

User's Guide

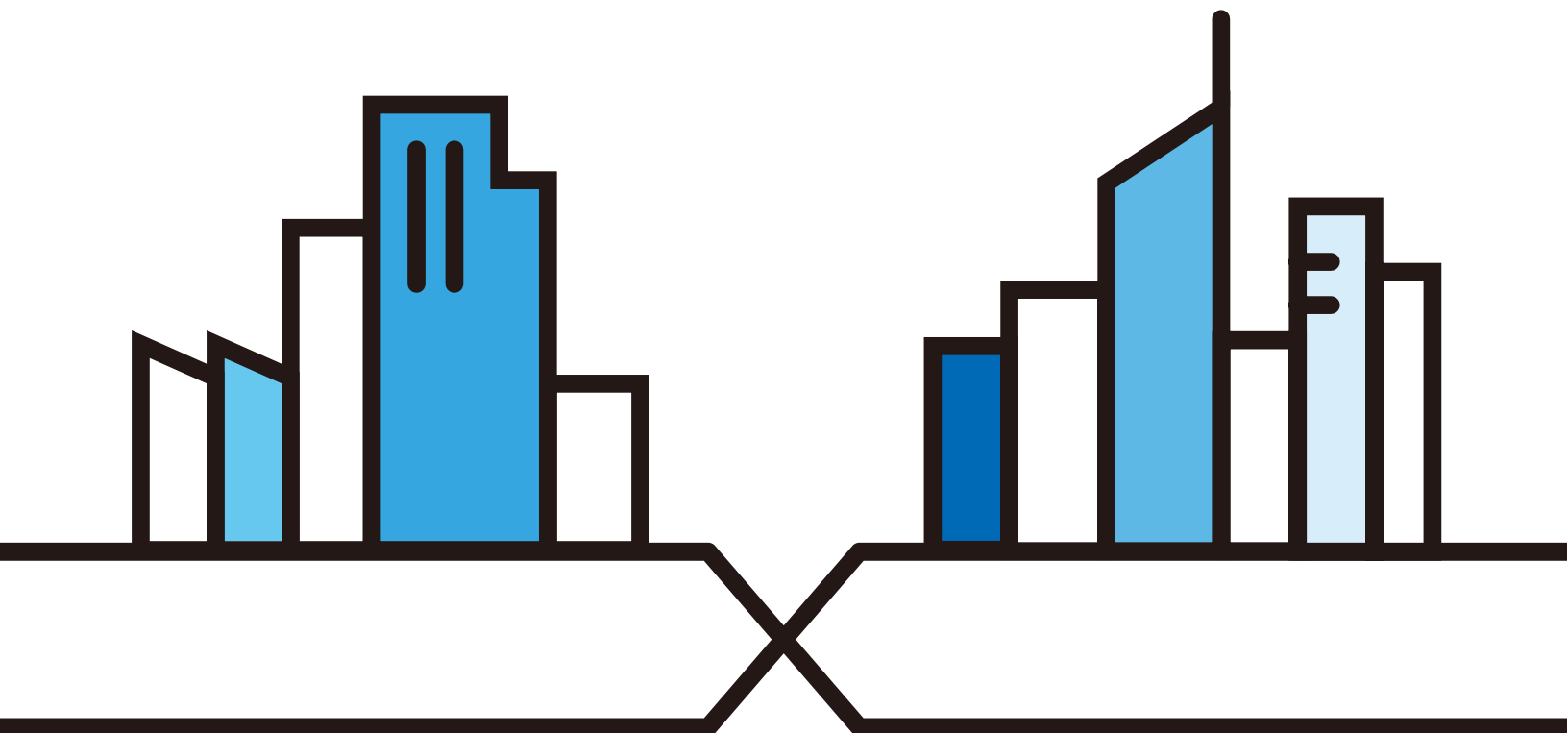
WX3310-B0

Dual-Band Wireless AX Gigabit Extender

Default Login Details

Web Address	http://zyxelsetup (Windows) http://zyxelsetup.local (Mac)
LAN IP Address	http://(DHCP-assigned IP) OR http://192.168.1.2
Password	(See the device label)

Version 1.0 Edition 2, 03/2020



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product 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 WX3310 and access the Web Configurator.

- More Information

Go to **support.zyxel.com** to find other information on the WX3310.



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 WX3310 may be referred to as the "WX" 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, **Configuration > Network > IP Setting** means you first click **Configuration** in the navigation panel, then the **Network** sub menu and finally the **IP Setting** tab to get to that screen.

Icons Used in Figures

Figures in this guide may use the following generic icons. The WX3310 icon is not an exact representation of your device.

WX3310 	Router 	Switch 	Internet 
Server 	Desktop 	Laptop 	

Contents Overview

User's Guide	9
Introduction	10
The Web Configurator	16
Modes	24
Easy Mode	26
Access Point Mode	31
Repeater Mode	36
Tutorials	41
Technical Reference	44
Monitor	45
Network	51
Wireless LAN	54
AP Connection (Repeater Mode)	75
Mesh	79
Maintenance	81
Troubleshooting	87

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	5
 Part I: User's Guide.....	 9
Chapter 1	
Introduction	10
1.1 Overview	10
1.2 Dual-Band WiFi	10
1.3 Securing the WX3310	11
1.4 Front Panel and LEDs	11
1.5 Back Panel	13
1.6 The WPS Button	14
1.6.1 Using the WPS Button	14
1.7 The RESET Button	15
1.7.1 Using the RESET Button	15
 Chapter 2	
The Web Configurator.....	16
2.1 Overview	16
2.1.1 What You Can Do in this Chapter	16
2.2 Accessing the Web Configurator	16
2.3 Preparing your Computer to Access the Web Configurator	18
2.3.1 Static IP Configuration in Microsoft Windows	19
2.3.2 Static IP Configuration in MAC OS X	21
 Chapter 3	
Modes	24
3.1 Overview	24
3.1.1 Web Configurator Modes	24
3.1.2 Device Operating Modes	24
 Chapter 4	
Easy Mode	26
4.1 Overview	26

4.1.1 What You Can Do in this Chapter	27
4.2 Navigation Panel	27
4.3 Network Map	28
4.4 Status Screen (Easy Mode)	28
Chapter 5	
Access Point Mode.....	31
5.1 Overview	31
5.1.1 What You Can Do in this Chapter	31
5.2 Setting your WX3310 to AP Mode	31
5.2.1 Status Screen (AP Mode)	32
5.2.2 AP Navigation Panel	34
Chapter 6	
Repeater Mode.....	36
6.1 Overview	36
6.1.1 What You Can Do in this Chapter	36
6.2 Setting your WX3310 to Repeater Mode	36
6.2.1 Status Screen (Repeater Mode)	37
6.2.2 Repeater Navigation Panel	39
Chapter 7	
Tutorials.....	41
7.1 Overview	41
7.2 Configuring the WX3310 as an Access Point	41
7.3 Configuring the WX3310 as a Repeater	41
7.3.1 Selecting an AP from an Automatically Detected List	41
7.3.2 Selecting an AP by Manually Entering Security Information	42
Part II: Technical Reference.....	44
Chapter 8	
Monitor.....	45
8.1 Overview	45
8.2 What You Can Do	45
8.3 Log	45
8.4 Wireless Monitor	46
8.5 MBSS Monitor	48
8.6 Multicast Monitor	50
Chapter 9	
Network.....	51

9.1 Overview	51
9.2 What You Can Do	51
9.3 What You Need To Know	51
9.4 Networking Screen	52
Chapter 10	
Wireless LAN	54
10.1 Overview	54
10.2 What You Can Do in this Chapter	55
10.3 What You Should Know	55
10.3.1 Wireless Basic	55
10.3.2 WiFi6 / IEEE 802.11ax	55
10.4 Basic Wireless Network Screen	56
10.5 Advanced Wireless Network Screen	57
10.6 WPS Screen	58
10.7 MAC Filter	59
10.8 MBSS Screen	60
10.9 Technical Reference	61
10.9.1 Wireless Network Overview	61
10.9.2 Wireless Security Overview	63
10.9.3 WiFi Protected Setup (WPS)	66
Chapter 11	
AP Connection (Repeater Mode)	75
11.1 Overview	75
11.2 What You Can Do in this Chapter	75
11.3 Station Screen	75
11.4 AP List Screen	76
11.5 WPS Screen	78
Chapter 12	
Mesh.....	79
12.1 Overview	79
12.2 Mesh Screen	80
Chapter 13	
Maintenance.....	81
13.1 Overview	81
13.2 What You Can Do in this Chapter	81
13.3 Password Screen	81
13.4 Time Screen	82
13.5 Firmware Upgrade Screen	83
13.6 Restore Screen	84

13.6.1 Backup Configuration	85
13.6.2 Restore Configuration	85
13.6.3 Back to Factory Defaults	85
13.7 Restart Screen	86
Chapter 14	
Troubleshooting.....	87
14.1 Power, Hardware Connections, and LEDs	87
14.2 WX3310 Access and Login	88
14.3 Internet Access	89
14.4 Resetting the WX3310 to Its Factory Defaults	90
14.5 Wireless Problems	90
Appendix A Wireless LANs	91
Appendix B Customer Support	103
Appendix C Legal Information	109
Index	116

PART I

User's Guide

CHAPTER 1

Introduction

1.1 Overview

The WX3310 is a wireless extender that can function as a repeater or an Access Point (AP).

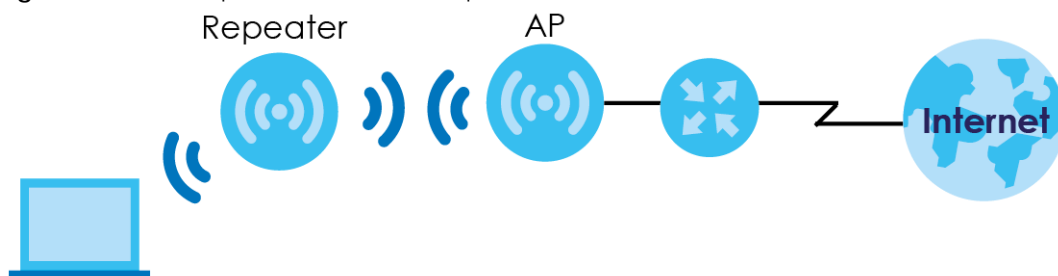
Set your WX3310 as an **AP** if you want to bridge a wired network (LAN) and a wireless LAN (WLAN) in the same subnet.

Set your WX3310 as a **Repeater** if you want to connect an existing wired network through another access point and also lets wireless clients connect to the network through it.

It supports WiFi6 that is most suitable in areas with a high concentration of users. See [Section 10.3.2 on page 55](#) for more information on WiFi6.

It can also use both 2.4GHz and 5GHz networks at the same time. See [Section 1.2 on page 10](#) for more information on dual-band WiFi.

Figure 1 Device Operation Mode Example



In **Figure 1**, the WX3310 that is acting as a **Repeater** is letting a wireless client connect to an existing wired network and also lets the wireless client connect to the network through the other WX3310 that is acting as an **AP**. The WX3310 that is acting as an **AP** is bridging a wired network and a wireless LAN in the same subnet. See [Chapter 3 on page 24](#) for more information on these modes.

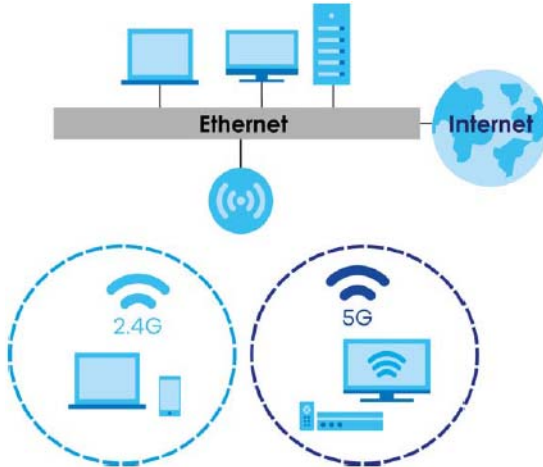
Use a (supported) web browser to manage the WX3310.

1.2 Dual-Band WiFi

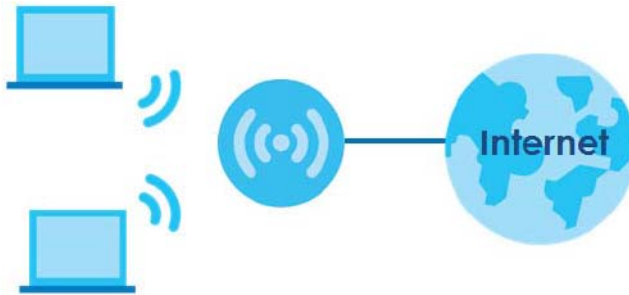
By default, the wireless LAN (WLAN) is enabled on the WX3310. IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the WX3310 to access network resources.

The WX3310 is a dual-band extender that can use both 2.4G and 5G networks at the same time.

You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

Figure 2 Dual-Band Application

The WX3310 can act as an Access Point (AP) for IEEE 802.11a/b/g/n/ac/ax wireless clients, such as notebook computers, iPads, smartphones, and so on. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

Figure 3 Wireless Access Example

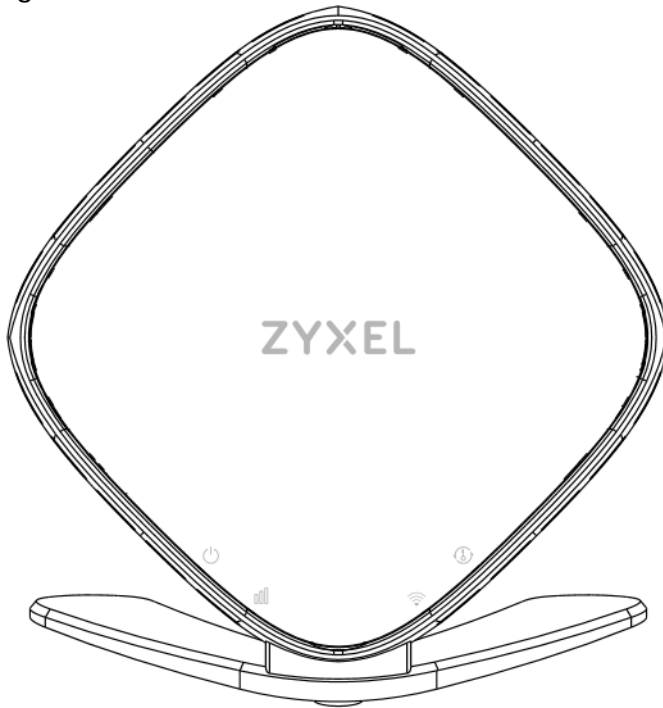
1.3 Securing the WX3310

Do the following things regularly to make the WX3310 more secure and to manage the WX3310 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the WX3310 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WX3310. You could simply restore your last configuration.

1.4 Front Panel and LEDs

The following figure is the front panel of the WX3310. Use the LEDs to determine if the WX3310 is behaving normally or if there are some problems on your network.

Figure 4 Front Panel

The following table describes the LEDs

Table 1 Front Panel LEDs






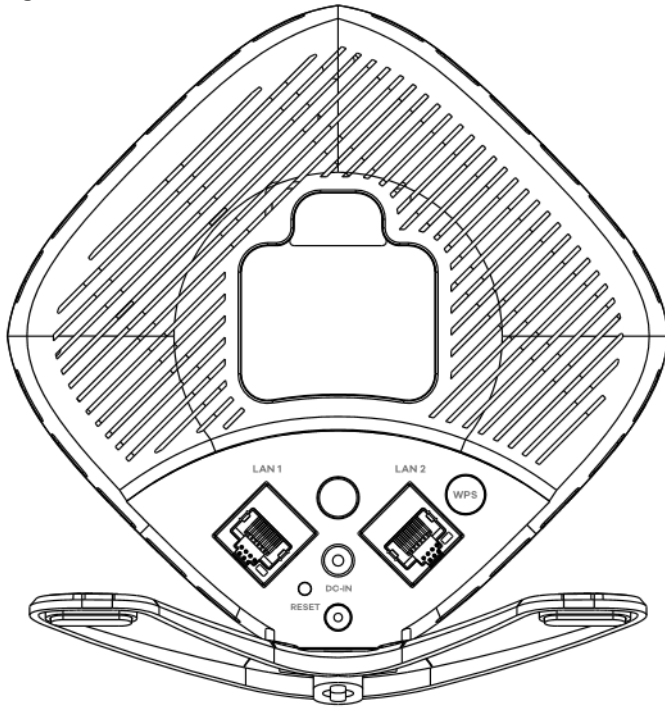
LED	COLOR	STATUS	DESCRIPTION
	Green	Blinking	WPS process in progress
	Red	On	WPS failed.
		Blinking	Overlapping WPS processes (two wireless clients are trying to simultaneously connect to the WX3310). Wait for the LED to go off, then initiate WPS again.
		Off	No WPS activity.
AP Mode Link Quality (wired connection) 	Green	On	Connected to the modem/router.
		Blinking	Connected, but not synced with the Zyxel MPro Mesh gateway (router controller).
		Off	There is no connection to the modem/router.

Table 1 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
Repeater Mode Link Quality (wireless connection) 	Green	On	Link quality is good.
		Blinking	Link quality is good, but not synced with the Zyxel MPro Mesh gateway (router controller). (see Chapter 12 on page 79 for more information on Easy Mesh)
	Amber	On	Place the WX3310 further from the modem/router.
		Blinking	Place the WX3310 further from the modem/router. Not synced with the Zyxel MPro Mesh gateway (router controller). (see Chapter 12 on page 79 for more information on Easy Mesh)
	Red	On	Place the WX3310 closer to the modem/router.
		Blinking	Place the WX3310 closer to the modem/router. Not synced with the Zyxel MPro Mesh gateway (router controller). (see Chapter 12 on page 79 for more information on Easy Mesh)
		Off	There is no connection to the modem/router.
WiFi 	Green	On	The 2.4G and 5G wireless radios are ready.
		Blinking	Sending and receiving data.
		Off	The 2.4G or 5G wireless radio is not ready or has failed.
POWER 	Green	On	The WX3310 is ready.
		Blinking	The WX3310 is booting.
	Red	On	System failure.
		Blinking	Firmware upgrading.
		Off	The WX3310 is not receiving power or is turned off.

1.5 Back Panel

The following figure is the back panel of the WX3310.

Figure 5 Rear Panel

1.6 The WPS Button

Your WX3310 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

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

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

The **WPS** button is located at the back panel of the WX3310.

1.6.1 Using the WPS Button

- 1 Make sure the power LED is on (not blinking).
- 2 Choose a mode
 - AP mode: Press the WX3310 **WPS** button once. The WPS LED should start blinking. Press the WPS button on the client within two minutes. Wait for the WPS LED to turn steady green indicating the WPS process has finished. If it turns red, the WPS process has failed.

- Repeater mode (modem/router to the WX3310): Press the WX3310 **WPS** button once to copy the WiFi settings from your modem/router to the WX3310. Press the WPS button on your modem/router within two minutes. Wait for the WPS LED to turn steady green, which indicates that the WPS process is finished. If it turns red, the WPS process has failed.
- Repeater mode (the WX3310 to the wireless client): Press the WX3310 **WPS** button twice within 7 seconds to copy the WiFi settings from the WX3310 to a wireless client, such as your smartphone or laptop. The WPS LED should start blinking. Press the WPS button on the client within two minutes. Wait for the WPS LED to turn steady green, which indicates that the WPS process has finished. If it turns red, the WPS process has failed.

Note: You must activate WPS in the WX3310 and in another wireless device within two minutes of each other.

Note: With WPS, wireless clients can only connect to the 5GHz or 2.4GHz wireless network using the first 5GHz or 2.4GHz SSID on the WX3310 (in AP or repeater mode).

For more information on using **WPS**, see [Section on page 43](#).

1.7 The RESET Button

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the WX3310 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. The WX3310 will be reset to obtain an IP address from a DHCP server.

1.7.1 Using the RESET Button

- 1 Make sure the power LED is on (not blinking).
- 2 Press the **RESET** button for one to five seconds to reboot the WX3310.
- 3 Press the **RESET** button for longer than five seconds to set the WX3310 back to its factory-default configurations.

CHAPTER 2

The Web Configurator

2.1 Overview

This chapter describes how to access the WX3310 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the WX3310 via Internet browser.

Use:

- Internet Explorer 11 and later version
- Mozilla Firefox 67.0.2 and later version
- Google Chrome 77 and later version
- Safari 5.0 and later version

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).

Refer to [Chapter 14 on page 87](#) to see how to make sure these functions are allowed in Internet Explorer.

2.1.1 What You Can Do in this Chapter

- To change your computer's IP address in Windows 7 operating system, see [Section 2.3.1 on page 19](#).
- To change your computer's IP address in MAC OS X 10.11 operating system, see [Section 2.3.2 on page 21](#).

2.2 Accessing the Web Configurator

- 1 Make sure your WX3310 hardware is properly connected and prepare your computer or computer network to connect to the WX3310 (refer to the Quick Start Guide).
- 2 Launch your web browser.

- 3 Type "http://zyxelsetup" (for Windows) or "http://zyxelsetup.local" (for Mac) as the website address to access any of the modes.

The WX3310 is a DHCP client by default. Alternatively, check the connected gateway for the WX3310's current IP address. Make sure your computer's IP address is in the same subnet as the WX3310's IP address. Type "http://(DHCP-assigned IP)" as the web address in your web browser.

If the WX3310 is not connecting to a router or DHCP server, type the WX3310's default static IP address (192.168.1.2). Your computer must be in the same subnet in order to access this website address. You must give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254 (see [Section 2.3 on page 18](#)).

- 4 Type the **Username** and **Password** on the device label (default) and click **Login**.


Figure 6 Login Screen



- 5 You will see the FCC safety warning after you log into the web configurator. You can also see the FCC safety warning by clicking on the i-note icon (ⓘ) in the **Status** screen.

Legal and Regulation

Model Name: WX3310-B0
 Product Name: Dual Band Wireless AX Gigabit Extender
 Importer: Zyxel Communications, Inc, 1130 North Miller Street Anaheim, CA92806-200

CE/FCC/IC: 

FCC ID: I88WX3310-B0
 IC ID: 2468C-WX3310B0
 IC Warning: CAN ICES-3 (B)/NMB-3(B)

FCC Warning Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
 (2) This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna
 Increase the separation between the equipment or devices
 Connect the equipment to an outlet other than the receiver's
 Consult a dealer or an experienced radio/TV technician for assistance


OK

- 6 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password. Click **Apply** to save your changes. Click **Ignore** if you do not want to change the password this time.

Figure 7 Change Password Screen

Change Password

Enter your new password in the two fields below and click "Apply". Otherwise click "Ignore" to keep the default password.

 **New Password:**

Retype to Confirm:

☐ Always ignore this page

Apply Ignore

Right after you log in, the easy mode network map screen is displayed. See [Chapter 3 on page 24](#) for more information about the easy mode.

2.3 Preparing your Computer to Access the Web Configurator

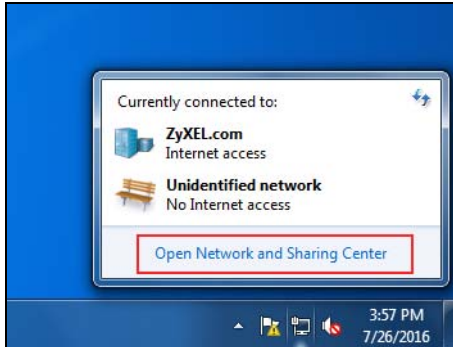
This section shows you how to assign a static IP address to your computer.

If the WX3310 is using the static IP address, your computer needs to be in the same subnet as the WX3310 in order to access the web configurator. Below you will find the steps to set a static IP on both Windows 7 (Section 2.3.1 on page 19) and MAC OS X 10.11 (Section 2.3.2 on page 21) operating systems.

2.3.1 Static IP Configuration in Microsoft Windows

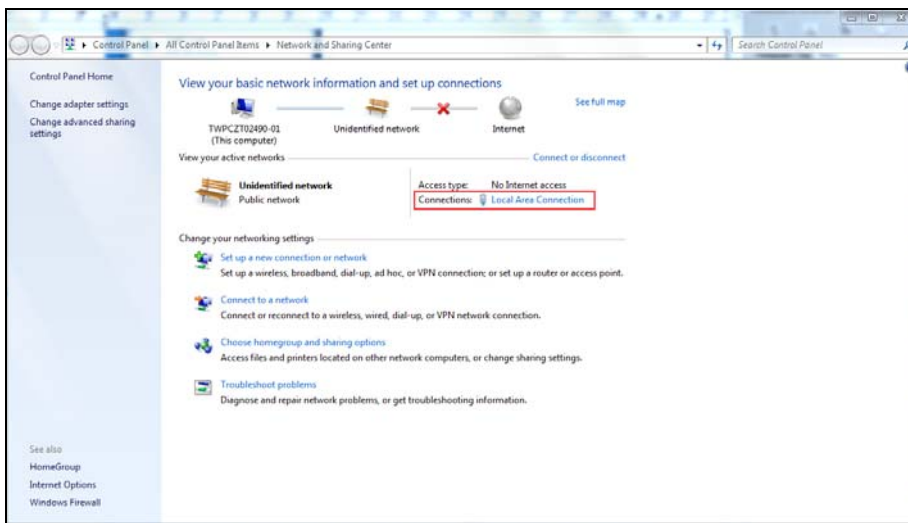
Follow these steps to change your computer's IP address in Windows 7 operating system.

- 1 Click on the **Network** Icon  located in the System Tray of your Task Bar. After you have clicked the icon a small message window will appear, select **Open Network and Sharing Center**.

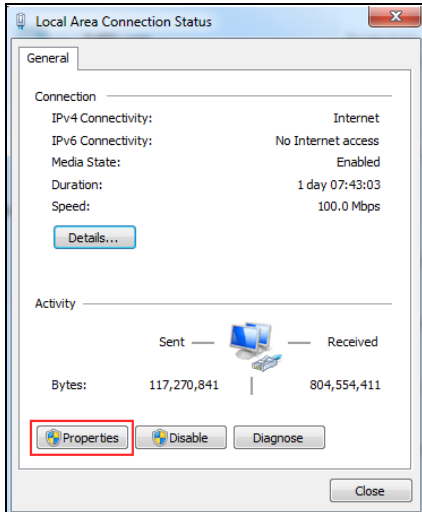


Note: You can also access the **Network and Sharing Center** by going to the **Control Panel** in the **Start Menu** and clicking on **Network and Sharing Center**.

- 2 Once you have accessed the **Network and Sharing Center**, click on **Local Area Connection** to access the adapter's settings.

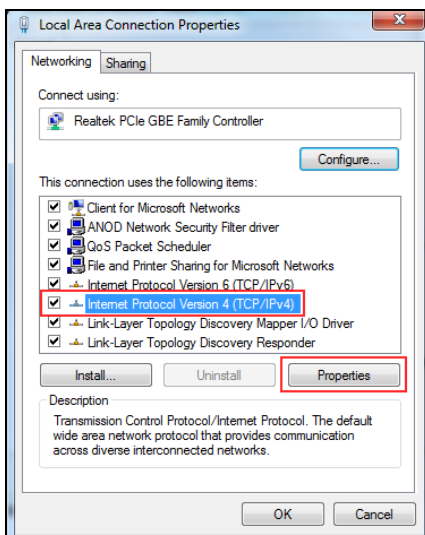


- 3 After accessing the connection's general settings, click on the **Properties** button.

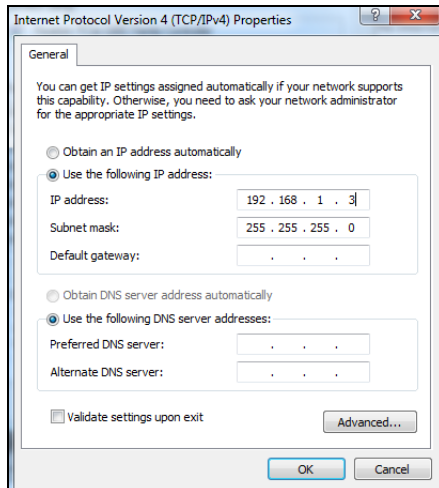


Note: You can also access the adapter's settings by clicking on **Change adapter settings** located on the left side bar. Then right-clicking on the **Local Area Connection** icon and selecting **Properties**.

- 4 In the connection's properties select the **Internet Protocol Version 4 (TCP/IPv4)** item, then click on the **Properties** button.



- 5 Once you have accessed the **Internet Protocol Version 4 (TCP/IPv4)** properties, click on the **Use the following IP address** radio button and type your new IP address. Your computer must be in the same subnet in order to access this website address. You must give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254. Then type 255.255.255.0 as your subnet mask, click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window. Then click **OK** to close the **Local Area Connection**

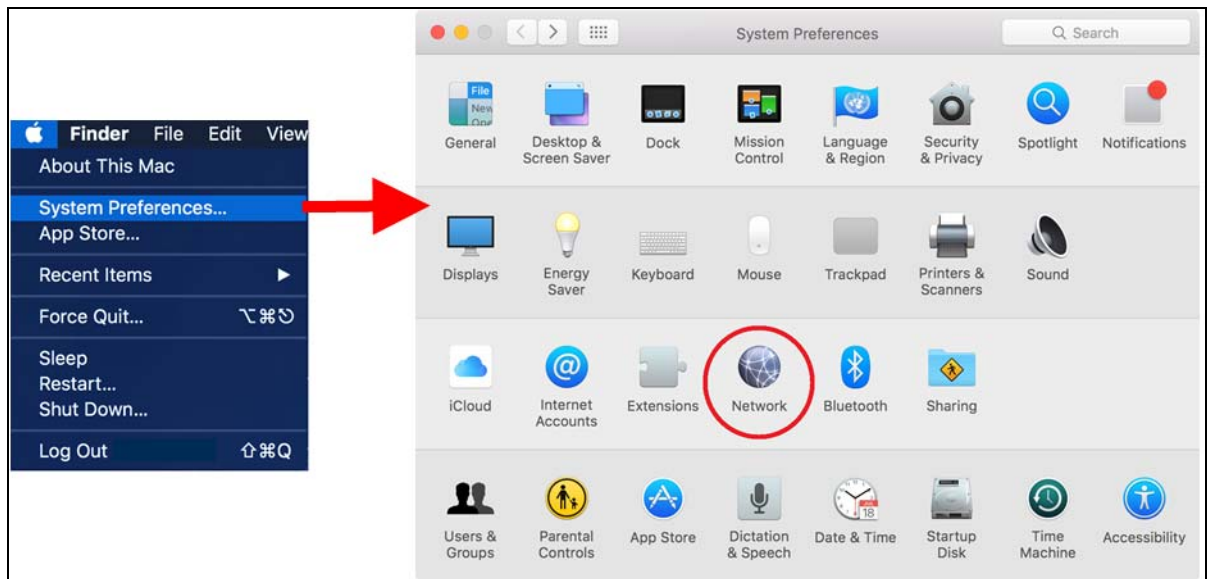


Note: After you have configured your WX3310, you must remember to change your static IP back to automatic to be able to access the Internet. If you want to change the IP address to automatic (default) then repeat steps 1 to 4, for step 5 select the **Obtain an IP address automatically** radio button, and click **OK**.

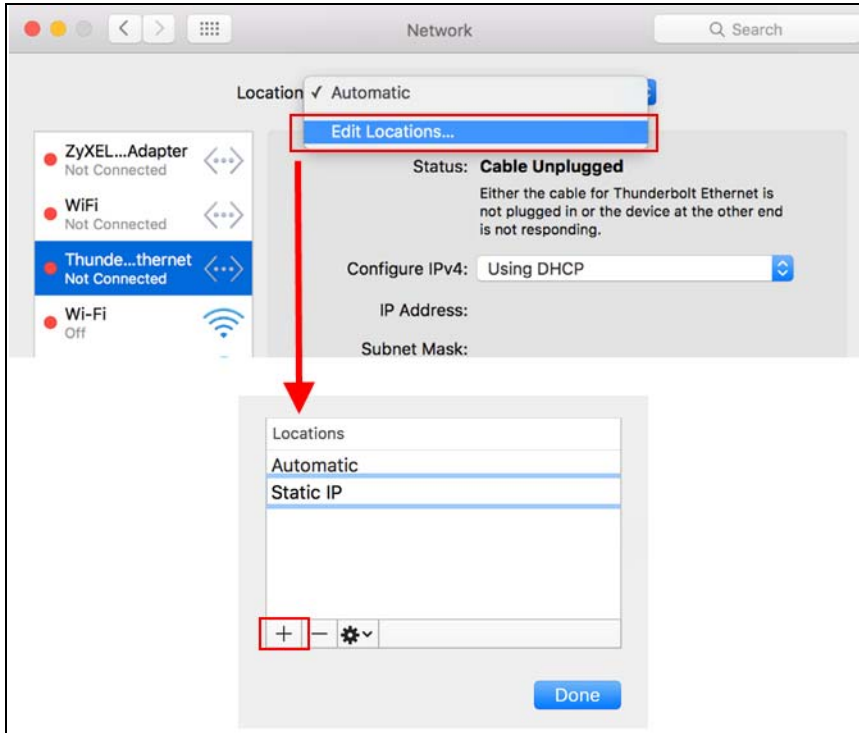
2.3.2 Static IP Configuration in MAC OS X

Follow these steps to change your computer's IP address in MAC OS X 10.11 operating system.

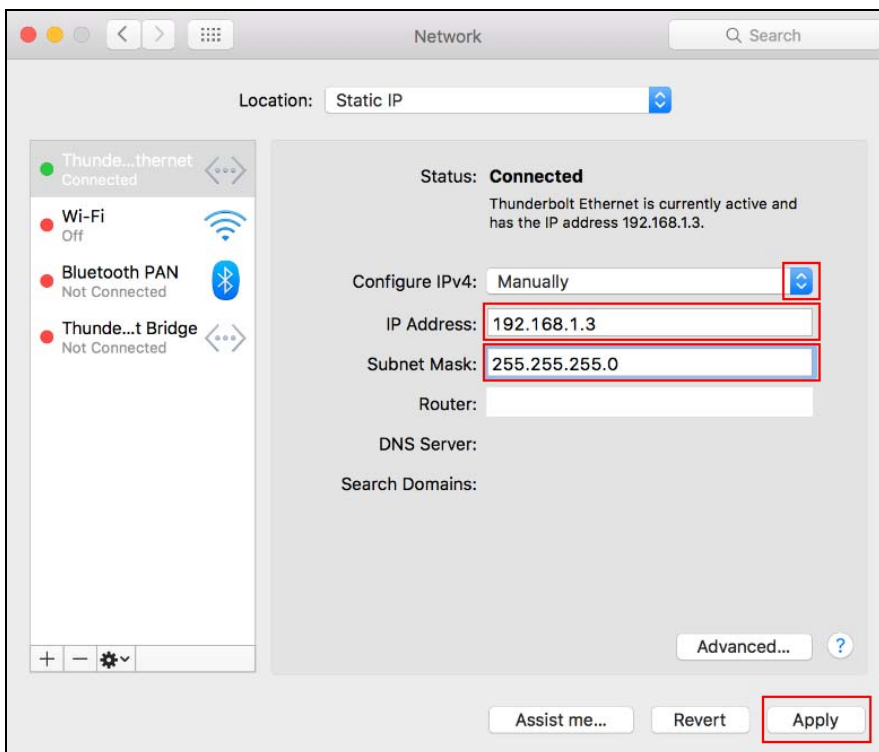
- 1 Open your **System Preferences**, then click on **Network**.



- 2 Once the **Network** screen is open, it is recommended you click on **Location > Edit Locations** to create a new profile. Use the + button to add a new profile, in this case it is called **Static IP**. This will easily help you change from static IP address to automatic.



- 3 After creating your **Static IP** profile, make sure it is selected, then click on the **Configure IPv4** scroll button and select **Manually**. Then modify your IP Address, your computer must be in the same subnet in order to access this website address. You must give it a fixed IP address in the range between 192.168.1.3 and 192.168.1.254. Then type 255.255.255.0 as your subnet mask, and click **Apply** to save your changes.



Note: After you have configured your WX3310, you must remember to change your static IP back to obtaining it automatically to be able to access the Internet. If you want to change the IP address to automatic (default) repeat step 1, then on **Location** select **Automatic** or a different profile you have configured.

CHAPTER 3

Modes

3.1 Overview

This chapter introduces the different modes available on your WX3310. First, the term “mode” refers to two things in this User’s Guide.

- Web Configurator mode. This refers to the Web Configurator screen you want to use for editing WX3310 features.
- Device mode. This is the operating mode of your WX3310, or simply how the WX3310 is being used in the network.

3.1.1 Web Configurator Modes

This refers to the configuration interface of the Web Configurator, which has two modes:

- Easy Mode. The Web Configurator shows this mode by default. Refer to [Chapter 4 on page 26](#) for more information on the screens in this mode. This shows how the WX3310's network is currently laid out.
- Expert Mode. Advanced users can change to this mode to customize all the functions of the WX3310. Click **Expert Mode** after logging into the Web Configurator. The User’s Guide [Chapter 2 on page 16](#) through [Chapter 13 on page 81](#) discusses the screens in this mode.

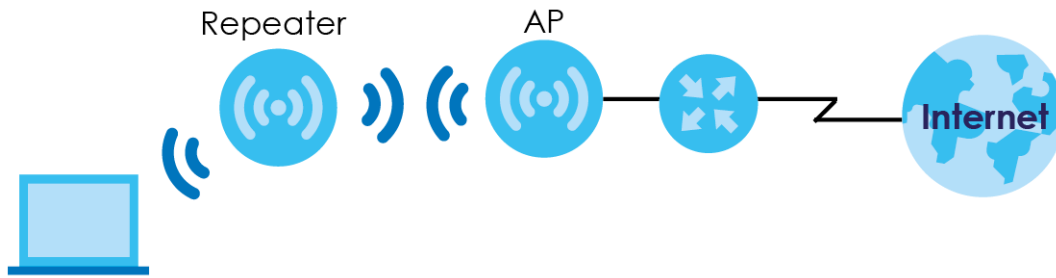
3.1.2 Device Operating Modes

This refers to the operating mode of the WX3310, which can act as a:

- **Access Point:** Use this mode if you already have a router in your network and you want to set up a wireless network and bridge the wired and wireless connections on the WX3310.
- **Repeater:** In this mode, the WX3310 can be an access point and a wireless client at the same time. Use this mode if there is an existing wireless router or access point in your network and you want the WX3310 to wirelessly relay communications from its wireless clients to the access point and from the access point to its wireless clients.

The following figure is an illustration of the device operating modes of the WX3310.

Figure 8 Device Operating Mode Example



In **Figure 5**, the WX3310 that is acting as a **Repeater** is letting a wireless client connect to an existing wired network and also lets the wireless client connect to the network through the other WX3310 that is acting as an **AP**. The WX3310 that is acting as an **AP** is bridging a wired network and a wireless LAN in the same subnet.

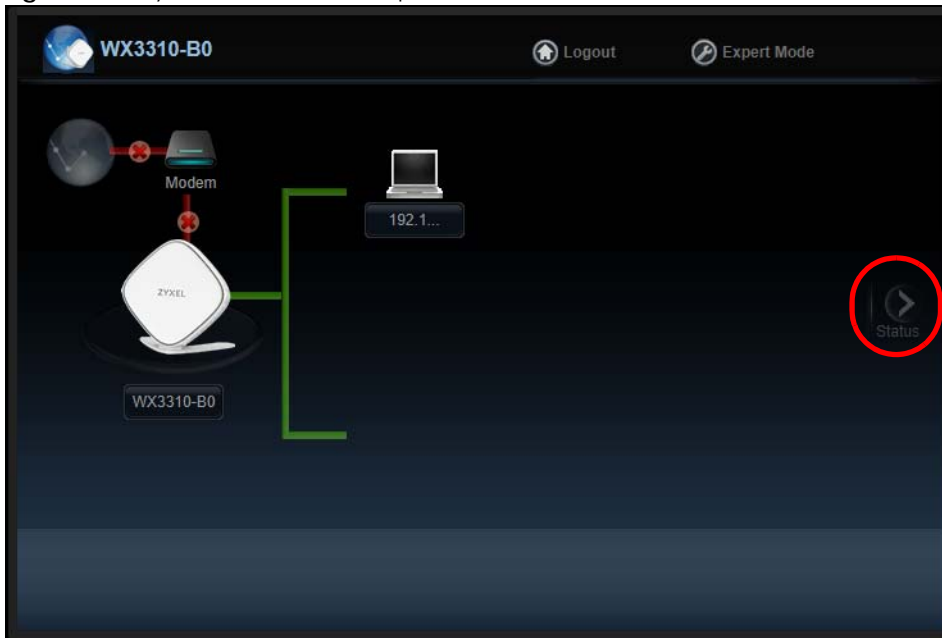
CHAPTER 4

Easy Mode

4.1 Overview

The Web Configurator is set to Easy Mode by default. This mode is useful to users by visualizing their networks' layout. You can view details about the devices connected to your WX3310 and their status. When you log in to the Web Configurator, the following screen opens.

Figure 9 Easy Mode: Network Map



Click **Status** to open the following screen.

Figure 10 Easy Mode: Status Screen (Repeater Mode)

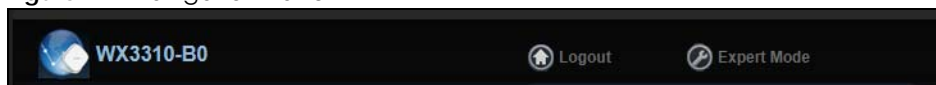
4.1.1 What You Can Do in this Chapter

You can do the following in this mode:

- Use the **Navigation Panel** to exit the Easy mode, see [Section 4.2 on page 27](#).
- Use the **Network Map** screen to check if your WX3310 can ping the gateway and whether it is connected to the Internet, see [Section 4.3 on page 28](#).
- Use the **Status** screen to view read-only information about the WX3310, including the WAN IP, MAC address of the WX3310 and the software version, see [Section 4.4 on page 28](#).

4.2 Navigation Panel

Use this navigation panel to opt out of the Easy mode.

Figure 11 Navigation Panel

The following table describes the labels in this screen.

Table 2 Navigation Panel

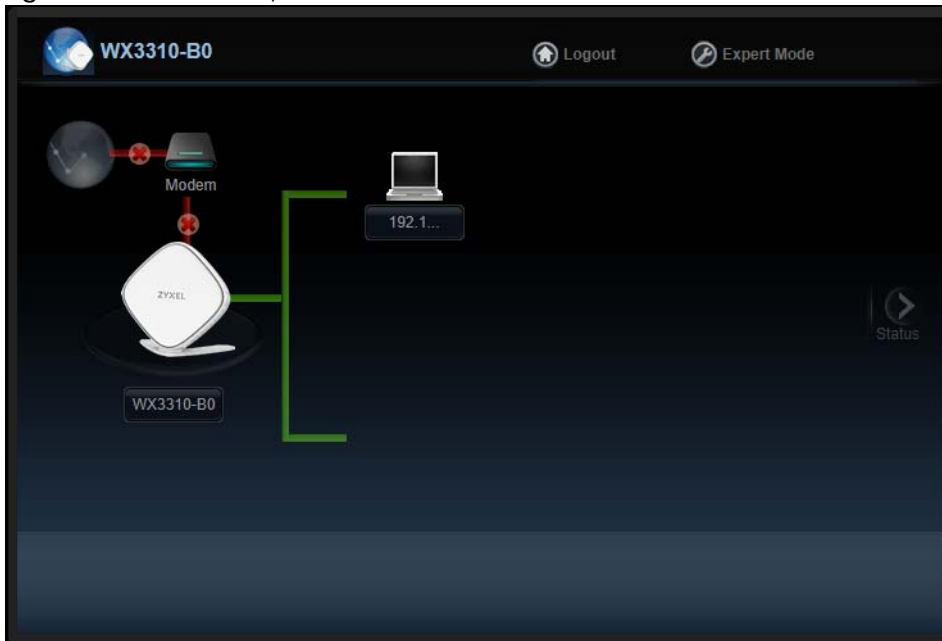
LABEL	DESCRIPTION
Logout	Click this to end the Web Configurator session.
Expert Mode	Click this to change to Expert Mode and customize features of the WX3310.

4.3 Network Map

Note: Don't worry if the Network Map does not display in your web browser. This feature may not be supported by your system. You can still configure your WX3310's features in **Expert Mode**.

When you log in to the Web Configurator, the **Network Map** is shown as follows.

Figure 12 Network Map



The line connecting the WX3310 to the modem/router becomes green when the WX3310 is able to ping the modem/router. It becomes red when the ping initiating from the WX3310 does not get a response from the modem/router.

The line connecting the modem/router to the Internet becomes green when the modem/router is able to ping the Internet. It becomes red when the ping initiating from the modem/router does not get a response from the Internet.

You can also view the devices (represented by icons indicating the kind of network device, such as Android device, iOS device or Windows OS) connected to the WX3310, including those connecting wirelessly. Right-click on the **Refresh** button located on the WX3310 icon to refresh the network map. Click on a device's name to view information about the device.

4.4 Status Screen (Easy Mode)

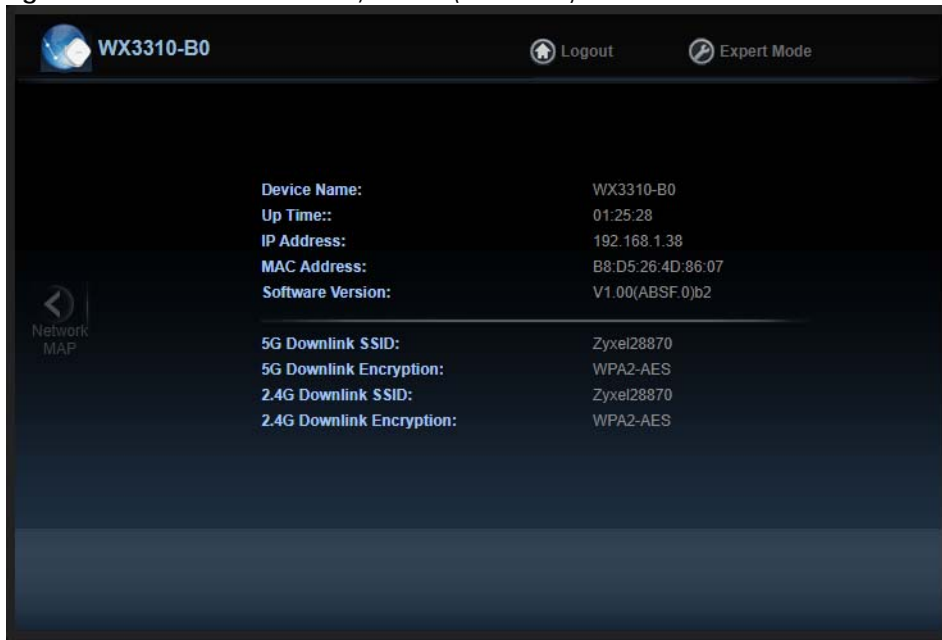
In the **Network Map**, click **Status** to view read-only information about the WX3310.

Note: The **Status** Screen displayed in Easy Mode varies according to the operating mode of your WX3310.

Figure 13 Status Screen in Easy Mode (Repeater Mode)



Figure 14 Status Screen in Easy Mode (AP Mode)



The following table describes the labels in this screen.

Table 3 Status Screen in Easy Mode

LABEL	DESCRIPTION
Device Name	This is the WX3310's model name.
Uptime	This displays the time in minutes the WX3310's system has been working.
IP Address	This shows the LAN port's IP address.
MAC Address	This shows the MAC address of the WX3310's LAN port.
Software Version	This is the firmware version.
Downlink Name (SSID)	This shows a descriptive name the client uses to connect to the WX3310.

Table 3 Status Screen in Easy Mode (continued)

LABEL	DESCRIPTION
Downlink Encryption	This shows the data encryption method the WX3310 uses for the wireless connection.
Uplink Name (SSID)	This shows a descriptive name the WX3310 uses to connect to the wireless LAN. This field is not available when the WX3310 is in AP mode.
Uplink Encryption	This shows the data encryption method the connected access point uses for the wireless connection. This field is not available when the WX3310 is in AP mode.

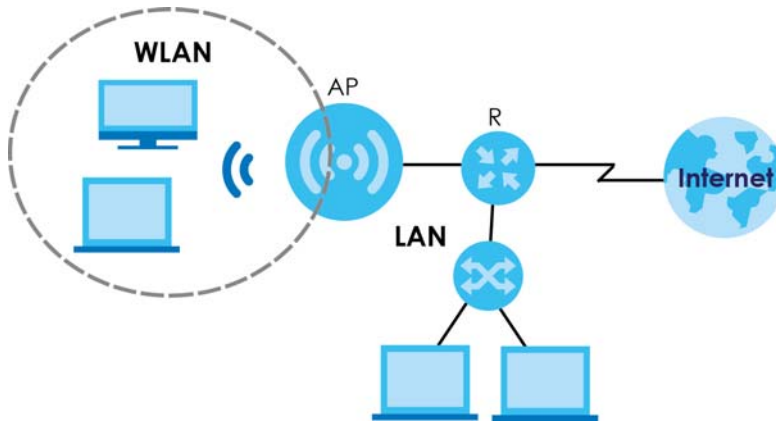
CHAPTER 5

Access Point Mode

5.1 Overview

In this mode your WX3310 (**AP**) bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 15 Access Point Mode



5.1.1 What You Can Do in this Chapter

- To set your WX3310 to AP mode, see [Section 5.2 on page 31](#).
- Use the **Status** screen to view read-only information about your WX3310 in AP mode, see [Section 5.2.1 on page 32](#).
- Use the **Navigation Panel** to configure WX3310 features in AP mode, see [Section 5.2.2 on page 34](#).

5.2 Setting your WX3310 to AP Mode

- 1 Connect your computer to one of the LAN port of the WX3310.
- 2 Connect a modem/router to the other LAN port of the WX3310 using an Ethernet cable.
- 3 If the WX3310 is not connected to a router or DHCP server, the WX3310 cannot assign your computer an IP address.

- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://zyxelsetup" (for Windows), http://zyxelsetup.local" (for Mac), or "http://(DHCP-assigned IP)" as the web address in your web browser.
- 5 Log into the Web Configurator. See the [Section 2.2 on page 16](#) for instructions on how to do this.

5.2.1 Status Screen (AP Mode)

Click on **Status**. The screen below shows the status screen in **AP Mode**.

Figure 16 Status Screen (AP Mode)

The screenshot shows the ZYXEL WX3310-B0 web interface in AP Mode. The top header includes the ZYXEL logo, model number, and user information (Welcome: admin | Logout | About). A 'Refresh Interval' dropdown is set to 'None' with a 'Refresh Now' button.

Status

Device Information

Item	Data
Device Name:	WX3310-B0
Software Version:	V1.00(ABSF.0)b2
Device Mode:	Access Point
Current Partition:	First
LAN Information:	
- Ethernet MAC Address:	B8:D5:26:4D:86:07
- IP Address:	192.168.1.38
- IP Subnet Mask:	255.255.255.0
- Gateway IP:	192.168.1.1
- IPv6 Address:	
- IPv6 Link Local Address:	fe80::bad5:26ff:fe4d:8607
- IPv6 Gateway:	

System Status

Item	Data
System Up Time:	01:27:47
Current Date/Time:	2019-10-03/11:46:17

Wireless Network Information - 5 GHz



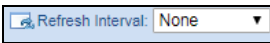
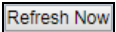




Item	Data
MAC Address:	B8:D5:26:4D:86:08
Wireless Network:	Enable
Name(SSID):	Zyxel28870
Link Rate:	4804 Mbps
Current Channel:	140/80
Authentication:	WPA2-AES
Mode:	802.11a/n/ac/ax Mixed
WPS Status:	Configured

Wireless Network Information - 2.4 GHz

Item	Data
MAC Address:	B8:D5:26:4D:86:09
Wireless Network:	Enable
Name(SSID):	Zyxel28870
Link Rate:	573 Mbps
Current Channel:	1
Authentication:	WPA2-AES
Mode:	802.11b/g/n/ax Mixed
WPS Status:	Configured

The following table describes the icons shown in the **Status** screen.

Table 4 Status Screen Icon Key (AP Mode)

ICON	DESCRIPTION
	Click this at any time to exit the Web Configurator.
	Click this icon to view copyright and a link for related product information.
	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the Monitor navigation menu.
	Click this icon to see the Configuration navigation menu.
	Click this icon to see the Maintenance navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 5 Status Screen (AP Mode)

LABEL	DESCRIPTION
Device Information	
Device Name	This is the WX3310's model name.
Software Version	This is the firmware version and the date created.
Device Mode	This is the device mode (Section 3.1.2 on page 24) to which the WX3310 is set - Access Point Mode .
Current Partition	This shows which partition the WX3310 uses. The WX3310 has two partitions and supports dual image function.
LAN Information	
Ethernet MAC Address	This shows the MAC Address of the WX3310's Ethernet LAN port.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
Gateway IP	This shows the LAN port's gateway IP address.
IPv6 Address	This shows the LAN port's IPv6 address.
IPv6 Link Local Address	This shows the LAN port's current IPv6 link-local address.
IPv6 Gateway	This shows the LAN port's gateway IPv6 address.
Wireless Network Information - 5 GHz/2.4 GHz	
MAC Address	This shows the MAC address of the WX3310's wireless interface.
Wireless Network	This shows if the wireless network is enabled or disabled.
Name (SSID)	This shows a descriptive name used to identify the WX3310 in the wireless LAN.
Link Rate (Mbps)	This shows the rate at which data is transferred across the wireless network.
Current Channel	This shows the channel number which you select manually or the WX3310 automatically scans and selects.
Authentication	This shows the data encryption method the WX3310 uses for the wireless connection.

Table 5 Status Screen (AP Mode) (continued)

LABEL	DESCRIPTION
Mode	This shows the wireless standard the WX3310 uses.
WPS Status	This displays Configured when the WPS has been set up. This displays Unconfigured if the WPS has not been set up.
System Status	
System Up Time	This is the total time the WX3310 has been on.
Current Date/Time	This field displays your WX3310's present date and time.

5.2.2 AP Navigation Panel

Use the menu in the navigation panel to configure WX3310 features in **AP Mode**.

The following screen and table show the features you can configure in **AP Mode**.

Figure 17 Menu (AP Mode)



The following table describes the sub-menus.

Table 6 Navigation Panel (AP Mode)

LINK	TAB	FUNCTION
Status	Status	This screen shows the WX3310's general device, system status information.
MONITOR		
Monitor		
Log	View Log	Use this screen to view the list of activities recorded by your WX3310.
Wireless Monitor	Wireless Monitor	Use this screen to view the wireless summary currently associated to the WX3310.
MBSS Monitor	MBSS Monitor	Use this screen to view a summary of the Multiple Basic Server Sets (MBSS) available on the WX3310. The MBSS allows you to use one access point to provide several Basic Serve Sets (BSS) simultaneously.
Multicast Monitor	Multicast Monitor	Use this screen to view the multicast group information.
CONFIGURATION		
Networking		
Network	Networking	Use this screen to configure the WX3310's LAN IPv4 and IPv6 addresses.
Wireless Network 5G	Basic	Use this screen to configure general wireless LAN settings.
	Advanced	Use this screen to configure advanced wireless settings.
	WPS	Use this screen to enable and configure WPS on your WX3310.
	MAC Filter	Use this screen to configure the WX3310 to block access to devices or block the devices from accessing the WX3310.
	MBSS	Use this screen to configure multiple BSSs on the WX3310.

Table 6 Navigation Panel (AP Mode) (continued)

LINK	TAB	FUNCTION
Wireless Network 2.4G	Basic	Use this screen to configure general wireless LAN settings.
	Advanced	Use this screen to configure advanced wireless settings.
	WPS	Use this screen to enable and configure WPS on your WX3310.
	MAC Filter	Use this screen to configure the WX3310 to block access to devices or block the devices from accessing the WX3310.
	MBSS	Use this screen to configure multiple BSSs on the WX3310.
Mesh	Mesh	Use this screen to enable or disable WX3310 Mesh.
MAINTENANCE		
Password	Password Setup	Use this screen to change the password of your WX3310.
Time	Time Setup	Use this screen to change your WX3310's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your WX3310.
Telnet	Telnet	Use this screen to enable or disable Telnet. Telnet allows you to access the WX3310's command line interface.
Restore	Restore	Use this screen to backup and restore the configuration or reset your WX3310 to the factory defaults.
Restart	Restart	Use this screen to reboot the WX3310 without turning the power off.

CHAPTER 6

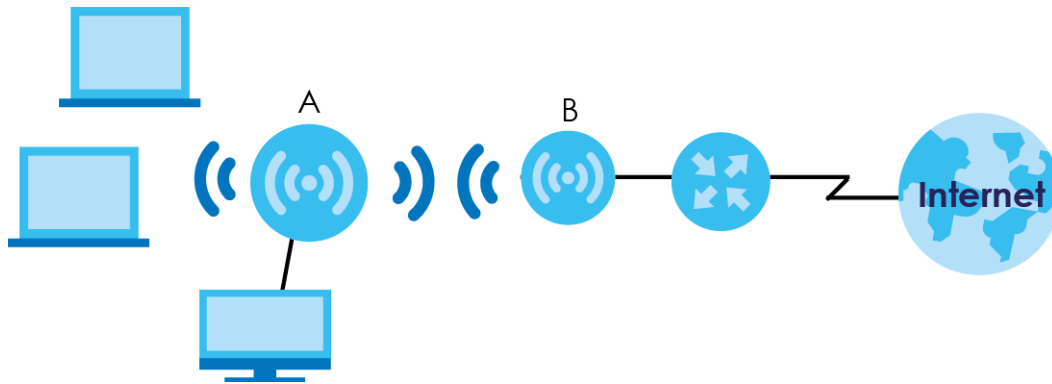
Repeater Mode

6.1 Overview

In repeater mode, your WX3310 can connect to an existing wired network through another access point and also lets wireless clients connect to the network through it. This helps you expand wireless coverage when you have an access point or wireless router already in your network.

In the example below, the WX3310 (A) is configured as a repeater. It has three clients that want to connect to the Internet. The WX3310 wirelessly connects to the available access point (B).

Figure 18 Repeater Mode



After the WX3310 and the access point connect, the WX3310 acquires its IP address from the access point. The clients of the WX3310 can now surf the Internet.

6.1.1 What You Can Do in this Chapter

- To set your WX3310 to repeater mode, see [Section 5.2 on page 31](#).
- Use the **Status** screen to view read-only information about your WX3310 in repeater mode, see [Section 6.2.1 on page 37](#).
- Use the **Navigation Panel** to configure WX3310 features in repeater mode, see [Section 6.2.2 on page 39](#).

6.2 Setting your WX3310 to Repeater Mode

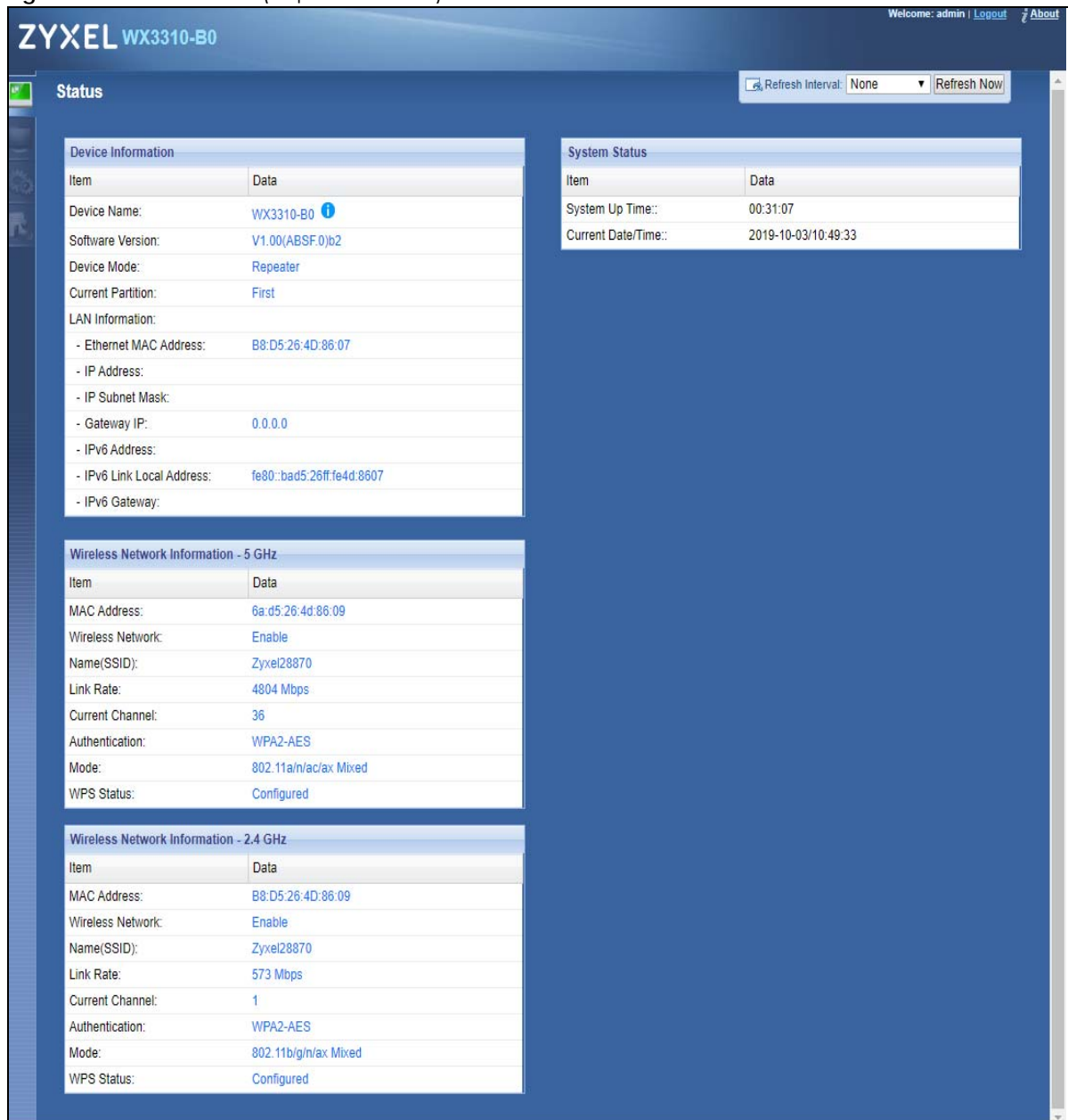
- 1 Connect your computer to the LAN port of the WX3310.
- 2 Connect a modem/router to the WX3310 wirelessly.

- 3 You must give your computer a fixed IP address in the range between 192.168.1.3 and 192.168.1.254 (Section 2.3 on page 18) if the WX3310 is not connected to a router or DHCP server.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://zyxelsetup" (for Windows), "http://zyxelsetup.local" (for Mac), "http://192.168.1.2", or "http://(DHCP-assigned IP)" as the web address in your web browser.
- 5 Log into the Web Configurator. See the Section 2.2 on page 16 for instructions on how to do this.

6.2.1 Status Screen (Repeater Mode)



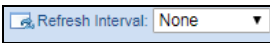
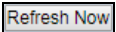




Click on **Status**. The screen below shows the status screen in **Repeater** mode.

Figure 19 Status Screen (Repeater Mode)



The following table describes the icons shown in the **Status** screen.

Table 7 Status Screen Icon Key (Repeater Mode)

ICON	DESCRIPTION
	Click this at any time to exit the Web Configurator.
	Click this icon to view copyright and a link for related product information.
	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the Monitor navigation menu.
	Click this icon to see the Configuration navigation menu.
	Click this icon to see the Maintenance navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 8 Status Screen (Repeater Mode)

LABEL	DESCRIPTION
Device Information	
Device Name	This is the WX3310's model name.
Software Version	This is the firmware version and the date created.
Device Mode	This is the device mode (Section 3.1.2 on page 24) to which the WX3310 is set - Repeater Mode .
Current Partition	This shows which partition the WX3310 uses. The WX3310 has two partitions and supports dual image function.
LAN Information	
Ethernet MAC Address	This shows the MAC Address of the WX3310's Ethernet LAN port.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
Gateway IP	This shows the LAN port's gateway IP address.
IPv6 Address	This shows the LAN port's IPv6 address.
IPv6 Link Local Address	This shows the LAN port's current IPv6 link-local address.
IPv6 Gateway	This shows the LAN port's gateway IPv6 address.
Wireless Network Information - 5 GHz/2.4 GHz	
MAC Address	This shows the MAC address of the WX3310's wireless interface.
Wireless Network	This shows if the wireless network is enabled or disabled.
Name (SSID)	This shows a descriptive name used to identify the WX3310 in the wireless LAN.
Link Rate (Mbps)	This shows the rate at which data is transferred across the wireless network.
Current Channel	This shows the channel number which you select manually or the WX3310 automatically scans and selects.
Authentication	This shows the data encryption method the WX3310 uses for the wireless connection.

Table 8 Status Screen (Repeater Mode)

LABEL	DESCRIPTION
Mode	This shows the wireless standard the WX3310 uses.
WPS Status	This displays Configured when the WPS has been set up. This displays Unconfigured if the WPS has not been set up.
System Status	
System Up Time	This is the total time the WX3310 has been on.
Current Date/Time	This field displays your WX3310's present date and time.

6.2.2 Repeater Navigation Panel

Use the menu in the navigation panel to configure WX3310 features in **Repeater Mode**.

The following screen and table show the features you can configure in **Repeater Mode**.

Figure 20 Menu (Repeater Mode)



The following table describes the sub-menus.

Table 9 Navigation Panel (Repeater Mode)

LINK	TAB	FUNCTION
Status	Status	This screen shows the WX3310's general device, system status information.
MONITOR		
Monitor		
Log	View Log	Use this screen to view the list of activities recorded by your WX3310.
Wireless Monitor	Wireless Monitor	Use this screen to view the wireless summary currently associated to the WX3310.
MBSS Monitor	MBSS Monitor	Use this screen to view a summary of the Multiple Basic Server Sets (MBSS) available on the WX3310. The MBSS allows you to use one access point to provide several Basic Serve Sets (BSS) simultaneously.
Multicast Monitor	Multicast Monitor	Use this screen to view the multicast group information.
CONFIGURATION		
Networking		
Network	Networking	Use this screen to configure the WX3310's LAN IPv4 and IPv6 addresses.

Table 9 Navigation Panel (Repeater Mode) (continued)

LINK	TAB	FUNCTION
Wireless Network 5G	Basic	Use this screen to configure general wireless LAN settings.
	WPS	Use this screen to enable and configure WPS on your WX3310.
	MAC Filter	Use this screen to configure the WX3310 to block access to devices or block the devices from accessing the WX3310.
	MBSS	Use this screen to configure multiple BSSs on the WX3310.
AP Connection	Station	Use this screen to enter the SSID and configure the wireless security between the WX3310 and the wireless network to which you want to connect.
	AP List	Use this screen to scan the wireless networks in the WX3310's area.
	WPS	Use this screen to quickly set up a wireless network with strong security between your WX3310 and the AP.
Wireless Network 2.4G	Basic	Use this screen to configure general wireless LAN settings.
	Advanced	Use this screen to configure advanced wireless settings.
	WPS	Use this screen to enable and configure WPS on your WX3310.
	MAC Filter	Use this screen to configure the WX3310 to block access to devices or block the devices from accessing the WX3310.
	MBSS	Use this screen to configure multiple BSSs on the WX3310.
Mesh	Mesh	Use this screen to enable or disable WX3310 Mesh.
MAINTENANCE		
Password	Password Setup	Use this screen to change the password of your WX3310.
Time	Time Setup	Use this screen to change your WX3310's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your WX3310.
Telnet	Telnet	Use this screen to enable or disable Telnet. Telnet allows you to access the WX3310's command line interface.
Restore	Restore	Use this screen to backup and restore the configuration or reset your WX3310 to the factory defaults.
Restart	Restart	Use this screen to reboot the WX3310 without turning the power off.

CHAPTER 7

Tutorials

7.1 Overview

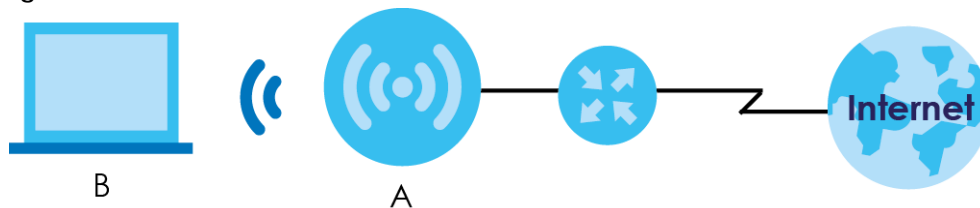
This chapter provides tutorials for your WX3310 as follows:

- [Configuring the WX3310 as an Access Point](#)
- [Configuring the WX3310 as a Repeater](#)

7.2 Configuring the WX3310 as an Access Point

This section gives you an example of how to set up an access point (AP) and wireless client (a notebook **(B)**, in this example) for wireless communication. **B** can access the Internet through the access point **(A)** wirelessly.

Figure 21 Wireless Access Point Connection to the Internet



7.3 Configuring the WX3310 as a Repeater

Repeater mode allows you to extend the original AP coverage.

- **Selecting an AP from an Automatically Detected List** - create a secure wireless network simply by selecting an AP from a list of detected APs. See [Section 11.4 on page 76](#). This is the easier method.
- **Selecting an AP by Manually Entering Security Information** - create a secure wireless network by manually entering the AP's wireless security settings in the WX3310's interface. See [Section 11.3 on page 75](#). This is useful when the AP is hidden.

7.3.1 Selecting an AP from an Automatically Detected List

This section demonstrates the procedures in Repeater mode. Follow the steps below to create a secure wireless network by selecting an AP from a list of detected APs.

The AP select function is available in Repeater mode.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see [Section 2.2 on page 16](#)).

- 1 Open the **Networking > AP Connection > AP List** screen. Select an AP from the **SSID** column. Type the WiFi key if wireless security is enabled on the selected AP and click **Connect**.

Check the connection status to see if your WX3310 is successfully connected to the AP.

Station AP List WPS

ACCESS POINT LIST

Connection Status: Connected
Current SSID: ZyXEL

Click on an access point below to connect.

	SSID	MAC Address	Channel	RSSI(dbm)	Security
1	ZyXEL	B0:B2:DC:70:C0:25	36	41	No
2	ZyXEL	B0:B2:DC:70:C2:0D	36	25	No
3	ZyXEL	B8:EC:A3:12:D6:DA	36	25	No
4	ZyXEL	B0:B2:DC:6A:9F:8A	36	18	No
5	ZyXEL	A0:E4:CB:84:BA:38	36	12	No
6	Zyxel	62:D8:97:0F:8D:D9	40	56	Yes
7	Zyxel1123	60:31:97:0F:8D:D8	40	56	Yes
8	Z2_Frank_test_5G	60:31:97:3E:82:21	153	53	Yes
9	ZyXEL_CSO_5G	4E:AB:FF:7F:D7:AC	36	47	Yes
10	R11test	4E:AB:FF:7F:D7:A0	36	46	Yes
11	Unizyx_WLAN	4E:AB:FF:7F:D7:AF	36	46	Yes
12	Unizyx_MANAGER	4E:AB:FF:7F:D7:AD	36	46	Yes
13	ZyXEL_CSO	4C:9E:FF:7F:D7:AB	36	46	Yes
14	TSD1_5G	60:31:97:3C:29:49	40	45	Yes
15	burninman5G_CSOTEST	E8:37:7A:FF:BA:C5	36	44	Yes
16	ZT01525_88523_5G	5C:6A:80:5F:A3:2E	36	39	Yes

AP: Zyxel1123
Passphrase:

7.3.2 Selecting an AP by Manually Entering Security Information

This example shows you how to configure wireless security settings with the following parameters on your WX3310.

SSID	Zyxel
Security	WPA(2)-PSK
WiFi Key	1234567890

Follow the steps below to create a secure wireless network by manually entering the AP's wireless security settings in the WX3310's interface.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see [Section 2.2 on page 16](#)).

- 1 Open the **Networking > AP Connection > Station or Basic** screen. Type the SSID of the AP into the **Wireless Name (SSID)** field, set the security settings and click **Apply**.

Check the connection status to see if your WX3310 is successfully connected to the AP.

Station

AP List

WPS

Repeater Setup

Network Name(SSID):

Zyxel

Connection Status:

Connected

Encryption:

WPA2 + WPA (mixed mode)

Pre-Shared Key:

Apply

Cancel

PART II

Technical Reference

CHAPTER 8

Monitor

8.1 Overview

This chapter discusses read-only information related to the device state of the WX3310.

8.2 What You Can Do

- Use the **Log** screen to view the logs for the categories such as system maintenance or system errors, see [Section 8.3 on page 45](#).
- Use the **Wireless Monitor** screen to view the wireless stations or AP that are currently associated with the WX3310, see [Section 8.4 on page 46](#).
- Use the **MBSS Monitor** screen to view a summary of the BSS configured in your WX3310, see [Section 8.5 on page 48](#).
- Use the **Multicast Monitor** screen to view the multicast group information, see [Section 8.6 on page 50](#).

8.3 Log

Click  to open the **Monitor** menu. Use the **View Log** screen to see the logged messages for the WX3310.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills.

Click **Monitor > Log > View Log**.

Figure 22 Monitor > Log

Summary		
#	Time	Message
1	Jan 1 13:47:00	user.err syslog: get_ssid_value(): i= 0 WLAN_IF_ptr->SSID=Zyxel00032!
2	Jan 1 13:47:00	user.err syslog: get_ssid_value(): i= 1 WLAN_IF_ptr->SSID=Zyxel00032_1!
3	Jan 1 13:47:00	user.err syslog: get_ssid_value(): i= 2 WLAN_IF_ptr->SSID=Zyxel00032_2!
4	Jan 1 13:47:00	user.err syslog: get_ssid_value(): i= 3 WLAN_IF_ptr->SSID=Zyxel00032_3!
5	Jan 1 13:47:00	user.err syslog: get_ssid_value(): i= 4 WLAN_IF_ptr->SSID=Zyxel00032_4!
6	Jan 1 13:47:00	user.err syslog: get_ssid_value(): i= 5 WLAN_IF_ptr->SSID=Zyxel00032_5!
7	Jan 1 13:47:00	user.err syslog: get_ssid_value(): arr_index = 0,1,8,4,5
8	Jan 1 13:47:00	user.err syslog: get_ssid_value(): sum_active_interface = 5

The following table describes the labels in this screen.

Table 10 Monitor > Log

LABEL	DESCRIPTION
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Refresh	Click Refresh to renew the log screen.
Clear	Click Clear to delete all the logs.

8.4 Wireless Monitor

Go to **Monitor > Wireless Monitor**. View a detailed summary of the AP's general settings and details of its **Associated Devices**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 23 Monitor > Wireless Monitor (Uplink in Repeater mode)

Wireless Monitor

Wireless

Wi-Fi Interface: (Uplink) ▼

Summary	
Item	Data
802.11 Mode:	802.11ax
Bandwidth:	20MHz
AP Mac Address (BSSID):	B8:D5:26:4D:85:C9
Channel:	36
Associated Devices Count:	Not Associated Association Table
Packets Received Successfully:	0
Bytes Received:	0
Packets Transmitted Successfully:	0
Bytes Transmitted:	0

Association Table

	Access Point	VAP	RSSI	TX PHY Data Rate(Mbps)	Rx Bytes	Tx Bytes	BW	Time Associated
Refresh								

Figure 24 Monitor > Wireless Monitor (AP mode)

Wireless Monitor

Wireless

Wi-Fi Interface: Zyxel28870 (5G) ▼

Summary	
Item	Data
802.11 Mode:	802.11ax
Bandwidth:	80MHz
AP Mac Address (BSSID):	B8:D5:26:4D:86:08
Channel:	140/80
Associated Devices Count:	0 Association Table
Packets Received Successfully:	0
Bytes Received:	0
Packets Transmitted Successfully:	0
Bytes Transmitted:	0

Association Table

	Wi-Fi Client	VAP	RSSI	TX PHY Data Rate(Mbps)	Rx Bytes	Tx Bytes	BW	Time Associated
Refresh								

The following table describes the labels in this screen.

Table 11 Monitor > Wireless Monitor

LABEL	DESCRIPTION
Wi-Fi Interface	This shows the name of the wireless network on the WX3310. Uplink only shows in Repeater mode.
802.11 Mode	This shows the wireless standard the WX3310 uses.
Bandwidth	This shows the wireless bandwidth allowed for the WX3310 (in Repeater mode) when the WX3310 is connected to an AP.
AP MAC Address (BSSID)	This shows the MAC Address of your WX3310 or the AP to which the WX3310 (in Repeater or Client mode) is connected.
Channel	This shows the current channel the WX3310 uses to associate with the wireless client or AP.
Associated Devices Count	This shows the number of devices connected to the WX3310 (in AP or Repeater mode).
Packets Received Successfully	This shows the number of packets that have been successfully received by the WX3310.
Bytes Received	This shows the number of bytes that have been received by the WX3310.
Packets Transmitted Successfully	This shows the number of packets that have been successfully transmitted by the WX3310.
Bytes Transmitted	This shows the number of bytes that have been transmitted by the WX3310.
Association Table	The table displays after you click the Association Table button.
Access Point	This shows the MAC address of the AP to which the WX3310 (in Repeater or Client mode) is connected.
Wi-Fi Client	This shows the MAC address of the wireless client which is associated with the WX3310 (in AP or Repeater mode).
VAP	This shows the SSID name of the wireless network to which the WX3310 is connecting.
RSSI (dbm)	This shows the RSSI (Received Signal Strength Indicator) of the WX3310's wireless connection.
TX PHY Data Rate (Mbps)	This shows the current data rate of the connected AP or client.
SNR	This Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power.
Rx Bytes	This shows the number of bytes that have been received by the connected AP or client.
Tx Bytes	This shows the number of bytes that have been transmitted by the connected AP or client.
BW	This shows the wireless bandwidth allowed for the connected wireless clients.
Time Associated	This shows the total amount of time (in seconds) the WX3310 has been associated with the AP or client.
Refresh	Click the Refresh button to refresh the WX3310 settings.

8.5 MBSS Monitor

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). For more information on BSS, see [Section 10.9.2.6 on page 64](#).

A Multiple Basic Server Set (MBSS) allows you to use your WX3310 to provide several Basic Server Sets (BSS) simultaneously. For more information on MBSS, see [Section 10.9.2.7 on page 65](#).

Go to **Monitor > MBSS Monitor**. A Multiple Basic Server Set (MBSS) allows you to use your WX3310 to provide several Basic Server Sets (BSS) simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point. This screen shows a summary of the BSS configured in your WX3310.

Figure 25 Monitor > MBSS Monitor

MBSS Monitor

MBSS

Summary - 5GHz

	SSID	Broadcast	Association	
MBSS 1:	ZyxeI28870_1	1	0	Detail
MBSS 2:	ZyxeI28870_2	1	0	Detail

Summary - 2.4GHz

	SSID	Broadcast	Association	
MBSS 1:	ZyxeI28870_1	1	0	Detail
MBSS 2:	ZyxeI28870_2	1	0	Detail
MBSS 3:	ZyxeI28870_3	1	0	Detail

Association Table

	Access point	RSSI	Rx Bytes	Tx Bytes	BW	Time Associated
1	N/A	N/A	N/A	N/A	N/A	N/A

Refresh

The following table describes the labels in this screen.

Table 12 Monitor > MBSS Monitor

LABEL	DESCRIPTION
SSID	This shows the name for each BSS.
Broadcast	This shows the broadcast status of a specific MBSS. It shows 0 for Disable and 1 for Enable .
Association	This shows the number of devices connected to each BSS.
Detail	Click this button and a summary table describing the BSS is displayed under the MBSS Summary table.
Association Table	The table displays after you click the Detail button.
Access Point	This shows the SSID name for each BSS.
RSSI (dbm)	This shows the RSSI (Received Signal Strength Indicator) of the wireless connection.
Rx Bytes	This shows the number of bytes that have been received by the connected client.
Tx Bytes	This shows the number of bytes that have been transmitted by the connected client.
BW	This shows the wireless bandwidth allowed for the connected wireless clients.
Time Associated	This shows the total amount of time (in seconds) the client has been associated with the BSS.
Refresh	Click this button to refresh the status of the MBSS.

8.6 Multicast Monitor

Go to **Monitor > Multicast Monitor**. IP packets are transmitted in one of these ways.

- Unicast (1 sender to 1 recipient)
- Broadcast (1 sender to everybody on the network)

Multicast delivers IP packets to just a group of hosts on the network. This screen shows a summary of the multicast group IP addresses.

Figure 26 Monitor > Multicast Monitor



The screenshot shows the 'Multicast Monitor' interface. It has a title bar 'Multicast Monitor' and a sub-header 'Multicast'. Below this is a 'Summary' section containing a table with two columns: 'Multicast IP' and 'Interface'. The table lists two entries: '239.192.152.143' on 'WiFi' and '239.2.0.252' on 'WiFi'. At the bottom of the interface is a 'Refresh' button.

Multicast IP	Interface
239.192.152.143	WiFi
239.2.0.252	WiFi

The following table describes the labels in this screen.

Table 13 Monitor > Multicast Monitor

LABEL	DESCRIPTION
Multicast IP	This field displays the multicast group IP address.
Interface	This field displays the interface that belongs to the multicast group.
Refresh	Click this button to refresh the status of the WDS.

CHAPTER 9

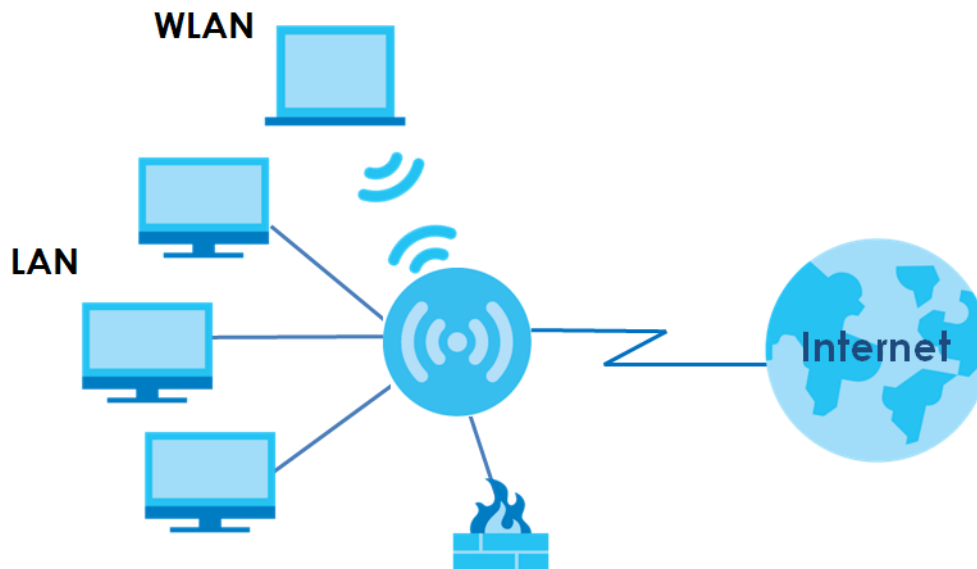
Network

9.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure the WX3310's IPv4 and IPv6 addresses on the LAN.

Figure 27 LAN Setup



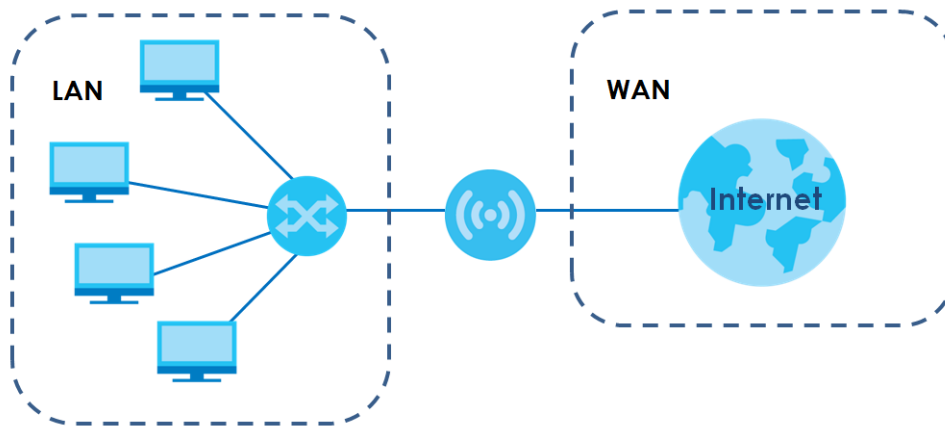
9.2 What You Can Do

Use the **Networking** screen ([Section 9.4 on page 52](#)) to change the LAN IP address for your WX3310.

9.3 What You Need To Know

The actual physical connection determines whether the WX3310 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 28 LAN and WAN IP Addresses



9.4 Networking Screen

Use this screen to change your basic LAN settings. Click **Network > Networking**.

Note: The fields and buttons in this screen is not available if you choose **DHCP** or **SLAAC**.

Figure 29 Network > Networking

Networking

LAN IP

☐ DHCP ☒ Static IP

IP Address:

IP Subnet Mask:

Gateway IP:

DNS Server 1:

DNS Server 2:

IPv6

☐ DHCP ☐ SLAAC(StateLess Address Auto-Configuration) ☒ Static IP

WAN IPv6 Address:

IPv6 Gateway:

The following table describes the labels in this screen.

Table 14 Network > Networking

LABEL	DESCRIPTION
LAN IP	<p>Select DHCP to deploy the WX3310 as a DHCP client in the network. When you enable this, the WX3310 gets its IP address from the network's DHCP server (for example, your ISP or router). Users connected to the WX3310 can now access the network (i.e., 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 WX3310 in the field below.</p> <p>Select Static IP if you want to specify the IP address of your WX3310. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.</p>
IP Address	Type the IPv4 address of your WX3310 in dotted decimal notation if you select Static IP .
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Gateway IP	Enter a gateway IPv4 address (if your ISP or network administrator gave you one) in this field.
DNS Server 1	Enter the first DNS server address assigned to WX3310.
DNS Server 2	Enter the second DNS server address assigned to WX3310.
IPv6	<p>Select DHCP to obtain an IPv6 address using IPv6 stateful autoconfiguration.</p> <p>Select SLAAC(StateLess Address Auto-Configuration) to obtain an IPv6 address using IPv6 stateless autoconfiguration.</p> <p>Select Static to configure a fixed IPv6 address for the WX3310.</p>
WAN IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for the 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 Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your WX3310's interface(s). The gateway helps forward packets to their destinations.
Apply	Click Apply to save your changes back to the WX3310.
Cancel	Click Cancel to exit this screen without saving.

CHAPTER 10

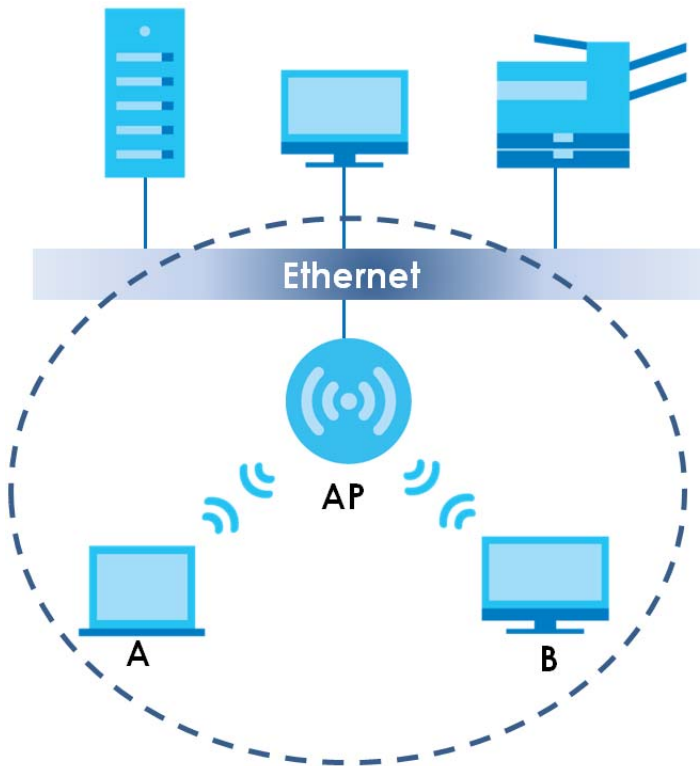
Wireless LAN

10.1 Overview

This chapter discusses how to configure the wireless network settings in your WX3310. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 30 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (**AP**) to interact with other devices (such as the printer) or with the Internet. Your WX3310 is the AP in the above example.

Note: This chapter is only for AP mode and Repeater mode. It shows how to configure a wireless connection for your wireless clients.

10.2 What You Can Do in this Chapter

Wireless screens vary according to the device mode you are using. See [Chapter 3 on page 24](#) for more information on device modes.

- Use the **Basic** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode, see [Section 10.4 on page 56](#).
- Use the **Advanced** screen to configure wireless advanced settings such as the wireless band or channel bandwidth, see [Section 10.5 on page 57](#).
- Use the **WPS** screen to quickly set up a wireless network with strong security without having to configure security settings manually, see [Section 10.6 on page 58](#).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the WX3310, see [Section 10.7 on page 59](#).
- Use the **MBSS** screen to enable and configure multiple BSSs on the WX3310, see [Section 10.8 on page 60](#).

10.3 What You Should Know

Every wireless network must follow these basic guidelines.

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

10.3.1 Wireless Basic

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

10.3.2 WiFi6 / IEEE 802.11ax

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

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

Table 15 WiFi Standards Comparison

WIFI STANDARD	MAXIMUM LINK RATE*	BAND	SIMULTANEOUS CONNECTIONS
802.11b	11 Mbps	2.4 GHz	1
802.11a/g	54 Mbps	2.4 GHz and 5 GHz	1
802.11n	600 Mbps	2.4 GHz and 5 GHz	1
802.11ac	3.47 Gbps	5 GHz	4
802.11ax	573 Mbps	2.4 GHz	128
	4.8 Gbps	5 GHz	

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

10.4 Basic Wireless Network Screen

Use this screen to enable the wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the WX3310 from a computer connected to the wireless LAN and you change the WX3310's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the WX3310's new settings.

Click **Networking > Wireless Network 5G/2.4G > Basic** to open the **Basic** screen.

Figure 31 Networking > Wireless Network 5G/2.4G > Basic (Repeater Mode)

The screenshot shows the 'Basic' tab of the 'Wireless Setup' screen. The 'Network Name(SSID)' field contains 'Zyxel28870'. The 'Broadcast SSID' checkbox is checked. The 'Channel Selection' dropdown is set to 'Auto', with a 'Current: 36' indicator below it. The 'Encryption' dropdown is set to 'WPA2-AES'. The 'Pre-Shared Key' field contains '5ECE858VTQ'. The 'Group Key Update Timer (in sec)' field contains '3600'. The 'Clone setting from AP connection' checkbox is unchecked. At the bottom, there are 'Apply' and 'Cancel' buttons.

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

Table 16 Networking > Wireless Network 5G/2.4G > Basic

LABEL	DESCRIPTION
Network Name(SSID)	The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Broadcast SSID	Select this to have the WX3310 broadcast the SSID in the area. If it is disabled the WX3310 does not broadcast the SSID.

Table 16 Networking > Wireless Network 5G/2.4G > Basic (continued)

LABEL	DESCRIPTION
Channel Selection	<p>Select the operating channel for the WX3310 and its wireless clients. The options vary depending on the frequency band and the country you are in.</p> <p>Select Auto and the WX3310 selects a channel automatically.</p> <p>Select Smart Channel Selection (SCS), and the WX3310 decides to switch channels, monitors several channels and chooses the one with higher capacity.</p>
Current Channel	This displays the channel the WX3310 is currently using.
Encryption	<p>Select the data encryption method the WX3310 uses.</p> <p>Select WPA2-AES or WPA2 + WPA (mixed mode) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. Or you can select No Security to allow any client to associate this network without authentication.</p>
Pre-Shared Key	Enter the password that lets you connect to the WX3310. Your password should be in a string of ASCII characters between 8 and 63 or hexadecimal characters between 8 and 64.
Group Key Update Timer	The Group Key Update Timer is the rate at which the WX3310 sends a new group key out to clients.
Clone setting from AP connection	<p>Select this to copy the password and SSID from the wireless router or AP to the WX3310. Wireless clients can then connect to the WX3310 using the same SSID and password as they did to connect to the wireless router.</p> <p>The check box is not available when the WX3310 is in AP mode.</p>
Apply	Click Apply to save your changes back to the WX3310.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.5 Advanced Wireless Network Screen

Use this screen to select the advanced wireless settings for the WX3310.

Click **Networking > Wireless Network 5G/2.4G > Advanced**. The screen appears as shown.

Figure 32 Networking > Wireless Network 5G/2.4G > Advanced

The screenshot shows the 'Advanced' configuration screen for the WX3310's wireless network. The top navigation bar includes tabs for 'Basic', 'Advanced', 'WPS', 'MAC Filter', and 'MBSS', with 'Advanced' currently selected. The main content area is titled 'Wireless Setup' and contains four configuration items, each with a dropdown or input field: 'Wireless Band' is set to '802.11ax', 'Channel Bandwidth' is set to '160 MHz', 'Beacon Interval (in ms)' is set to '100', and 'DTIM Period' is set to '1'. At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 17 Networking > Wireless Network 5G/2.4G > Advanced

LABEL	DESCRIPTION
Wireless Band	Select the wireless standard you want to use for your wireless network.
Channel Bandwidth	Select the channel bandwidth you want to use for your wireless network. Select whether the WX3310 uses a wireless channel width of 20MHz , 40MHz or 80MHz . A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz 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 wireless 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 wireless signal.
Beacon Interval	This is the time lag between each of the beacons sent by the wireless network.
DTIM Period	The Delivery Traffic Indication Map (DTIM) period, is the moment the WX3310 will broadcast any buffered broadcast frames, after the WX3310 broadcasts the beacon. Enter 1, and the WX3310 will transmit broadcast frames after every beacon, enter 2 and the WX3310 will transmit every other beacon.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

10.6 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Networking > Wireless Network 5G/2.4G > WPS**.

Note: With WPS, wireless clients can only connect to the 5GHz or 2.4GHz wireless network using the first SSID on the WX3310.

Figure 33 Networking > Wireless Network 5G/2.4G > WPS

The screenshot displays the 'WPS Setup' configuration page. At the top, there are navigation tabs: 'Basic', 'Advanced', 'WPS' (selected), 'MAC Filter', 'WDS', and 'MBSS'. Below the tabs, the 'WPS Setup' section contains the following elements:

- State:** A dropdown menu currently showing 'Configured'.
- WPS PBC:** A button labeled 'Push Button'.
- WPS PIN:** An input field followed by a button labeled 'WPS PIN'.
- Device PIN Enable:** A checkbox that is checked.
- PIN Number:** An input field containing the text '93806053' and a button labeled 'Generate'.

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

The following table describes the labels in this screen.

Table 18 Networking > Wireless Network 5G/2.4G > WPS

LABEL	DESCRIPTION
WPS Setup	
State	<p>Select Configured to enable WPS and do NOT change the wireless security key after the WPS connection is established.</p> <p>Select Unconfigured to enable WPS but change the wireless security key after the WPS connection is established.</p> <p>Select Disabled to turn off WPS.</p>
WPS PBC	Click the Push Button to perform wireless security information synchronization using the Push Button Configuration (PBC) Method.
WPS PIN	<p>Use this field to type the same PIN number generated in the wireless station's utility to perform wireless security information synchronization using the PIN Configuration Method.</p> <p>Click the WPS PIN button to establish the synchronization. The PIN should be between 4 and 8 characters.</p>
Device PIN Enable	Select this to allow the WX3310 to create a new PIN number. Wireless clients then can use the generated PIN number to perform wireless security information synchronization with the WX3310 via WPS.
PIN Number	This displays a PIN number last time system generated. Click Generate to generate a new PIN number.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

10.7 MAC Filter

The MAC filter screen allows you to configure the WX3310 to give exclusive access to devices (**Allow**) or exclude devices from accessing the WX3310 (**Reject**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your WX3310's MAC filter settings, click **Networking > Wireless Network 5G/2.4G > MAC Filter**. The screen appears as shown.

Figure 34 Networking > Wireless Network 5G/2.4G > MAC Filter

MAC Filter Setup

Interface:

Policy:

MAC Addresses:

The format of MAC Address should be 00:19:CB:00:00:01

The following table describes the labels in this menu.

Table 19 Networking > Wireless Network 5G/2.4G > MAC Filter

LABEL	DESCRIPTION
Interface	Select the SSID for which you want to configure MAC filtering.
Policy	<p>Define the filter action for the list of specified MAC addresses.</p> <p>Select None to deactivate the MAC filtering rule you configure below.</p> <p>Select Allow to permit access to the WX3310. MAC addresses not listed will be denied access to the WX3310.</p> <p>Select Reject to block access to the WX3310. MAC addresses not listed will be allowed to access the WX3310.</p>
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the WX3310 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.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

10.8 MBSS Screen

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). For more information on BSS, see [Section 10.9.2.6 on page 64](#).

A Multiple Basic Server Set (MBSS) allows you to use your WX3310 to provide several Basic Server Sets (BSS) simultaneously. For more information on MBSS, see [Section 10.9.2.7 on page 65](#).

Use this screen to assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.

To open this screen, click **Networking > Wireless Network 5G/2.4G > MBSS**.

Figure 35 Networking > Wireless Network 5G/2.4G > MBSS

The following table describes the labels in this screen.

Table 20 Networking > Wireless Network 5G/2.4G > MBSS

LABEL	DESCRIPTION
MBSS Selection	Select the BSS you want to configure.
Enable	Click on the check box to enable the BSS.
Network Name (SSID)	Type a name for one of your BSS. You can enable up to 4 simultaneous BSSs on your WX3310.
Broadcast SSID	Click on the check box if you want your SSID to be broadcasted to users in the area.
Encryption	Select the type of security to protect the information through the wireless network.
Pre-Shared Key	Type the password users need to connect to this BSS.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

10.9 Technical Reference

This section discusses WiFis in depth. For more information, see [Appendix A on page 91](#).

10.9.1 Wireless Network Overview

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

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

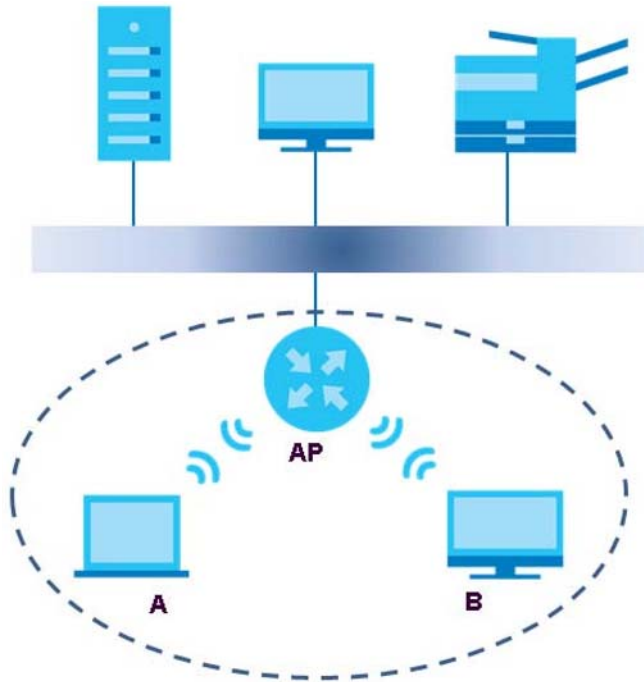
Traditionally, a wireless network operates in one of two ways:

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.

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

The following figure provides an example of a wireless network.

Figure 36 Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

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

Radio Channels

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

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

10.9.2 Wireless Security Overview

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

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

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

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

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

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

10.9.2.1 SSID

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

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

10.9.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example,

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

00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the WX3310 which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

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

10.9.2.3 User Authentication

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

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

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

10.9.2.4 Encryption

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

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

10.9.2.5 Signal Problems

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

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

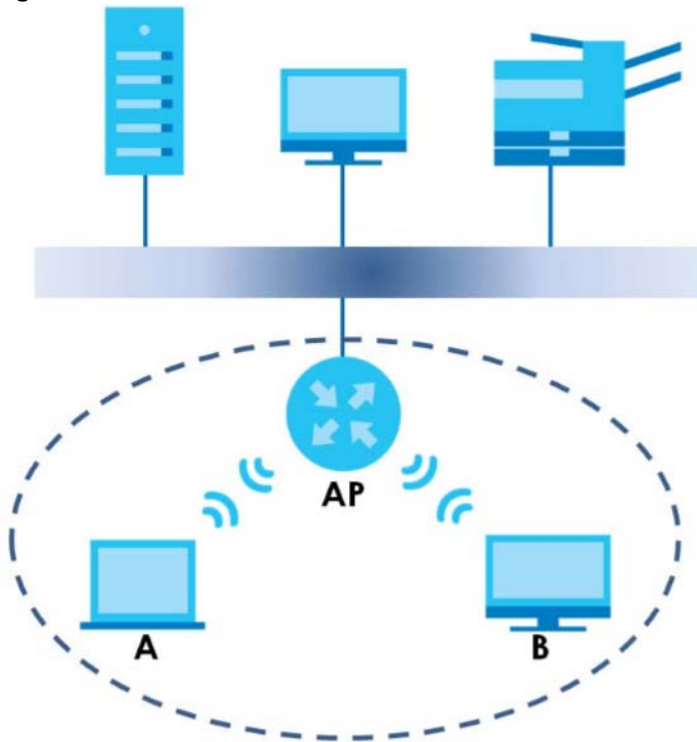
10.9.2.6 BSS

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

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When

IntraBSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 37 Basic Service Set



10.9.2.7 MBSSID

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

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

10.9.2.8 Notes on Multiple BSS

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

10.9.2.9 Preamble Type

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

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

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

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

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

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

10.9.3 WiFi Protected Setup (WPS)

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

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

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

This section gives you an example of how to set up wireless networks using WPS when the WX3310 is in AP or Repeater mode. The following example uses the WX3310 as the AP and a WPS-enabled Android smartphone as the wireless client.

The following WPS methods for creating a secure connection are described in the tutorial.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section 10.9.3.2 on page 67](#). This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the WX3310's interface. See [Section 10.9.3.3 on page 68](#). This is the more secure method, since one device can authenticate the other.

10.9.3.1 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 21 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable


Table 21 Wireless Security Relational Matrix (continued)

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

10.9.3.2 Push Button Configuration (PBC)

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.

The push button configuration function found in the interfaces is available both in AP mode and Repeater mode. The WPS button, see [Section 1.4 on page 11](#), can also be used for PBC configurations in either AP or Repeater mode.

- 1 Make sure that your WX3310 is turned on and set to work in AP mode and that it is within range of the wireless client.
- 2 Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap **WPS Push Button** or the WPS icon ().
- 3 Log into WX3310's Web Configurator. Make sure WPS is enabled in the **Networking > Wireless Network 2.4G** or **Wireless Network 5G > WPS** screen.
- 4 Navigate to **Networking > Wireless Network 2.4G** or **Wireless Network 5G > WPS** and press the **Push Button**.

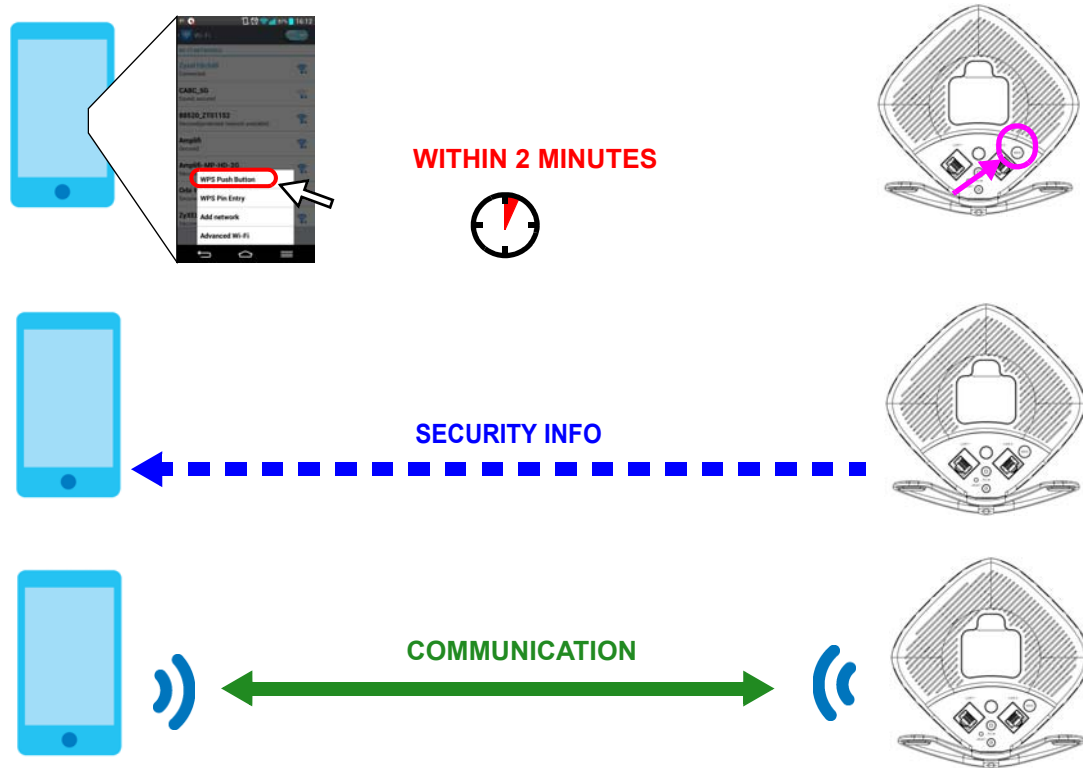
Note: Your WX3310 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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

The WX3310 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WX3310 securely.

The following figure shows you how to set up wireless network and security by pressing a button on both WX3310 and wireless client (the Android smartphone in this example).

Figure 38 Example WPS Process: PBC Method

Wireless Client**AP****10.9.3.3 PIN Configuration**

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

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

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

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

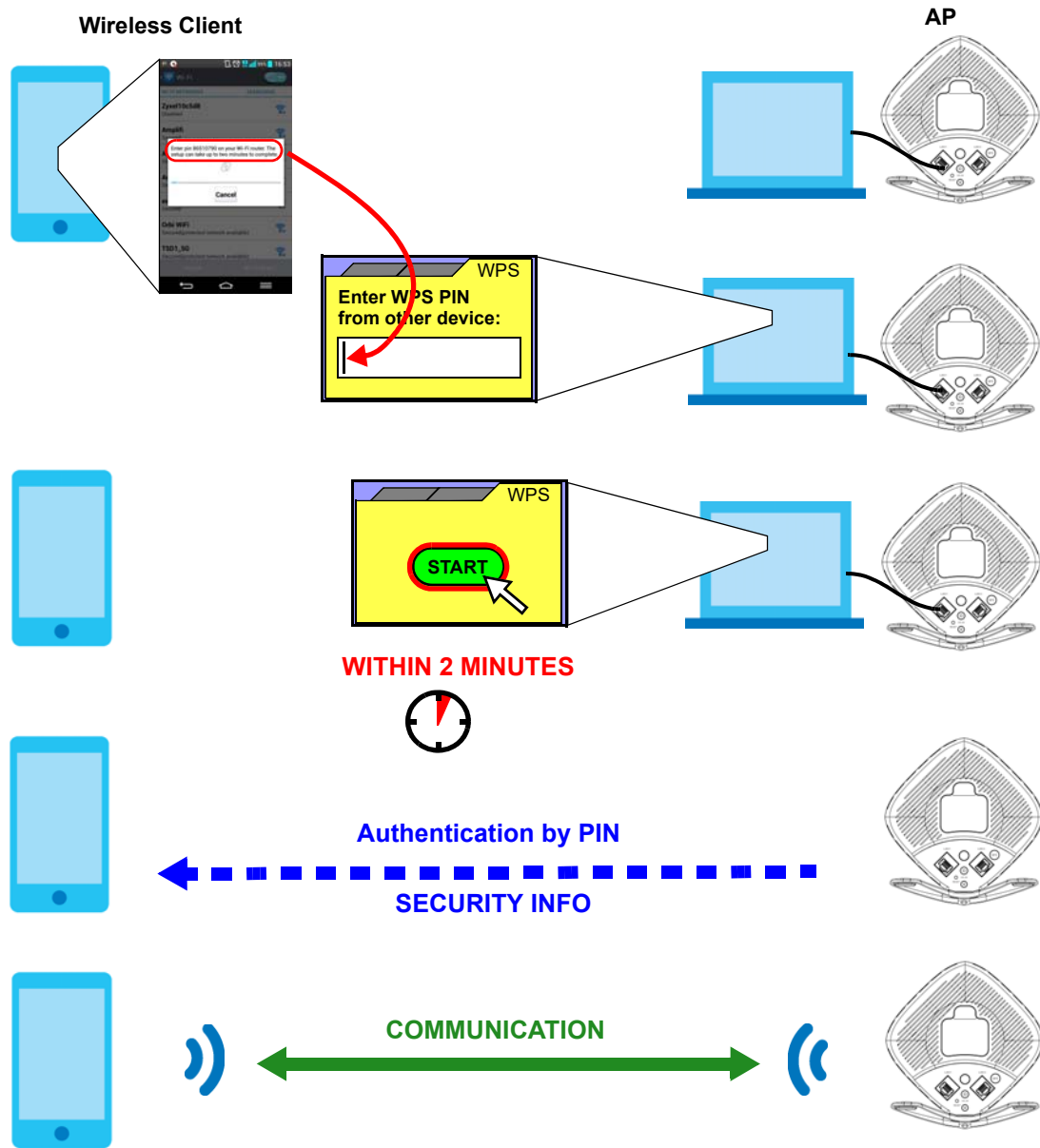
When you use the PIN configuration method, you need to check the client's PIN number and use the configuration interface of the WX3310 in AP mode.

- 1** Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap **WPS PIN Entry** to get a PIN number.
- 2** Enter the client's PIN number to the PIN field in the **Networking > Wireless Network 2.4G** or **Wireless Network 5G > WPS** screen on the WX3310 (in AP mode).
- 3** Click the **WPS PIN** button (or button next to the PIN field) on the WX3310's **WPS** screen within two minutes.

The WX3310 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the WX3310 securely.

The following figure shows an example of how to set up wireless network and security on WX3310 and wireless client (the Android smartphone in this example) by using PIN method.

Figure 39 Example WPS Process: PIN Method

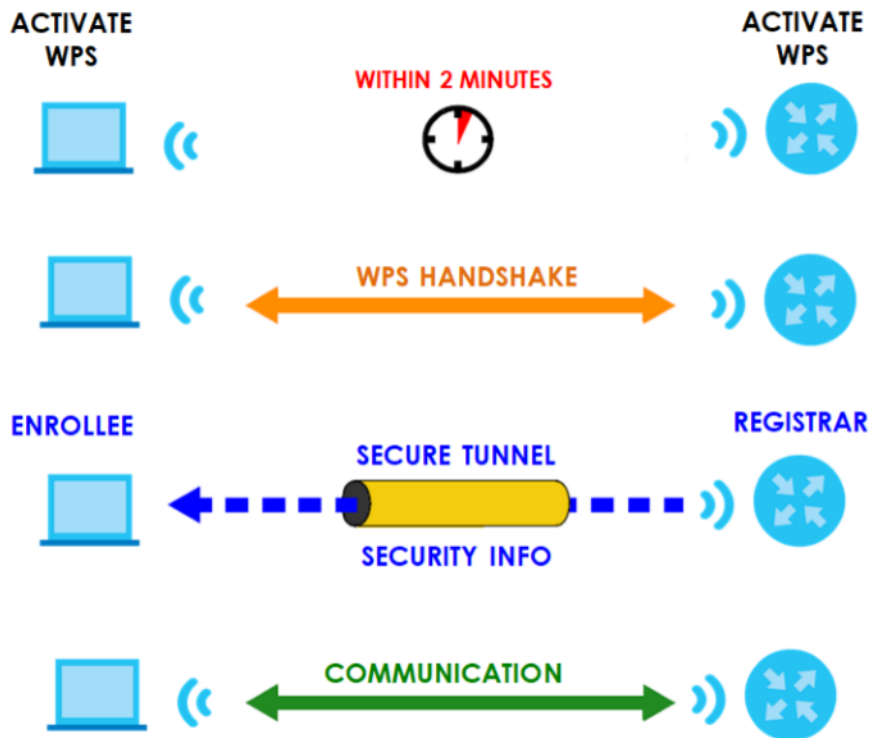


10.9.3.4 How WPS Works

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 40 How WPS Works



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

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

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

By default, a WPS 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 wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

10.9.3.5 Example WPS Network Setup

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

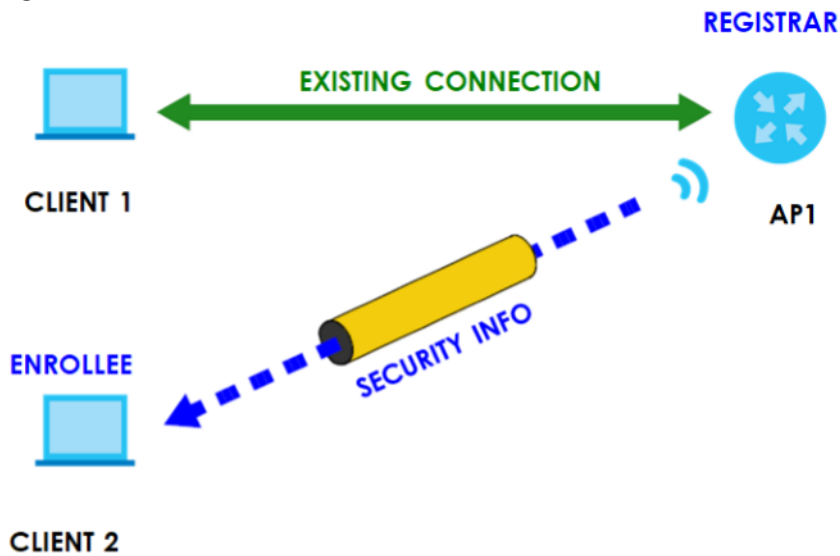
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 41 WPS: Example Network Step1



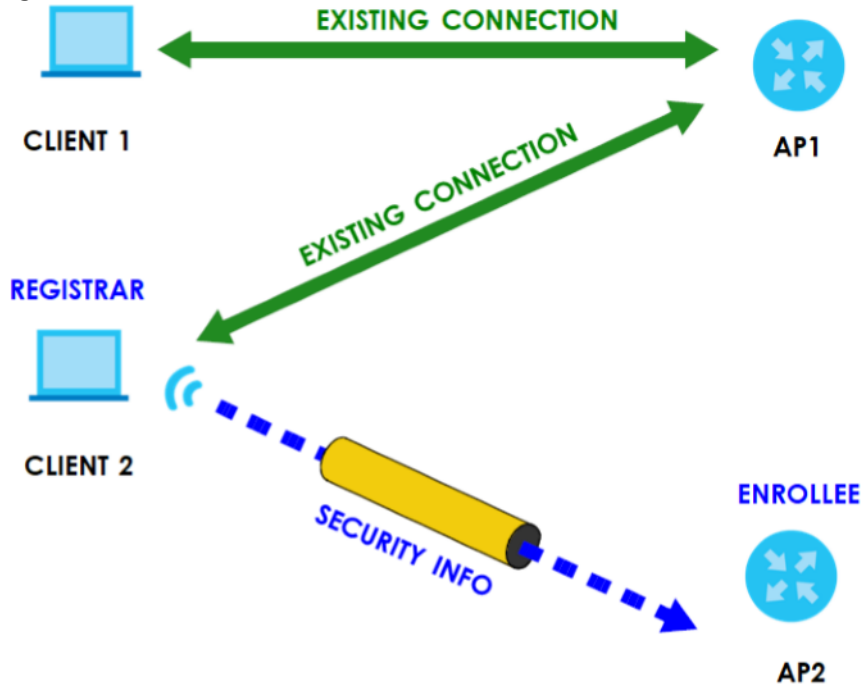
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 42 WPS: Example Network Step2



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 43 WPS: Example Network Step 3



10.9.3.6 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

CHAPTER 11

AP Connection (Repeater Mode)

11.1 Overview

This chapter discusses how to establish a wireless connection between your WX3310 and another AP or wireless network when the WX3310 is in repeater mode. It allows you to connect to and/or extend the existing wireless network. The following figure provides an example of two wireless networks connected together.

Use these screens to choose an access point that you want the WX3310 to connect to. You should know the security settings of the target AP.

Note: The fields and buttons in this screen is not available if the WX3310 is in AP mode.

11.2 What You Can Do in this Chapter

- Use the **Station** screen to manually enter the SSID and security settings of the AP to which you want the WX3310 to connect, see [Section 11.3 on page 75](#).
- Use the **AP List** screen to scan the wireless networks in the WX3310's area. You can also select an AP from the list and enter its WiFi password to connect the wireless network, see [Section 11.4 on page 76](#)
- Use the **WPS** screen to enable/disable WPS, view or generate a new PIN number, see [Section 11.5 on page 78](#).

11.3 Station Screen

Use this screen to manually enter the SSID and security settings of the AP to which you want the WX3310 to connect. This screen allows you to set a profile so that the WX3310 will automatically try to connect to the AP specified in the profile each time the WX3310 in Repeater mode is turned on.

Click **Networking > AP Connection > Station** in repeater mode to open this screen.

Figure 44 Networking > AP Connection > Station (Repeater mode)

The screenshot shows a web interface for configuring a wireless station. At the top, there are three tabs: 'Station' (selected), 'AP List', and 'WPS'. Below the tabs is the 'Wireless Setup' section. It contains three fields: 'Network Name(SSID):' with an empty text input box, 'Connection Status:' with the text 'Not Connected', and 'Encryption:' with a dropdown menu showing 'No Security'. At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

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

Table 22 Networking > AP Connection > Basic/Station

LABEL	DESCRIPTION
Network Name(SSID)	Enter the name of the wireless network to which the WX3310 is connecting
Connection Status	This shows whether the WX3310 is already connected, attempting to connect, or not connected to a wireless network.
Encryption	Select the data encryption method the wireless network uses.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

11.4 AP List Screen

You can use this screen to select an AP and enter its WiFi password to connect the wireless network. After connecting to an AP its SSID is automatically displayed in the **Basic/Station** screen.

Click **Networking > AP Connection > AP List**. The screen appears as shown.

Figure 45 Networking > AP Connection > AP List (Repeater mode)

Station **AP List** **WPS**

ACCESS POINT LIST

Connection Status: Connecting ...
Current SSID:

Click on an access point below to connect.

	SSID	MAC Address	Channel	RSSI(dbm)	Security
1	Zyxel	62:D8:97:0F:8D:D9	40	58	Yes
2	Zyxe11123	60:31:97:0F:8D:D8	40	57	Yes
3	Z2_Frank_test_5G	60:31:97:3E:82:21	153	52	Yes
4	TSD1_5G	60:31:97:3C:29:49	40	46	Yes
5	R11test	4E:AB:FF:7F:D7:A0	36	45	Yes
6	Unizyx_WLAN	4E:AB:FF:7F:D7:AF	36	45	Yes
7	Unizyx_MANAGER	4E:AB:FF:7F:D7:AD	36	45	Yes
8	ZyXEL_CSO_5G	4E:AB:FF:7F:D7:AC	36	45	Yes
9	ZyXEL_CSO	4C:9E:FF:7F:D7:AB	36	45	Yes
10	Zyxe1_5CCD_5G	1C:74:0D:A9:5C:CE	36	44	Yes
11	ZyXEL866F40_5G	E8:37:7A:86:6F:41	157	44	Yes
12	Zyxe1_AB6D_5G	60:31:97:10:AB:6E	36	40	Yes
13	burninman5G	E8:37:7A:FF:BA:C5	36	39	Yes
14	Elisa_5G_999999999	46:8B:F3:B5:36:D9	44	39	Yes
15	Zyxe1_ZT01152_5G	28:6C:07:5E:E4:9A	161	38	Yes
16	VIDEOTRON0051_5GHz	FC:F5:28:D3:88:B5	40	38	Yes
17	ZyXEL_F6E1_5G	E8:37:7A:84:F6:E2	161	37	Yes
18	ZyXEL_CSO_5G	62:09:97:0F:8D:0A	149	35	Yes
19	Application Patrol Test	60:31:97:7D:5B:A2	40	35	Yes
20	3425Test_5G	E8:37:7A:86:6F:71	157	34	Yes
21	Unizyx_WLAN	62:09:97:0F:8D:0D	149	34	Yes
22	Unizyx_MANAGER	62:09:97:0F:8D:0B	149	34	Yes
23	ZyXEL_CSO	60:31:97:0F:8D:09	149	34	Yes
24	Unizyx_WLAN	62:75:97:82:F7:71	161	32	Yes
25	Fioptics00049	60:31:97:10:BF:F6	48	32	Yes

Rescan

The following table describes the labels in this screen.

Table 23 Networking > AP Connection > AP List

LABEL	DESCRIPTION
Connection Status	This shows whether the WX3310 is already connected, attempting to connect, or not connected to a wireless network.
Current SSID	This shows the name of the AP to which your WX3310 is currently connected.
SSID	This shows the network name of the AP the WX3310 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 WX3310 needs a security password to connect to the AP. It shows No if the WX3310 does not need a password to connect.
AP	This shows the name of the AP you click and try to connect.
Passphrase	The Passphrase input box displays when the Security column is Yes for the selected SSID. Enter the password for this wireless network in the Passphrase input box.
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.

11.5 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number. To open this screen, click **Networking > AP Connection > WPS**.

Figure 46 Networking > AP Connection > WPS (Repeater mode)

The following table describes the labels in this screen.

Table 24 Networking > AP Connection > WPS

LABEL	DESCRIPTION
WPS Setup	
WPS PBC	Click the Push Button to perform wireless security information synchronization using the Push Button Configuration (PBC) Method.
WPS PIN	This field displays the PIN number for the WX3310 you will use to perform wireless security information synchronization using the PIN Configuration Method. Click the WPS PIN button to establish the synchronization. Click Generate to create a new PIN and display it in the WPS PIN field.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 12

Mesh

12.1 Overview

The WX3310 supports Wi-Fi Certified EasyMesh Version 1.

Use this screen to enable or disable EasyMesh, known as Mesh in this product. Mesh supports AP steering and Band steering.

- AP steering allows wireless 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 wireless clients and drop their connections to optimize the Zyxel 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 Mesh supported device with a strong signal.
- Band steering allows 2.4G/5G dual-band wireless clients to steer from one band to another. For example, if the 2.4G channel is congested, wireless clients that support 5G could be moved to the 5G channel.

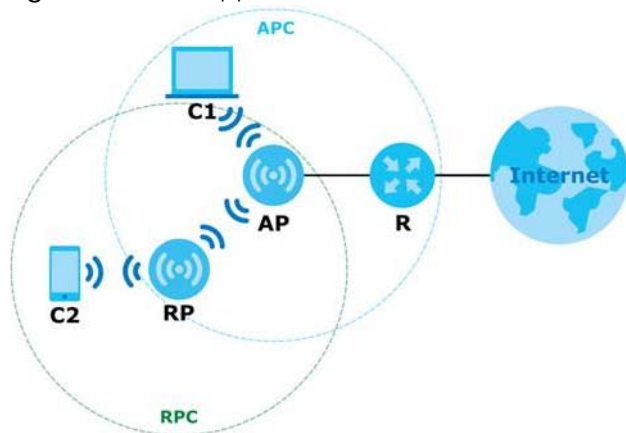
You need a router that can function as a controller in order to set up a Mesh network. A controller manages and coordinates WiFi activity in a network, such as:

- 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.

See the steps below on how to set up a Mesh network.

- 1 To set the WX3310 in **AP** mode, connect it to a router using an Ethernet cable.
- 2 To set the WX3310 in **Repeater** mode, do the following:
 - Enable wireless LAN in the **Networking > Wireless Network 5G/2.4G > Basic** screen.
 - Enable Mesh in the **Configuration > Mesh** screen.
 - Press the WPS button on both the router (controller) and the WX3310. See the Quick Start Guide for more information.

Figure 47 Mesh Application

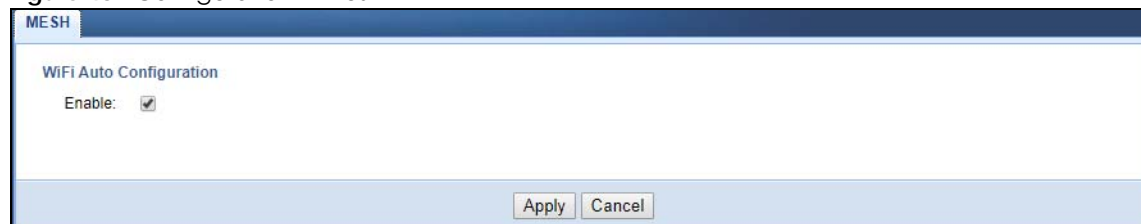
Icons used in Figure 47:

- R- router
- AP- Access Point
- RP- Repeater
- C1- Client1
- C2- Client2
- APC- Access Point coverage area
- RPC- Repeater coverage area

Note: R is a router controller

12.2 Mesh Screen

Click **Configuration > Mesh**. The following screen displays.

Figure 48 Configuration > Mesh

Click on the check box to enable Easy Mesh on the WX3310.

CHAPTER 13

Maintenance

13.1 Overview

This chapter provides information on the **Maintenance** screen.

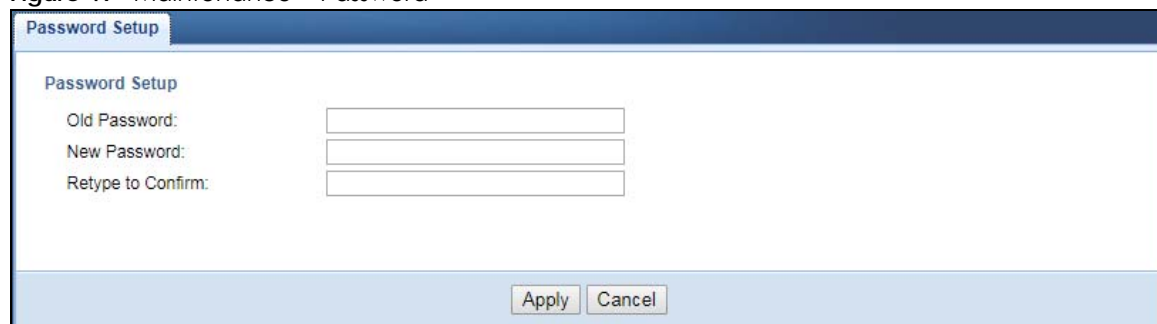
13.2 What You Can Do in this Chapter

- Use the **Password** screen to set the password, see [Section 13.3 on page 81](#).
- Use the **Time** screen to change your WX3310's time and date, see [Section 13.4 on page 82](#).
- Use the **Firmware Upgrade** screen to update firmware, see [Section 13.5 on page 83](#).
- Use the **Telnet** screen to enable or disable access to the WX3310 using Telnet, see [Section 13.6 on page 84](#).
- Use the **Restore** screen to back up and restore device configurations, see [Section 13.6 on page 84](#).
- Use the **Restart** screen to reboot the WX3310 without turning the power off, see [Section 13.7 on page 86](#).

13.3 Password Screen

Use this screen to set the web configurator password. Click **Maintenance > Password**. The following screen displays.

Figure 49 Maintenance > Password



The screenshot shows a web browser window with a title bar. The page has a blue header with the text "Password Setup". Below the header, the main content area is white and contains the text "Password Setup" followed by three input fields labeled "Old Password:", "New Password:", and "Retype to Confirm:". At the bottom of the page, there is a light blue footer bar containing two buttons: "Apply" and "Cancel".

The following table describes the labels in this screen.

Table 25 Maintenance > Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

13.4 Time Screen

Use this screen to configure the WX3310's time based on your local time zone. To change your WX3310's time and date, click **Maintenance > Time**. The screen appears as shown.

Figure 50 Maintenance > Time

The following table describes the labels in this screen.

Table 26 Maintenance > Time

LABEL	DESCRIPTION
NTP Time Server	
NTP Server 1	Enter the first IP address or URL (up to 29 extended ASCII characters in length) of your time server.
NTP Server 2	Enter the second IP address or URL (up to 29 extended ASCII characters in length) of your time server. The second NTP server will work as your backup server if connection to the first NTP server fails.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving Enable	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.

Table 26 Maintenance > Time (continued)

LABEL	DESCRIPTION
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected Daylight Saving Enable. The at field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and select 2 in the at field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March. The time you select in the at field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Enable. The at field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and select 2 in the at field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October. The time you select in the at field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

13.5 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a “*.bin” extension, e.g., “WX3310.bin”. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your WX3310.

Figure 51 Maintenance > Firmware Upgrade

Firmware Upgrade

Firmware Upgrade

To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.

While upgrading, please do not power off or unplug ethernet.

File Path: No file chosen

The following table describes the labels in this screen.

Table 27 Maintenance > Firmware Upgrade

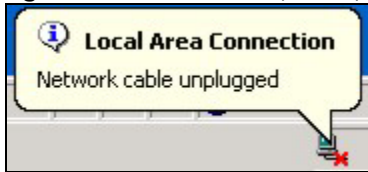
LABEL	DESCRIPTION
Firmware Upgrade	
File Path	Click Choose file to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the WX3310 while firmware upload is in progress!

Wait until the upgrade process is complete.

The WX3310 automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 52 Network Temporarily Disconnected



After the WX3310 restarts, log in again and check your new firmware version in the **Status** screen.

13.6 Restore Screen

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

Figure 53 Maintenance > Restore

Restore

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

Restore Configuration
File Path: No file chosen

Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 5f67c57Sd4
- LAN IP address will be 192.168.1.2

13.6.1 Backup Configuration

Backup configuration allows you to back up (save) the WX3310's current configuration to a file on your computer. Once your WX3310 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the WX3310's current configuration to your computer.

13.6.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your WX3310.

Table 28 Maintenance > Restore Configuration

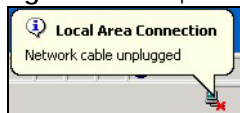
LABEL	DESCRIPTION
File Path	Click Choose file to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin the upload process.

Note: Do not turn off the WX3310 while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait one minute before logging into the WX3310 again.

The WX3310 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 54 Temporarily Disconnected

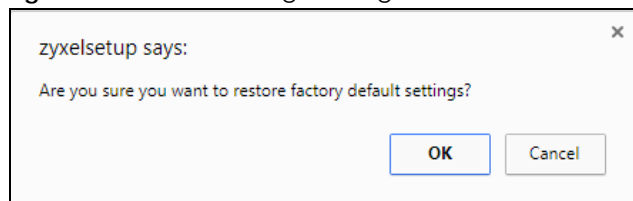


If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default WX3310 IP address (192.168.1.2). Refer to your operating system's help files for details on how to set up your computer's IP address.

13.6.3 Back to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the WX3310 to its factory defaults. The following warning screen appears.

Figure 55 Reset Warning Message

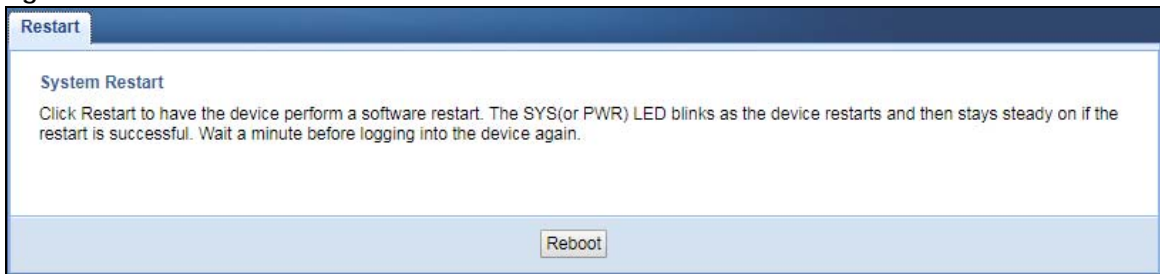


You can also press the **RESET** button on the rear panel for more than 5 seconds to reset the factory defaults of your WX3310. Refer to [Section 1.7 on page 15](#) for more information on the resetting the WX3310.

13.7 Restart Screen

System restart allows you to reboot the WX3310 without turning the power off. Click **Maintenance > Restart**. The following screen displays. Click **Reboot** to have the WX3310 restart. This does not affect the WX3310's configuration.

Figure 56 Maintenance > Restart



CHAPTER 14

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [WX3310 Access and Login](#)
- [Internet Access](#)
- [Resetting the WX3310 to Its Factory Defaults](#)
- [Wireless Problems](#)

14.1 Power, Hardware Connections, and LEDs

[The WX3310 does not turn on. None of the LEDs turn on.](#)

- 1 Make sure the WX3310 is plugged in to an appropriate power source. Make sure the power source is turned on.
- 2 Disconnect and re-connect the WX3310.
- 3 Remove the WX3310 from the outlet. Then connect an electrical device that you know works into the same power outlet. This checks the status of the power outlet.
- 4 If the problem continues, contact the vendor.

[One of the LEDs does not behave as expected.](#)

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.4 on page 11](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the WX3310.
- 5 If the problem continues, contact the vendor.

14.2 WX3310 Access and Login

I forgot the password.

- 1 The default password is in the device label.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 14.4 on page 90](#).

I cannot see or access the **Login** screen in the Web Configurator.

- 1 Make sure you are using the correct address.
 - The default web address (URL) of the WX3310 is **http://zyxelsetup** (for Windows) or **http://zyxelsetup.local** (for Mac).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.4 on page 11](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
- 4 Reset the device to its factory defaults, and try to access the WX3310 with the default address.
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- If your computer is connected wirelessly, use a computer that is connected to a **LAN** port.

I can see the **Login** screen, but I cannot log in to the WX3310.

- 1 Make sure you have entered the password correctly. The default password is in the device label.
- 2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 3 Disconnect and re-connect the WX3310.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 14.4 on page 90](#).

14.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
 - 2 Try to connect directly to the gateway. If you can access the Internet, check that the WX3310 has connected to the gateway by checking the **Status** screen. See [Section 4.4 on page 28](#).
 - 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the WX3310.
 - 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
 - 5 If the problem continues, contact the network administrator or vendor.
-

I cannot access the Internet anymore. I had access to the Internet (with the WX3310), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.4 on page 11](#).
 - 2 Reboot the WX3310.
 - 3 Try to connect directly to the gateway. If you can access the Internet, check that the WX3310 has connected to the gateway by checking the **Status** screen. See [Section 4.4 on page 28](#).
 - 4 If the problem continues, contact the network administrator or vendor.
-

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.4 on page 11](#). If the WX3310 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
 - 2 Check the signal strength. If the signal strength is low, try moving the WX3310 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
 - 3 Reboot the WX3310.
 - 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.
-

14.4 Resetting the WX3310 to Its Factory Defaults

If you reset the WX3310, you lose all of the changes you have made. The WX3310 re-loads its default settings, and the password resets to the back-label default key. You have to make all of your changes again.

You will lose all of your changes when you reset the WX3310 to its factory defaults.

To reset the WX3310,

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 5 seconds, the Power LED begins to blink, to set the WX3310 back to its factory-default configuration.

OR

- 3 Click **Maintenance > Restore** and then click **Reset**.

If the WX3310 restarts automatically, wait for the WX3310 to finish restarting, and log in to the Web Configurator. The password is in the device label.

If the WX3310 does not restart automatically, disconnect and reconnect the WX3310. Then, follow the directions above again.

14.5 Wireless Problems

I cannot access the WX3310 or ping any computer from the WLAN.

- 1 Make sure the WX3310 is working in AP or Repeater mode and the wireless LAN is enabled on the WX3310.
- 2 Make sure the wireless adapter on the wireless client is working properly.
- 3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the WX3310.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the WX3310.
- 5 Check that both the WX3310 and your wireless station are using the same wireless and wireless security settings.
- 6 Make sure traffic between the WLAN and the LAN is not blocked by the MAC Address List of the WX3310. See [Section 10.7 on page 59](#).

APPENDIX A

Wireless LANs

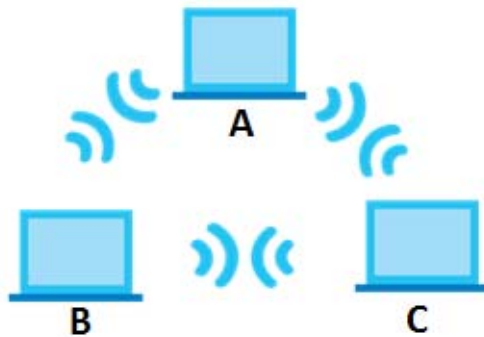
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 57 Peer-to-Peer Communication in an Ad-hoc Network

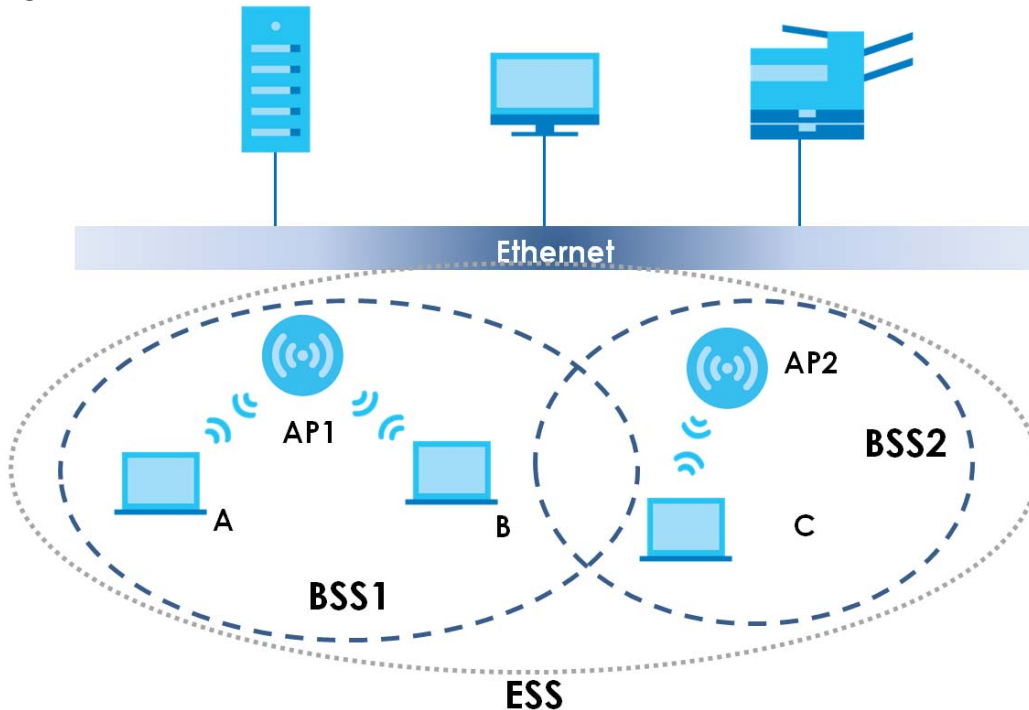


ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 58 Infrastructure WLAN

Channel

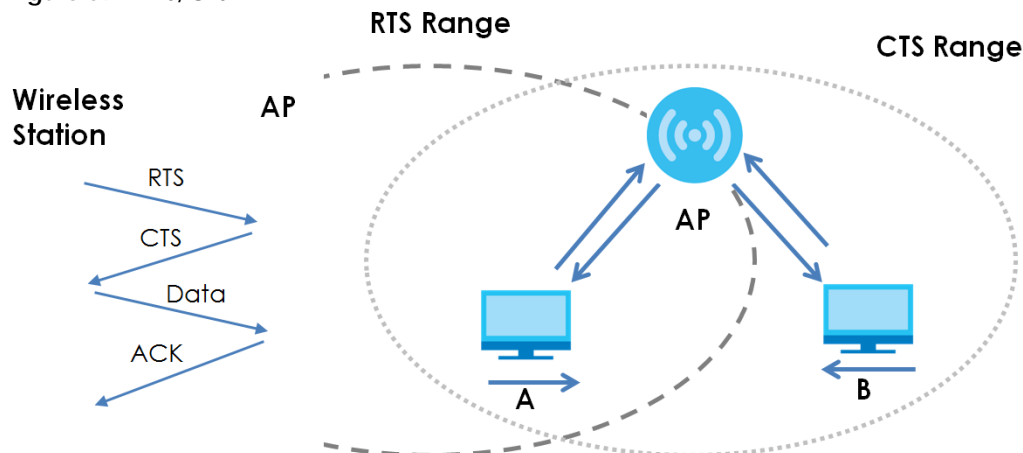
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 59 RTS/CTS



Note: Stations cannot hear each other. They can hear the AP.

When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 29 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the WAP6804 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the WAP6804 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your WAP6804.

Table 30 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the WAP6804 and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.
- Access-Challenge
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
Sent by the access point requesting accounting.

- Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client

authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or re-authentication times out. A new WEP key is generated each time re-authentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 31 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a WiFi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other

WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

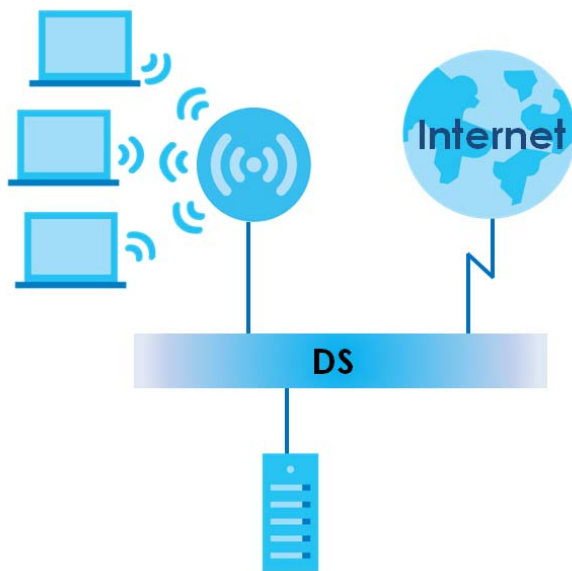
A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

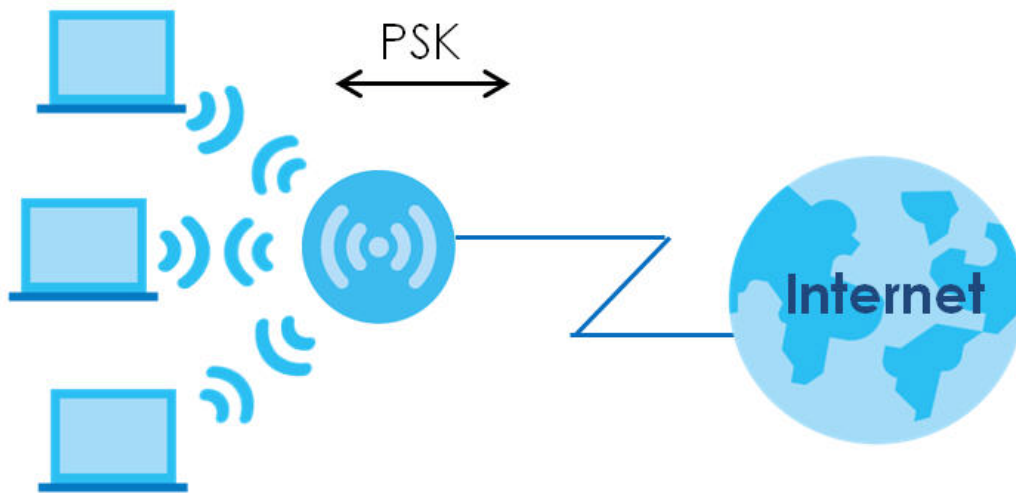
- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 60 WPA(2) with RADIUS Application Example

WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1** First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2** The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3** The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
- 4** The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 61 WPA(2)-PSK Authentication

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz or 5GHz is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

APPENDIX B

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- Zyxel BY
- <http://www.zyxel.by>

Belgium

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

Bulgaria

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- Zyxel Communications A/S
- <http://www.zyxel.dk>

Estonia

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- Zyxel Communications
- <http://www.zyxel.fi>

France

- Zyxel France
- <http://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

Italy

- Zyxel Communications Italy
- <http://www.zyxel.it/>

Latvia

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- Zyxel Benelux
- <http://www.zyxel.nl>

Norway

- Zyxel Communications
- <http://www.zyxel.no>

Poland

- Zyxel Communications Poland
- <http://www.zyxel.pl>

Romania

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

Russia

- Zyxel Russia
- <http://www.zyxel.ru>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

Sweden

- Zyxel Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Ecuador

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

Oceania

Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

APPENDIX C

Legal Information

Copyright

Copyright © 2020 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna
 - Increase the separation between the devices
 - Connect the equipment to an outlet other than the receiver's
 - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for the relevant user's manual mention that this device can be installed into the external environment.
-

CANADA

The following information applies if you use the product within Canada area.

Industry Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Industry Canada RSS-GEN & RSS-247 Statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-WX3310B0) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna Information

	TYPE	MANUFACTURER	GAIN	CONNECTOR
2.4G ANT1+5G ANT1	PIFA	WALSIN	0(2400-2483.5MHz), 0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex
2.4G ANT2+5G ANT2	PIFA	WALSIN	0(2400-2483.5MHz), 0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex
5G ANT3	Dipole	WALSIN	0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex
5G ANT4	Dipole	WALSIN	0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid.

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-WX3310B0) de modèle s'il fait partie du matériel de catégoriel) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Informations Antenne

	TYPE	FABRICANT	GAIN	CONNECTEUR
2.4G ANT1+5G ANT1	PIFA	WALSIN	0(2400-2483.5MHz), 0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex
2.4G ANT2+5G ANT2	PIFA	WALSIN	0(2400-2483.5MHz), 0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex
5G ANT3	Dipole	WALSIN	0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex
5G ANT4	Dipole	WALSIN	0.5(5150-5250MHz), 1(5250-5350MHz), 1.5(5470-5725MHz), 1.75(5725-5850MHz)	i-pex

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 23 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 23 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of xx cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
 - The band 2,400 to 2,483.5 MHz is xxx mW,
 - The bands 5,150 MHz to 5,350 MHz is xxx mW,
 - The 5,470 MHz to 5,725 MHz is xxx mW.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. National Restrictions <ul style="list-style-type: none"> The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízený je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. National Restrictions <ul style="list-style-type: none"> In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΙΑ Ζyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.

Italiano (Italian)	<p>Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details. Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	<p>Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. 2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoją, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/EU.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/EU.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

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

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

(Wireless setting, please refer to "Wireless" chapter for more detail.)

European Union - Disposal and Recycling Information

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

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

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

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

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

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



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

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

以下訊息僅適用於產品操作於 5.25-5.35 兆赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 兆赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

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

安全警告 - 為了您的安全，請先閱讀以下警告及指示：





- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。

- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

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

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

A

Advanced Encryption Standard
See AES.

AES [98](#)

antenna

directional [102](#)
gain [101](#)
omni-directional [102](#)

AP

automatic selection [41](#)
configuring [41](#), [42](#)
connection [41](#)
manual selection [42](#)

AP (access point) [92](#)

AP Mode

menu [34](#)
overview [24](#)
status screen [32](#), [37](#)

B

backup configuration [85](#)

C

CA [96](#)

Certificate Authority
See CA.

certifications [113](#)
viewing [115](#)

channel [55](#), [92](#)
interference [92](#)

configuration

backup [85](#)
reset factory defaults [86](#)
restore [85](#)

connection

AP [41](#)

contact information [103](#)

copyright [109](#)

CTS (Clear to Send) [93](#)

customer support [103](#)

D

Daylight saving [82](#)

disclaimer [109](#)

dynamic WEP key exchange [97](#)

E

EAP Authentication [96](#)

encryption [98](#)

ESS [91](#)

Extended Service Set, See ESS [91](#)

F

factory defaults

restore [85](#)

filters

MAC address [63](#)

firmware upgrade

screen [83](#)

firmware upload [83](#)

file extension

using HTTP

firmware version [33](#), [38](#)

fragmentation threshold [93](#)

G

General wireless LAN screen [56](#)

H

hidden node [92](#)

I

IBSS [91](#)

IEEE 802.11g [94](#)

Independent Basic Service Set
See IBSS [91](#)

initialization vector (IV) [98](#)

Internet
connection [41](#)

IP Address [53](#)

L

LAN [51](#)

LAN overview [51](#)

LAN setup [51](#)

language [86](#)

Local Area Network [51](#)

Log [45](#)

M

MAC [59](#)

MAC address
filter [63](#)

MAC address filtering [59](#)

MAC filter [59](#)

MAC OS X [21](#)

managing the device
good habits [11](#)

Media access control [59](#)

Message Integrity Check (MIC) [98](#)

Microsoft Windows [19](#)

N

Navigation Panel [34, 39](#)

navigation panel [34, 39](#)

O

operation mode
access point [24](#)
client [31](#)
router [24](#)
universal repeater [24](#)

P

Pairwise Master Key (PMK) [98, 100](#)

PIN
configuration [66, 68](#)

PSK [98](#)

push button
configuration [67](#)

Q

Quality of Service (QoS) [58](#)

R

RADIUS [95](#)
message types [95](#)
messages [95](#)
shared secret key [96](#)

Reset button [15](#)

Reset the device [15](#)

restore configuration [85](#)

Roaming [57](#)

RTS (Request To Send) [93](#)
threshold [92, 93](#)

S

- security
 - PBC [67](#)
 - PIN [66, 68](#)
- Service Set [56](#)
- Service Set IDentity. See SSID.
- SSID [33, 38, 55](#)
- Subnet Mask [53](#)
- system [81](#)
- system password
 - screen [81](#)

T

- Temporal Key Integrity Protocol (TKIP) [98](#)
- Time setting [82](#)

W

- warranty [115](#)
 - note [115](#)
- Web Configurator
 - how to access [16](#)
 - Overview [16](#)
- Wi-Fi Protected Access [97](#)
- wireless channel [90](#)
- wireless client WPA supplicants [99](#)
- wireless LAN [90](#)
 - MAC address filter [63](#)
- Wireless network
 - basic guidelines [55, 75](#)
 - channel [55](#)
 - example [54](#)
 - overview [54](#)
 - security [55](#)
 - SSID [55](#)
- Wireless security [55](#)
- wireless security [94](#)
 - troubleshooting [90](#)
- WLAN
 - interference [92](#)
 - security parameters [66](#)

- WPA [97](#)
 - key caching [99](#)
 - pre-authentication [99](#)
 - user authentication [98](#)
 - vs WPA-PSK [98](#)
 - wireless client supplicant [99](#)
 - with RADIUS application example [99](#)
- WPA2 [97](#)
 - user authentication [98](#)
 - vs WPA2-PSK [98](#)
 - wireless client supplicant [99](#)
 - with RADIUS application example [99](#)
- WPA2-Pre-Shared Key [98](#)
- WPA2-PSK [98](#)
 - application example [100](#)
- WPA-PSK [98](#)
 - application example [100](#)
- WPS [14](#)
- WPS button [14](#)