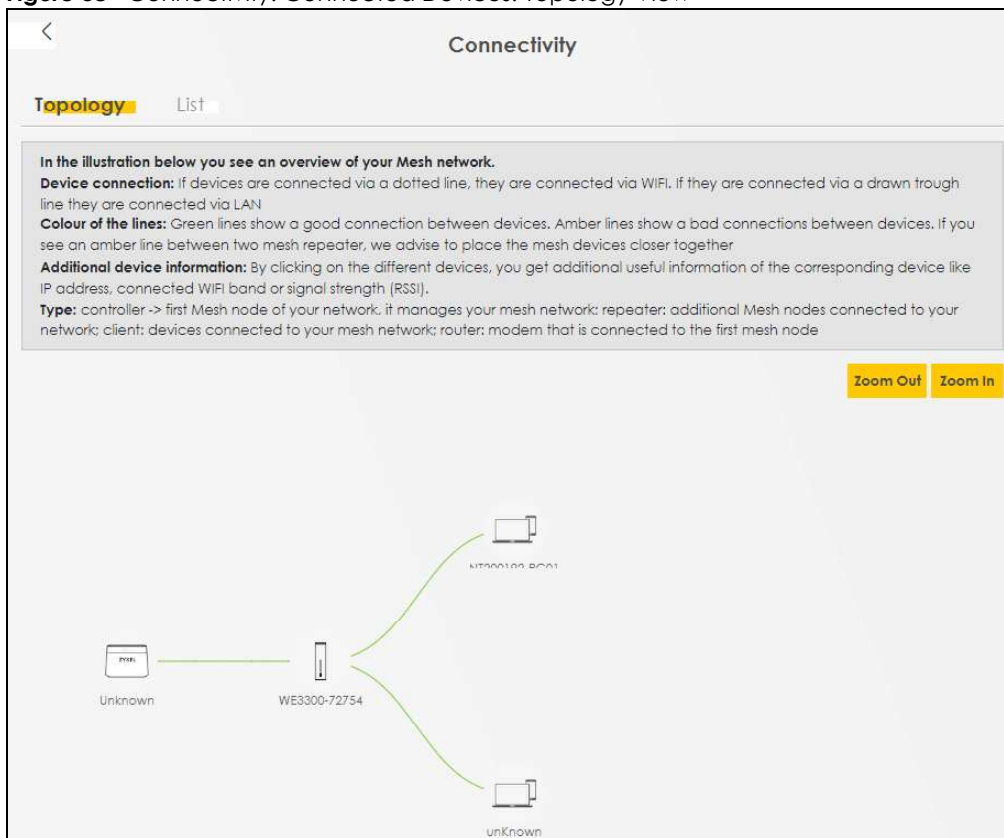
4.1.2 Connectivity

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

Figure 37 Connectivity

Click the Arrow icon () to open the following screen.

Use the **Topology** view screen to display an overview of your Mesh network.

Figure 38 Connectivity: Connected Devices: Topology View

Use the **List** view screen to view IP addresses and MAC addresses of the WiFi and wired devices connected to the WE Device.

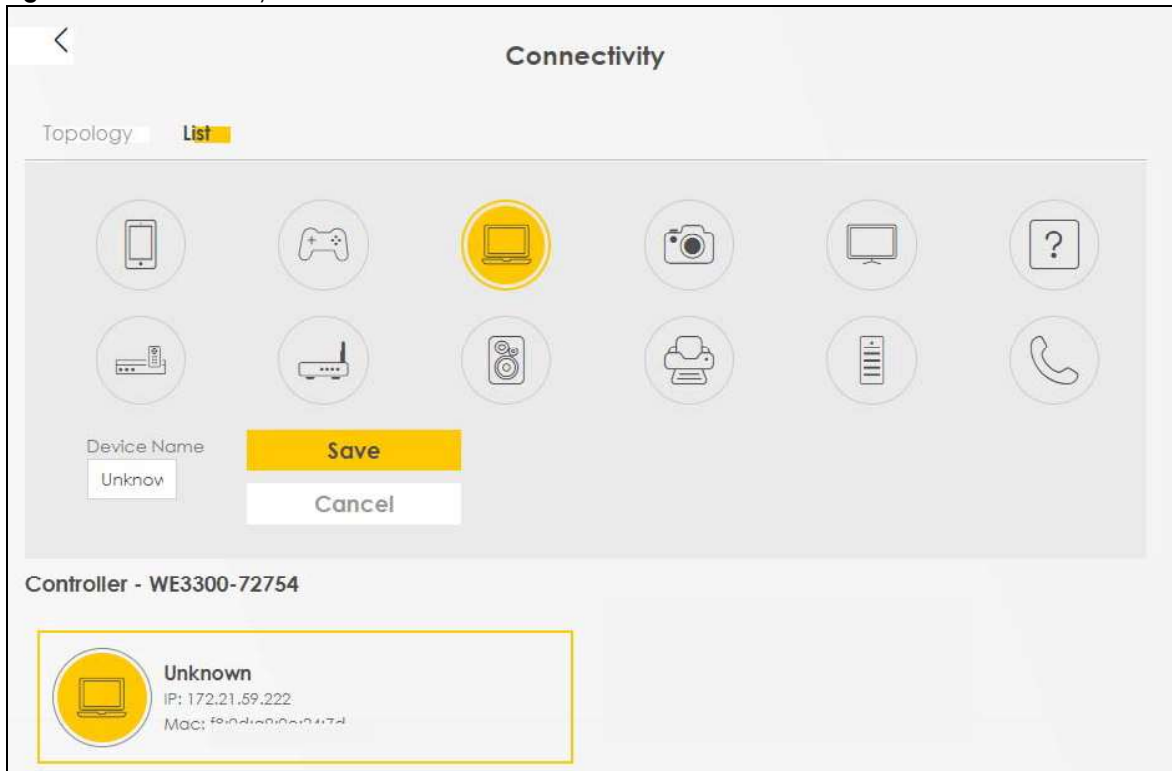
Place your mouse within the device block, and an Edit icon (✎) will appear. Click the Edit icon to change the icon and name of a connected device.

Figure 39 Connectivity: Connected Devices: List View

Icon and Device Name

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

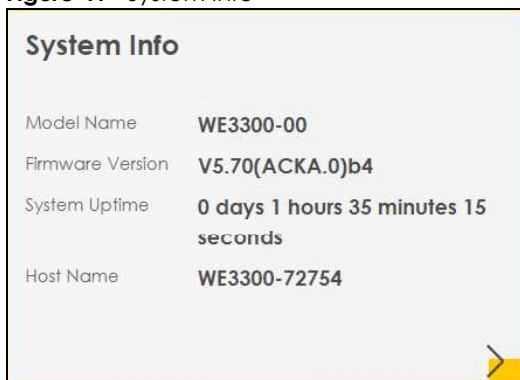
Figure 40 Connectivity: Edit



4.1.3 System Info

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

Figure 41 System Info



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

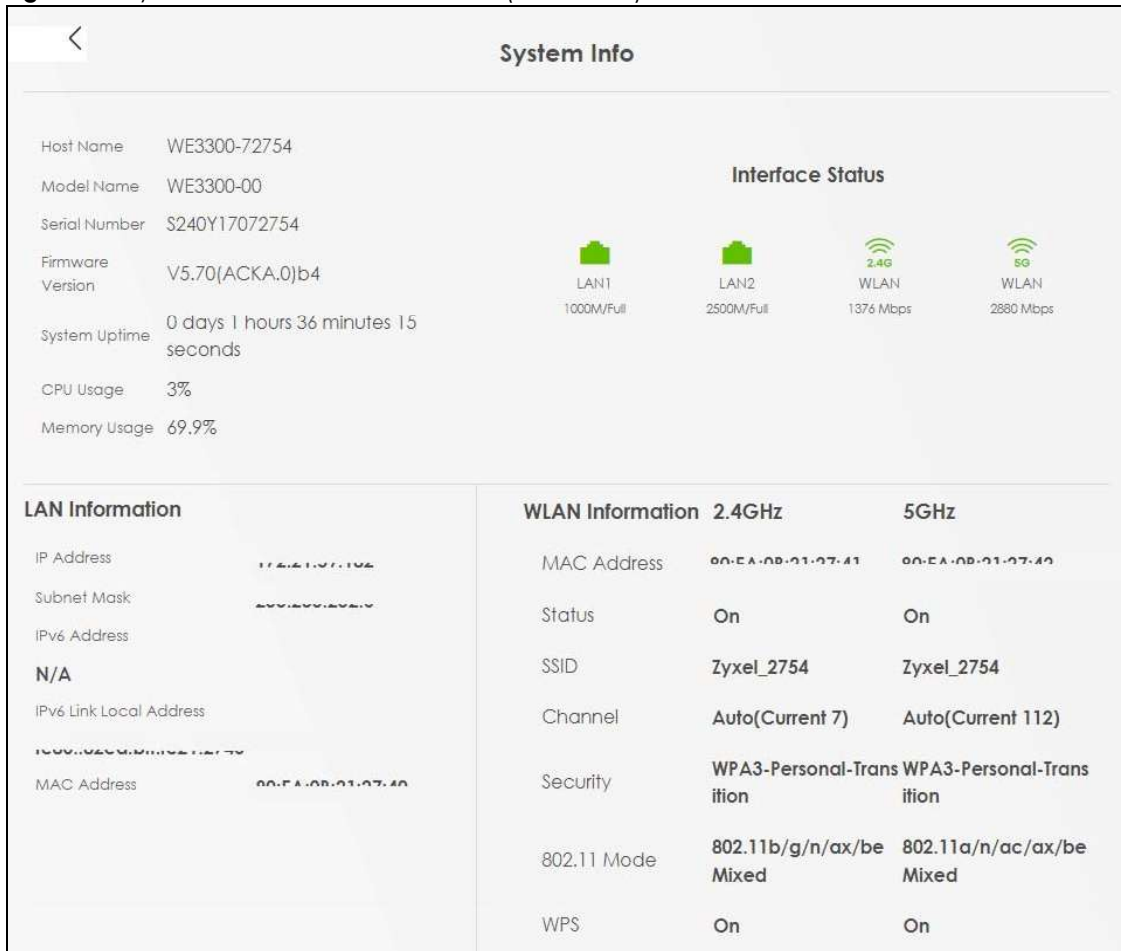
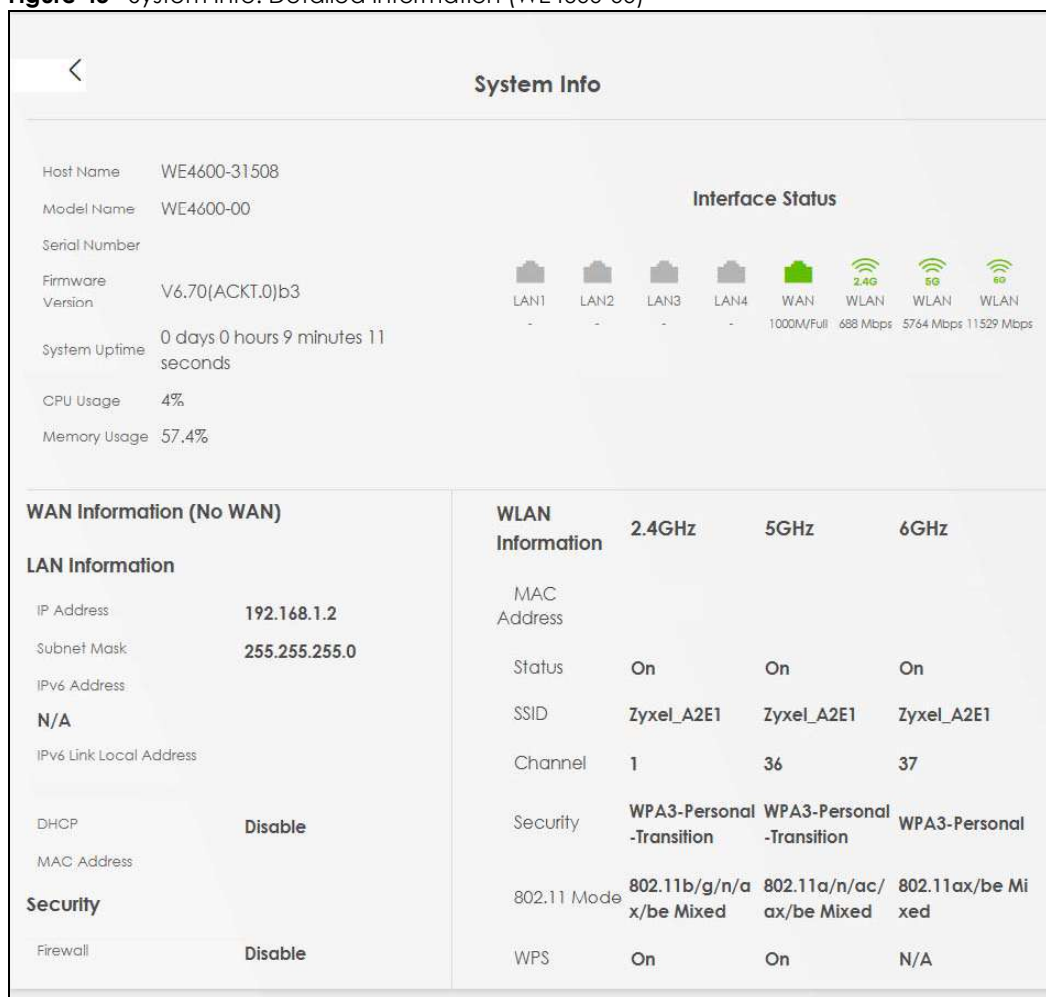
Figure 42 System Info: Detailed Information (WE3300-00)

Figure 43 System Info: Detailed Information (WE4600-00)

Each field is described in the following table.

Table 17 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the WE Device system name. It is used for identification.
Model Name	This shows the model number of your WE Device.
Serial Number	This field displays the serial number of the WE Device.
Firmware Version	The firmware on each WE Device is identified by the firmware trunk version, followed by a unique code which identifies the model, and then the release number after the period. For example, 5.70(ACKA.0) is a firmware for the 5.70 version trunk, the ACKA code identifies the specific WE Device model, and .0 is the first firmware release for this model.
System Uptime	This field displays how long the WE Device has been running since it last started up. The WE Device starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it.
CPU Usage	This displays the current CPU usage percentage.
Memory Usage	This displays the current RAM usage percentage.
Interface Status	Virtual ports are shown here. You can see whether the ports are in use and their transmission rate.

Table 17 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
LAN Information (These fields display information about the LAN ports.)	
IP Address	This is the current IPv4 address of the WE 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 WE Device in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the WE Device for the LAN interface.
MAC Address	This field displays the LAN Ethernet adapter MAC (Media Access Control) address of your WE Device.
WLAN Information 2.4GHz / 5GHz / 6GHz	
MAC Address	This shows the WiFi adapter MAC (Media Access Control) address of the WiFi interface.
Status	This displays whether WiFi is activated.
SSID	This is the descriptive name used to identify the WE Device in a WiFi network.
Channel	This is the channel number used by the WiFi interface now.
Security	This displays the type of security mode the WiFi interface is using in the WiFi network.
802.11 Mode	This displays the type of 802.11 mode the WiFi interface is using in the WiFi network.
WPS	This displays whether WPS is activated on the WiFi interface.

4.2 WiFi Settings

Use this screen to configure the main 2.4G, 5G and/or 6G WiFi network settings. When the switch goes to the right (), the function is enabled. Otherwise, it is not. You can use this screen or the QR code on the upper right to check the SSIDs (WiFi network name) and passwords of the main WiFi networks. If you want to show or hide your WiFi passwords, click the Eye icon ().

Figure 44 WiFi Settings (2.4 GHz and 5 GHz)

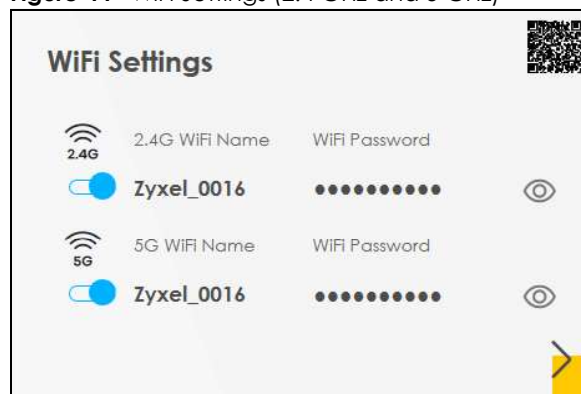
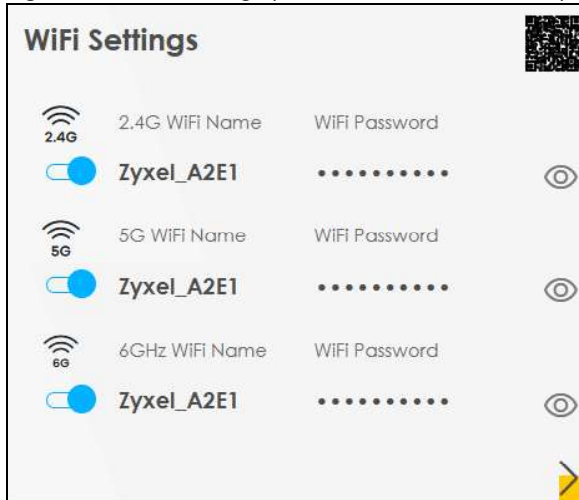


Figure 45 WiFi Settings (2.4 GHz, 5 GHz and 6GHz)

Click the Arrow icon (➡) to open the following screen. Use this screen to configure the SSIDs and/or passwords for your main WiFi networks. When the switch goes to the right (🔵), the function is enabled. Otherwise, it is not.

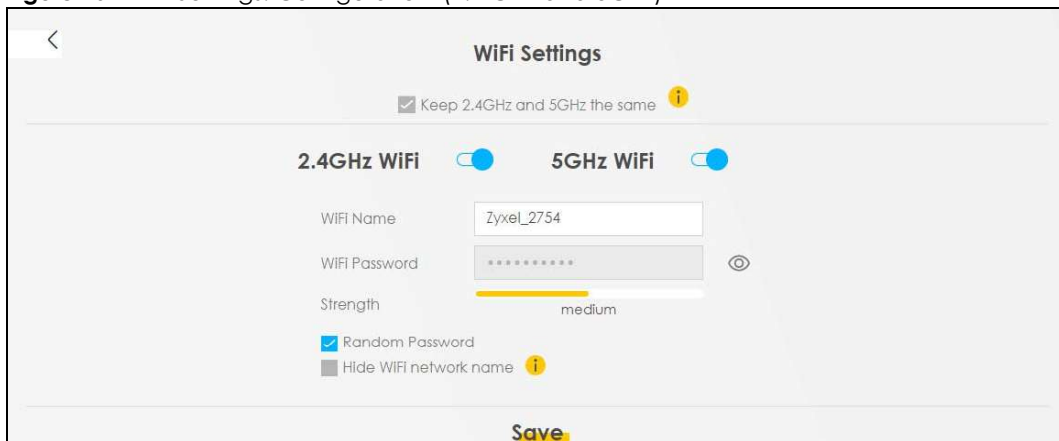
Figure 46 WiFi Settings: Configuration (2.4 GHz and 5GHz)

Figure 47 WiFi Settings: Configuration(2.4 GHz, 5GHz, and 6GHz)

Each field is described in the following table.

Table 18 WiFi Settings: Configuration

LABEL	DESCRIPTION
Keep 2.4GHz, 5GHz, and 6GHz the same	Select the checkbox to set up the 2.4GHz, 5GHz, and 6GHz WiFi networks with the same WiFi Settings. This checkbox cannot be cleared when MESH or MLO is active.
2.4G / 5G / 6G WiFi	Click this switch to enable or disable the 2.4G, 5G and/or 6G WiFi networks. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the WiFi network. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (of up to 32 English keyboard characters) for the WiFi network.
WiFi Password	If you selected Random Password , this field displays a pre-shared key generated by the WE Device. If you did not select Random Password , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password for your WiFi network. When the Eye icon is slashed  , you will see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the WE Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.
Hide WiFi network name	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID.
Save	Click Save to save your changes.

4.3 Guest WiFi Settings

Use this screen to enable or disable the guest 2.4G, 5G and/or 6G WiFi networks. When the switch goes to the right (), the function is enabled. Otherwise, it is not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the Eye icon.

Figure 48 Guest WiFi Settings (2.4GHz and 5GHz)

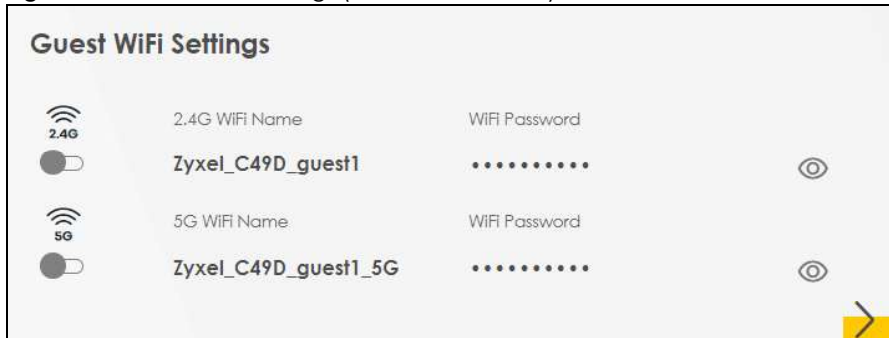


Figure 49 Guest WiFi Settings (2.4GHz, 5GHz, 6GHz)



Click the Arrow icon () to open the following screen. Use this screen to configure the 2.4G and 5G SSIDs and/or passwords for your guest WiFi networks.

Figure 50 Guest WiFi Settings: Configuration (2.4 GHz and 5 GHz)

Figure 51 Guest WiFi Settings: Configuration (2.4 GHz, 5 GHz, and 6GHz)

Each field is described in the following table.

Table 19 WiFi Settings: Configuration

LABEL	DESCRIPTION
2.4G / 5G / 6G WiFi	Click this switch to enable or disable the 2.4G, 5G and/or 6G WiFi networks. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi network.
WiFi Password	If you selected Random Password , this field displays a pre-shared key generated by the WE Device. If you did not select Random Password , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed  , you will see the password in plain text. Otherwise, it is hidden.

Table 19 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
Random Password	Select this option to have the WE Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.
Hide WiFi network name	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID.
Save	Click Save to save your changes.

4.4 LAN Settings

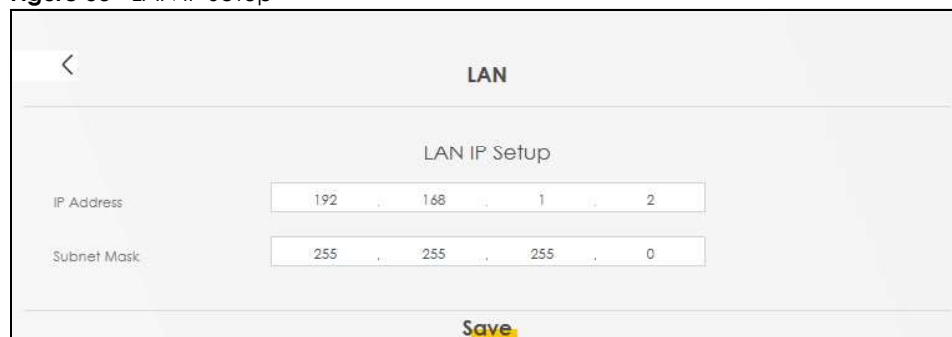
Use this screen to view the LAN IP address and subnet mask of your WE Device.

Figure 52 LAN



Click the Arrow icon () to open the following screen. Use this screen to configure the LAN IP address and subnet mask for your WE Device.

Figure 53 LAN IP Setup



Each field is described in the following table.

Table 20 LAN IP Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your WE Device in dotted decimal notation, for example, 192.168.1.2 (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your WE 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.
Save	Click Save to save your changes.

CHAPTER 5

Web Tutorials

5.1 Overview

This chapter provides Web Configurator tutorials for setting up a secure WiFi network for your WE Device.

5.2 What You Can Do

- [How to Change an Interface IP](#)
- [How to Rename Your Device](#)
- [How to Change the Admin Password](#)
- [How to Set Up a WiFi Network Using WPS](#)
- [How to Set Up a WiFi Network Without WPS](#)
- [How to Set Up Different WiFi Networks Including a Guest Network](#)
- [How to View the Interface Status](#)
- [How to View the WLAN Station Status](#)
- [How to Upgrade the Firmware](#)
- [How to Back up the Device Configuration](#)
- [How to Restore the Device Configuration](#)
- [How to Reset the Device to the Factory Defaults](#)
- [How to View Logs](#)
- [How to Send the System Log through E-mail](#)

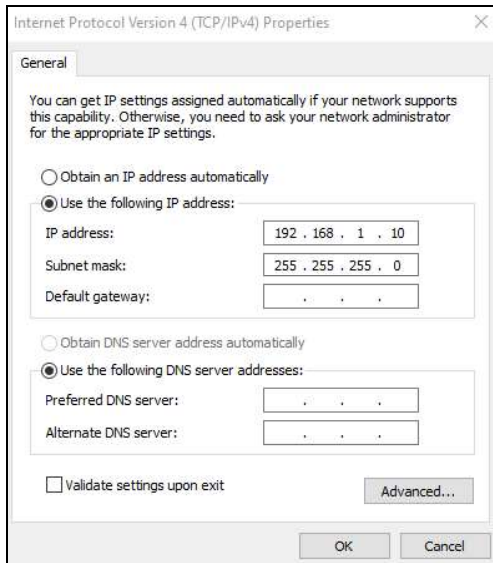
5.3 Device Settings

This section shows you how to change an interface IP, rename your device, and change the admin password.

5.3.1 How to Change an Interface IP

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

- 1 Change your computer's IP address to the same subnet mask as the WE Device. For example, if the default static IP address of the WE Device is 192.168.1.2. Set your computer IP address between 192.168.1.3 and 192.168.1.254.



- 2 Log into the WE Device using the default IP address "192.168.1.2". Go to **Network Setting > Home Networking**. Select **Static IP** in **LAN IP Setup**. Enter your preferred IPv4 address in the **IP Address** field. For instance, "192.168.1.15". Click **Apply** and the web configurator will be disconnected due to the IP address change.

- 3 Enter the new IP address "192.168.1.15" in the address bar to see if you can access the WE Device's web configurator.

5.3.2 How to Rename Your Device

Duplicated device names may confuse network administrators. To change the host name, please follow the steps below:

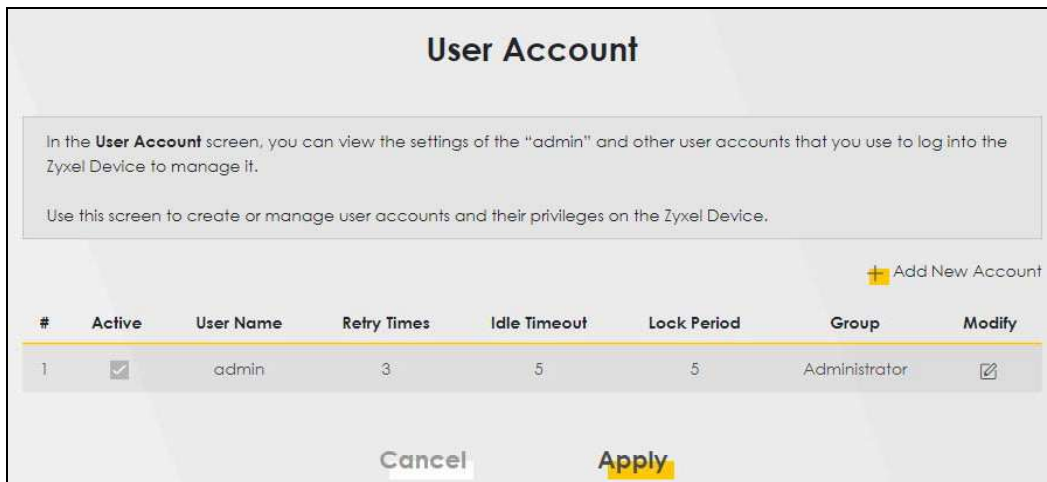
- 1 Go to the **Maintenance > System** screen. Enter a new host name. Click **Apply** to save the new host name.

- 2 Go to the **Connection Status > System Info**. Check if the new host name has been applied successfully.

5.3.3 How to Change the Admin Password

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

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



User Account

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.

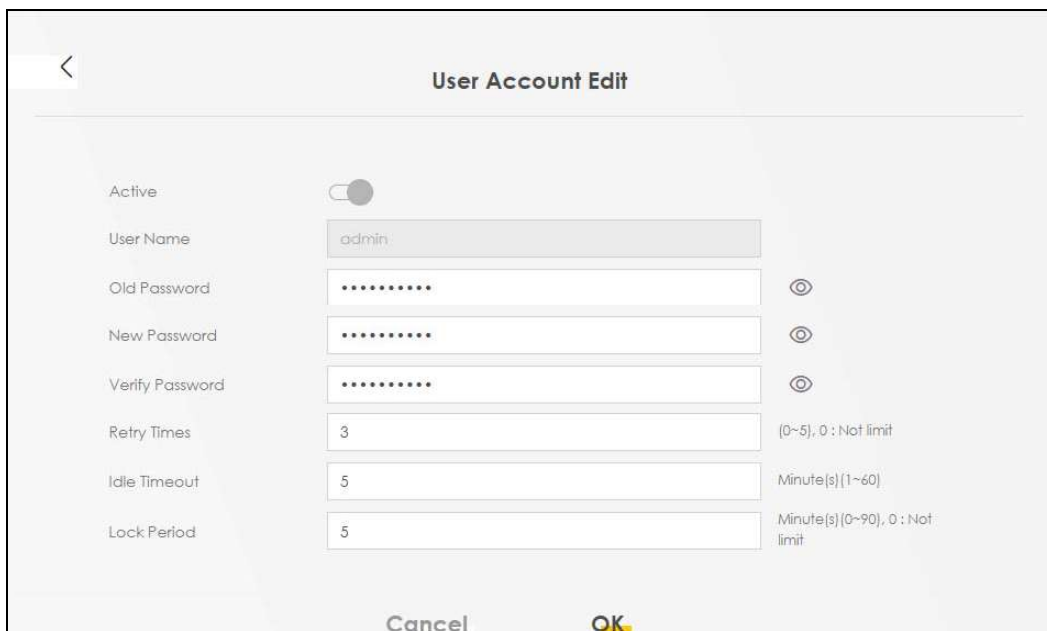
Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

[+ Add New Account](#)

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

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

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



User Account Edit

Active ☒

User Name

Old Password

New Password

Verify Password

Retry Times (0~5), 0 : Not limit

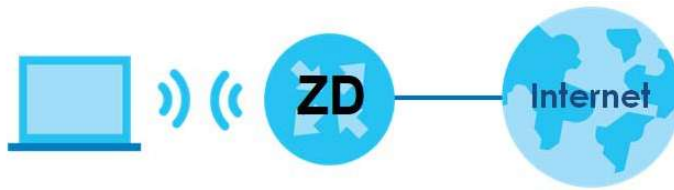
Idle Timeout Minute(s) (1~60)

Lock Period Minute(s) (0~90), 0 : Not limit

[Cancel](#) [OK](#)

5.4 WiFi Network Setup

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



Thomas has to configure the WiFi network settings on the WE Device. Then he can set up a WiFi network using WPS ([Section 5.4.2 on page 72](#)) or manual configuration ([Section 5.4.3 on page 73](#)).

5.4.1 Setting Up a WiFi Network

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

SSID	Example
Security Mode	WPA2-PSK
Pre-Shared Key	DoNotStealMyZyxel1234!
802.11 Mode	802.11b/g/n/ax Mixed

- 1 Click **Network Setting > Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see [Section 5.4.1 on page 70](#)). Click **Apply**.

Wireless

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

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

☐ Keep the same settings for 2.4GHz and 5GHz wireless networks ⓘ

Note

To enable MLO, please enable **Keep the same setting for 2.4G and 5G WiFi networks**

MLO

☐

Wireless Network Setup

Band

2.4GHz

▼

Wireless

☒

Channel

Auto

▼

Current: 3 / 40 MHz

Bandwidth

20/40MHz

▼

Control Sideband

Upper

Wireless Network Settings

Wireless Network Name

ZyxeL_2754

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

80:EA:0B:21:27:41

Security Level

No Security

More Secure
(Recommended)

Security Mode

WPA3-SAE/WPA2-PSK

▼

Protected Management Frames

Capable

☒ Generate password automatically

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

Password

👁

Strength

medium

Cancel

Apply

WE Series User's Guide

71

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

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

Use this screen to configure advanced wireless settings additional security settings, power saving, and data transmission settings.

Output Power 100%

Beacon Interval 100 ms

DTIM Interval 1 ms

802.11 Mode 802.11b/g/n/ax Mixed

Protected Management Frames Capable

Cancel Apply

- 3 You can now use the WPS feature to establish a WiFi connection between your notebook and the WE Device (see [Section 5.4.2 on page 72](#)). You can also use the notebook's WiFi client to search for the WE Device (see [Section 5.4.4 on page 73](#)).

5.4.2 How to Set Up a WiFi Network Using WPS

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

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

- **Push Button Configuration (PBC)** – create a secure WiFi network simply by pressing a button. This is the easier method.
- **PIN Configuration** – create a secure WiFi network simply by entering a WiFi client's PIN (Personal Identification Number) in the WE Device's interface. This is the more secure method, since one device can authenticate the other.

Note: When using WPS in the Web Configurator, and depending on your **Band** selection (**2.4 GHz** or **5 GHz**), the secure connection will apply for the selected **Band** only.

Push Button Configuration (PBC)

- 1 Make sure that your WE Device is turned on and your notebook is within the cover range of the WiFi signal.
- 2 Push and hold the **WPS** button located on the WE Device's front panel for one second. Alternatively, you may log into the WE Device's Web Configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function for method 1 and click **Apply**. Then click the **WPS** button.

(WE3300-00)

Wireless

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

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

General

Band 2.4GHz

WPS

Add a new device with WPS Method

 **Method 1 PBC**

Step1. Click WPS button WPS

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

Note
 (1) The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection.
 (2) The WPS switch is grayed out when wireless LAN is disabled.

Cancel Apply

5.4.3 How to Set Up a WiFi Network Without WPS

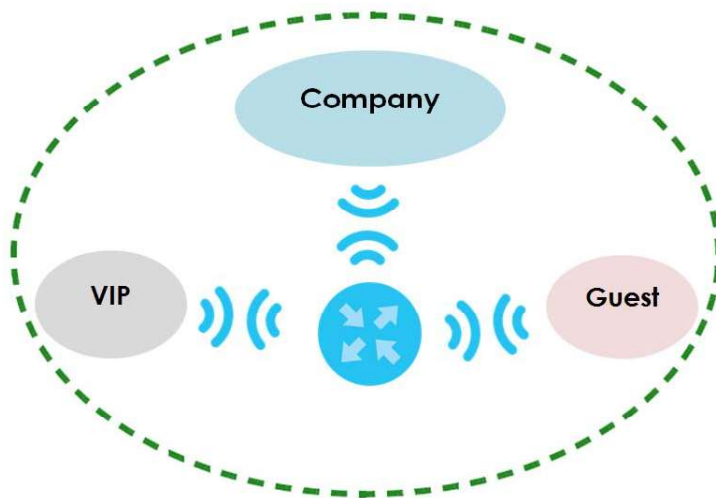
Use the WiFi adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyZyxel1234!" pre-shared key to establish a WiFi Internet connection.

Note: The WE Device supports IEEE 802.11ac/ax WiFi clients. Make sure that your notebook or computer's WiFi adapter supports one of these standards.

5.4.4 How to Set Up Different WiFi Networks Including a Guest Network

A Guest network is for Internet access only through the WE Device.

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



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

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

	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK	WPA2-PSK
Pre-Shared Key	Zyxel8888!	Zyxel1234!	Zyxel4321!

- 1 Click **Network Setting > Wireless** to open the **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**.

Wireless

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

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 ☐ Keep the same settings for 2.4GHz and 5GHz wireless networks ⓘ

Note

To enable MLO, please enable **Keep the same setting for 2.4G and 5G Wifi networks**

MLO ☐

Wireless Network Setup

Band 2.4GHz

Wireless ☒

Channel Auto Current: 5 / 20 MHz

Bandwidth 20/40MHz

Control Sideband Upper

Wireless Network Settings

Wireless Network Name Company

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.

SSID 00:EA:00:21:27:41

Security Level

No Security More Secure (Recommended)

☐ ☒

Security Mode WPA2-PSK

Protected Management Frames Capable

☒ Generate password automatically

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

Password ***** ⓘ

Strength medium

ⓘ

Cancel Apply

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



- 3 Configure the screen using the provided parameters and click **OK**.

More AP Edit

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

Wireless Network Setup

Wireless ☐

Wireless Network Settings

Wireless Network Name: VIP

☐ Hide SSID

☒ Guest WLAN

Access Scenario: External Guest

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

Security Level

No Security More Secure (Recommended)

Security Mode: WPA2-PSK

Protected Management Frames: Capable

☐ Generate password automatically

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

Password:

Strength: medium

Cancel OK

The Guest SSID (**Wireless Network Name**) depends on the state of the Main SSID. For example, when the 2.4 GHz Main SSID is enabled, then the 2.4 GHz Guest SSID can be enabled. But when the 2.4 GHz Main SSID is disabled, then the 2.4 GHz Guest SSID is automatically disabled (cannot be enabled by the user).

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

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

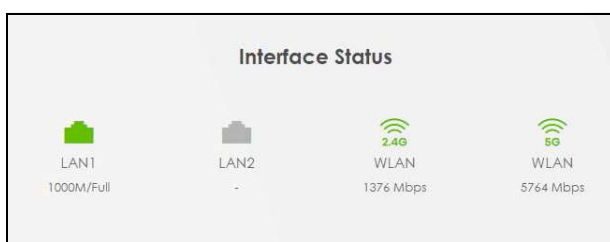
#	Status	SSID	Security	Guest WLAN	Modify
1		Guest	WPA2-Personal	External Guest	
2		VIP	WPA2-Personal	External Guest	

5.5 Traffic Usage

A low transmission rate or weak WiFi signal may cause slow speed or Internet disconnection. Check the transmission rate and signal strength to see if there is any connectivity issue.

5.5.1 How to View the Interface Status

Go to **Connection Status > System Info**. You can view the transmission rate on the WE Device's wired and WiFi connections from **Interface Status**.



5.5.2 How to View the WLAN Station Status

Go to **System Monitor > WLAN Station Status**. You can view the MAC address of the connected devices in each WiFi network band. Check the signal strength, transmission rate, and the ratio of signal power to noise power between the WE Device and connected devices. The **Level** determines the WiFi signal on a scale from 1 to 5. The higher the number, the better the WiFi signal that the WE Device is receiving.

WLAN Station Status

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

Refresh Interval

None

WLAN 2.4G Station Status

#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level
---	-------------	-------------	------------	-----	-------

WLAN 5G Station Status

#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level
1	85:37:00:01:00:03	1201	-46	44	5
2	88:08:10:00:07:00	1201	-48	42	5

WLAN MLO Station Status

#	MAC Address	Rate (Mbps)	RSSI (dBm)	SNR	Level
---	-------------	-------------	------------	-----	-------

5.6 Device Maintenance

This section shows you how to upgrade the firmware, backup and restore the device configuration, and reset the device to the factory default.

5.6.1 How to Upgrade the Firmware

Upload the firmware to the WE Device for feature enhancements.

- 1 Download the firmware file at www.zyxel.com in a compressed file. Decompress the file.
- 2 Go to the **Maintenance > Firmware Upgrade** screen.
- 3 Click **Browse/Choose File** and select a .bin file to upload. Click **Upload**.

Firmware Upgrade

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

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

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

Upgrade Firmware

Reset All Settings After Firmware Upgrade ☐

Reset All Settings Except Mesh After Firmware Upgrade ☐

Current Firmware Version: **V5.70(ACEB.3)b3**

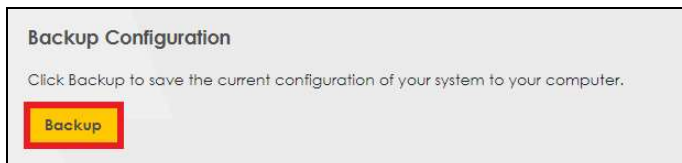
File Path No file chosen

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

5.6.2 How to Back up the Device Configuration

Back up a configuration file in case you want to return to your previous settings.

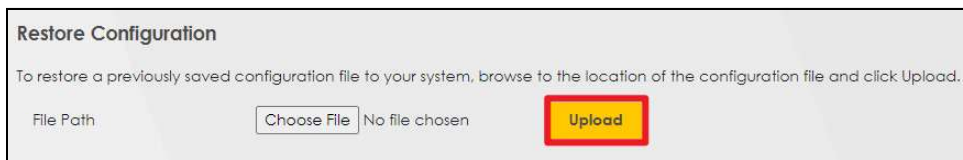
- 1 Go to the **Maintenance > Backup/Restore** screen.
- 2 Click **Backup** in the **Backup Configuration** section, and a configuration file will be saved to your computer.



5.6.3 How to Restore the Device Configuration

You can upload a previously saved configuration file from your computer to your WE Device to restore that previous configuration.

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

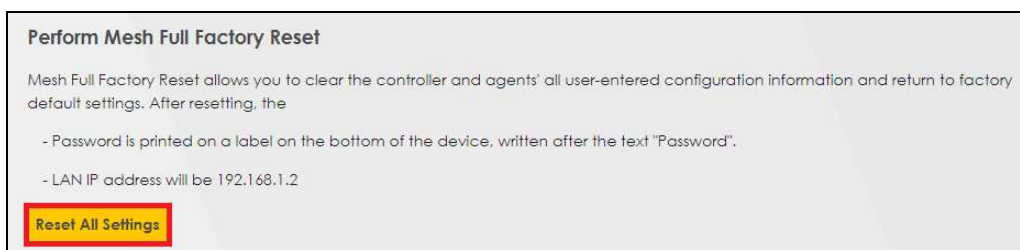


- 3 The WE Device will restart automatically after the configuration file is successfully uploaded. Wait for one minute before logging into the WE Device again.

5.6.4 How to Reset the Device to the Factory Defaults

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

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



If you want to reset the WE Device while keeping the Mesh WiFi Settings, click the **Reset All Settings Except Mesh** button. See [Section 33.2 on page 263](#) for more details.

5.7 System Log

This section will show you how to view logs of the device and send the system log through the E-mail.

5.7.1 How to View Logs

To view the system log of the WE Device, go to **System Monitor > Log**.

Select the **Level** to filter the log by severity. Select the **Category** to filter the log by different features. If you want to download the Log file on your local computer, click **Export Log** to download the WE Device's system log to your local computer.

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

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

#	Time	Facility	Level	Category	Messages
1	Jul 30 09:18:02	user	info	wireless	zcmdModuleCfg: Wifi: Enable SSID(Zyxe1_2754_guest1)
2	Jul 30 08:57:07	user	info	wireless	zHttpd: Wifi:security mode changed!
3	Jul 30 07:21:05	user	info	wireless	zcmdModuleCfg: Wifi: Disable SSID(Zyxe1_2754_guest1)
4	Jul 30 07:12:59	user	info	wireless	zcmdModuleCfg: Wifi: Enable SSID(Zyxe1_2754_guest1)
5	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [ERROR] cwmp_monitor_cwmp(): acs info not ok
6	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [ERROR] cwmp_get_acsInfo(): parse url fail !
7	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [DB] cwmp_get_wanInfo(): boundInterface = IP.Interface.1
8	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [DB] cwmp_get_wanInfo():
9	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [DB] cwmp_cmd_proc(): ipcCmd=19, data=[]
10	Jul 30 04:19:29	daemon	info	tr69	ZTR69: [ERROR] cwmp_init(): get acs info fail!!

5.7.2 How to Send the System Log through E-mail

You can also use the web configurator to send the system log of the WE Device to the specific email addresses. Please follow the steps below:

- 1 Go to **Maintenance > E-mail Notification** and click **Add New e-mail** to create an account to receive notifications and logs.

E-mail Notification

A mail server is an application or a computer that can receive, forward and deliver e-mail messages.

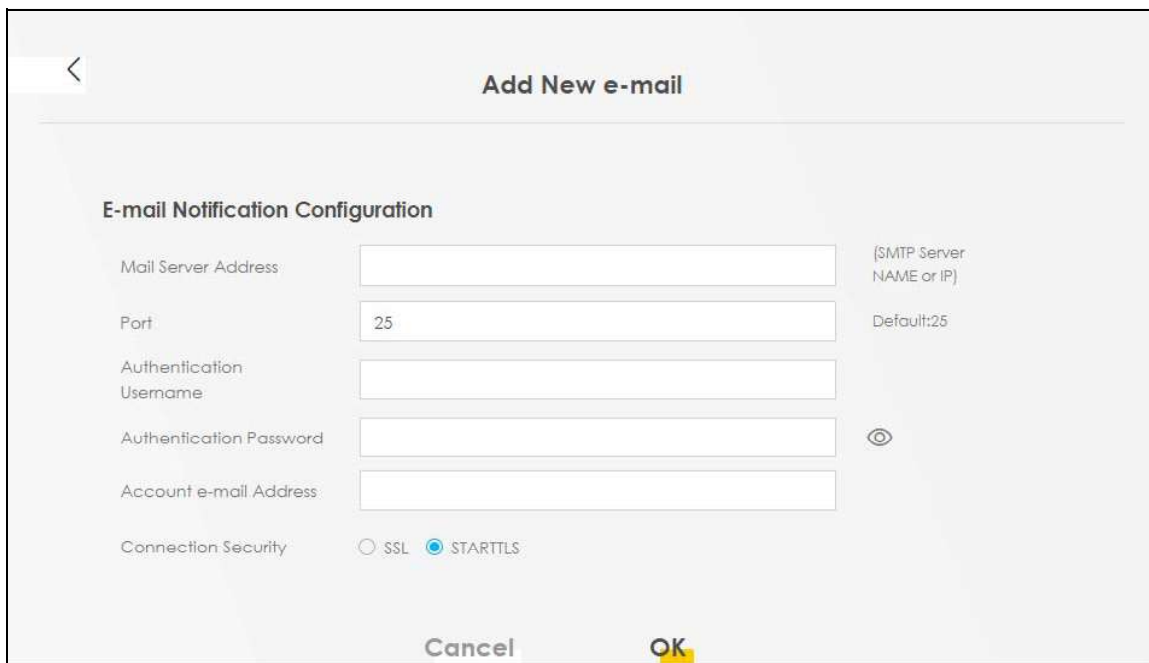
To have the Zyxel Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

Use this screen to view, remove and add e-mail account information on the Zyxel Device. This account can be set to receive e-mail notifications for logs.

[Add New e-mail](#)

Mail Server Address	Username	Port	Security	E-mail Address	Remove

- The **Add New e-mail** screen displays. Enter your server name or the IP address of the mail server for the email address specified in the **Account e-mail Address** field. Enter the port number used by the mail server in the **Port** field. Provide the account user name and password in the **Authentication Username** and **Authentication Password** fields. Choose the protocol used for encryption in **Connection Security** and click **OK**.



The screenshot shows the 'Add New e-mail' configuration screen. At the top, there is a back arrow and the title 'Add New e-mail'. Below the title is the section 'E-mail Notification Configuration'. It contains several input fields: 'Mail Server Address' (with a hint '(SMTP Server NAME or IP)'), 'Port' (with a hint 'Default:25' and the value '25' entered), 'Authentication Username', 'Authentication Password' (with a toggle icon), and 'Account e-mail Address'. At the bottom, there is a 'Connection Security' section with two radio buttons: 'SSL' and 'STARTTLS' (which is selected). At the very bottom, there are 'Cancel' and 'OK' buttons.

- Go to **Maintenance > Log Settings**. Slide the switch for **E-mail Log Settings** to the right. Select the email account you created in **Maintenance > Email Notifications** from the drop-down list in the **Mail Account** field. Enter the subject of the system log email in the **System Log Mail Subject** field and specify the email address to which you want to send the log and the alarm. Set the **Alarm Interval** and click **Apply**.

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 on the syslog server.

Syslog Settings

Syslog Logging ☒

Mode: Local File ▼

Syslog Server: 0.0.0.0 (Server NAME or IPv4/IPv6 Address)

UDP Port: 514 (Server Port)

E-mail Log Settings

E-mail Log Settings ☒

Mail Account: Select one account ▼

System Log Mail Subject:

Send Log to: (E-Mail Address)

Send Alarm to: (E-Mail Address)

Alarm Interval: 60 (seconds)

Active Log

System Log

- ☒ WAN-DHCP
- ☒ TR-069
- ☒ Wireless

Cancel Apply

- 4 Go to **System Monitor > Log** and click **E-mail Log Now**. The system log of the WE Device will be sent to the email address you set up in **Maintenance > Log Settings**.

Log

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

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

#	Time	Facility	Level	Category	Messages
1	Jul 30 09:18:02	user	info	wireless	zcmdModuleCfg: Wifi: Enable SSID(ZyxeI_2754_guest1)
2	Jul 30 08:57:07	user	info	wireless	zHttpd: Wifi:security mode changed!
3	Jul 30 07:21:05	user	info	wireless	zcmdModuleCfg: Wifi: Disable SSID(ZyxeI_2754_guest1)
4	Jul 30 07:12:59	user	info	wireless	zcmdModuleCfg: Wifi: Enable SSID(ZyxeI_2754_guest1)
5	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [ERROR] cwmp_monitor_cwmp(): acs info not ok
6	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [ERROR] cwmp_get_acsInfo(): parse url fail!
7	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [DB] cwmp_get_wanInfo(): boundInterface = IP.Interface.1
8	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [DB] cwmp_get_wanInfo():
9	Jul 30 04:19:30	daemon	info	tr69	ZTR69: [DB] cwmp_cmd_proc(): ipcCmd=19, data=[]
10	Jul 30 04:19:29	daemon	info	tr69	ZTR69: [ERROR] cwmp_init(): get acs info fail!!

CHAPTER 6

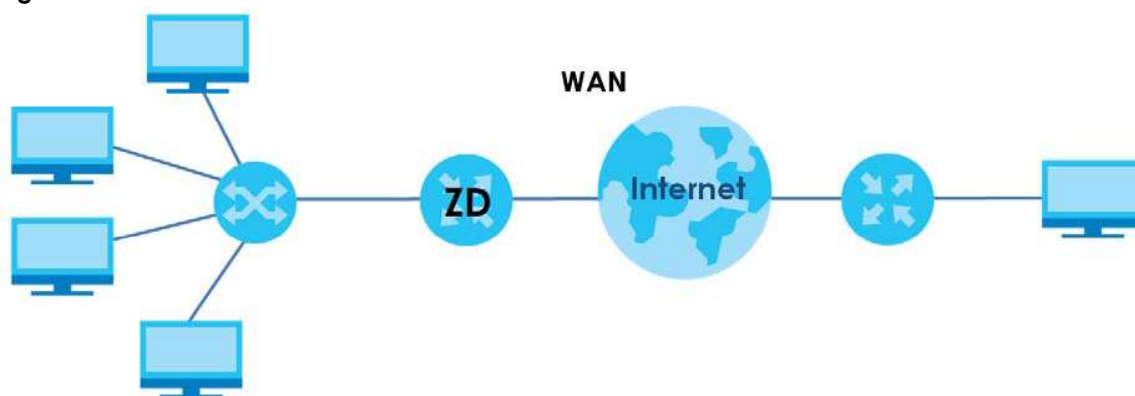
Broadband

6.1 Broadband Overview

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

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

Figure 54 LAN and WAN



6.1.1 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 WE Device for Internet access. See for more information.

Table 21 WAN Setup Overview

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

6.1.2 What You Need to Know

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

WAN IP Address

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

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC).

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

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 3.4×10^{38} IP addresses. The WE 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

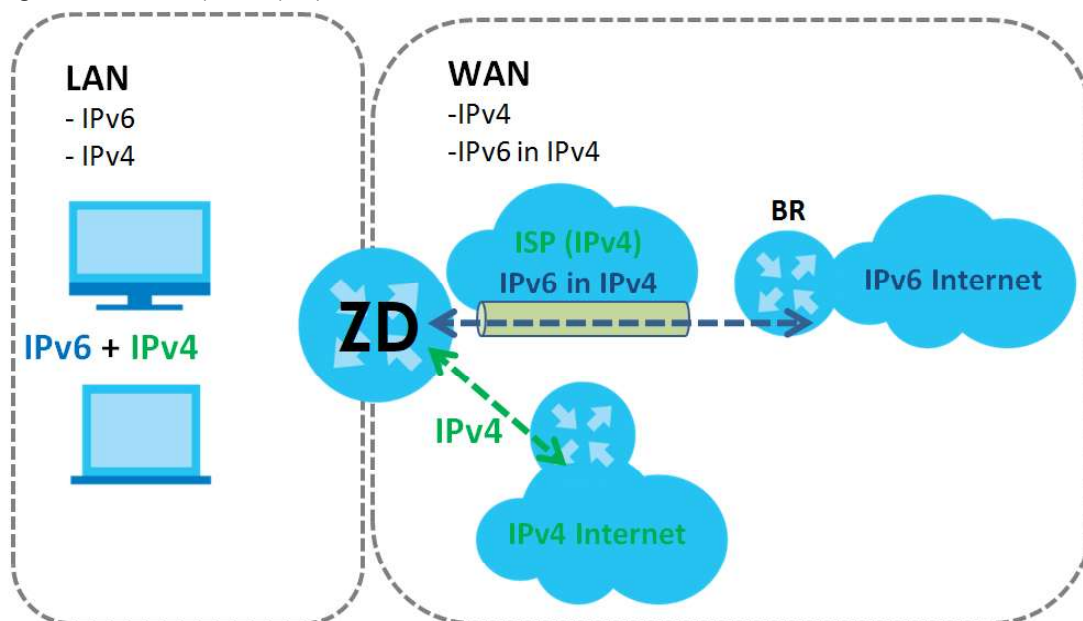
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example, 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 WE 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 WE 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 WE Device uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

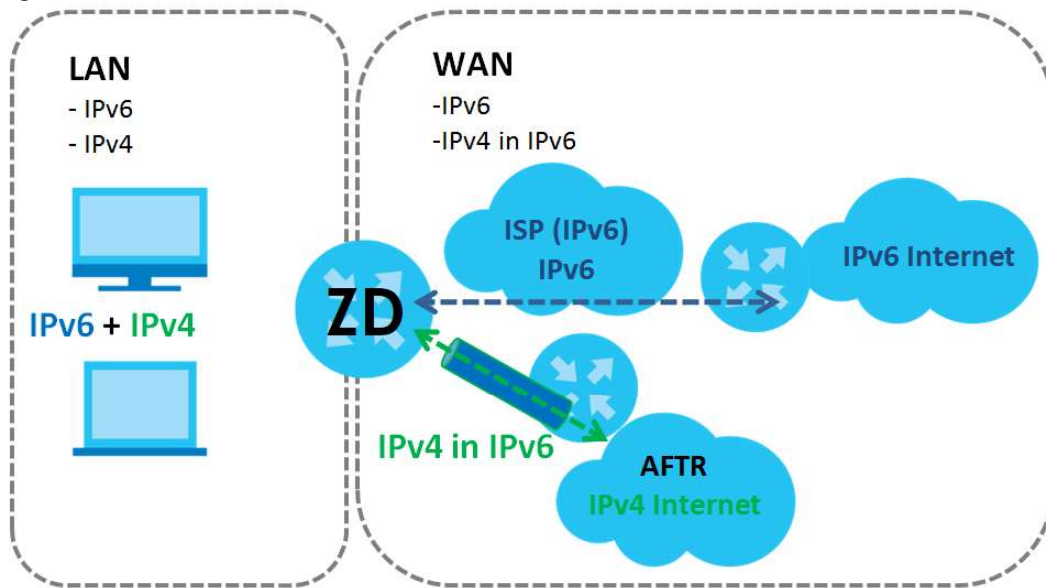
Figure 55 IPv6 Rapid Deployment



Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the WE 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 WE 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 WE Device uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 56 Dual Stack Lite**Carrier-Grade NAT (CGNAT)**

CGNAT allows an Internet Service Provider (ISP) to use a single public WAN IP address for multiple customers with different Internet access devices.

6.1.3 Before You Begin

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

6.2 Broadband Settings for Ethernet Routers

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

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

Figure 57 Network Setting > Broadband

Broadband

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

Add New WAN Interface

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

The following table describes the labels in this screen.

Table 22 Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This displays the type of connections available.
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 WE 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 WE Device use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the Edit icon to configure the WAN connection. Click the Delete icon to remove the WAN connection.

6.2.1 Add or Edit Internet Connection

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

Figure 58 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode)

Add New WAN Interface

General ☒ Name: Type: Ethernet ▼ Mode: Routing ▼ Encapsulation: IPoE ▼ IPv4/IPv6 Mode: IPv4 IPv6 DualStack ▼	VLAN ☒ 802.1p: 0 ▼ 802.1q: (0~4094) MTU MTU: 1500
IP Address ☒ Obtain an IP Address Automatically ☐ Static IP Address DNS Server ☒ Obtain DNS Info Automatically ☐ Use Following Static DNS Address:	Routing Feature NAT: ☒ IGMP Proxy: ☒ Apply as Default Gateway: ☐ Fullcone NAT: ☐
DHCP Options Request Options: ☐ option 42 ☐ option 43 ☐ option 120 ☐ option 121 Sent Options: ☐ option 60: Vendor ID: ☐ option 61: IAID: DUID: ☐ option 125	IPv6 Address ☒ Obtain an IPv6 Address Automatically ☐ Static IPv6 Address IPv6 DNS Server ☒ Obtain IPv6 DNS Info Automatically ☐ Use Following Static IPv6 DNS Address:
IPv6 Routing Feature MLD Proxy: ☒ Apply as Default Gateway: ☒	DHCPv6 Option IPv6 Address From DHCPv6 Server: ☒ Other Information From DHCPv6 Server: ☐

Cancel **Apply**

The following table describes the labels in this screen.

Table 23 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode)

LABEL	DESCRIPTION
General	Click this switch to enable the WAN interface.
Name	Specify a descriptive name for this connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [;]. Spaces are allowed. This field is read-only is you are editing the WAN interface.
Type	This field shows Ethernet and indicates an Ethernet connection. This field is read-only is 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. The choices are PPPoE and IPoE .
IPv4/IPv6 Mode	Select IPv4 Only if you want the WE Device to run IPv4 only. Select IPv4 IPv6 DualStack to allow the WE Device to run IPv4 and IPv6 at the same time. Select IPv6 Only if you want the WE Device to run IPv6 only.
PPP Information (This is available only when you select PPPoE in the Encapsulation field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select password unmask to show your entered password in plain text.
PPP Connection Trigger	Select when to have the WE Device establish the PPP connection. Auto Connect – select this to not let the connection time out. On Demand – select this to automatically bring up the connection when the WE Device receives packets destined for the Internet.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is only available if you select On Demand in the PPP Connection Trigger field.
PPPoE Passthrough	This field is available when you select PPPoE encapsulation. In addition to the WE Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP through the WE Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
VLAN	Click this switch to enable or disable VLAN on this WAN interface. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.

Table 23 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
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. This is available only when you set the Encapsulation to IPoE .
Gateway IP Address	Enter the gateway IP address provided by your ISP. 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.)	
	Select Obtain DNS Info Automatically if you want the WE Device to use the DNS server addresses assigned by your ISP. Select Use Following Static DNS Address if you want the WE Device to use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Routing Feature (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
NAT	Click this switch to activate or deactivate NAT on this connection. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
IGMP Proxy	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Click this switch to have the WE Device act as an IGMP proxy on this connection. When the switch goes to the right  , the function is enabled. Otherwise, it is not. This allows the WE 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 WE Device use the WAN interface of this connection as the system default gateway. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Fullcone NAT Enable	Click this switch to enable or disable full cone NAT on this connection. When the switch goes to the right  , the function is enabled. Otherwise, it is not. This field is available only when you activate NAT . In full cone NAT, the WE Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The WE Device also maps packets coming to that external IP address and port to the internal IP address and port.
DHCP Options (This is available only when you set the Encapsulation to IPoE and select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
Note: The available DHCP options may differ by model.	

Table 23 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
Request Options	Select Option 42 to have the WE Device get NTP time server information from DHCP packets sent from the DHCP server. Select Option 43 to have the WE Device get vendor specific information from DHCP packets sent from the DHCP server. Select Option 120 to have the WE Device get static route information from DHCP packets sent from the DHCP server. Select Option 121 to have the WE Device get SIP server information from DHCP packets sent from the DHCP server.
Sent Options	
option 60	Select this and enter the device identity you want the WE Device to add in the DHCP discovery packets that go to the DHCP server.
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.
option 61	Select this and enter any string that identifies the device.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID	Enter the hardware type, a time value and the MAC address of the device.
option 125	Select this to have the WE Device automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
IPv6 Address (This is available only when you select IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field.)	
Obtain an IPv6 Address Automatically	Select Obtain an IPv6 Address Automatically if you want to have the WE 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 WE 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 WE 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 WE 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 checkbox to have the WE Device act as an MLD proxy on this connection. This allows the WE Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the WE Device use the WAN interface of this connection as the system default gateway.

Table 23 Network Setting > Broadband > Add or Edit New WAN Interface (Routing Mode) (continued)

LABEL	DESCRIPTION
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 87 for more information. Click this switch to enable DS-Lite to let local computers use IPv4 through an ISP's IPv6 network.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
6RD	The 6RD (IPv6 rapid deployment) fields display when you set the IPv6/IPv4 Mode field to IPv4 Only . See IPv6 Rapid Deployment on page 87 for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
	Select Manually Configured if you have the IPv4 address of the relay server. Otherwise, select Automatically configured by DHCP to have the WE Device detect it automatically through DHCP. The Automatically configured by DHCP option is configurable only when you set the method of encapsulation to IPoE .
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1 – 32) for the IPv4 network.
Border Relay IPv4 Address	When you select Manually Configured , specify the relay server's IPv4 address in this field.
DHCPv6 Option (This is available only when you select IPv6 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
IPv6 Address From DHCPv6 Server	Click the switch (to the right) to let the WE Device send DHCP requests to the DHCPv6 server to obtain an IPv6 address.
Other Information From DHCPv6 Server	Click the switch (to the right) to have the WE Device get other information, such as DNS information, from DHCPv6 packets sent from the DHCPv6 server. This will be enabled if IPv6 Address From DHCPv6 Server is enabled.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

Bridge Mode

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

Figure 59 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)

Edit WAN Interface

General ☒

Name: ETHWAN

Type: Ethernet

Mode: Bridge

VLAN ☐

802.1p: 0

802.1q: (0~4094)

MTU

MTU: 1500

Cancel Apply

The following table describes the fields in this screen.

Table 24 Network Setting > Broadband > Add or Edit New WAN Interface (Bridge Mode)

LABEL	DESCRIPTION
General	Click this switch to enable the interface.
Name	Enter a service name of the connection. You can use up to 15 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [\$], [], [&], or [:]. Spaces are allowed. This field is read-only is you are editing the WAN interface.
Type	This field shows Ethernet and indicates an Ethernet connection. 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 QoS, Firewall, DHCP server and NAT on traffic from the selected LAN ports.
VLAN	Click this switch to enable VLAN on this WAN interface.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for traffic through this connection.
Cancel	Click Cancel to exit this screen without saving any changes.
Apply	Click Apply to save your changes.

Figure 60 Network Setting > Broadband > Backup WAN

Use this screen to have the fourth LAN port act as an Ethernet WAN port

State: ☐

Note

(1) Click the switch to set up the configuration. When the switch goes to the right, the fourth LAN port act as an Ethernet WAN port. Otherwise, the fourth LAN port remains as a LAN port.

(2) The Ethernet WAN connection has priority over the DSL connection.

Cancel Apply

The following table describes the fields in this screen.

Table 25 Network Setting > Broadband > Backup WAN

LABEL	DESCRIPTION
State:	Click this switch to enable backup WAN to have the LAN/WAN port act as an Ethernet WAN port. Otherwise, the LAN/WAN port remains as a LAN port.
Cancel	Click Cancel to exit this screen without saving any changes.
Apply	Click Apply to save your changes.

6.3 Technical Reference

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

Encapsulation

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

IP over Ethernet

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

PPP over ATM (PPPoA)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The WE Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

PPP over Ethernet (PPPoE)

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

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

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

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

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

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum

speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

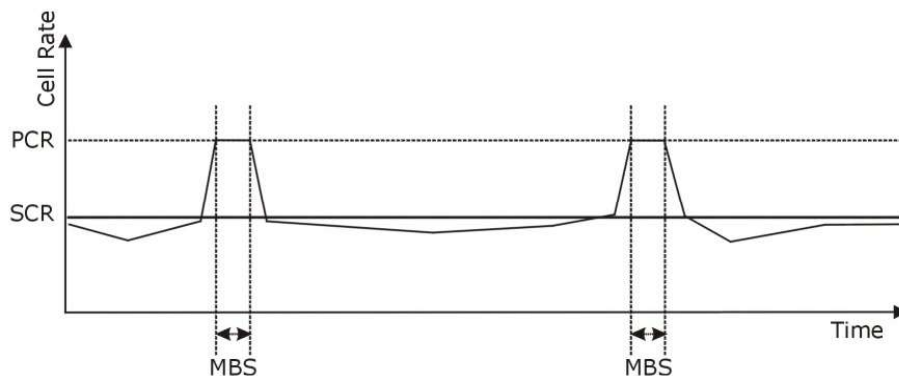
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 61 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (does not tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of a VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR does not guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

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 WE Device queries all directly connected networks to gather group membership. After that, the WE 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 WE 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 WE Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

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

IPv6 Prefix and Prefix Length

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

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

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

CHAPTER 7

Wireless

7.1 Wireless Overview

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

7.1.1 What You Can Do in this Chapter

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

- Use the **General** screen to enable WiFi, enter the SSID and select the WiFi security mode ([Section 7.2 on page 104](#)).
- Use the **Guest/More AP** screen to set up multiple WiFi networks on your WE Device ([Section 7.3 on page 110](#)).
- Use the **MAC Authentication** screen to allow or deny Wi-Fi clients based on their MAC addresses from connecting to the WE Device ([Section 7.4 on page 113](#)).
- Use the **WPS** screen to enable or disable WPS. ([Section 7.5 on page 115](#)).
- Use the **Channel Status** screen to scan WiFi channel noises and view the results ([Section 7.6 on page 117](#)).
- Use the **Mesh** screen to allow wireless clients to roam seamlessly between Mesh supported devices in your Mesh network by using the same SSID and Wi-Fi password ([Section 7.7 on page 118](#)).
- Use the **Operating Modes** screen to manually enter the SSID and security settings of the AP to which you want the WE Device to connect ([Section 7.8 on page 119](#)).
- Use the **AP List** screen to scan the WiFi networks in the WE Device's area. You can also select an AP from the list and enter its WiFi password to connect to the WiFi network ([Section 7.9 on page 122](#)).

7.1.2 What You Need to Know

WiFi Basics

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

WiFi 6 / IEEE 802.11ax

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

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

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 7.10 on page 125](#) for advanced technical information on WiFi networks.

7.2 Wireless General Settings

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

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

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

Figure 62 Network Setting > Wireless > General (2.4 GHz and 5 GHz)

Wireless

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

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 ☐ Keep the same settings for 2.4GHz and 5GHz wireless networks ⓘ

Note

To enable MLO, please enable **Keep the same setting for 2.4G and 5G WiFi networks**

MLO ☐

Wireless Network Setup

Band 2.4GHz ▾

Wireless ☒

Channel Auto ▾ Current: 3 / 40 MHz

Bandwidth 20/40MHz ▾

Control Sideband Upper

Wireless Network Settings

Wireless Network Name ZyxeL_2754

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 80:EA:08:21:27:41

Security Level

No Security More Secure (Recommended)

Security Mode WPA3-SAE/WPA2-PSK ▾

Protected Management Frames Capable

☒ Generate password automatically

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

Password ⓘ

Strength medium

☒

Cancel Apply

Figure 63 Network Setting > Wireless > General (2.4 GHz, 5 GHz, and 6GHz)

Wireless

General

Guest/More AP

WPS

Channel Status

Mesh

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

☒ Keep the same settings for 2.4GHz, 5GHz and 6GHz wireless networks

Keep 2.4GHz, 5GHz and 6GHz the same cannot be turned off when MESH or MLO is active

MLO

☒

Wireless Network Setup

Band

2.4GHz

Wireless

☒

Channel

Auto

Current: 1 / 20MHz

Bandwidth

20/40MHz

Control Sideband

Upper

Wireless Network Settings

Wireless Network Name

Zyxel_A199

Max Clients

64

☐ Hide SSID

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

☒ 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

30:8D:13:6E:A1:99

Security Level

More Secure
(Recommended)

Security Mode

WPA3-SAE/WPA2-PSK

Protected Management Frames

Capable

☒ Generate password automatically

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

Password

☐

Strength

medium

Encryption

AES

Timer

3600

SEC

Cancel

Apply

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

Table 26 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	Select Keep the same settings for 2.4GHz, 5GHz, and 6GHz wireless networks and the 2.4 GHz, 5 GHz, and 6 GHz WiFi networks will use the same SSID and wireless security settings. The setting of 5GHz and 6GHz WiFi networks will follow 2.4G. This switch cannot be turned off when MESH or MLO is enabled. To see if your model supports 6GHz, see Section 1.1 on page 17 for more information.
MLO	Select MLO to allow a WiFi 7 client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K / 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Note: To use MLO, both the AP and the WiFi client have to support MLO.
Wireless Network Setup	
Band	This shows the WiFi band which this radio profile is using. 2.4GHz is the frequency used by IEEE 802.11b/g/n/ax/be WiFi clients, 5GHz is used by IEEE 802.11a/n/ac/ax/be WiFi clients while 6GHz is used by IEEE 802.11a/n/ac/ax/be WiFi clients. Note: For WE3300-00, the Operating Modes and AP List screen are only available if you select the 5GHz Band.
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue , the function is enabled. Otherwise, it is not.
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use Auto to have the WE Device automatically determine a channel to use.
Bandwidth	Select whether the WE Device uses a WiFi channel width of 20MHz, 40MHz, 20/40MHz, 20/40/80MHz, or 20/40/80/160MHz. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The WiFi clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher. Select 20MHz if you want to lessen radio interference with other WiFi devices in your neighborhood or the WiFi clients do not support channel bonding. Because not all devices support 40 MHz channels, select 20MHz or 20/40MHz to allow the WE Device to adjust the channel bandwidth.
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 Network Settings	

Table 26 Network Setting > Wireless > General (continued)

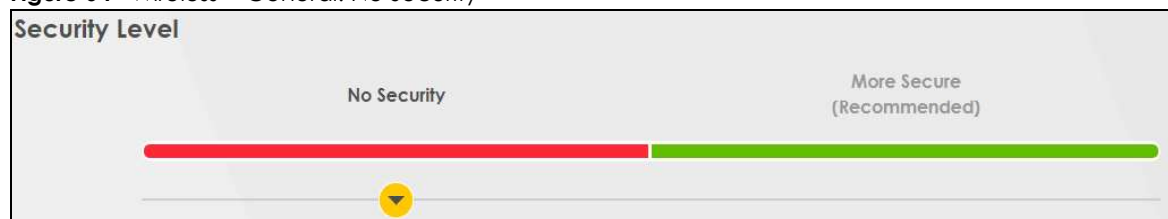
LABEL	DESCRIPTION
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for this WiFi network of up to 32 printable characters, including spaces.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This checkbox is grayed out if the WPS function is enabled in the Network Setting > Wireless > WPS screen.
Multicast Forwarding	Select this checkbox to allow the WE Device to convert WiFi multicast traffic into WiFi unicast traffic.
BSSID	This shows the MAC address of the WiFi interface on the WE Device when WiFi is enabled.
Security Level	
Security Mode	Select More Secure (Recommended) to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as the WE Device. When you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Protected Management Frames	This option is only available when using WPA2-PSK as the Security Mode and AES Encryption in Network Setting > Wireless > General . Management frame protection (MFP) helps prevent WiFi DoS attacks. Select Capable to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select Required to allow only clients that support MFP to join the WiFi network. Note: When Mesh is enabled, the settings of Protected Management Frames of 5G will follow 2.4G.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

7.2.1 No Security

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

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

Figure 64 Wireless > General: No Security



The following table describes the labels in this screen.

Table 27 Wireless > General: No Security

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

7.2.2 More Secure (Recommended)

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

Click **Network Setting > Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA2-PSK**, **WPA3-SAE** or **WPA3-SAE/WPA2-PSK** from the **Security Mode** list.

Figure 65 Wireless > General: More Secure

The following table describes the labels in this screen.

Table 28 Wireless > General: More Secure

LABEL	DESCRIPTION
Security Level	Select More Secure to enable data encryption.
Security Mode	Select the data encryption method the WE Device uses. Select WPA2-PSK , WPA3-SAE or WPA3-SAE/WPA2-PSK to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as this device. Or you can select No Security to allow any client to associate this network without authentication.

Table 28 Wireless > General: More Secure (continued)

LABEL	DESCRIPTION
Protected Management Frames	This option is only available when using WPA2-PSK as the Security Mode and AES Encryption in Network Setting > Wireless > General. Management frame protection (MFP) helps prevent WiFi DoS attacks. Select Capable to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select Required to allow only clients that support MFP to join the WiFi network. Note: When Mesh is enabled, the settings of Protected Management Frames of 5G, 6G will follow 2.4G.
Generate password automatically	Select this option to have the WE Device automatically generate a password. The password field will not be configurable when you select this option.
Password	Select Generate password automatically or enter a Password. The password has two uses. 1. Manual. Manually enter the same password on the WE Device and the client. Make sure the new password must be at least 8 characters, must contain at least one uppercase letter, one lowercase letter, one number, and one special character. Please see the password requirement displayed on the screen. 2. WPS. When using WPS, the WE Device sends this password to the client. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
	Click this  to show more fields in this section. Click again to hide them.
Encryption	This field shows the AES type of data encryption.
Timer	The Timer is the rate at which the RADIUS server sends a new group key out to all clients.

7.3 Guest/More AP

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

The following table introduces the supported WiFi networks.

Table 29 Supported WiFi Networks

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

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

Figure 66 Network Setting > Wireless > Guest/More AP

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

Band 2.4GHz

#	Status	SSID	Security	Guest WLAN	Modify
1		Zyxel_2754_guest1	WPA3-Personal-Transition	External Guest	
2		Zyxel_2754_guest2	WPA3-Personal-Transition	External Guest	
3		Zyxel_2754_guest3	WPA3-Personal-Transition	External Guest	

The following table describes the labels in this screen.

Table 30 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
Band	Select a 2.4GHz , 5GHz , or 6GHz frequency band to display the SSID profile of the selected band.
#	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 WE Device's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a WiFi device is associated. This field displays the name of the WiFi profile on the network. When a WiFi client scans for an AP to associate with, this is the name that is broadcast and seen in the WiFi client utility.
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	This displays if the guest WiFi function has been enabled for this WiFi network. If Home Guest displays, clients can connect to each other directly. If External Guest displays, clients are blocked from connecting to each other directly. N/A displays if the guest WiFi network is disabled.
Modify	Click the Edit icon to configure the SSID profile.

7.3.1 Edit Guest/More AP Settings

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

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

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

More AP Edit

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

Wireless Network Setup

Wireless ☒

Wireless Network Settings

Wireless Network Name: Zyxel_7417_guest1

☐ Hide SSID

☒ Guest WLAN

Access Scenario: External Guest

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

Security Level

No Security More Secure (Recommended)

Security Mode: WPA3-SAE/WPA2-PSK

Protected Management Frames: Capable

☒ Generate password automatically

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

Password:

Strength: weak

Cancel OK

The following table describes the fields in this screen.

Table 31 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Click this switch to enable or disable WiFi in this field. When the switch turns blue  , the function is enabled; otherwise, it is not.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a WiFi device is associated. WiFi devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (of up to 32 English keyboard characters) for WiFi.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WiF is for home and external clients. Select the WiFi type in the Access Scenario field.

Table 31 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Access Scenario	If you select Home Guest, clients can connect to each other directly. If you select External Guest, clients are blocked from connecting to each other directly.
BSSID	This shows the MAC address of the WiFi interface on the WE Device when WiFi is enabled.
Security Level	Select More Secure (Recommended) to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the WE Device. After you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 108 for more details about this field.
Security Mode	Select the security mode the WE Device uses. Select WPA2-PSK, WPA3-SAE or WPA3-SAE/WPA2-PSK to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as this device. Or you can select No Security to allow any client to associate this network without authentication.
Protected Management Frames	This option is only available when using WPA2-PSK as the Security Mode and AES Encryption in Network Setting > Wireless > General. Management frame protection (MFP) helps prevent WiFi DoS attacks. Select Capable to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select Required to allow only clients that support MFP to join the WiFi network. Note: When Mesh is enabled, the settings of Protected Management Frames of 5G, 6G will follow 2.4G.
Generate password automatically	Select this option to have the WE Device automatically generate a password. The password field will not be configurable when you select this option.
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. If you did not select Generate password automatically, you can manually type a pre-shared key that is at least 8 characters and must contains at least one uppercase letter, one lowercase letter, one number, and one special character. Please see the password requirement displayed on the screen. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed , you will see the password in plain text. Otherwise, it is hidden.
	Click this  to show more fields in this section. Click again to hide them.
Encryption	This field shows the AES type of data encryption.
Timer	The Timer is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

7.4 MAC Authentication

This screen allows you to configure the WE Device to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the WE Device (**Deny**) based on the device(s) MAC address. Every Ethernet device has a unique MAC (Media Access Control) address. It is assigned at the factory

and consists of six pairs of hexadecimal characters; for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the device(s) you want to allow/deny to configure this screen.

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

Figure 68 Network Setting> Wireless > MAC Authentication

Wireless

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

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

General

SSID:

MAC Restrict Mode: ☐ Disable ☐ Deny ☒ Allow

MAC address List

Add new MAC address

#	MAC Address	Modify

Cancel **Apply**

The following table describes the labels in this screen.

Table 32 Network Setting > Wireless > MAC Authentication

LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the MAC Address table. Select Disable to turn off MAC filtering. Select Deny to block access to the WE Device. MAC addresses not listed will be allowed to access the WE Device. Select Allow to permit access to the WE Device. MAC addresses not listed will be denied access to the WE Device.
MAC Address List	
Add New MAC Address	This field is available when you select Deny or Allow in the MAC Restrict Mode field. Click this if you want to add a new MAC address entry to the MAC filter list below.
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the Wi-Fi devices that are allowed or denied access to the WE Device.
Modify	Click the Edit icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the Delete icon to delete the entry.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

7.4.1 Add/Edit MAC Addresses

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

Enter the MAC addresses of the Wi-Fi devices that are allowed or denied access to the WE Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

Figure 69 Network Setting > Wireless > MAC Authentication > Add/Edit

7.5 WPS Settings

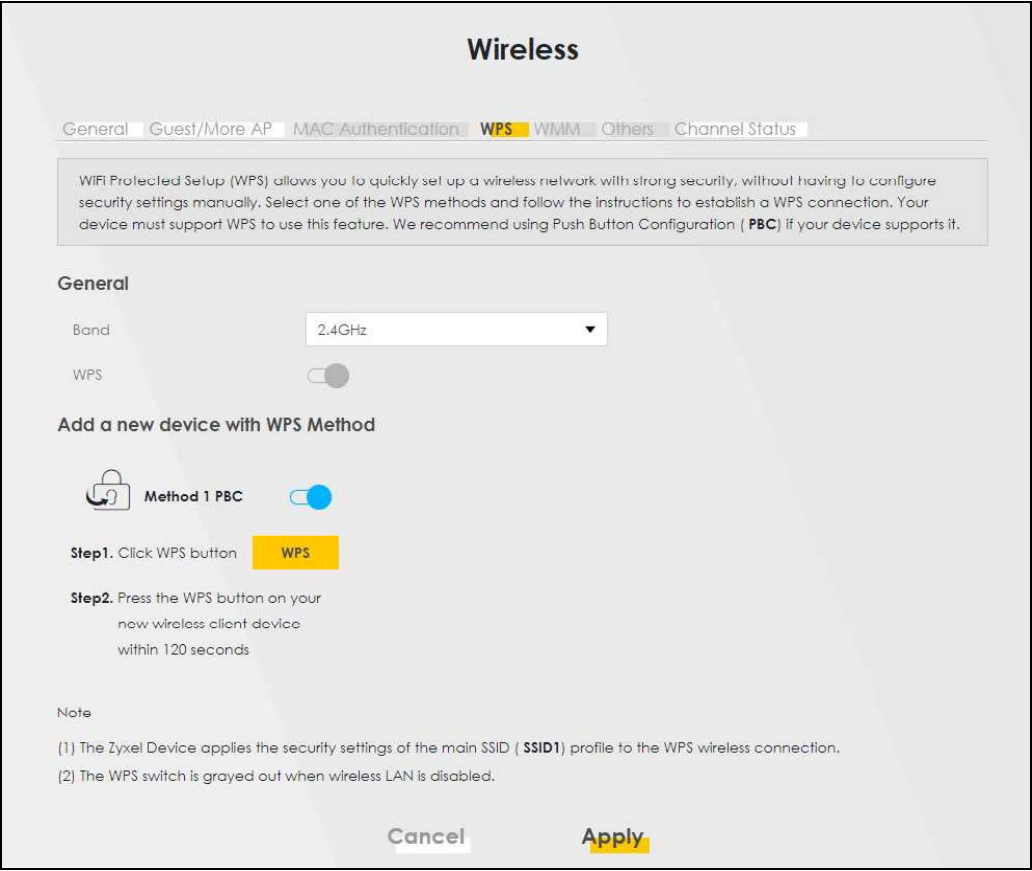
WiFi Protected Setup (WPS) allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (**PBC**) method if your WiFi client supports it. See [Section 7.10.8.3 on page 133](#) for more information about WPS.

Note: The WE Device applies the security settings of the main SSID (**SSID1**) profile (see [Section 7.2 on page 104](#)).

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

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

Figure 70 Network Setting > Wireless > WPS



The following table describes the labels in this screen.

Table 33 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
Band	Select a 2.4GHz, 5GHz, and 6GHz frequency band to enable WPS for all WiFi networks in the selected band.
WPS	Click this switch to activate or deactivate WPS on this WE Device. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS WiFi network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click Apply to activate WPS method 1 on the WE Device.
WPS	Click this button to add another WPS-enabled WiFi device (within WiFi range of the WE Device) to your WiFi network. This button may either be a physical button on the outside of device, or a menu button similar to the WPS button on this screen. Note: You must press the other WiFi device's WPS button within 2 minutes of pressing this button.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

7.6 Channel Status Settings

Use the **Channel Status** screen to scan WiFi channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Select a band and click **Scan** to scan for available WiFi channels in the band. You can view the results in the **Channel Scan Result** section.

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

Figure 71 Network Setting > Wireless > Channel Status



7.7 Mesh

Use this screen to enable or disable AP steering and band steering.

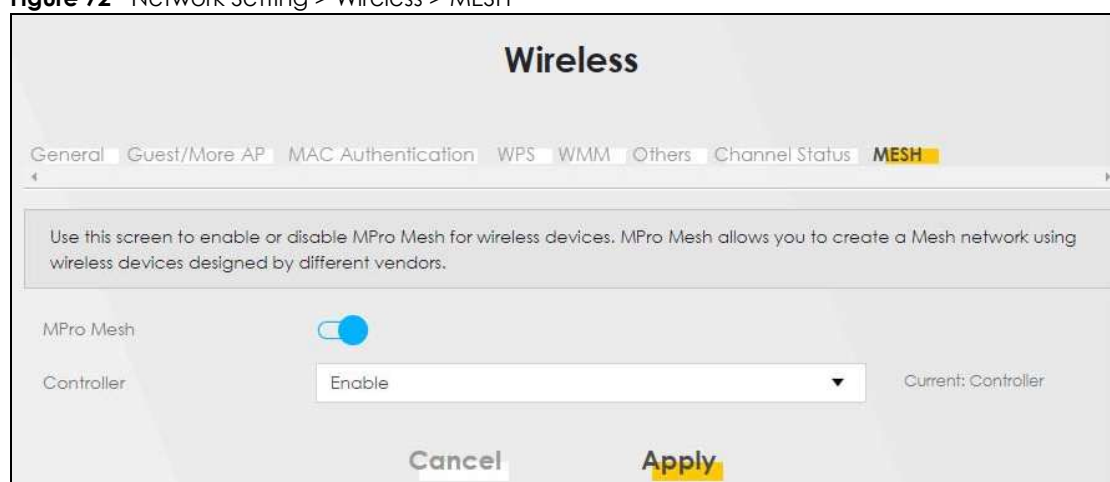
- AP steering allows wireless clients to roam seamlessly between supported devices in your network by using the same SSID and Wi-Fi password. Also, AP steering helps monitor wireless clients and drop their connections to optimize the WE Device bandwidth when the clients are idle or have a low signal. When a wireless client is dropped, it has the opportunity to steer to a supported device with a strong signal.
- Band steering allows wireless clients to steer from one band to another. For example, if the 2.4GHz channel is congested/lower signal strength, wireless clients that support 5GHz could be moved to the 5GHz channel. The wireless client can also return to the 2.4GHz channel.

The WE Device acts as a controller to manage and coordinate wireless activity in a network, such as:

- AP steering
- Band steering
- Management of SSIDs and password on all APs in a network

For example, if you change the SSID on a router, all the SSIDs of APs in a network will be changed as well. Click **Network > Wireless > MESH**. The following screen displays.

Figure 72 Network Setting > Wireless > MESH



The following table describes the labels in this screen.

Table 34 Network Setting > Wireless > MESH

LABEL	DESCRIPTION
MPro Mesh	Click this switch to allow the wireless client to steer to a supported device with a strong signal, or connect to the less congested 2.4GHz/5GHz channel. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
Controller	Select Enable to have the WE Device act as the Controller in the MPro Mesh Wi-Fi Network. The Controller synchronizes the configuration of all the Wi-Fi devices, including APs and extenders (Agents) in the MPro Mesh Wi-Fi network. Select Disable to have the WE Device act as an extender (Agent) in the MPro Mesh Wi-Fi Network. Select Auto for the WE Device to select its role automatically. The WE Device sends the packet first as an extender (Agent). If the WE Device fails to receive the response packet from other controllers, it becomes the Controller.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

7.8 Operating Modes Settings

Use this screen to manually enter the SSID and security settings of the AP to which you want the WE Device to connect. This screen allows you to set up a profile when the WE Device is in Repeater mode. The WE Device will connect to the AP specified in the profile each time it turns on.

Click **Network Setting > Wireless > Operating Modes**. The screen appears as shown.

Note: For the WE Devices that does not meet Wi-Fi 7 standards, the **Operating Modes** is available when you select 5 GHz Wi-Fi connection. (See [Table 1 on page 17](#) for more information).

Figure 73 Network Setting > Wireless > Operating Modes

Wireless

General

Guest/More AP

MAC Authentication

WPS

WMM

Others

Channel Status

Operating Modes

AP List

Use the Operating Modes screen to access the Wireless AP, enter the SSID and select the wireless security mode. You can also use WiFi Protected Setup (WPS) to access AP without having to configure security settings manually.

Operating Modes

Modes

Repeater Mode

Wireless Setup

Wireless Network Name

Connection Status

Not Connected

No Security

More Secure
(Recommended)

Security Mode

WPA2-PSK

Password

WPS Setup

WPS

Add a new device with WPS Method

Method 1 PBC

Step1. Click WPS button

WPS

Cancel

Apply

WE Series User's Guide

120

Figure 74 Network Setting > Wireless > Operating Modes

Wireless

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

AP List

Use the Operating Modes screen to access the Wireless AP, enter the SSID and select the wireless security mode. You can also use WiFi Protected Setup (WPS) to access AP without having to configure security settings manually.

Operating Modes

Band 2.4GHz

Modes Repeater Mode

Wireless Setup

Wireless Network Name

Connection Status Not Connected

No Security More Secure (Recommended)

Security Mode WPA2-PSK

Password

WPS Setup

WPS

Add a new device with WPS Method

Method 1 PBC

Step 1. Click WPS button

WPS

Cancel Apply

The following table describes the labels in this screen.

Table 35 Network Setting > Wireless > Operating Modes

LABEL	DESCRIPTION
Operating Modes	
Band	Select the band you want to use for the WiFi connection.

Table 35 Network Setting > Wireless > Operating Modes (continued)

LABEL	DESCRIPTION
Modes	This displays the operating mode of the WE Device. • If the WE Device is connected to the AP using a cable, the WE Device will be in the AP mode. • If the WE Device is connected to the AP wirelessly, the WE Device will be in the repeater mode.
Wireless Setup	
Wireless Network Name	Enter the name of the WiFi network (SSID) to which the WE Device is connecting.
Security Mode	Select the security mode the AP uses from the drop down list box.
Password	Enter the password of the WiFi network to which the WE Device is connecting.
WPS Setup	
WPS	Select this to activate or deactivate the WPS method.
Click WPS button	Click this to connect the WE Device to the AP using the WPS method.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

7.9 AP List Screen

You can use this screen to select an AP and enter its WiFi password to connect to the WiFi network.

Click **Network Setting > Wireless > AP List**. The screen appears as shown.

Note: For the WE Devices that does not meet Wi-Fi 7 standards, the **AP List** is available when you select 5 GHz Wi-Fi connection.

Figure 75 Network Setting > Wireless > AP List

Wireless

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

AP List

Use the AP List screen to scan wireless APs and view the results. Click Rescan to scan the wireless APs. You can view the results in the following table.

ACCESS POINT LIST:

Connection Status: Not Connected
Current SSID:

#	Active:	SSID:	MAC Address:	Channel:	RSSI(dbm):	Security:
AP: Password: Connect						

Rescan

Network Setting > Wireless > AP List

Wireless

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

AP List

Use the AP List screen to scan wireless APs and view the results. Click Rescan to scan the wireless APs. You can view the results in the following table.

ACCESS POINT LIST:

Band: 2.4GHz

Connection Status: Not Connected

Current SSID:

#	Active	SSID	MAC Address	Channel	RSSI(dbm)	Security

AP:

Password:

Connect

Rescan

The following table describes the labels in this screen.

Table 36 Network Setting > Wireless > AP List

LABEL	DESCRIPTION
Band	Select the band you want to use for the WiFi connection.
Connection Status	This shows whether the WE Device is already connected, attempting to connect, or not connected to a WiFi network.
Current SSID	This shows the name of the AP to which your WE Device is currently connected.
#	This is the index number of the AP the WE Device can detect.
Active	This field indicates whether the AP is active or not.
SSID	This shows the network name of the AP the WE Device can detect.
MAC Address	This shows the MAC address of the AP.
Channel	This shows the channel the AP uses.
RSSI (dbm)	This shows the strength of the AP's radio signal measured in dbm.
Security	This shows Yes if the WE Device needs a security password to connect to the AP. It shows No if the WE Device does not need a password to connect.
AP	This shows the name of the AP you click and try to connect.
Password	The Password input box displays when the Security column is Yes for the selected SSID. Enter the password for this WiFi network in the Password input box.

Table 36 Network Setting > Wireless > AP List

LABEL	DESCRIPTION
Connect	The Connect button appears at the end of the table after you click on a SSID. Click this button to connect to the selected AP.
Rescan	Click Rescan to refresh the list of APs available.

7.10 Technical Reference

This section discusses WiFi in depth. For more information, see [Appendix B on page 282](#).

7.10.1 WiFi Network Overview

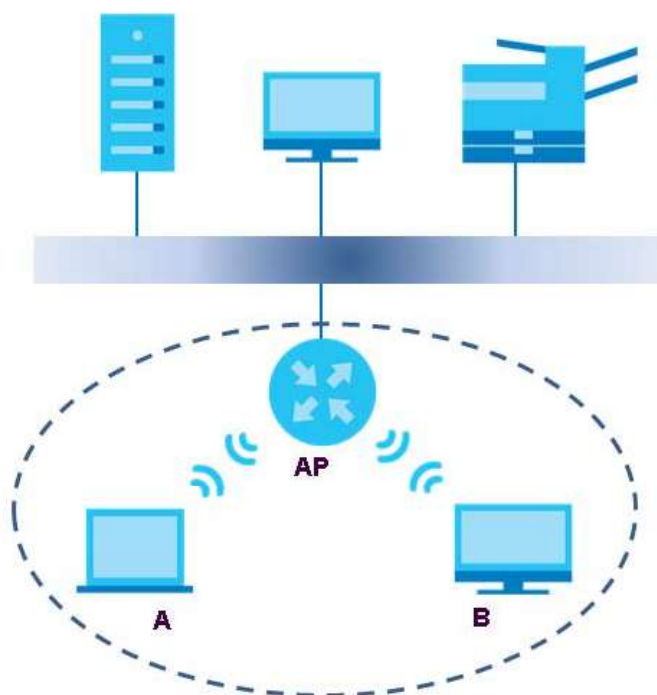
WiFi networks consist of WiFi clients, access points and bridges.

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

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

- 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.
- An "ad-hoc" type of network is one in which there is no access point. WiFi clients connect to one another in order to exchange information.

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 WE 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.

Radio Channels

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

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

7.10.2 Additional WiFi Terms

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

Table 37 Additional WiFi Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a WiFi network which covers a large area, WiFi devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the WiFi devices must sometimes get permission to send information to the WE Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then WiFi devices never have to get permission to send information to the WE 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 WE Device does, it cannot communicate with the WE 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.

7.10.3 WiFi Security Overview

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

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a user name 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.

7.10.3.1 SSID

Normally, the WE Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the WE 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.

7.10.3.2 MAC Address Filter

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

You can use the MAC address filter to tell the WE 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.

7.10.3.3 User Authentication

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

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

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

7.10.3.4 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.

1. Some WiFi devices, such as scanners, can detect WiFi networks but cannot use WiFi networks. These kinds of WiFi 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 38 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.

7.10.4 Signal Problems

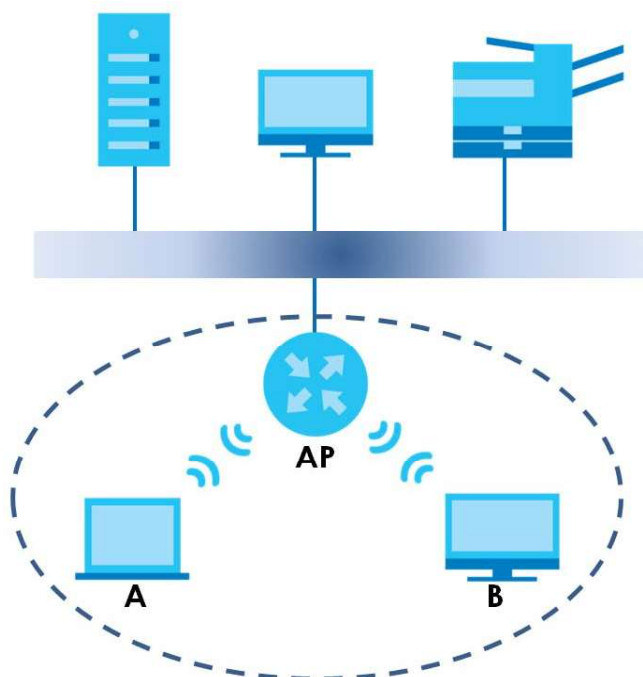
Because WiFi networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

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

7.10.5 BSS

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

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

Figure 77 Basic Service Set

7.10.6 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 WE 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.

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

7.10.6.1 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 WiFi devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

7.10.7 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 WiFi adapters support long preamble, but not all support short preamble.

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

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

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

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

7.10.8 WiFi Protected Setup (WPS)

Your WE 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.

7.10.8.1 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 WiFi range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the WE Device, see [Section 7.5 on page 115](#)).
- 3 Press the button on one of the devices (it does not matter which). For the WE Device you must press the WPS 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.

7.10.8.2 PIN Configuration

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

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

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

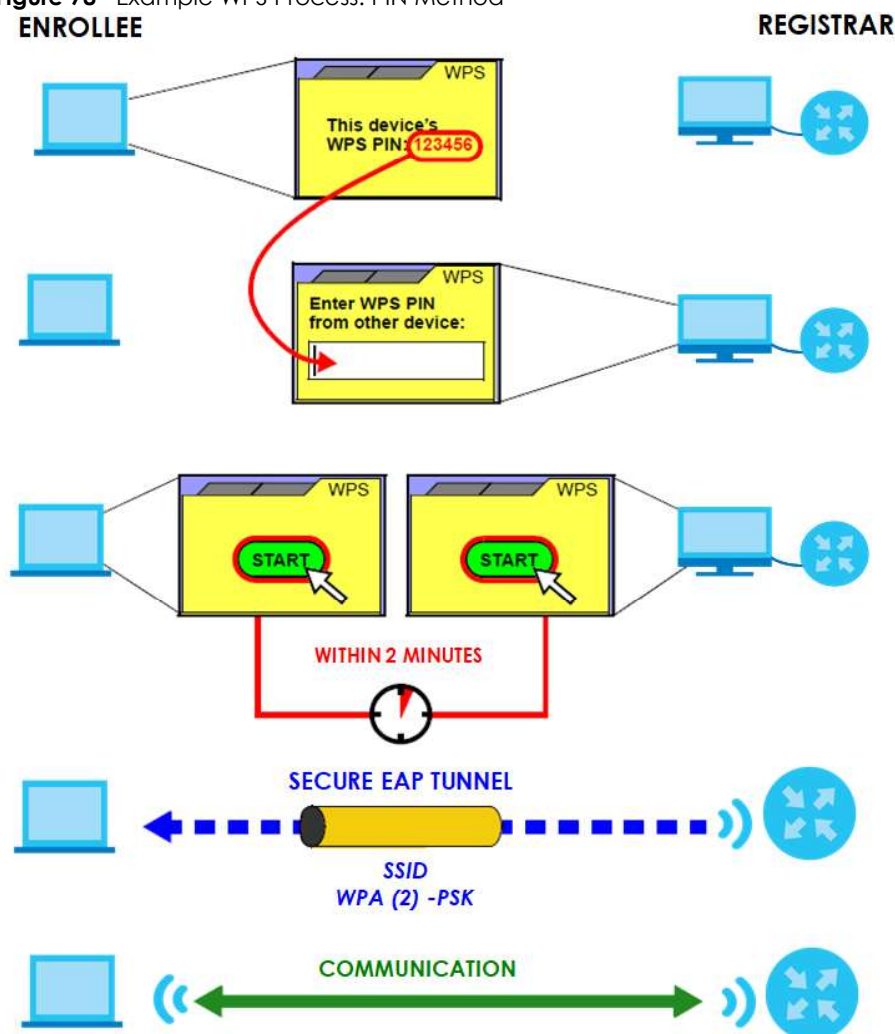
Take the following steps to set up a WPS connection between an access point or WiFi router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN – for the WE Device, see [Section 7.5 on page 115](#)).
- 4 Enter the client's PIN in the AP's configuration interface.
- 5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client – it does not matter which.
- 6 Start WPS on both devices within 2 minutes.
- 7 Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8 On a computer connected to the WiFi client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

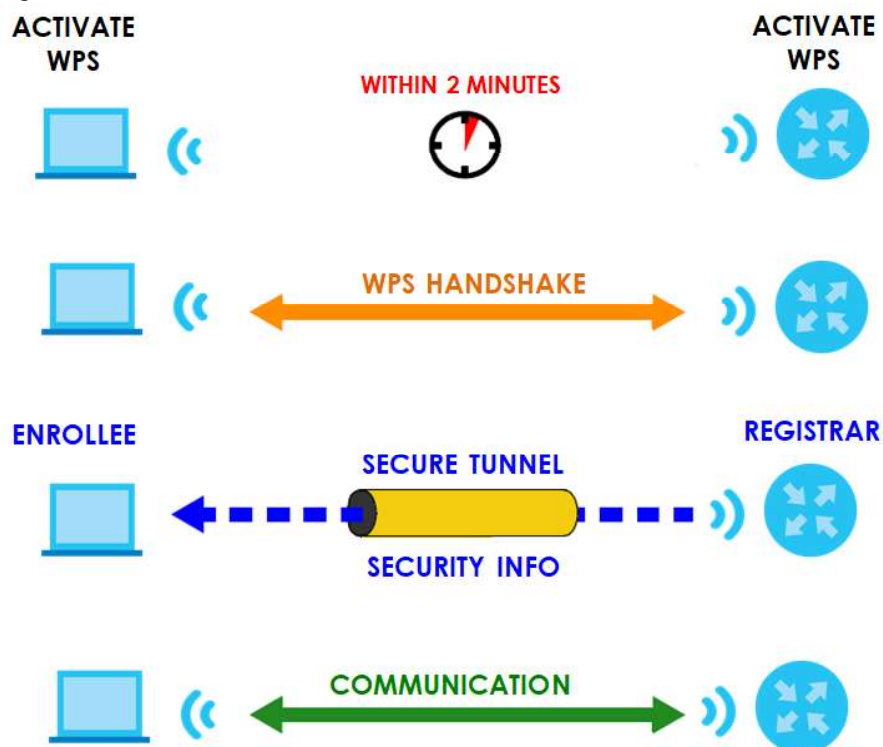
Figure 78 Example WPS Process: PIN Method
ENROLLEE



7.10.8.3 How WPS Works

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

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

Figure 79 How WPS Works

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

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

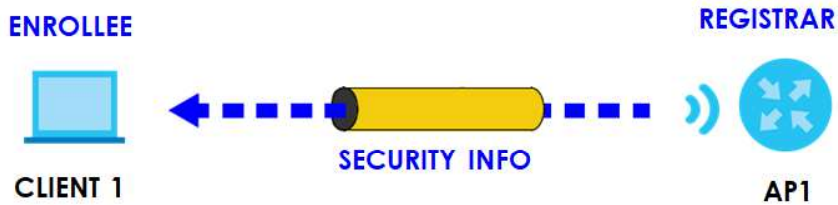
Note that the access point (AP) is not always the registrar, and the WiFi client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled WiFi clients.

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

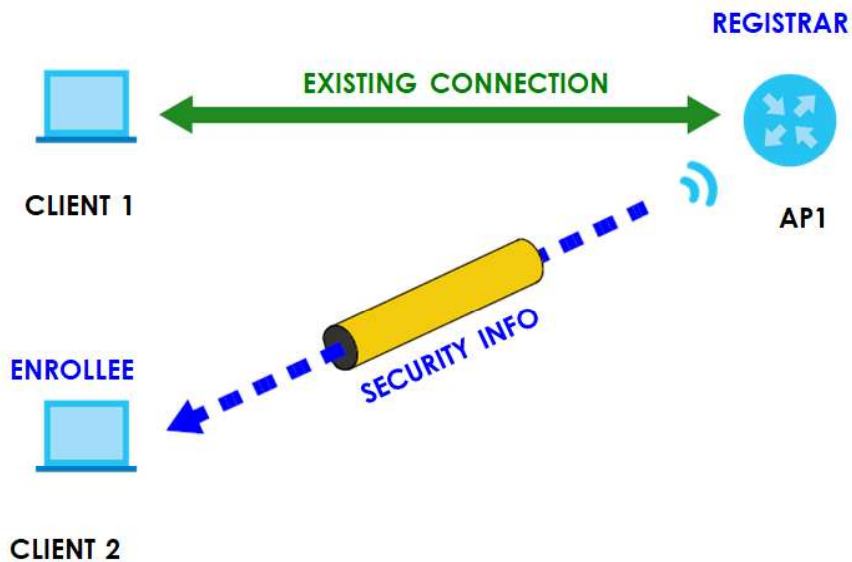
7.10.8.4 Example WPS Network Setup

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

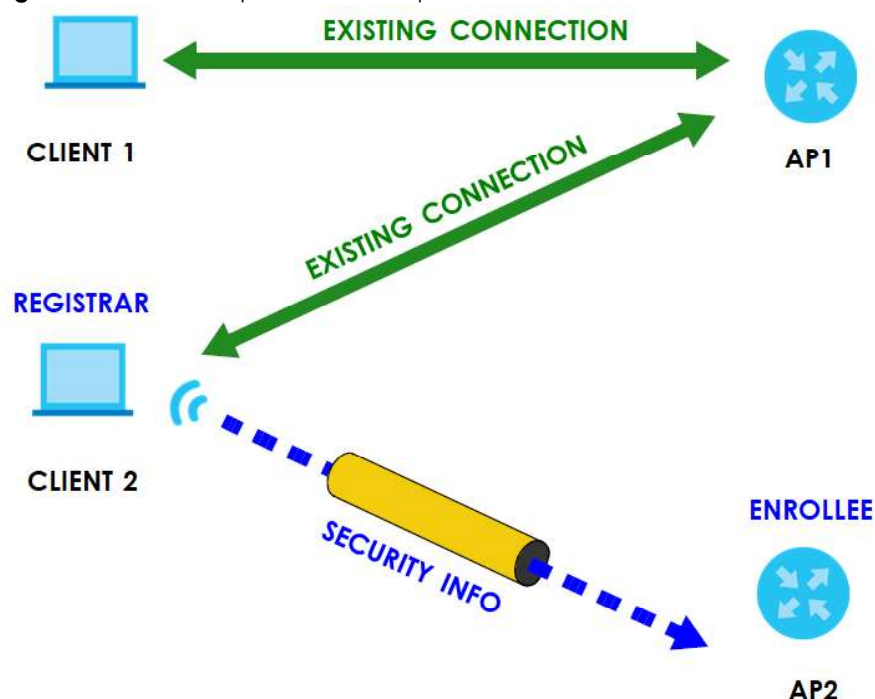
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 80 WPS: Example Network Step 1

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

Figure 81 WPS: Example Network Step 2

In step **3**, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 82 WPS: Example Network Step 3

7.10.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a WiFi client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

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

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

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

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

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access

point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your 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 8

Home Networking

8.1 Home Networking Overview

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

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

Figure 83 Home Networking Example



8.1.1 What You Can Do in this Chapter

- Use the **Home Networking** screen to set the LAN IP address, subnet mask, and DHCP settings of your WE Device ([Section 8.2 on page 140](#)).
- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings ([Section 8.3 on page 142](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses ([Section 8.4 on page 147](#)).
- Use the **UPnP** screen to enable UPnP ([Section 8.5 on page 149](#)).
- Use the **Additional Subnet** screen to configure IP alias and public static IP ([Section 8.6 on page 151](#)).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the WE Device automatically create static DHCP entries for the STB devices when they request IP addresses ([Section 8.7 on page 152](#)).

8.1.2 What You Need To Know

8.1.2.1 About LAN

IP Address

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

Subnet Mask

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

DHCP

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

8.1.2.2 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 WE 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 8.9 on page 156](#) for examples on installing and using UPnP.

8.1.3 Before You Begin

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

8.2 Home Networking

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

Note: This screen appears when the WE Device is in Repeater (RP) mode.

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 WE Device.
- 2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
- 3 Click **Apply** to save your settings.

Figure 84 Network Setting > Home Networking (DHCP)

Home Networking

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device.
Configure DHCP settings to get the Local Area Network IP address from the DHCP server in the network.

LAN IP Setup ☒ DHCP ☐ Static IP

IP Address 172 . 21 . 59 . 225

Subnet Mask 255 . 255 . 252 . 0

Gateway IP Address 172 . 21 . 59 . 222

IPv6 Setup ☐ Stateful ☒ Stateless ☐ StaticIP

WAN IPv6 Address

IPv6 Gateway

Cancel Apply

Figure 85 Network Setting > Home Networking (Static IP)

Home Networking

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to get the Local Area Network IP address from the DHCP server in the network.

LAN IP Setup: ☐ DHCP ☒ Static IP

IP Address: 172 . 21 . 56 . 220

Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 172 . 21 . 59 . 254

Primary DNS Server: . . .

Secondary DNS Server: . . .

IPv6 Setup: ☐ Stateful ☒ Stateless ☐ StaticIP

WAN IPv6 Address:

IPv6 Gateway:

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

The following table describes the fields in this screen.

Table 39 Network Setting > Home Networking

LABEL	DESCRIPTION
LAN IP Setup	Select DHCP to deploy the WE Device as a DHCP client in the network. When you enable this, the WE Device gets its IP address from the network's DHCP server (for example, your ISP or router). Users connected to the WE Device can now access the network (for example, the Internet if the IP address is given by the ISP or a router with Internet access). When you select this, you cannot enter an IP address for your WE Device in the field below. Select Static IP if you want to specify the IP address of your WE Device. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Enter the LAN IPv4 IP address you want to assign to your WE Device in dotted decimal notation, for example, 192.168.1.2 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your WE 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.
Gateway IP Address	Enter a gateway IPv4 address (if your ISP or network administrator gave you one) in this field.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Second DNS Server	Enter the second DNS server address assigned by the ISP.
IPv6 Setup	Select how you want to obtain an IPv6 address: Select Stateful to obtain an IPv6 address using IPv6 stateful autoconfiguration. Select Stateless to obtain an IPv6 address using IPv6 stateless autoconfiguration. Select Static to configure a fixed IPv6 address for the WE Device.

Table 39 Network Setting > Home Networking (continued)

LABEL	DESCRIPTION
WAN IPv6 Address	Enter an IPv6 IP address that your ISP gave you for the WAN interface.
IPv6 Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your WE Device's interfaces. The gateway helps forward packets to their destinations.
Cancel	Click Cancel to restore the default or previously saved settings.
Apply	Click Apply to save your changes.

8.3 LAN Setup

A LAN IP address is the IP address of a networking device in the LAN. You can use the WE 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.

Note: This screen appears when the WE Device is in Router or Access Point (AP) mode.

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

Follow these steps to configure your LAN settings.

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

Figure 86 Network Setting > Home Networking > LAN Setup (DHCP)

Home Networking

LAN Setup Static DHCP IPv6 Additional Subnet STB Vendor ID

Use this screen to set the Local Area Network IP address and subnet mask of your Zynel Device. Configure DHCP settings to have the Zynel Device or a DHCP server assign IP addresses to devices.

Interface Group

Group Name:

LAN IP Setup

IP Address:

Subnet Mask:

DHCP Server State

DHCP: ☒ Enable ☐ Disable ☐ DHCP Relay

IP Addressing Values

Beginning IP Address:

Ending IP Address:

Auto reserve IP for the same host: ☐

DHCP Server Lease Time

days hours minutes

DNS Values

DNS: ☒ DNS Proxy ☐ Static ☐ From ISP

LAN IPv6 Mode Setup

IPv6 Active: ☒

Link Local Address Type

☒ EUI64 ☐ Manual

LAN Global Identifier Type

☒ EUI64 ☐ Manual

LAN IPv6 Prefix Setup

☒ Delegate prefix from WAN ☐ Static

Default

LAN IPv6 Address Assign

Active: ☒

LAN IPv6 Address Assign Setup

LAN IPv6 DNS Assign Setup

DHCPv6 Configuration

DHCPv6 Active: ☐ DHCPv6 Server:

IPv6 Router Advertisement State

RADVD Active: ☐ Enable: ☐

IPv6 DNS Values

IPv6 DNS Server 1:

IPv6 DNS Server 2:

IPv6 DNS Server 3:

IPv6 Domain Name

DNS Query Scenario

Cancel **Apply**

Figure 87 Network Setting > Home Networking > LAN Setup (DHCP Relay)

Home Networking

LAN Setup Static DHCP IPv6 Additional Subnet STS Vendor ID

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices.

Interface Group

Group Name: lan

LAN IP Setup

IP Address: 192 . 168 . 1 . 2

Subnet Mask: 255 . 255 . 255 . 0

DHCP Server State

DHCP: ☐ Enable ☐ Disable ☒ DHCP Relay

DHCP Relay Server Address

IP Address: . . .

LAN IPv6 Mode Setup

IPv6 Active: ☒

Link Local Address Type

☒ EUI64 ☐ Manual

LAN Global Identifier Type

☒ EUI64 ☐ Manual

LAN IPv6 Prefix Setup

☒ Delegate prefix from WAN: Default ☐ Static

LAN IPv6 Address Assign

Active: ☒

LAN IPv6 Address Assign Setup

Stateless

LAN IPv6 DNS Assign Setup

From RA & DHCPv6 Server

DHCPv6 Configuration

DHCPv6 Active: ☐ DHCPv6 Server: ☐

IPv6 Router Advertisement State

RADVD Active: ☐ Enable: ☐

IPv6 DNS Values

IPv6 DNS Server 1: From ISP

IPv6 DNS Server 2: From ISP

IPv6 DNS Server 3: From ISP

IPv6 Domain Name

home.orpa

DNS Query Scenario

IPv4/IPv6 DNS Server

Cancel Apply

The following table describes the fields in this screen.

Table 40 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group that you want to configure for the LAN settings. You must enable DHCP.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your WE Device in dotted decimal notation, for example, (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your WE 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 WE Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN. If you select DHCP Relay, the WE Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
DHCP Relay Server Address	
This field is only available when you select DHCP Relay in the DHCP field.	
IP Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.
IP Addressing Values	
The IP Addressing Values fields appear only when you select Enable in the DHCP field.	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
DHCP Server Lease Time	
This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select Enable in the DHCP field.	
Days/Hours/Minutes	DHCP server leases an address to a new client device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different client device.
DNS Values	
This field appears only when you select Enable in the DHCP field.	

Table 40 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION						
DNS	The WE Device supports DNS proxy by default. The WE 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 WE Device. The WE Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the WE Device queries an outside DNS server and relays the response to the DHCP client. Select DNS Proxy to have the DHCP clients use the WE Device's own LAN IP address. The WE Device works as a DNS relay. Select Static if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select From ISP if your ISP dynamically assigns DNS server information (and the WE Device's WAN IP address).						
LAN IPv6 Mode Setup							
IPv6 Active	Use this to enable or disable IPv6 on the WE Device. When IPv6 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 WE Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select Manual. Link-local Unicast Address Format <table><tr><td>1111 1110 10</td><td>0</td><td>Interface ID</td></tr><tr><td>10 bits</td><td>54 bits</td><td>64 bits</td></tr></table>	1111 1110 10	0	Interface ID	10 bits	54 bits	64 bits
1111 1110 10	0	Interface ID					
10 bits	54 bits	64 bits					
EUI64	Select this to have the WE 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 WE 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 WE 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 WE 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 WE Device's LAN IPv6 address.						
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: Stateless: The WE Device uses IPv6 stateless auto-configuration. RADVD (Router Advertisement Daemon) is enabled to have the WE Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. Stateful: The WE Device uses IPv6 stateful auto-configuration. The DHCPv6 server is enabled to have the WE Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.						

Table 40 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 DNS Assign Setup	Select how the WE Device provide DNS server and domain name information to the clients: From RA & DHCPv6 Server: The WE Device provides DNS information through both router advertisements and DHCPv6. From DHCPv6 Server: The WE Device provides DNS information through DHCPv6. From Router Advertisement: The WE 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 WE 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. User Defined – Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the WE Device passes to the DHCP clients. From ISP – Select this if your ISP dynamically assigns IPv6 DNS server information. Proxy – Select this if the DHCP clients use the IP address of this interface and the WE Device works as a DNS relay. Otherwise, select None if you do not want to configure IPv6 DNS servers.
IPv6 Domain Name	Specify the domain name of the DNS server for the DHCP clients to use.
DNS Query Scenario	Select how the WE Device handles clients' DNS information requests. IPv4/IPv6 DNS Server: The WE Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. IPv6 DNS Server Only: The WE Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. IPv4 DNS Server Only: The WE Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. IPv6 DNS Server First: The WE Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. IPv4 DNS Server First: The WE 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.

8.4 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.

8.4.1 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 WE Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Note: This screen appears when the WE Device is in Router or Access Point (AP) mode.

Figure 88 Network Setting > Home Networking > Static DHCP

Home Networking

LAN Setup **Static DHCP** UPnP Additional Subnet STB Vendor ID

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.

+ Static DHCP Configuration

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

The following table describes the labels in this screen.

Table 41 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 WE Device.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the Edit icon to configure the connection. Click the Delete icon to remove the connection.

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

Figure 89 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

The following table describes the labels in this screen.

Table 42 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

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

8.5 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 8.9 on page 156](#) for more information on UPnP.

Note: This screen appears when the WE Device is in Router or Access Point (AP) mode.

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

Figure 90 Network Setting > Home Networking > UPnP

Home Networking

LAN Setup Static DHCP **UPnP** Additional Subnet STB Vendor ID

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

UPnP State

UPnP ☐

UPnP NAT-T State

UPnP NAT-T ☐

Note

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

#	Description	Destination IP Address	External Port	Internal Port	Protocol
---	-------------	------------------------	---------------	---------------	----------

Cancel Apply

The following table describes the labels in this screen.

Table 43 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 WE 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.