

User's Guide

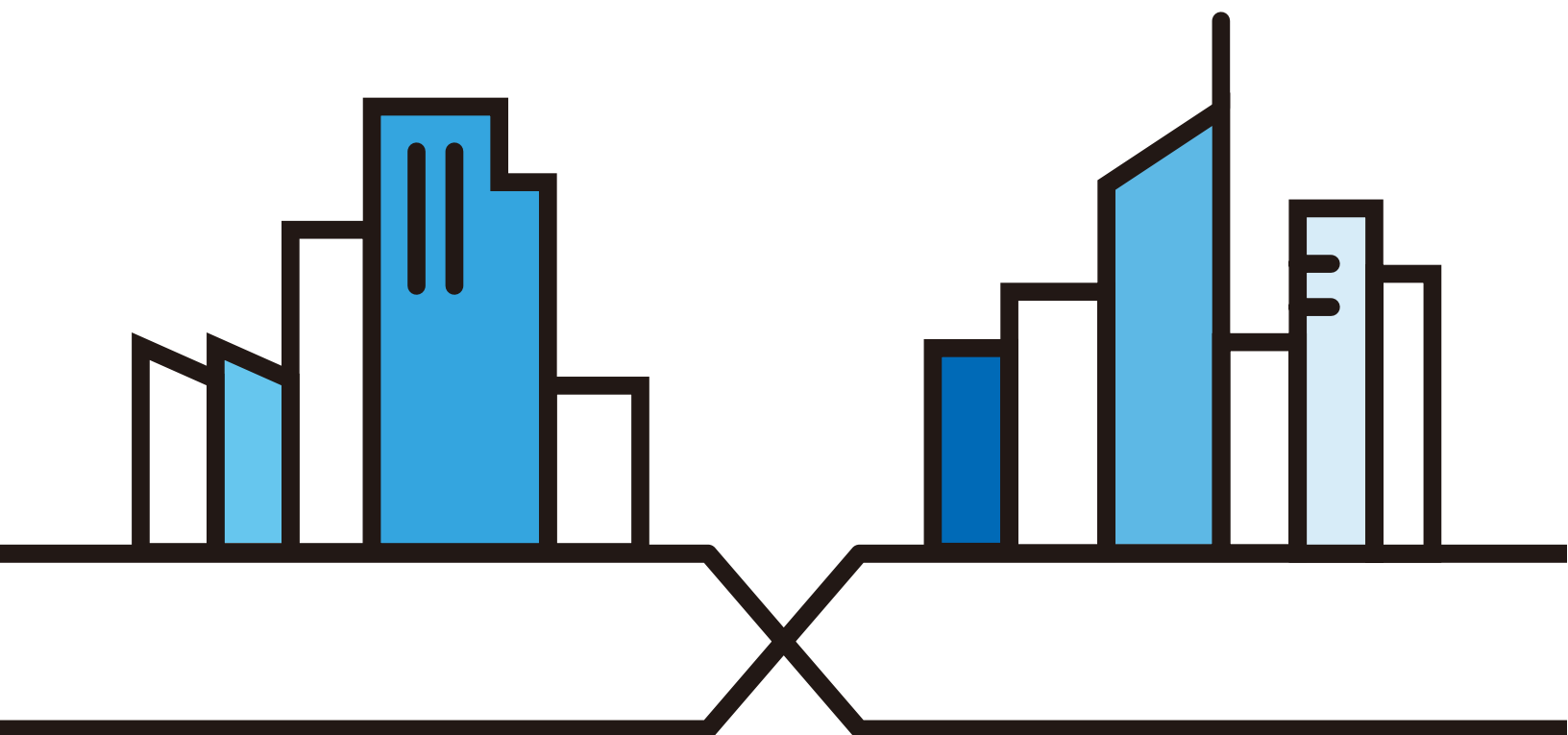
WAP6807

Dual-band AC2100 Gigabit Wireless Extender

Default Login Details

Management IP Address	http://(DHCP-assigned IP) OR http://192.168.1.5
User Name	admin
Password	(See the device label)

Version 1.0 Edition 5, 12/2021



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 WAP6807.

- More Information

Go to **support.zyxel.com** to find other information on the WAP6807.



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

- 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, **Wireless > WiFi Configuration** means you first click **Wireless** in the navigation panel, then the **WiFi Configuration** sub menu to get to that screen.

Icons Used in Figures

Figures in this guide may use the following generic icons. The WAP6807 icon is not an exact representation of your device.

WAP6807 	Router 	Switch 	Internet 
Server 	Desktop 	Laptop 	

Contents Overview

User's Guide9

 Introduction 10

 Hardware 17

 App Tutorials 23

 Web Tutorials 38

 Web Configurator 47

Technical Reference56

 Status 57

 System 60

 Wireless LAN 65

 Troubleshooting 86

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 How to Set Up the WAP6807	10
1.3 MPro Mesh	11
1.3.1 AP Steering and Band Steering	11
1.3.2 Network Controller	13
1.4 Dual-Band WiFi	14
1.5 Setting Up Multiple Wireless Groups	15
1.6 Daisy Chain	15
 Chapter 2	
Hardware	17
2.1 Front Panel and LEDs	17
2.2 Rear Panel	18
2.3 Wall Mounting	18
2.4 WPS Button	20
2.4.1 Using the WPS Button	20
2.5 RESET Button	22
2.5.1 Using the RESET Button	22
 Chapter 3	
App Tutorials.....	23
3.1 Overview	23
3.2 What You Can Do	23
3.3 MPro Mesh Network	23
3.4 General WiFi Settings	24
3.5 Locations of Devices	25
3.6 MPro Mesh Network Setup	26
3.6.1 Setting up an MPro Mesh Router and a WAP6807 with a WiFi Connection	27

3.6.2 Setting up a non-MPro Mesh Router and a WAP6807 with a Wired Connection	28
3.7 Network Management with the MPro Mesh App	30
3.7.1 Home Screen	30
3.7.2 Devices Screen	31
3.7.3 WiFi Screen	33
3.7.4 Account Screen	37
Chapter 4	
Web Tutorials	38
4.1 Overview	38
4.2 WiFi Network Setup	38
4.2.1 Setting Up a WiFi Network	38
4.2.2 Connecting to the WAP6807's WiFi Network Using WPS	39
4.2.3 Without WPS	42
4.2.4 Setting Up a Guest WiFi Network	42
4.3 Device Maintenance	44
4.3.1 Backing Up the Device Configuration	44
4.3.2 Restoring the Device Configuration	44
4.3.3 Upgrading the Firmware	45
Chapter 5	
Web Configurator.....	47
5.1 Overview	47
5.1.1 What You Can Do in this Chapter	47
5.2 Accessing the Web Configurator	47
5.2.1 Status Overview Screen (AP Mode)	48
5.2.2 Status Overview Screen (Repeater Mode)	49
5.3 Navigation Panel	50
5.4 Preparing Your Computer to Access the Web Configurator	51
5.4.1 Static IP Configuration in Microsoft Windows	51
5.4.2 Static IP Configuration in MAC OS X	53
Part II: Technical Reference.....	56
Chapter 6	
Status.....	57
6.1 Overview	57
6.2 What You Can Do	57
6.3 Overview Screen	57
6.4 System Log Screen	58

Chapter 7	
System.....	60
7.1 Overview	60
7.2 What You Can Do in this Chapter	60
7.3 Time Screen	60
7.4 Password Screen	61
7.5 Restore/ Firmware Upgrade Screen	61
7.5.1 Restore	62
7.5.2 Firmware Upgrade	63
7.6 Restart Screen	64
 Chapter 8	
Wireless LAN	65
8.1 Overview	65
8.2 What You Can Do in this Chapter	66
8.3 What You Should Know	66
8.3.1 Wireless Basic	66
8.4 WiFi Configuration Screen	66
8.5 2.4G/ 5G Interface Configuration	68
8.5.1 Basic Screen	68
8.5.2 Advanced Screen	69
8.6 2.4G/ 5G Main WiFi Configuration	71
8.6.1 Basic Screen	71
8.7 WPS Screen	73
8.8 Stations Screen	74
8.9 One SSID Screen	75
8.10 Technical Reference	75
8.10.1 Wireless Network Overview	75
8.10.2 Wireless Security Overview	76
8.10.3 WiFi Protected Setup (WPS)	78
8.10.4 MPro Mesh Overview	84
 Chapter 9	
Troubleshooting.....	86
9.1 Power, Hardware Connections, and LEDs	86
9.2 WAP6807 Web Configurator Access and Login	87
9.3 Internet Access	88
9.4 Resetting the WAP6807 to its Factory Defaults	89
9.5 WiFi Problems	89
9.6 MPro Mesh Problems	90
9.7 MPro Mesh App Problems	90
9.8 Daisy Chain Problems	90

Appendix A Wireless LANs	92
Appendix B Customer Support	103
Appendix C Legal Information	109
Index	115

PART I

User's Guide

CHAPTER 1

Introduction

1.1 Overview

The WAP6807 is a dual-band wireless extender that can extend WiFi coverage from a router/modem with Internet access. The WAP6807 supports MPro Mesh that lets a controller manage your WiFi network.

Use any of the following methods to manage the WAP6807.

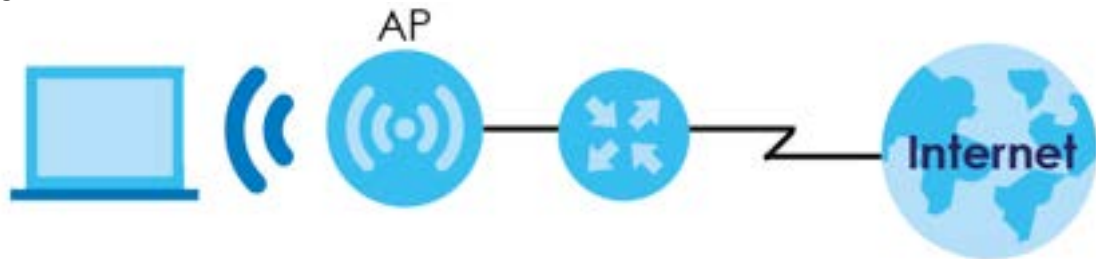
- Web Configurator. This is the simplest way to manage the WAP6807.
- MPro Mesh App. Download the MPro Mesh app from Google Play or Apple Store to manage the WAP6807.

1.2 How to Set Up the WAP6807

The WAP6807 can function as a Repeater or an Access Point (AP).

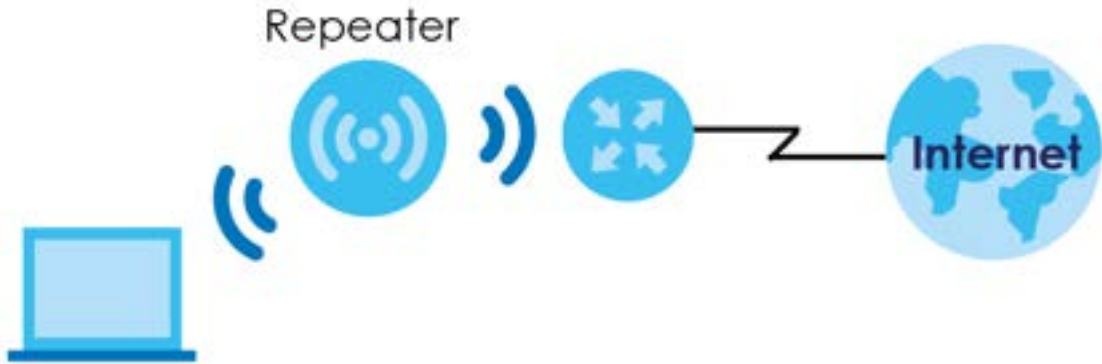
Set your WAP6807 as an **AP** if you already have a router in your network and you want to bridge a wired network (LAN) and another LAN or wireless LAN (WLAN) in the same subnet. If the WAP6807 has a wired uplink connection, it is in AP mode.

Figure 1 Device Operation Mode Example: AP Mode



In **Figure 1**, the WAP6807 that is acting as an **AP** is bridging a wired network and a wired LAN in the same subnet.

Set your WAP6807 as a **Repeater** if you want to connect an existing wireless network through another Access Point and also provide network connection to wireless clients. In this mode, the WAP6807 can be an access point and a wireless client at the same time. If the WAP6807 has a wireless uplink connection, it is in RP mode.

Figure 2 Device Operation Mode Example: Repeater Mode

In **Figure 2**, the WAP6807 that is acting as a **Repeater** is letting a wireless client connect to the network wirelessly through a router. This helps you expand wireless coverage when you have an access point or wireless router already in your network.

Set up a Mesh network with your WAP6807 to enjoy band steering, AP steering, auto-configuration and other advances for your wireless network, see [Section 1.3 on page 11](#) for more information.

The WAP6807 can use both 2.4 GHz and 5 GHz networks at the same time. See [Section 1.4 on page 14](#) for more information on dual-band WiFi.

You can add more WAP6807s to your network to form a daisy chain, see [Section 1.6 on page 15](#) for more information.

Manage the WAP6807 and your WiFi network using the MPro Mesh app. You can check your WiFi network status, change passwords or set up guest WiFi access with QR code, see [Chapter 4 on page 38](#) for more information.

1.3 MPro Mesh

A controller can automatically configure WiFi settings on extenders in the network as well as optimize bandwidth usage. The controller optimizes bandwidth usage by directing wireless clients to an extender (AP steering) or 2.4G/ 5G band (band steering) that is less busy.

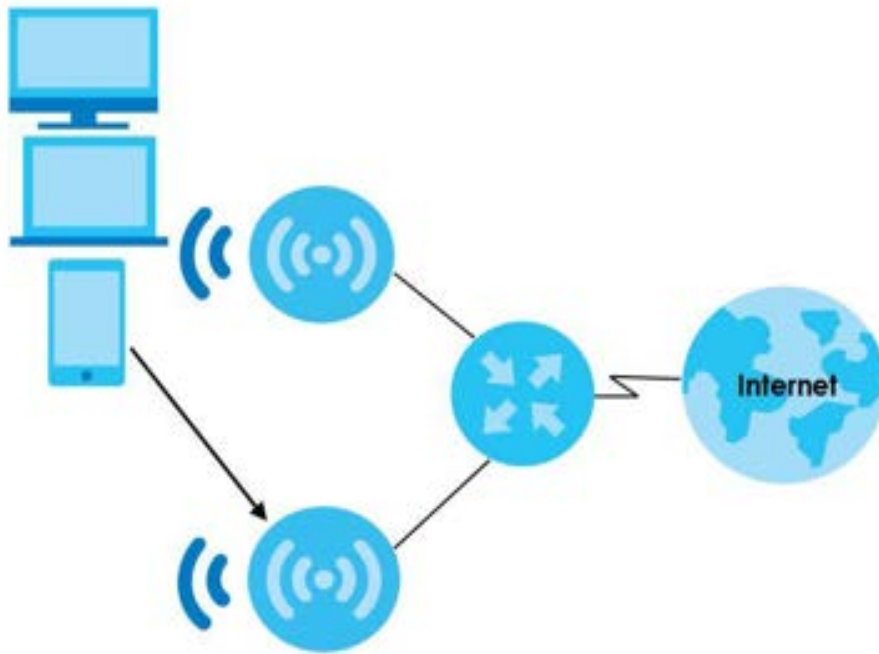
- If the router/ modem is an MPro Mesh router/ modem, then the router/ modem is the controller.
- If the router/ modem is not an MPro Mesh router/ modem, then the WAP6807 is the controller.

1.3.1 AP Steering and Band Steering

Zyxel MPro Mesh supports AP steering and Band steering.

AP 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 WAP6807 bandwidth when the clients are idle or have a low signal. When a wireless client is dropped, it has the opportunity to reconnect to a Mesh AP supported device with a strong signal.

Figure 3 AP Steering Application

Band Steering

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

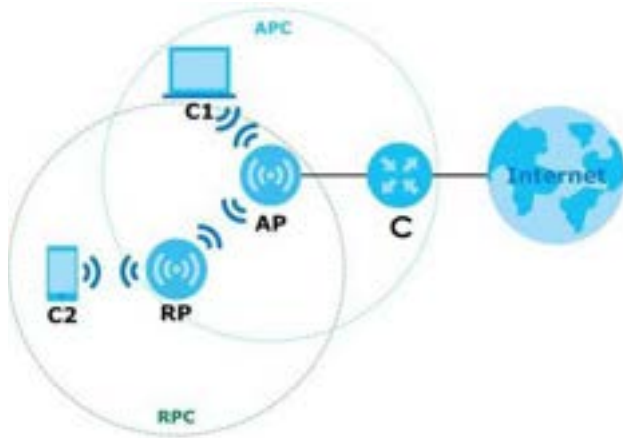
Figure 4 Band Steering Application

1.3.2 Network Controller

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

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

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

Figure 5 Mesh Application

The following table describes the icons used in the figure.

Table 1 Icon Used in Figure 5

ICON	DESCRIPTION
C	router controller (MPro Mesh Router in Scenario 1, see Section 3.6.1 on page 27) or AP controller (the first Extender in Scenario 2, see Section 3.6.2 on page 28)
AP	Access Point
RP	Repeater
C1	Client 1
C2	Client 2
APC	Access Point coverage area
RPC	Repeater coverage area

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

Note: If your router supports Zyxel MPro Mesh, it will serve as the router controller in a Mesh network with the WAP6807.

If your router does not support Zyxel MPro Mesh, your WAP6807 will automatically become the AP controller.

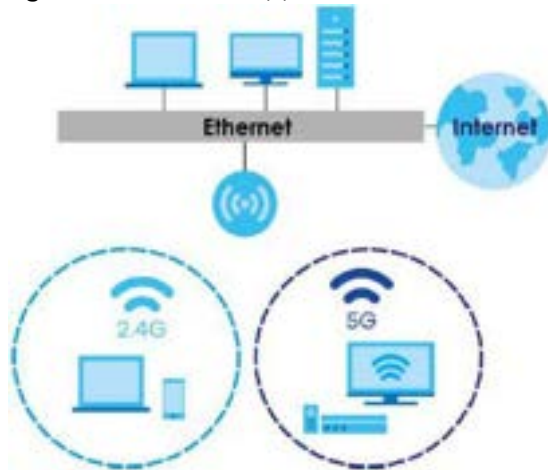
1.4 Dual-Band WiFi

By default, the wireless LAN (WLAN) is enabled on the WAP6807. IEEE 802.11a/b/g/n/ac compliant clients can wirelessly connect to the WAP6807 to access network resources.

The WAP6807 is a dual-band extender that can use both 2.4GHz and 5GHz networks at the same time.

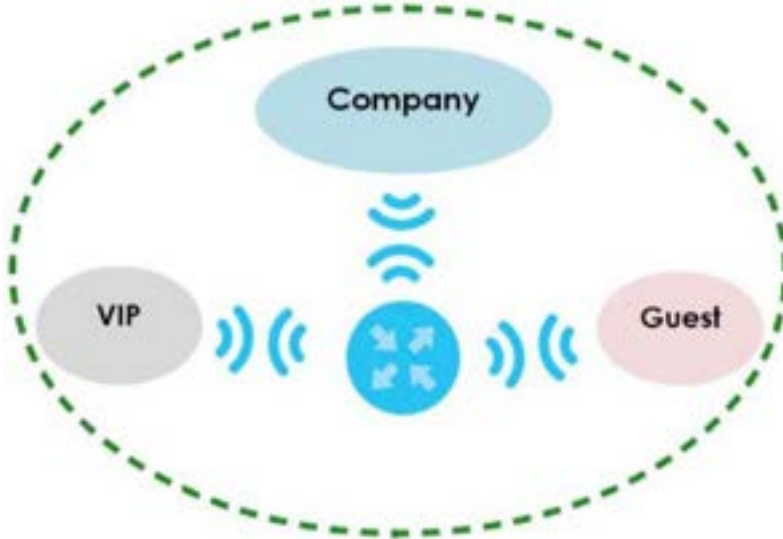
You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

Figure 6 Dual-Band Application



1.5 Setting Up Multiple Wireless Groups

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



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

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

Table 2 WiFi settings for different wireless network group

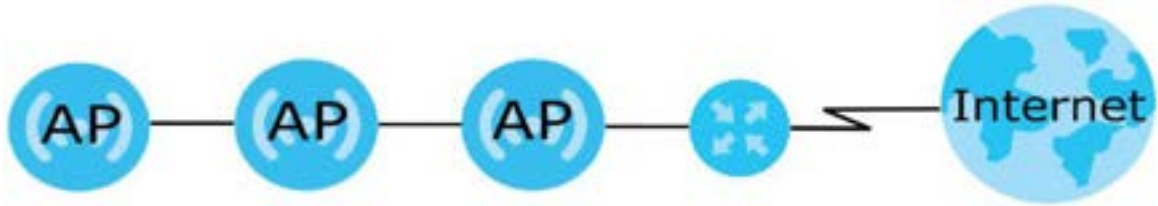
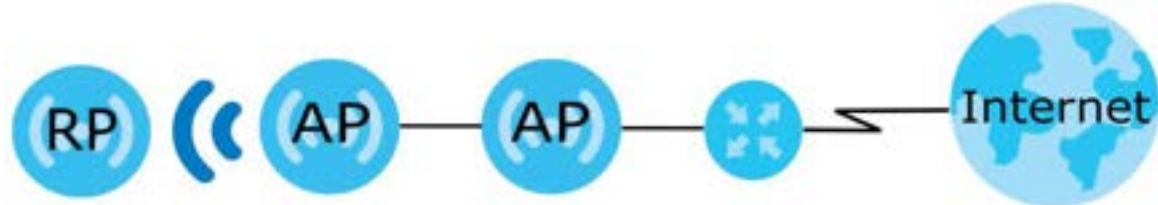
	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK	WPA2-PSK
Pre-Shared Key	ForCompanyOnly	123456789	guest123

1.6 Daisy Chain

You can add more extenders to your network to form a daisy chain. Daisy chain refers to the connection from the first WAP6807 to other WAP6807s to extend the WiFi connection from the router to the client. The WAP6807 uplink connection determines the mode: Access Point or Repeater.

- If the WAP6807 has a wired uplink connection, it is in AP mode.
- If the WAP6807 has a wireless uplink connection, it is in RP mode.

Here are some example scenarios for the WAP6807's daisy chain connection:

Figure 7 Scenario 1: Three APs**Figure 8** Scenario 2: Two APs and one RP**Figure 9** Scenario 3: One AP and two RPs**Figure 10** Scenario 4: Two RPs

Note: Set up your network as in Scenarios 1-3 if your router does not support Zyxel MPro Mesh. Scenario 4 in [Figure 10](#) is only for routers that support Zyxel MPro Mesh.

Note: We do not recommend connecting more than three WAP6807s in your daisy chain network. If you already have two WAP6807s acting as repeaters, we do not recommend adding another WAP6807 as a repeater.

Note: If one of the WAP6807 has a wireless uplink connection, we do not recommend linking the other WAP6807s in your daisy chain network with a wired connection.

Figure 11 Not Recommended Connection Example

CHAPTER 2

Hardware

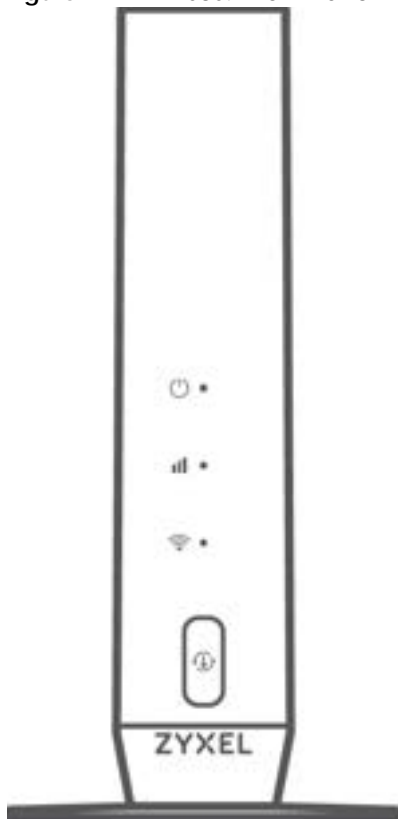
This section describes the front and back panel of the WAP6807. Refer to the Quick Start Guide to see how to make the hardware connections.

2.1 Front Panel and LEDs

The figure below shows the front panel of the WAP6807. Use the LEDs to determine if the WAP6807 is behaving normally or if there are problems on your network.

See [Table 13 on page 27](#) and [Table 15 on page 29](#) for more information on the LEDs.

Figure 12 WAP6807 Front Panel



2.2 Rear Panel

Figure 13 WAP6807 Rear Panel

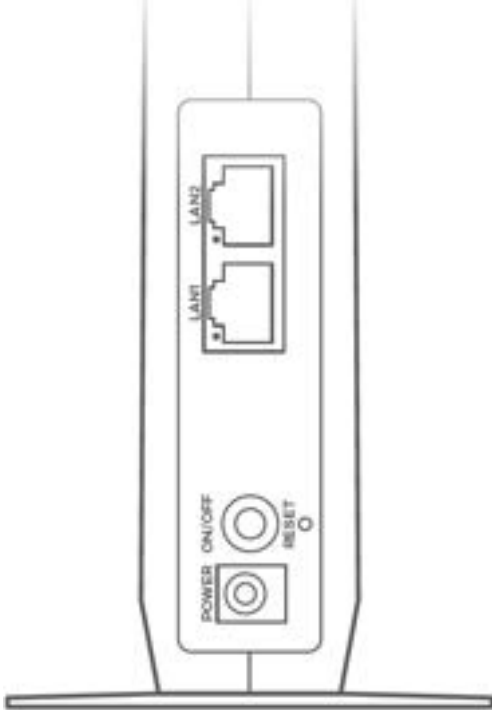


Table 3 Panel Ports and Buttons

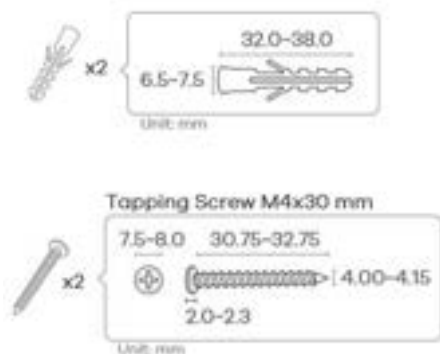
LABEL	DESCRIPTION
WPS	See Section 2.4 on page 20 for more information on WPS button.
LAN1~2	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
ON/OFF	Press the button to turn the WAP6807 on or off.
POWER	Connect the power cable and then can press the power button to start the device.
RESET	Press the button to return the WAP6807 to the factory defaults.

2.3 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

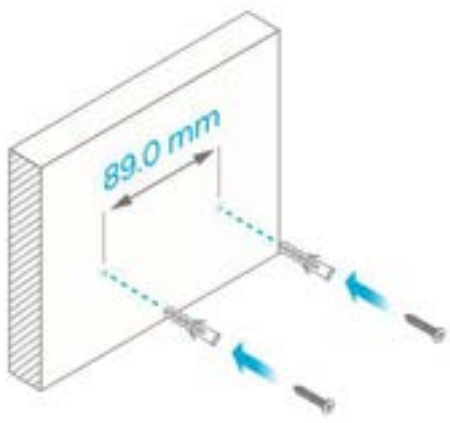
Table 4 Wall Mounting Information

Distance between holes	89.00 mm
M4 Screws	Two
Screw anchors (optional)	Two

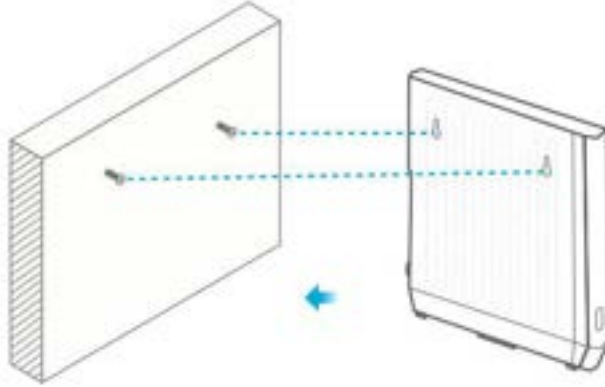
Figure 14 Screw Specifications

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

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

Figure 15 Wall Mounting Distance

- 3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.
If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.
- 4 Make sure the screws are fastened well enough to hold the weight of the WAP6807 with the connection cables.
- 5 Align the holes on the back of the WAP6807 with the screws on the wall. Hang the WAP6807 on the screws.

Figure 16 Wall Mounting Example

2.4 WPS Button

Your WAP6807 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 web configurator. 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 front panel of the WAP6807.

2.4.1 Using the WPS Button

Make sure the power LED is on (not blinking). Then check the mode of your WAP6807, see [Section 1.2 on page 10](#) for more information.

Note: You must activate WPS in the WAP6807 and in another wireless device within two minutes of each other.

Note: With WPS, wireless clients can only connect to the 5 GHz or 2.4 GHz wireless network using the first 5 GHz or 2.4 GHz SSID on the WAP6807 (in AP or repeater mode).

WAP6807e as the Controller

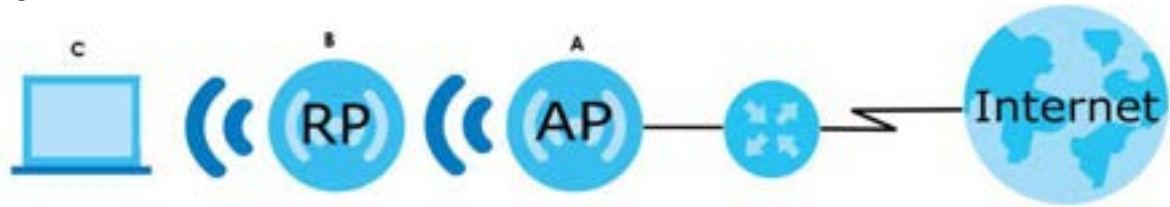
In this scenario, your WAP6807 is the network controller. See [Section 1.3.2 on page 13](#) for more information on network controller.

In the figure below:

- **A** is a WAP6807 in AP mode.
- **B** is a WAP6807 in repeater mode.

- C is a WiFi client connected to B.

Figure 17 WAP6807 as the Controller



Follow the instructions in the table below to copy the WiFi settings using the WPS button from **A** to **B**.

Table 5 WPS Methods

DEVICE	A	B
WPS	Once	Once

Follow the instructions in the table below to copy the WiFi settings using the WPS button from **B** to **C**.

Table 6 WPS Methods

DEVICE	B	C
WPS	Once	Once

Router as the Controller

In this scenario, your Zyxel MPro Mesh is the network controller. See [Section 1.3.2 on page 13](#) for more information on network controller.

In the figure below:

- R is a Zyxel MPro Mesh router.
- A and B are WAP6807s in repeater mode.
- C is a WiFi client connected to B.

Figure 18 MPro Mesh Router as the Controller



Follow the instructions in the table below to copy the WiFi settings using the WPS button from **R** to **A**.

Table 7 WPS Methods

DEVICE	R	A
WPS	Once	Once

Follow the instructions in the table below to copy the WiFi settings using the WPS button from **A** to **B**.

Table 8 WPS Methods

DEVICE	A	B
WPS	Twice	Once

Follow the instructions in the table below to copy the WiFi settings using the WPS button from **B** to **C**.

Table 9 WPS Methods

DEVICE	B	C
WPS	Twice	Once

2.5 RESET Button

If you forget your password or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the WAP6807 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to the default key on the device label.

2.5.1 Using the RESET Button

- 1 Make sure the power LED is on (not blinking).
- 2 Press the **RESET** button for longer than five seconds to set the WAP6807 back to its factory-default configurations.

CHAPTER 3

App Tutorials

3.1 Overview

This shows you how to use the MPro Mesh app to manage the WAP6807 and its MPro Mesh network.

The table below explains the terms used in this chapter:

Table 10 Tutorial Terms Definition

TERM	DEFINITION
MPro Mesh Router	Zyxel routers that support MPro Mesh
Non-MPro Mesh Router	Zyxel routers that don't support MPro Mesh
WAP6807	Zyxel extenders that support MPro Mesh

3.2 What You Can Do

- Set up your WAP6807 with a Zyxel MPro Mesh Router using a WiFi connection; see [Section 3.6.1 on page 27](#).
- Set up your WAP6807 with a non-MPro Mesh Router using a wired connection; see [Section 3.6.2 on page 28](#).
- Use the **Home** screen to reboot your WAP6807 or add WAP6807s to your network; see [Section 3.7.1 on page 30](#).
- Use the **Devices** screen to view the information of WiFi clients connected to the WAP6807; see [Section 3.7.2 on page 31](#).
- Use the **WiFi Settings** screen to configure your main or guest WiFi network; see [Section 3.7.3 on page 33](#).
- Use the **Account** screen to view your app version or logout; see [Section 3.7.4 on page 37](#).

3.3 MPro Mesh Network

The WAP6807 supports MPro Mesh to manage your WiFi network. The WAP6807 can function as a controller to automatically configure WiFi settings on extenders in the network as well as optimize bandwidth usage. See [Section 1.3.2 on page 13](#) for more information on network controller.

The WAP6807 optimizes bandwidth usage by directing WiFi clients to an extender (AP steering) or a 2.4GHz/ 5GHz band (band steering) that is less busy. See [Section 1.3.1 on page 11](#) for more information on AP steering and band steering.

3.4 General WiFi Settings

Change the SSID and key for your general WiFi for better security.

Use the following parameters to change the general WiFi SSID and key.

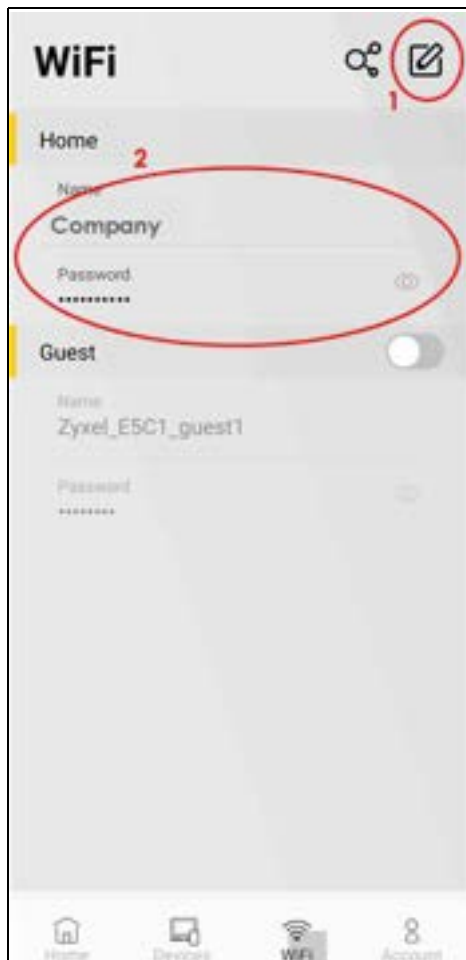
Table 11 WiFi Settings Parameters Example

	GENERAL WIFI
SSID	Company
Password	company123

Setting Up General WiFi

Follow the steps below to change your general WiFi settings.

- 1 Tap on **WiFi** in the navigation panel.
- 2 Tap on the edit icon (✎) to edit the general WiFi network group SSID and password using the parameters given above.



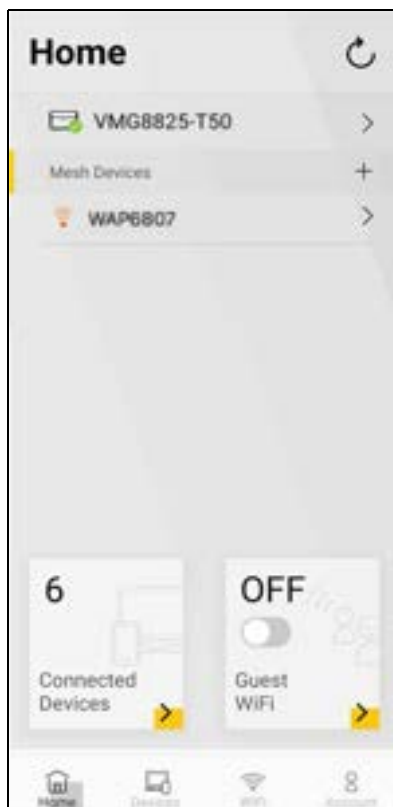
- 3 Tap on the (QR) icon to show the QR code for connecting to the WAP6807 general WiFi. Scan the QR code with your device to connect to the general WiFi network.







3.5 Locations of Devices

Follow the steps below to adjust the locations of your devices in your MPro Mesh network for better WiFi signals.

- 1 Tap on **Home** in the navigation panel.



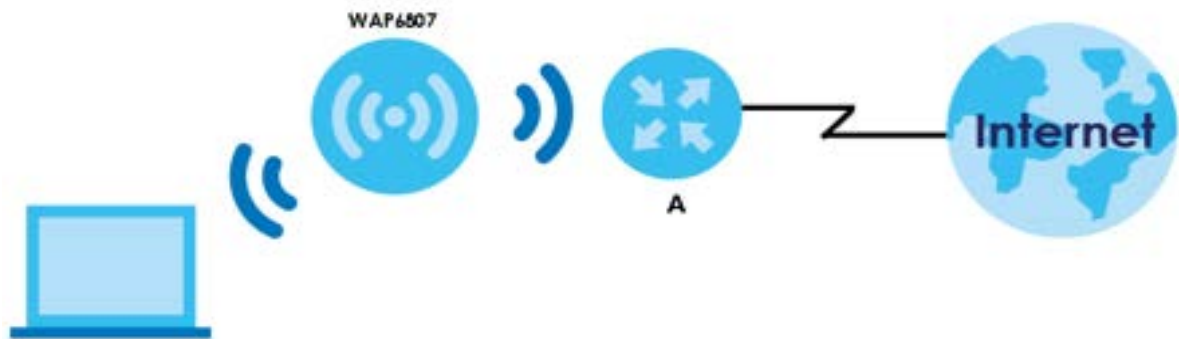
- 2 Look for the device with a red WiFi icon () in front of it. Move the device closer to the router.
- 3 Tap the refresh button at the top right corner () to check the updated status of your devices. The WiFi icons in front of your devices should be green () or amber () if they're placed in appropriate locations.

3.6 MPro Mesh Network Setup

Configure your MPro Mesh router with a WAP6807 using a WiFi connection, see [Section 3.6.1 on page 27](#) for more information.

In the figure below, **A** is a Zyxel router that supports MPro Mesh. The WAP6807 that is acting as a **Repeater** is letting a wireless client connect to the network wirelessly through a router. See [Section 1.2 on page 10](#) for more information on WAP6807 network scenarios.

Figure 19 WAP6807 with a WiFi Connection



Configure your non-MPro Mesh Router with a WAP6807 using a wired connection, see [Section 3.6.2 on page 28](#) for more information.

In the figure below, **A** is a Zyxel router that does not support MPro Mesh. The WAP6807 that is acting as an **AP** is bridging a wired network and a wired LAN in the same subnet. See [Section 1.2 on page 10](#) for more information on WAP6807 network scenarios.

Figure 20 WAP6807 with a Wired Connection



3.6.1 Setting up an MPro Mesh Router and a WAP6807 with a WiFi Connection

Follow the steps below to set up your MPro Mesh Router with the WAP6807.

Table 12 Devices Role

Zyxel Devices	MPro Mesh Router	WAP6807
Role	Internet Access& Mesh Network Controller	Mesh Network Repeater/ AP

- 1 Turn on both devices near each other. Note the power LEDs when you're done. The power LEDs should be steady green.
- 2 Download the app to your smart phone and log into the MPro Mesh Router. You may need to forget your current WiFi connection on your smartphone.



- 3 Change the default SSID and WiFi key on the MPro Mesh Router; see [Section 3.4 on page 24](#) for more information. After applying changes, you will need to reconnect to the MPro Mesh Router again using the new SSID and WiFi key.
- 4 Use WPS to copy the SSID and WiFi key from the MPro Mesh Router to the WAP6807.
- 5 Turn off the WAP6807 and place it where you need to extend WiFi coverage. Use the app to see if the extender is too far from the router; see [Section 3.5 on page 25](#) for more information.

The following table describes the WAP6807 LED behaviors when it is connected to an MPro Mesh router.

Table 13 LED Table (for the WAP6807)




LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Device ready in Repeater mode.
		Blinking	Device booting. Please wait.
	Amber	On	Device ready in AP mode.
		Blinking	Device is joining WiFi network. Please wait.
	Red	On	Device failed to join the WiFi network. Check that the Zyxel MPro Mesh Router is on with WiFi enabled.
	Off		Device is not receiving power. Check the power connection.

Table 13 LED Table (for the WAP6807)

LED	COLOR	STATUS	DESCRIPTION
Link 	Green	On	Steady WiFi connection to the Zyxel MPro Mesh Router.
	Amber	On	Signal is too strong. Suggest to move the WAP6807 away from the Zyxel MPro Mesh Router.
		Blinking	Connecting to the Zyxel MPro Mesh Router. Please wait.
	Red	On	Signal is too weak. Move the WAP6807 closer to the Zyxel MPro Mesh Router.
	Off		Device is not connected to the Zyxel MPro Mesh Router.
WiFi 	Green	On	The 2.4G and 5G wireless radios are ready.
		Blinking (Slow)	WPS process in progress.
		Blinking (Fast)	The WAP6807 is sending/receiving data through the wireless LAN.
		Off	The 2.4G or 5G wireless radio is not ready or has failed.

3.6.2 Setting up a non-MPro Mesh Router and a WAP6807 with a Wired Connection

This scenario describes the process to create an MPro Mesh network with a wired connection from the non-MPro Mesh router to two WAP6807s.

Make sure the non-MPro Mesh router is connected to the Internet. The first WAP6807 must be connected to your router using an Ethernet cable. Then, connect the second WAP6807 wirelessly to the first WAP6807.

Follow the steps below to set up your Non-MPro Mesh Router with the WAP6807.

Table 14 Devices Role




Zyxel Devices	Non-MPro Mesh Router	WAP6807
Role	Internet Access	Mesh Network Controller& Repeater/ AP

- 1 Turn on the router. Note the power LEDs when you're done.
- 2 Connect an Ethernet cable from the router to WAP6807-1. The SSID and key is copied from WAP6807-1 to the router. Place WAP6807-1 where you want WiFi coverage.
- 3 Download the app to your smart phone and log into WAP6807-1 (the MPro Mesh controller) using the default label information on WAP6807-1. You may need to forget your current WiFi connection on your smartphone.



- 4 Change the default SSID and WiFi key on WAP6807-1; see [Section 3.4 on page 24](#) for more information. After applying changes, you will need to reconnect to WAP6807-1 again using the new SSID and WiFi key.
- 5 Use WPS to copy the SSID and WiFi key from WAP6807-1 to WAP6807-2. Press the WPS button in the app and on your WAP6807 within 2 minutes of each other.

Table 15 LED Table (for the second WAP6807)

LED	COLOR	STATUS	DESCRIPTION
POWER 	Green	On	Device ready in Repeater mode.
		Blinking	Device booting. Please wait.
	Amber	On	Device ready in AP mode.
		Blinking	Device is joining WiFi network. Please wait.
	Red	On	Device failed to join the WiFi network. Check that the WAP6807-1 is on with WiFi enabled.
	Off		Device is not receiving power. Check the power connection.
Link 	Green	On	Steady WiFi connection to the WAP6807-1.
	Amber	On	Signal is too strong. Suggest to move the WAP6807-2 away from the WAP6807-1.
		Blinking	Connecting to the WAP6807-1. Please wait.
	Red	On	Signal is too weak. Move the WAP6807-2 closer to the WAP6807-1.
	Off		Device is not connected to the WAP6807-1.
WiFi 	Green	On	The 2.4G and 5G wireless radios are ready.
		Blinking (Slow)	WPS process in progress.
		Blinking (Fast)	The WAP6807 is sending/receiving data through the wireless LAN.
		Off	The 2.4G or 5G wireless radio is not ready or has failed.

3.7 Network Management with the MPro Mesh App


You can manage the Zyxel MPro Mesh controller and its WiFi settings through the MPro Mesh app. The WAP6807 is the network controller in the examples below.

3.7.1 Home Screen

Use this screen to view the navigation panel and the status of your WAP6807.

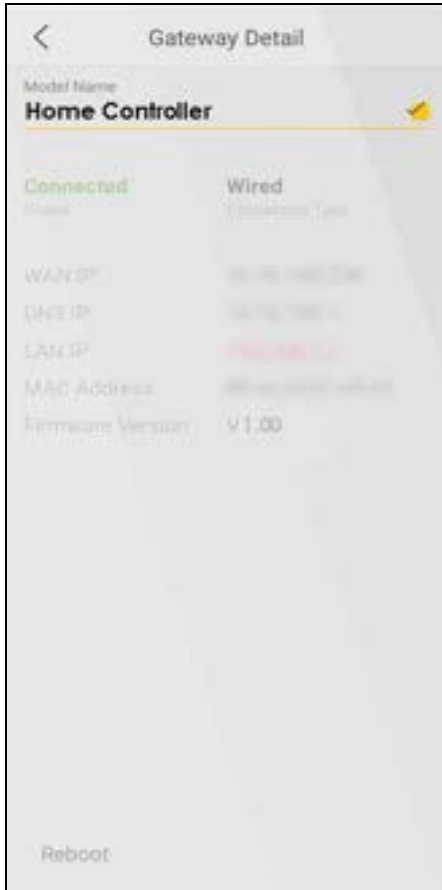
Changing the WAP6807 Name

Follow the steps below to change the name of your WAP6807, which identifies it in your network.

- 1 Tap on the  icon next to the model name to show the **Gateway Detail** screen.



- 2 Tap on the edit icon () to change the model name shown on the app to **Home Router**.





- 3 Tap the  icon to save the changes made.

3.7.2 Devices Screen


Use this screen to view WiFi clients that are connected to the WAP6807 and their link quality.

Stopping a Client from Connecting to Your Network

Follow the steps below to stop a specific client named **Jane's Phone** from connecting to your MPro Mesh network.

- 1 Tap on **Devices** in the navigation panel.
- 2 Tap on the search icon . Type **Jane's Phone** in the field.
- 3 Tap on the  icon to show the **Device Detail** screen.



- 4 Tap the switch in the **Pause Internet** field. When the switch goes to the right (), the function is enabled. The **Jane's Phone** client will not be able to connect to your MPro Mesh network.

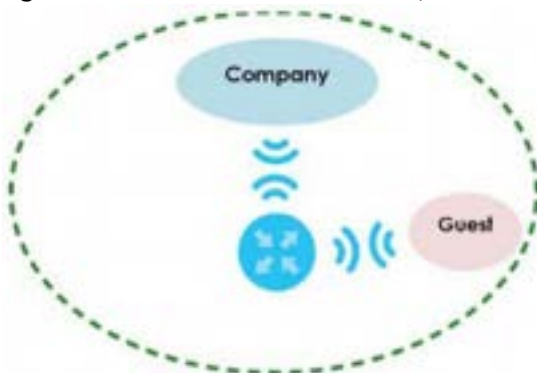


3.7.3 WiFi Screen

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

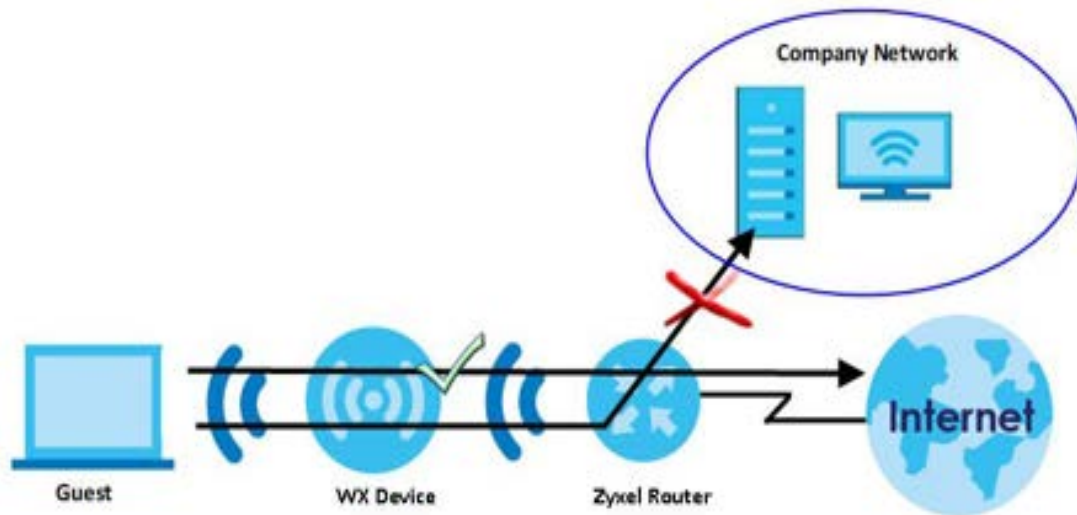
You can set up a guest WiFi network for your WAP6807. Company A wants to create a different WiFi network group for different types of users as shown in the following figure. This group has its own SSID and password.

Figure 21 Guest WiFi Network Example



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

Figure 22 Visiting Guests Blocked from Company Network



For more information on setting up your general WiFi network group, see [Section 3.4 on page 24](#).


Use the following parameters to set up the guest WiFi network group.

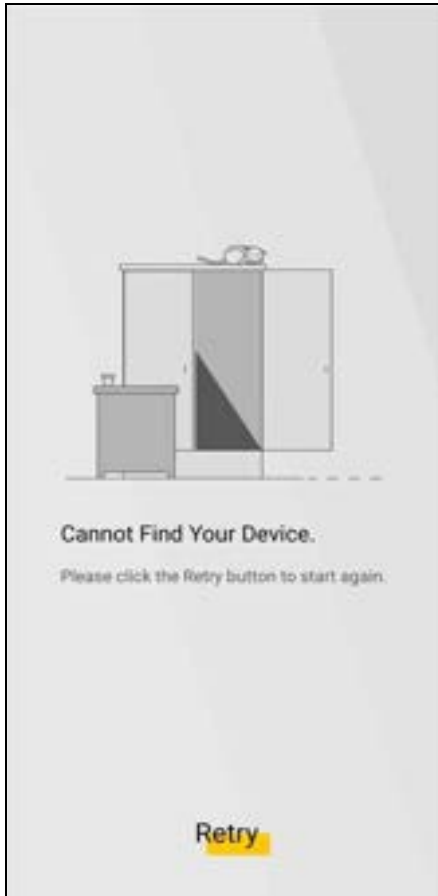
Table 16 WiFi Settings Parameters Example


	GUEST WIFI
SSID	Guest
Password	guest123

Setting Up Guest WiFi

Follow the steps below to set up a guest WiFi network group.

- 1 Tap on **WiFi** in the navigation panel.
- 2 Tap the switch in the **Guest** field. When the switch goes to the right (, guest WiFi is enabled.
- 3 Your phone will disconnect from the WAP6807 WiFi when you enable the guest WiFi. Close the MPro Mesh app.



- 4 Reconnect your phone to the WAP6807 WiFi in your phone WiFi setting screen. Then open the MPro Mesh app.
- 5 Tap on the edit icon () to edit the guest WiFi network group SSID and password using the parameters given above.



- 6 Tap on the (📄) icon to show the QR code.



- 7 Swipe to the left to see the **Share Guest WiFi** QR code for connecting to the WAP6807 guest WiFi. Take a screenshot of the QR code with your phone. Print it out and place it in a place where your guests could scan it to join the guest WiFi network.



3.7.4 Account Screen

Use this screen to:

- Log out of the app.
- View the app version.
- View privacy policy.



CHAPTER 4

Web Tutorials

4.1 Overview

This chapter provides web configurator tutorials for setting up a secure WiFi network for your WAP6807.

- To configure basic settings such as SSID, pre-shared key or authentication mode for your WiFi network, see [Section 4.2.1 on page 38](#).
- To set up a secure WiFi network using the WPS button, see [Section 4.2.2 on page 39](#).
- To set up WiFi groups for different users, see [Section 4.2.4 on page 42](#).
- To backup/restore your configuration file or to upload latest firmware, see [Section 4.3 on page 44](#).

4.2 WiFi Network Setup

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the WAP6807 serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the WAP6807. Then he can set up a wireless network using WPS or manual configuration.

4.2.1 Setting Up a WiFi Network

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

Table 17 Wireless Network Settings Example

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

- 1 Click **Wireless > WiFi configuration** to open the **Wireless Overview** screen. Click on the **Config** button for the 2.4G/5G interface to configure the settings for the main or guest WiFi. Select WPS2PSK as the security mode. Configure the screen using the provided parameters in the table above. Click **Apply**.

Interface Configurations - 2.4G Main

Basic WPS Stations

SSID: Example

Auth Mode: WPA2PSK

Encryption: AES

Key Renewal Interval: 3600 (seconds) (0 - 4194300)

Key: DoNotStealMyWirelessNet

Hidden: No

Apply Reset

- Click **Wireless > WiFi configuration** to open the **Wireless Overview** screen. Click on the **Config** button for the 2.4G/5G interface to configure the settings for the 2.4G/5G interface. Select **B/G/N mode** in the **Mode** field. Click **Apply**.

Device Configurations - 2.4G

Basic Advanced

Mode: B/G/N mode

Channel: Channel 6 (2437 GHz)

Repeater Mode:

Apply Reset

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the WAP6807. He can also use the notebook's wireless client to search for the WAP6807.

4.2.2 Connecting to the WAP6807's WiFi Network Using WPS

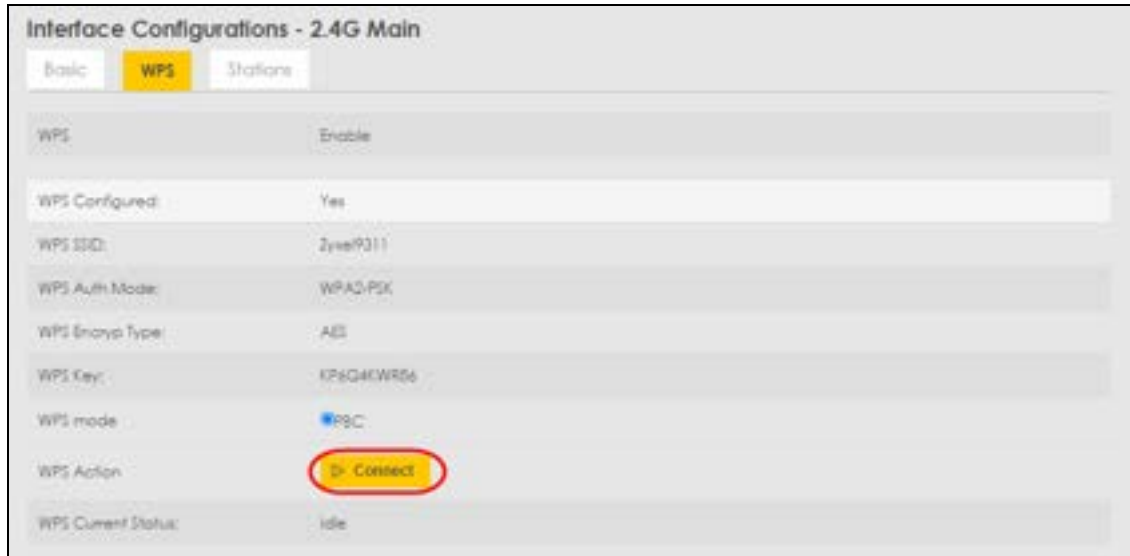
This section shows you how to connect a WiFi device to the WAP6807's WiFi network using WPS. WPS (Wi-Fi Protected Setup) is a security standard that allows devices to connect to a router securely without you having to enter a password.

This tutorial shows you how to use the PBC method to create a secure connection. Push Button Configuration (PBC) creates a secure wireless network simply by pressing a button. This is the easier mode.

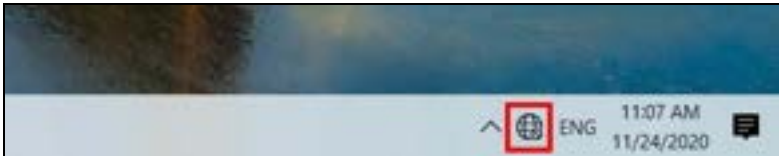
4.2.2.1 WPS Push Button Configuration (PBC)

This example shows how to connect to the WAP6807's WiFi network from a notebook computer running Windows 10.

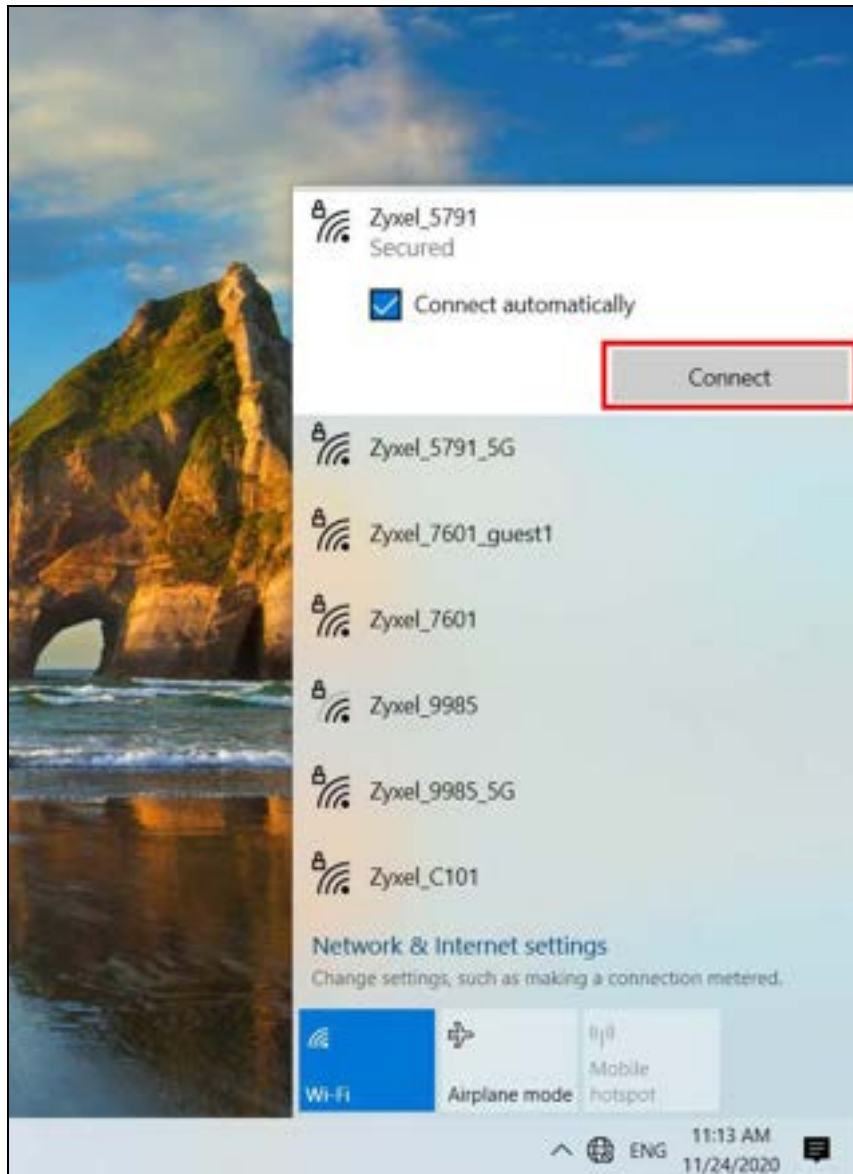
- 1 Make sure that your WAP6807 is turned on, and your notebook is within range of the WAP6807's WiFi signal.
- 2 Push and hold the **WPS** button located on the WAP6807 until the **WiFi** LED starts blinking slowly. Alternatively, log into the WAP6807's Web Configurator, and then go to the **Wireless > WiFi Configuration > Interface Configurations- 2.4G/5G Main > WPS** screen. Click the **Connect** button on the screen.



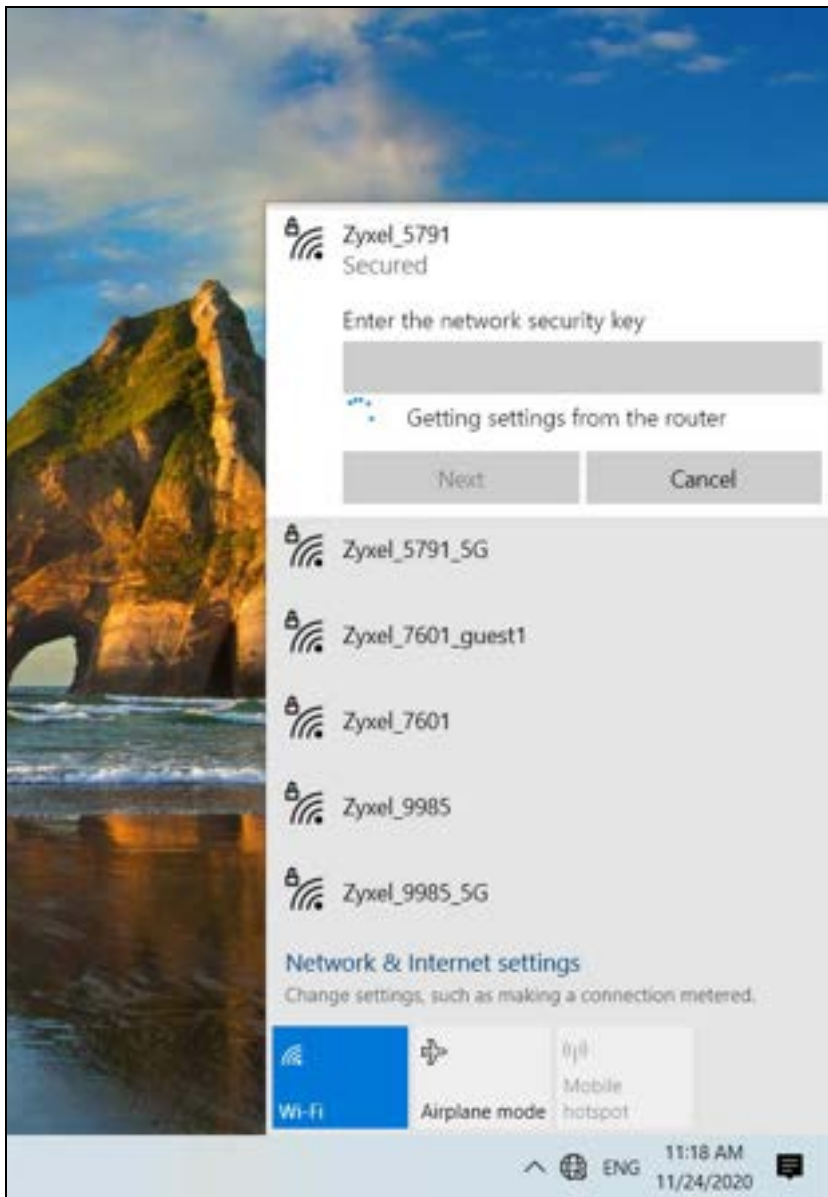
- 3 In Windows 10, click on the Network icon in the system tray to open the list of available WiFi networks.



- 4 Locate the WiFi network of the WAP6807. The default WiFi network name is "ZyxeL_XXXX" (2Ghz) or ZyxeL_XXXX_5G" (5Ghz). Then click **Connect**.



The WAP6807 sends the WiFi network settings to Windows using WPS. Windows displays "Getting settings from the router".



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

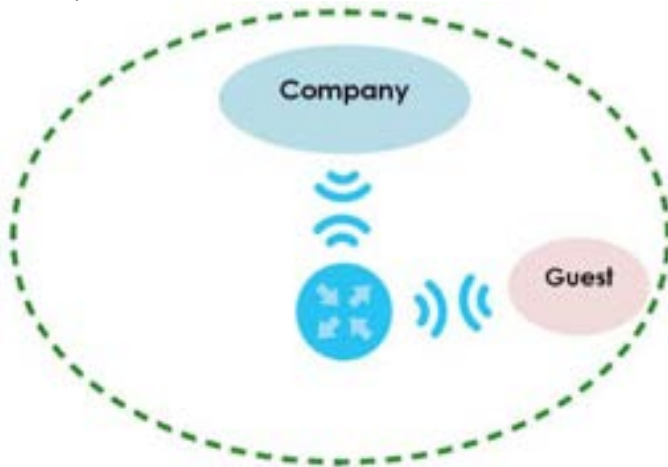
4.2.3 Without WPS

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

4.2.4 Setting Up a Guest WiFi Network

You can set up a guest WiFi network for your WAP6807. Company A wants to create a different WiFi network group for different types of users as shown in the following figure. This group has its own SSID and

security mode.



- Employees in Company A will use a general **Company** WiFi network group. For more information on setting up general WiFi network group, see [Section 4.2.1 on page 38](#).
- Visiting guests will use the **Guest** group, which has a different SSID and password.

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

Table 18 WiFi Settings Parameters Example

	GUEST
SSID	Guest
Security Mode	WPA2-PSK
Pre-Shared Key	guest123

- 1 Click **Wireless> WiFi Configuration> 2.4G interface Guest 1> Config** to open the **Interface Configurations-2.4G Guest 1** screen. Configure the screen using the provided parameters and click **Apply**.

4.3 Device Maintenance

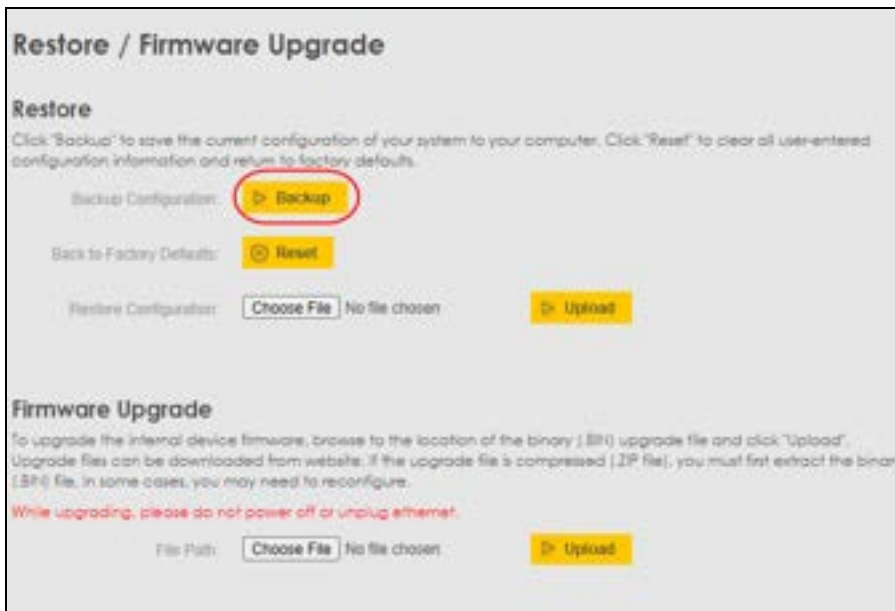
This section shows you how to:

- Backup and restore your configuration file.
- Upgrade firmware when new firmware is released.

4.3.1 Backing Up the Device Configuration

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

- 1 Click **System> Restore/ Firmware Upgrade** to go to the **Restore/ Firmware Upgrade** screen.
- 2 Click **Backup** in the **Restore** section to back up a configuration file.



- 3 The configuration file will be saved to the download file in your computer.

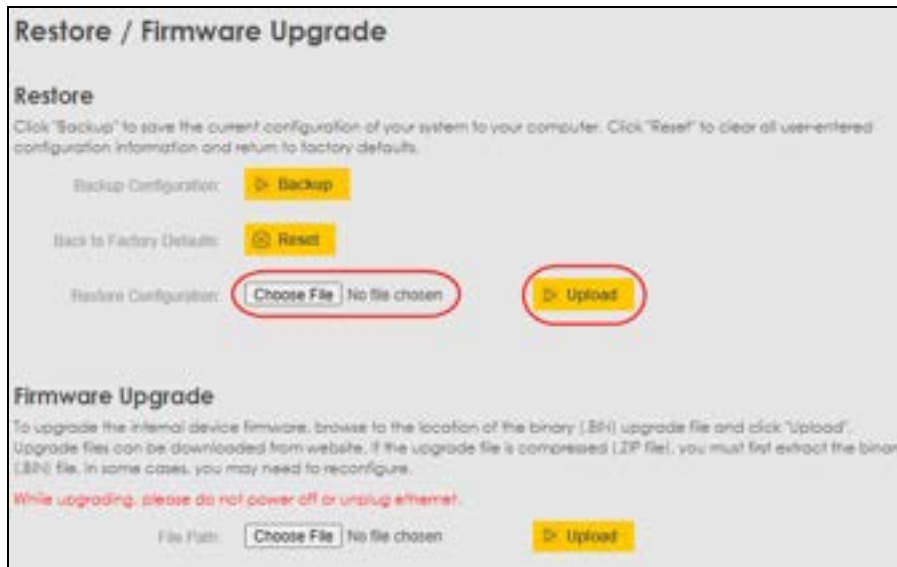


4.3.2 Restoring the Device Configuration

This section shows you how to restore a previously saved configuration from your computer to your WAP6807.

- 1 Click **System> Restore/ Firmware Upgrade** to go to the **Restore/ Firmware Upgrade** screen.

- 2 Click **Choose File** in the **Restore** section. Select the configuration file that you want to upload and click **Upload**.



- 3 The WAP6807 will restart automatically after the configuration file is successfully uploaded. Wait for one minute before logging into the WAP6807.
- 4 Check that your previously saved configuration has been applied in the web configurator.

4.3.3 Upgrading the Firmware

Upload the firmware to the WAP6807 for feature enhancements.

- 1 Download the correct firmware file from the download library at the Zyxel website. The model code for the WAP6807 is ABTB. Note the model code for your device.
- 2 Click **System> Restore/ Firmware Upgrade** to go to the **Restore/ Firmware Upgrade** screen.
- 3 Click **Choose File** and select the .bin file, then click **Upload**.

Restore / Firmware Upgrade

Restore

Click "Backup" to save the current configuration of your system to your computer. Click "Reset" to clear all user-entered configuration information and return to factory defaults.

Backup Configuration:

Back to Factory Defaults:

Restore Configuration: No file chosen

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

- 4 The power LED will start blinking in green, wait for it to turn steady green. This process may take a few minutes to finish. When the process is done, you will be redirected to the log in page. Log in to check your new firmware version in the **Status** screen.

CHAPTER 5

Web Configurator

5.1 Overview

This chapter describes how to access the WAP6807 Web Configurator and provides an overview of its screens.

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

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

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

5.1.1 What You Can Do in this Chapter

- Use the **Status** screen to view read-only information about your WAP6807 in AP mode or Repeater mode.
See [Section 5.2.1 on page 48](#) for more information on **AP** mode **Status** screen.
See [Section 5.2.2 on page 49](#) for more information on **Repeater** mode **Status** screen.
- Use the **Navigation Panel** to configure WAP6807 features in AP mode and Repeater mode, see [Section 5.3 on page 50](#)
- To change your computer's IP address in Windows 7 operating system, see [Section 5.4.1 on page 51](#).
- To change your computer's IP address in MAC OS X 10.11 operating system, see [Section 5.4.2 on page 53](#).

5.2 Accessing the Web Configurator

- 1 Connect your WAP6807 to a modem/router using wired or wireless connection (see [Section 1.4 on page 14](#)).
- 2 Make sure your modem/router hardware is properly connected.
- 3 Make sure your modem/router has an Internet connection.
- 4 Connect your computer to the LAN port of your modem/router.
- 5 Launch your web browser.

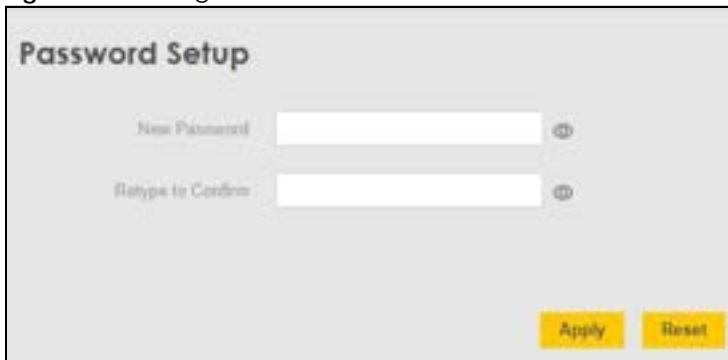
- 6 Enter the modem/router's default static IP address. Check the IP address the modem/router has assigned to you WAP6807 in its web configurator.
- 7 Enter "http:// (DHCP-assigned IP)" as the WAP6807 web address in your web browser.
- 8 Type the **Username** and **Password** on the device label (default) and click **Login**.

Figure 23 Login Screen

The image shows the WAP6807 login screen. At the top, it says "WAP6807" in bold. Below that, a welcome message reads: "Welcome to the router configuration interface. Enter the username & password and click 'Login'." There are two input fields: "Username" with the text "admin" entered, and "Password" which is empty. A yellow button with a right-pointing arrow and the text "Login" is at the bottom left.

- 9 You should see a screen asking you to change your password as shown next. Enter a new password. Click **Apply** to save your changes. Click **Reset** if you want to erase the password you entered.

Figure 24 Change Password Screen

The image shows the "Password Setup" screen. It has two input fields: "New Password" and "Retype to Confirm". Each field has a small circular icon to its right. At the bottom right, there are two yellow buttons: "Apply" and "Reset".

Right after you log in, the **Status** screen is displayed.

5.2.1 Status Overview Screen (AP Mode)

The screen below shows the status screen in **AP** mode.

Figure 25 Status Screen (AP Mode)



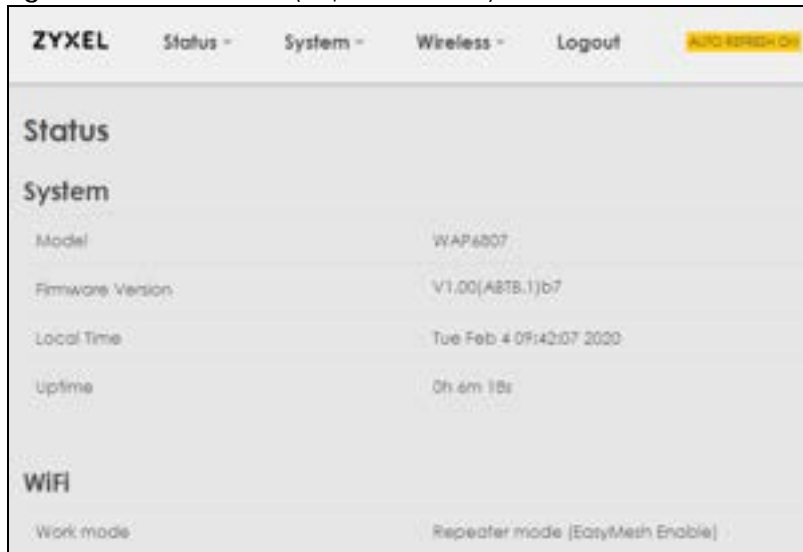
The following table describes the labels shown in the **Status** screen.

Table 19 Status Screen (AP Mode)

LABEL	DESCRIPTION
System	
Model	This is the WAP6807's model name.
Firmware Version	This is the firmware version and the date created.
Local Time	This field displays your WAP6807's present date and time.
Uptime	This is the total time the WAP6807 has been on.
WiFi	
Work Mode	This is the device mode (Section 1.4 on page 14) to which the WAP6807 is set - AP mode .

5.2.2 Status Overview Screen (Repeater Mode)

The screen below shows the status screen in **Repeater** mode.

Figure 26 Status Screen (Repeater Mode)

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

Table 20 Status Screen (Repeater Mode)

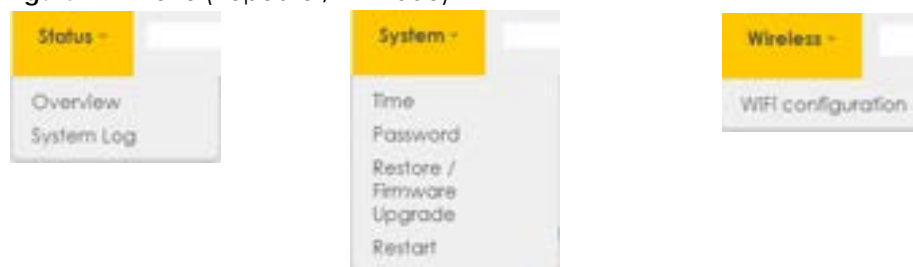
LABEL	DESCRIPTION
System	
Model	This is the WAP6807's model name.
Firmware Version	This is the firmware version and the date created.
Local Time	This field displays your WAP6807's present date and time.
Uptime	This is the total time the WAP6807 has been on.
WiFi	
Work Mode	This is the device mode (Section 1.4 on page 14) to which the WAP6807 is set - Repeater Mode .

5.3 Navigation Panel

Use the menu in the navigation panel to configure WAP6807 features in **Repeater Mode** and **AP Mode**.

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

See [Section 5.1 on page 47](#) for more information on different modes.

Figure 27 Menu (Repeater/AP Mode)

The following table describes the sub-menus.

Table 21 Navigation Panel (Repeater/AP Mode)

LINK	TAB	FUNCTION
Status		
Overview	Overview	Use this screen to view the WAP6807's basic information, such as firmware version or work mode.
System Log	System Log	Use this screen to view the status of events that occurred to the WAP6807.
System		
Time	Time	Use this screen to change the WAP6807's time and date.
Password	Password	Use this screen to change user password on the WAP6807.
Restore / Firmware Upgrade	Restore / Firmware Upgrade	Use this screen to backup and restore the WAP6807's configuration (settings) or reset the factory default settings. Use this screen to upload firmware to the WAP6807.
Restart	Restart	Use this screen to restart the WAP6807 without turning the power off.
Wireless		
WiFi Configuration	WiFi Configuration	Use this screen to configure the WiFi settings and WLAN authentication/ security settings.


5.4 Preparing Your Computer to Access the Web Configurator

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

Your computer needs to be in the same subnet as the WAP6807 in order to access the Web Configurator. Below you will find the steps to set a static IP on both Windows 7 ([Section 5.4.1 on page 51](#)) and MAC OS X 10.11 ([Section 5.4.2 on page 53](#)) operating systems.

5.4.1 Static IP Configuration in Microsoft Windows

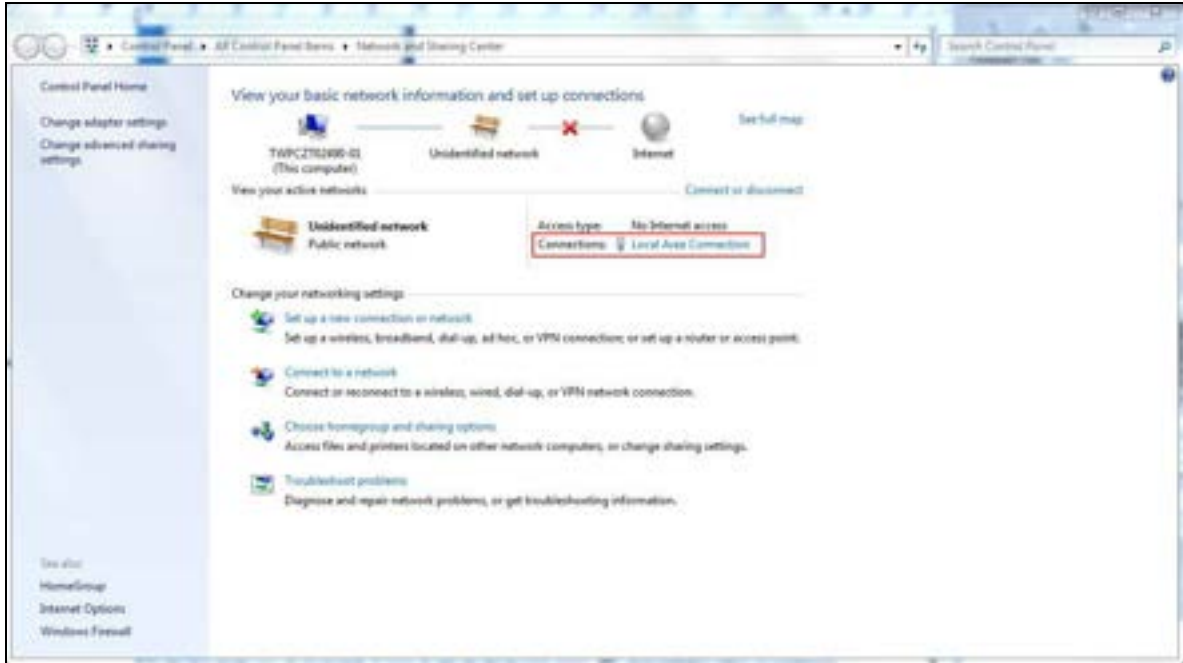
Follow these steps to change your computer's IP address in Windows 7 operating system.

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

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

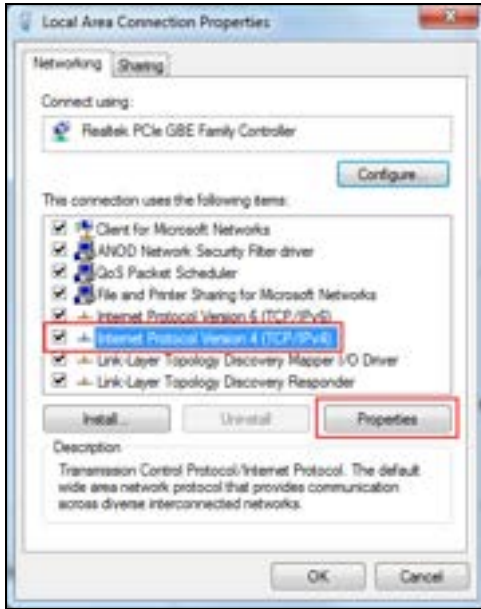


- 3 After accessing the connection's general settings, click the **Properties** button.



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

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



- 5 In the **Internet Protocol Version 4 (TCP/IPv4)** properties, click **Use the following IP address** radio button and enter the 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 (except 192.168.1.5). 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 Properties** window.



Note: After you have configured your WAP6807, 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**.

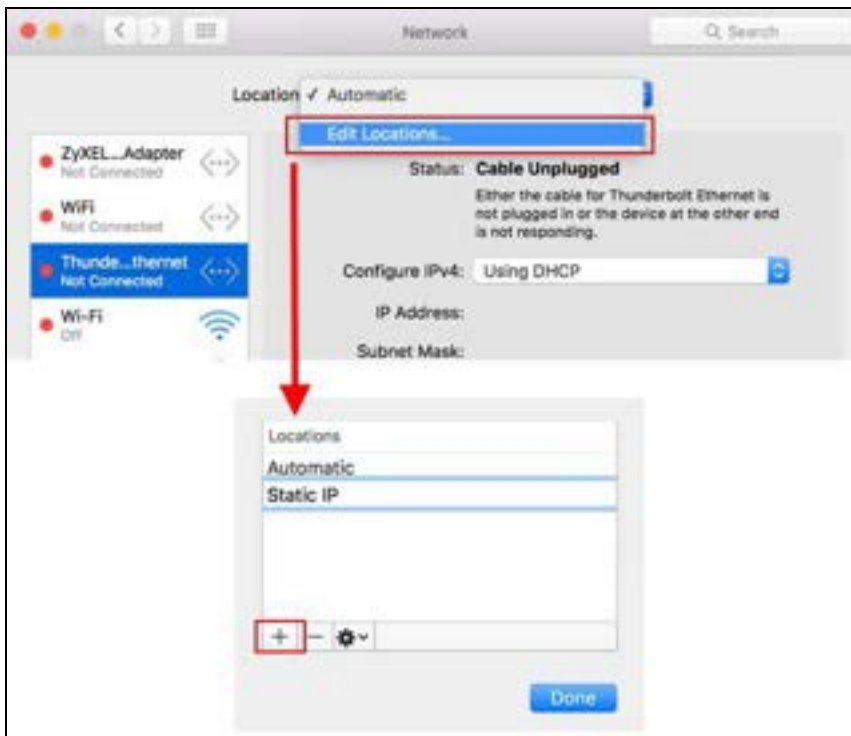
5.4.2 Static IP Configuration in MAC OS X

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

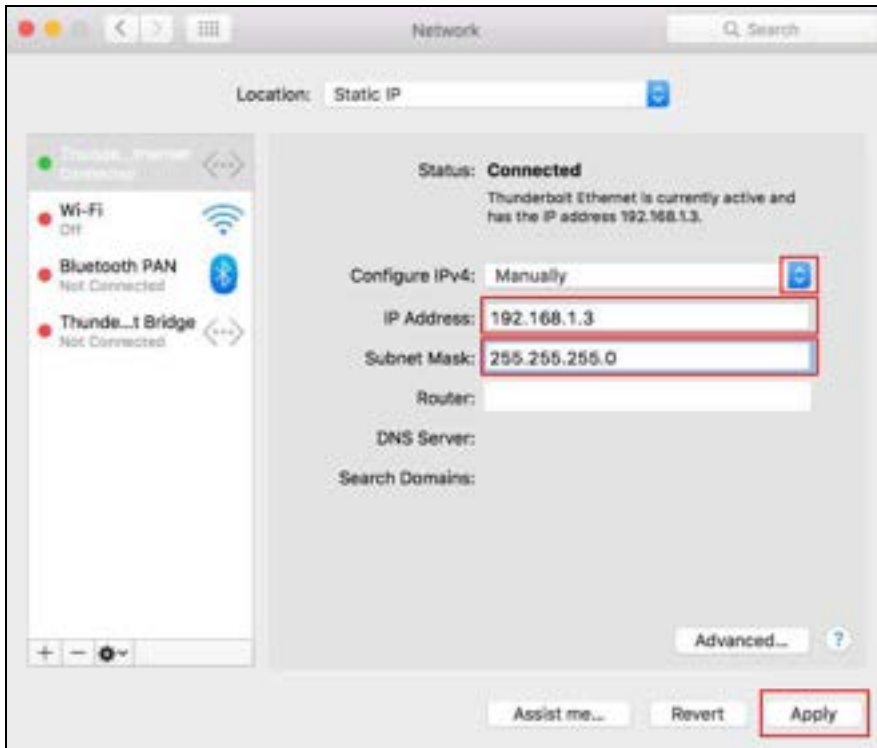
- 1 Open your **System Preferences**, then click **Network**.



- 2 Once the **Network** screen is open, it is recommended you click **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 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 (except 192.168.1.5). Then type 255.255.255.0 as your subnet mask, and click **Apply** to save your changes.



Note: After you have configured your WAP6807, 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.

PART II

Technical Reference

CHAPTER 6

Status

6.1 Overview

This chapter discusses read-only information related to the device state of the WAP6807.

6.2 What You Can Do

- Use the **Overview** screen to view the WAP6807's basic information, such as firmware version or work mode, see [Section 6.3 on page 57](#).
- Use the **System Log** screen to view the logs for the categories such as system maintenance or system errors, see [Section 6.4 on page 58](#).

6.3 Overview Screen

Use the **Overview** screen to see the basic information for WAP6807.

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

Figure 28 Status > Overview (Repeater mode)



Figure 29 Status > Overview (AP mode)



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

Table 22 Status Screen

LABEL	DESCRIPTION
System	
Model	This is the WAP6807's model name.
Firmware Version	This is the firmware version and the date created.
Local Time	This field displays your WAP6807's present date and time.
Uptime	This is the total time the WAP6807 has been on.
WiFi	
Work Mode	This is the device mode (see Chapter 4 on page 26 for more information) to which the WAP6807 is set - Repeater/AP Mode .

6.4 System Log Screen

Use the **System Log** screen to see the logged messages for the WAP6807. Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills.

Click **Status > System Log** to open the following screen.

Figure 30 Status > System Log

System Log

```

Wed Feb 5 01:40:19 2020 daemon.notice easycompd: retry session in 3840 sec, RetryCount = 24
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: start session
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: configured acs url http://10.12.0.10:7547
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: external script init
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: send Inform
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: sending http message failed
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: sending Inform failed
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: external: execute apply service
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: external script exit
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: end session failed
Wed Feb 5 02:44:19 2020 daemon.notice easycompd: retry session in 3840 sec, RetryCount = 25
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: start session
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: configured acs url http://10.12.0.10:7547
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: external script init
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: send Inform
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: sending http message failed
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: sending Inform failed
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: external: execute apply service
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: external script exit
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: end session failed
Wed Feb 5 03:48:19 2020 daemon.notice easycompd: retry session in 3840 sec, RetryCount = 26
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: start session
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: configured acs url http://10.12.0.10:7547
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: external script init
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: send Inform
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: sending http message failed
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: sending Inform failed
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: external: execute apply service
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: external script exit
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: end session failed
Wed Feb 5 04:52:19 2020 daemon.notice easycompd: retry session in 3840 sec, RetryCount = 27
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: start session
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: configured acs url http://10.12.0.10:7547
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: external script init
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: send Inform
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: sending http message failed
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: sending Inform failed
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: external: execute apply service
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: external script exit
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: end session failed
Wed Feb 5 05:56:20 2020 daemon.notice easycompd: retry session in 3840 sec, RetryCount = 28
Wed Feb 5 07:00:20 2020 daemon.notice easycompd: start session
Wed Feb 5 07:00:20 2020 daemon.notice easycompd: configured acs url http://10.12.0.10:7547
Wed Feb 5 07:00:20 2020 daemon.notice easycompd: external script init

```

CHAPTER 7

System

7.1 Overview

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

7.2 What You Can Do in this Chapter

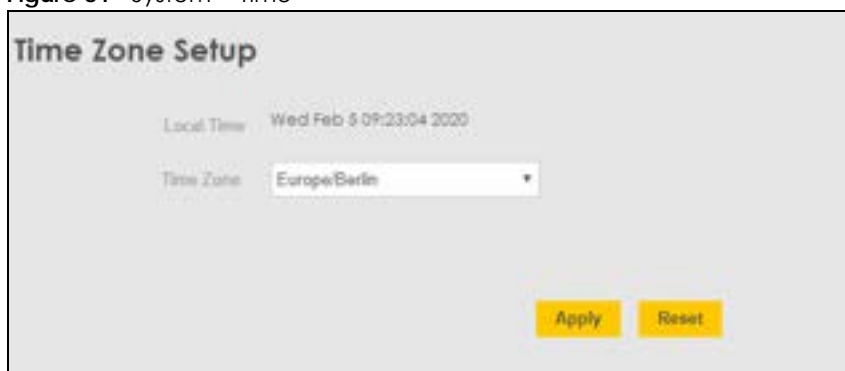
- Use the **Time** screen to change your WAP6807's time and date, see [Section 7.3 on page 60](#).
- Use the **Password** screen to set the password, see [Section 7.4 on page 61](#).
- Use the **Restore/ Firmware Upgrade** screen to back up and restore device configurations or to update firmware, see [Section 7.5 on page 61](#).
- Use the **Restart** screen to reboot the WAP6807 without turning the power off, see [Section 7.6 on page 64](#).

7.3 Time Screen

Use this screen to configure the WAP6807's time and date based on your local time zone.

Click **System** > **Time** to open the following screen.

Figure 31 System > Time



The screenshot shows the 'Time Zone Setup' screen. At the top, it says 'Time Zone Setup'. Below that, there are two labels: 'Local Time' and 'Time Zone'. The 'Local Time' value is 'Wed Feb 5 09:23:04 2020'. The 'Time Zone' is a dropdown menu currently set to 'Europe/Berlin'. At the bottom right, there are two yellow buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 23 Maintenance > Time

LABEL	DESCRIPTION
Local Time	This field displays the time of your Zyxel Device. Each time you reload this page, the Zyxel Device synchronizes the time with the time server.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

7.4 Password Screen

Use this screen to set the web configurator password.

Click **System > Password** to open following screen.

Figure 32 System > Password

The following table describes the labels in this screen.

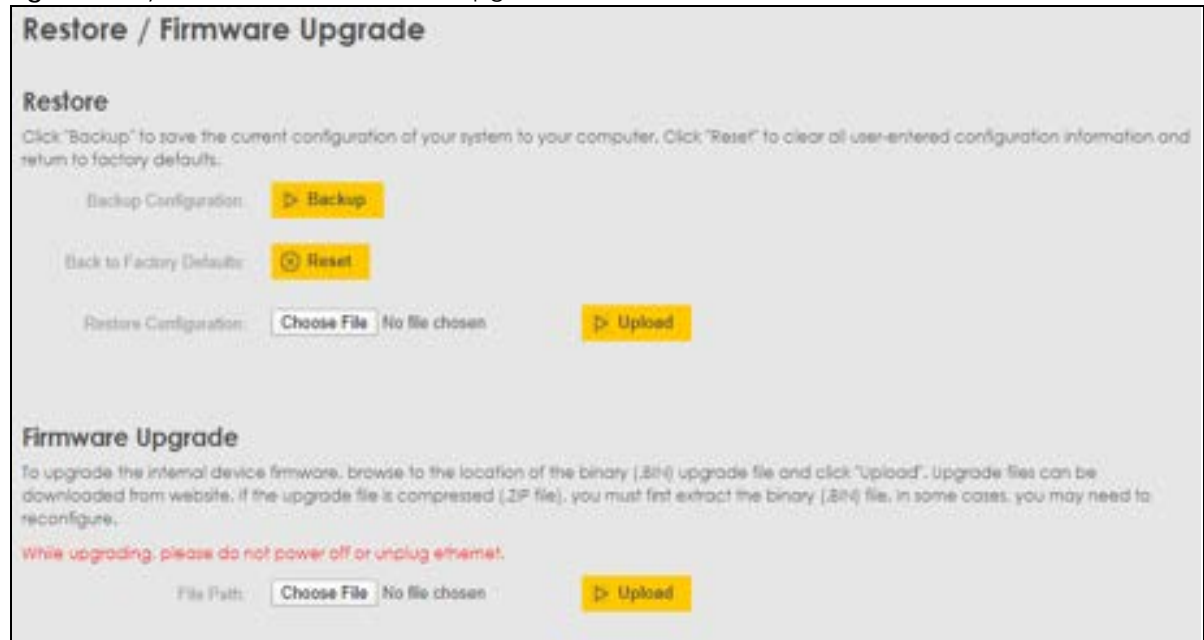
Table 24 System > Password

LABEL	DESCRIPTION
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.
Reset	Click Reset to begin configuring this screen afresh.

7.5 Restore/ Firmware Upgrade Screen

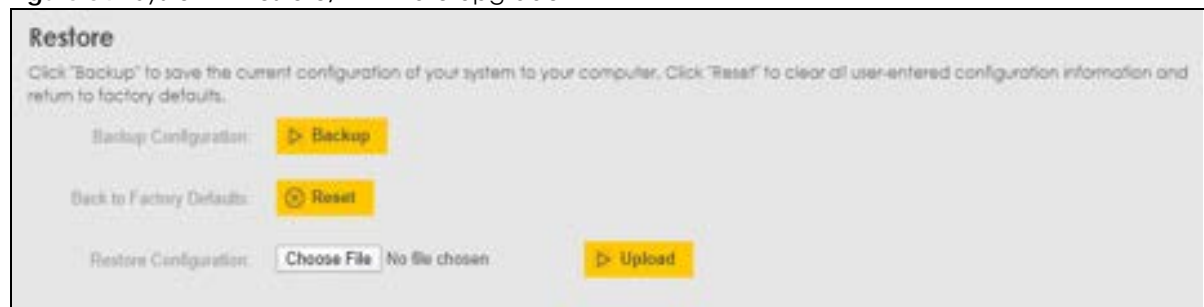
Use this screen to back up and restore device configurations or to update firmware.

Click **System > Restore/ Firmware Upgrade** to open the following screen.

Figure 33 System > Restore/ Firmware Upgrade

7.5.1 Restore

Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 34 System > Restore/ Firmware Upgrade

Backup Configuration

Backup Configuration allows you to back up (save) the WAP6807's current configuration to a file on your computer. Once your WAP6807 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 WAP6807's current configuration to your computer.

Back to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the WAP6807 to its factory defaults. The following warning screen appears.

Figure 35 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 WAP6807. Refer to [Section 2.5 on page 22](#) for more information on resetting the WAP6807 to the factory defaults.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your WAP6807.

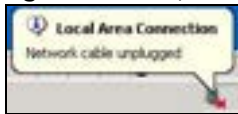
Table 25 System > Restore/ Firmware Upgrade > Restore Configuration

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 WAP6807 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 WAP6807 again.

The WAP6807 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 36 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 WAP6807 IP address (192.168.1.5). Refer to your operating system's help files for details on how to set up your computer's IP address.

7.5.2 Firmware Upgrade

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "WAP6807.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Follow the instructions in this screen to upload firmware to your WAP6807.

Figure 37 System > Restore/ Firmware Upgrade > Firmware Upgrade

The following table describes the labels in this screen.

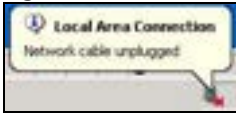
Table 26 System > Restore/ Firmware Upgrade > Firmware Upgrade

LABEL	DESCRIPTION
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 WAP6807 while firmware upload is in progress!

Wait until the firmware upload process is complete.

The WAP6807 automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 38 Network Temporarily Disconnected

After the WAP6807 restarts, log in again and check your new firmware version in the **Status** screen.

7.6 Restart Screen

System restart allows you to reboot the WAP6807 without turning the power off. Click **Reboot** to have the WAP6807 restart. This does not affect the WAP6807's configuration.

Click **System > Restart** to open the following screen displays.

Figure 39 System > Restart

CHAPTER 8

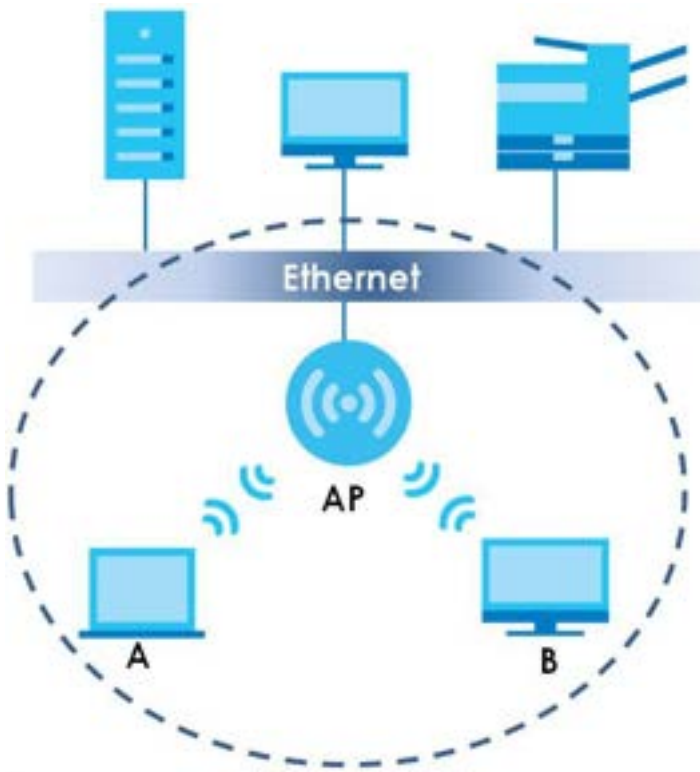
Wireless LAN

8.1 Overview

This chapter discusses how to configure the wireless network settings in your WAP6807. See [Section 8.10.1 on page 75](#) and the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 40 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 WAP6807 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.

8.2 What You Can Do in this Chapter

Wireless screens vary according to the device mode you are using. See [Section 1.2 on page 10](#) for more information on device modes.

- Use the **Basic** screen in **2.4G/ 5G Interface Config** to view read-only information on the 2.4G/ 5G wireless radios, see [Section 8.5.1 on page 68](#).
- Use the **Advanced** screen in **2.4G/ 5G Interface Config** to configure wireless advanced settings such as the guard interval or channel bandwidth, see [Section 8.5.2 on page 69](#).
- Use the **Basic** screen in **2.4G/ 5G Main Config** to enter the SSID and select the wireless security mode, see [Section 8.6.1 on page 71](#).
- Use the **WPS** screen in **2.4G/ 5G Main Config** to quickly set up a wireless network with strong security without having to configure security settings manually, see [Section 8.7 on page 73](#).
- Use the **Stations** screen in **2.4G/ 5G Main Config** to view a detailed summary of WAP6807's associated devices, see [Section 8.8 on page 74](#).

8.3 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.

8.3.1 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.

8.4 WiFi Configuration Screen

Use this screen to view the status of your WAP6807 in the Easy Mesh network. Your WAP6807 can be an AP controller, an AP agent or a repeater.

If your router supports Zyxel MPro Mesh, the WAP6807 will function as an AP agent. If your router does not support Zyxel MPro Mesh, the WAP6807 will function as an AP controller.

You can also view the basic information of your 2.4G/ 5G wireless network.

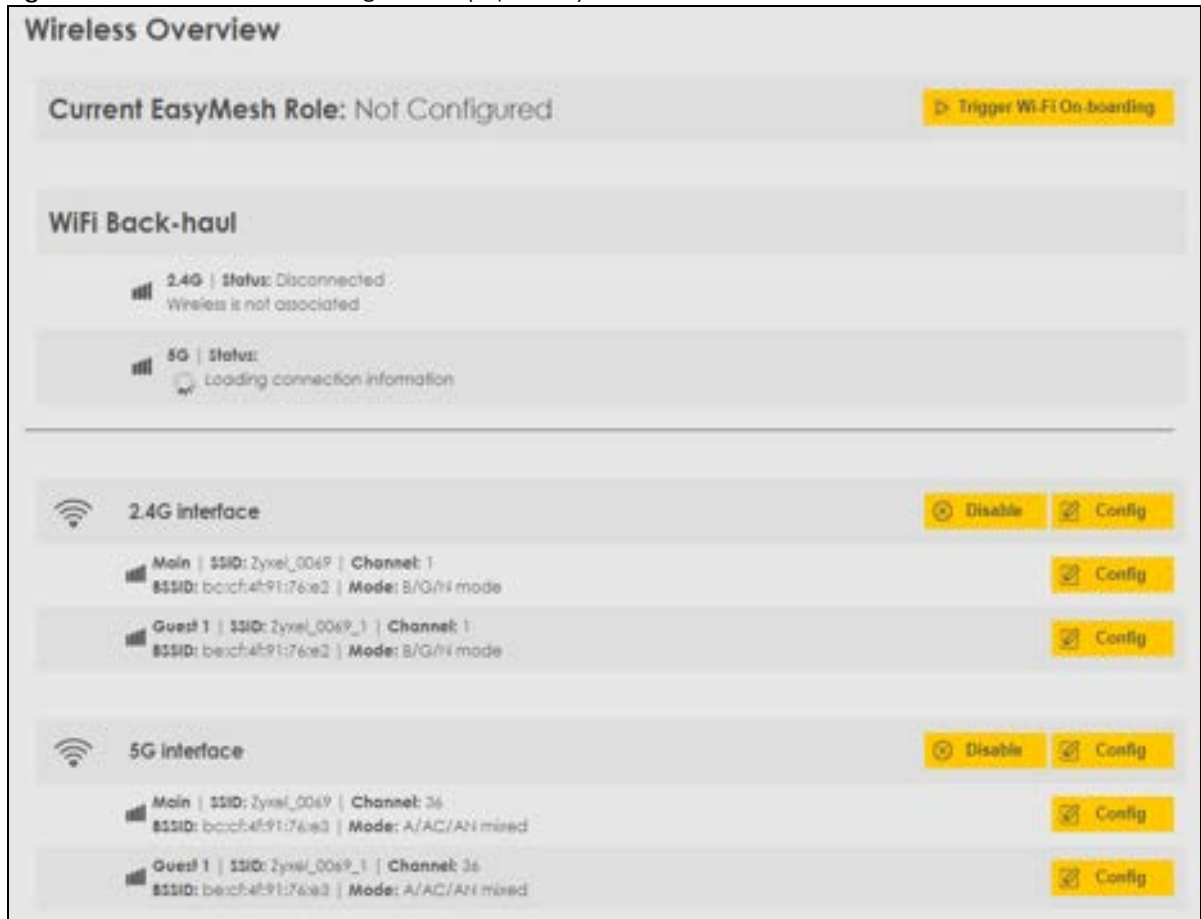
Click **Wireless > WiFi Configuration** to open the following screen.

Figure 41 Wireless > WiFi Configuration (AP controller)



Figure 42 Wireless > WiFi Configuration (AP agent)



Figure 43 Wireless > WiFi Configuration (repeater)

Click **Trigger Wi-Fi On-boarding** to activate MPro Mesh.

Note: To trigger MPro Mesh successfully, we recommend using a router that supports Zyxel MPro Mesh for your network.

8.5 2.4G/ 5G Interface Configuration

8.5.1 Basic Screen

Use this screen to view read-only information on the 2.4G/ 5G wireless radios.

Click **Wireless > WiFi Configuration > 2.4G/ 5G Interface Config > Basic** to open the following screen.

Figure 44 Wireless > WiFi Configuration > 2.4G/ 5G Interface Config > Basic

The following table describes the labels in this screen.

Table 27 Wireless > WiFi Configuration > 2.4G/ 5G Interface Config > Basic

LABEL	DESCRIPTION
Mode	Select a mode for your WAP6807 to decide if it allows IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with it. The transmission rate of your WAP6807 might be reduced.
Channel	This field displays the channel the WAP6807 is currently using. It varies depending on the frequency band and the country you are in.
Apply	Click Apply to save your changes back to the WAP6807.
Cancel	Click Cancel to reload the previous configuration for this screen.

8.5.2 Advanced Screen

Use this screen to select the advanced wireless settings for the WAP6807.

Click **Wireless > WiFi Configuration > 2.4G/ 5G Interface Config > Advanced** to open the following screen.

Figure 45 Wireless > WiFi Configuration > 2.4G/ 5G Interface Config > Advanced

The following table describes the labels in this screen.

Table 28 Wireless > WiFi Configuration > 2.4G/ 5G Interface Config > Advanced

LABEL	DESCRIPTION
HT Guard Interval	<p>Select Auto to increase data throughput. However, this may make data transfer more prone to errors.</p> <p>Select Short to improve data throughput. Use this method if the WAP6807 is located in an environment not prone to radio interference, or if you not using mixed mode for your wireless connection.</p> <p>Select Long to prioritize data integrity. Use this method if your wireless network is busy and congested or the WAP6807 is located in an environment prone to radio interference.</p>
Channel Bandwidth	<p>Select the channel bandwidth you want to use for your wireless network.</p> <p>Select whether the WAP6807 uses a wireless channel width of 20 MHz, 40 MHz or 80 MHz. 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.</p> <p>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.</p>
Beacon Interval	This is the time lag between each of the beacons sent by the wireless network.
Data Beacon Rate (DTIM)	The Data Beacon Rate (DTIM) period, is the moment the WAP6807 will broadcast any buffered broadcast frames, after the WAP6807 broadcasts the beacon. Enter 1, and the WAP6807 will transmit broadcast frames after every beacon, enter 2 and the WAP6807 will transmit every other beacon.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

8.6 2.4G/ 5G Main WiFi Configuration

8.6.1 Basic Screen

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

Click **Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Basic** to open the following screen.

Note: If you are configuring the WAP6807 from a computer connected to the wireless LAN and you change the WAP6807'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 WAP6807's new settings.

Figure 46 Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Basic (AP controller and repeater)

The screenshot shows the 'Interface Configurations - 2.4G Main' web interface. At the top, there are three tabs: 'Basic' (selected), 'WPS', and 'Stations'. Below the tabs, the configuration fields are as follows:

Field	Value
SSID	Zyxel_0069
Auth Mode	WPA2PSK
Encryption	AES
Key Renewal Interval	3600 second(s) [0 - 4194303]
Key	T5DRQ5JH8Q
Hidden	No

At the bottom right, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 29 Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Basic (AP controller and repeater)

LABEL	DESCRIPTION
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.
Auth Mode	Select the data encryption method the WAP6807 uses. Select WPA2PSK or WPAPSKWPA2PSK (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 Disable to allow any client to associate this network without authentication.
Encryption	This field shows the AES type of data encryption.
Key Renewal Interval	The Key Renewal Interval is the rate at which the WAP6807 sends a new group key out to clients.
Key	Enter the password that lets you connect to the WAP6807. Your password should be in a string of ASCII characters between 8 and 63 or hexadecimal characters between 8 and 64.
Hidden	This field shows if the SSID is hidden in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. You can hide the guest WiFi SSID but not the main WiFi SSID. Note: You cannot enable WPS for your guest WiFi if this check box is selected.
Apply	Click Apply to save your changes back to the WAP6807.
Reset	Click Reset to reload the previous configuration for this screen.

Figure 47 Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Basic (AP agent)

Interface Configurations - 2.4G Main

WARNING: EasyMesh feature is enabled!

Basic WPS Stations

SSID: TM16-9003A1

Auth Mode: WPA2PSK

Encryption: AES

Pass-phrase: 12345678

Hidden: Disabled

Key Renewal Interval: 3600 second(s) (0 ~ 4194300)

Apply Reset

The following table describes the labels in this screen.

Table 30 Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Basic (AP agent)

LABEL	DESCRIPTION
SSID	This field shows the SSID of the WAP6807 wireless network. 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.
Auth Mode	This field shows the data encryption method the WAP6807 uses.
Encryption	This field shows the AES type of data encryption.
Pass-phrase	This field shows the wireless network key that the WAP6807 get from its uplink router.
Hidden	This field shows if the WAP6807's SSID is hidden in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Key Renewal Interval	The Key Renewal Interval is the rate at which the WAP6807 sends a new group key out to clients.
Apply	Click Apply to save your changes back to the WAP6807.
Reset	Click Reset to reload the previous configuration for this screen.

8.7 WPS Screen

Use this screen to enable or disable WPS and check current WPS status.

Click **Wireless > WiFi Configuration > 2.4G/ 5G Main Config > WPS** to open the following screen.

Note: With WPS, wireless clients can only connect to the 5GHz or 2.4GHz wireless network using the first SSID on the WAP6807.

Figure 48 Wireless > WiFi Configuration > 2.4G/ 5G Main Config > WPS

The following table describes the labels in this screen.

Table 31 Wireless > WiFi Configuration > Main Config > WPS

LABEL	DESCRIPTION
WPS	This field shows the status of the WPS on the WAP6807.
WPS Configured	This field shows Yes if WPS is enabled and the wireless security key will not be changed after the WPS connection is established.
WPS SSID	This field shows the SSID of WAP6807.
WPS Auth Mode	This field shows the data encryption method the WAP6807 uses.
WPS Encryp Type	This field shows the AES type of data encryption.
WPS Key	This field shows the wireless network key of WAP6807.
WPS mode	This field shows WPS wireless network is using Push Button Configuration (PBC).
WPS Action	Click this button to add another WPS-enabled wireless device (within wireless range of the WAP6807) to your wireless network.
WPS Current Status	This field shows if WPS connection has been established successfully.

8.8 Stations Screen

View a detailed summary of WAP6807's associated devices. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the WAP6807 (or wireless router) using the same SSID, channel and security settings.

Click **Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Stations** to open the following screen.

Figure 49 Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Stations



Interface Configurations - 2.4G Main					
Basic	WPS	Stations			
MAC Addr	Tx Rate	RSSI	Stream SNR	Last RX Rate	Connect Time

The following table describes the labels in this screen.

Table 32 Wireless > WiFi Configuration > 2.4G/ 5G Main Config > Stations

LABEL	DESCRIPTION
MAC Addr	This shows the MAC address of the wireless client which is associated with the WAP6807.
TX Rate	This shows the number of bytes that have been transmitted by the connected AP or client.
RSSI	This shows the RSSI (Received Signal Strength Indicator) of the WAP6807's wireless connection.
Stream SNR	This Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power.
Last RX Rate	This shows the number of bytes that have been received by the connected AP or client.
Connect Time	This shows the total amount of time (in seconds) the WAP6807 has been associated with the AP or client.

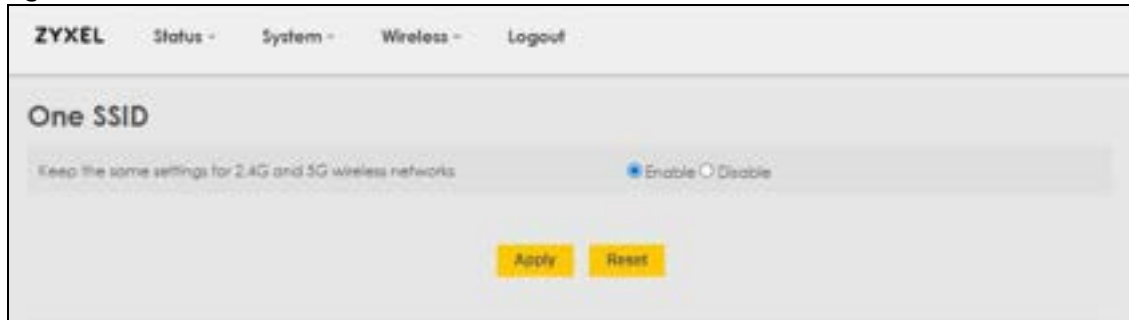
8.9 One SSID Screen

Select **Enable** to use the same settings for 2.4G and 5G WiFi networks. Otherwise, select **Disable**.

Band steering will not work if you select **Disable** here. For more information on band steering, see [Section 1.3.1 on page 11](#).

Click **Wireless > One SSID** to open the following screen.

Figure 50 Wireless > One SSID



8.10 Technical Reference

This section discusses WiFi in depth. For more information, see [Appendix A on page 92](#).

8.10.1 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.

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.

8.10.2 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.

8.10.2.1 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.

8.10.2.2 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.

8.10.2.3 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.

8.10.2.4 Signal Problems

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

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

8.10.2.5 BSS

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

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

8.10.2.6 MBSSID

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

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

8.10.2.7 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

8.10.2.8 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.

8.10.3 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 WAP6807 is in AP or Repeater mode. The following example uses the WAP6807 as the AP and a WPS-enabled Android smartphone as the wireless client.

You can use the **Push Button Configuration (PBC)** to create a secure wireless network simply by pressing a button. See [Section 8.10.3.2 on page 79](#) for more information.

Note: The WAP6807 does not support PIN configuration method.

8.10.3.1 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 33 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
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

8.10.3.2 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 2.1 on page 17](#), can also be used for PBC configurations in either AP or Repeater mode.

- 1 Make sure that your WAP6807 is turned on 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 WAP6807'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**.

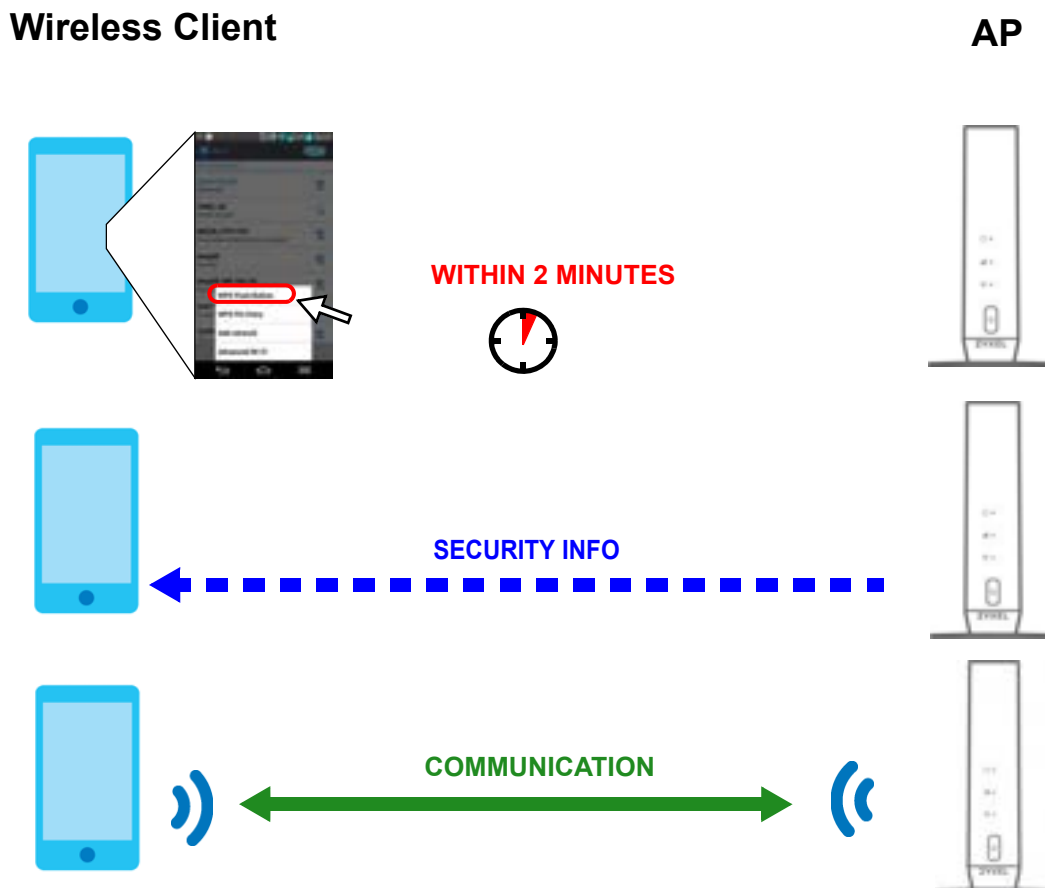
Note: Your WAP6807 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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 WAP6807 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 WAP6807 securely.

The following figure shows you how to set up wireless network and security by pressing a button on both WAP6807 and wireless client (the Android smartphone in this example).

Figure 51 Example WPS Process: PBC Method



8.10.3.3 How WPS Works

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

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

Figure 52 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.

8.10.3.4 Example WPS Network Setup

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

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

Figure 53 WPS: Example Network Step1



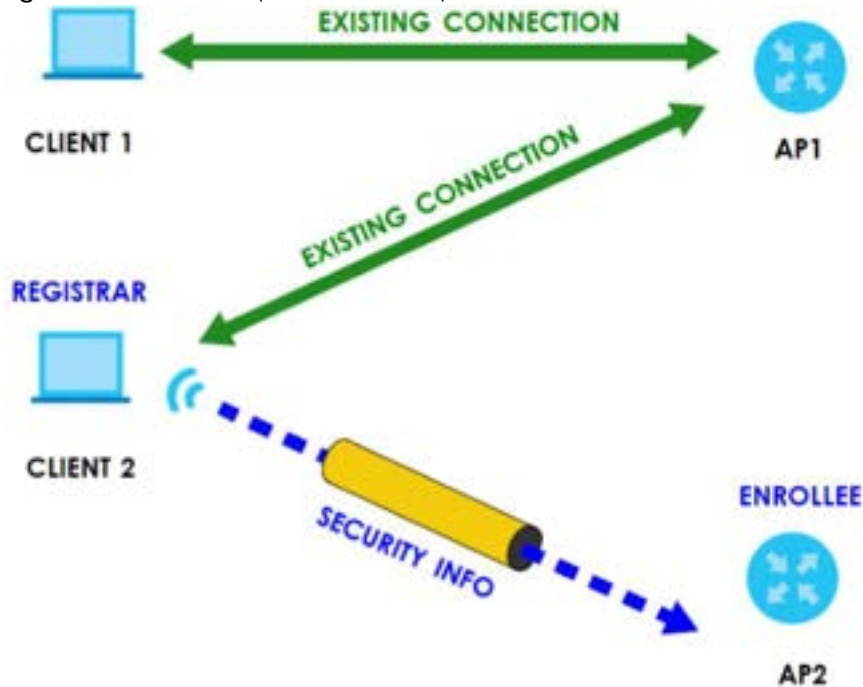
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 54 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 55 WPS: Example Network Step 3



8.10.3.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

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

8.10.4 MPro Mesh Overview

Zyxel MPro Mesh supports AP steering and Band steering.

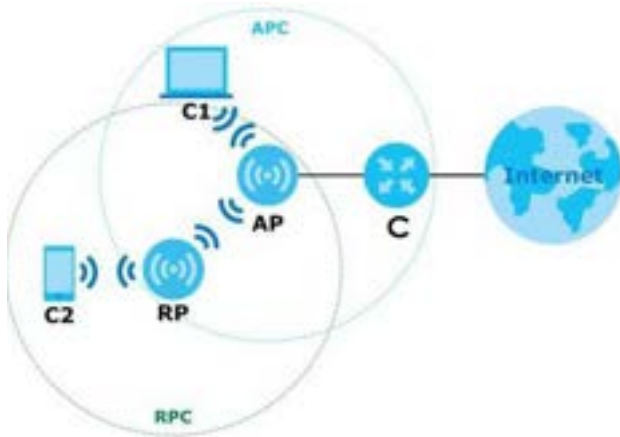
- AP steering allows wireless clients to roam seamlessly between Mesh supported devices in your Mesh network by using the same SSID and WiFi password. Also, AP steering helps monitor wireless clients and drop their connections to optimize the WAP6807 bandwidth when the clients are idle or have a low 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 or an AP 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.

Figure 56 Mesh Application



Icons used in [Figure 56](#):

- C- router controller or AP controller
- AP- Access Point
- RP- Repeater
- C1- Client1
- C2- Client2
- APC- Access Point coverage area
- RPC- Repeater coverage area

Note: If your router supports Zyxel MPro Mesh, it will serve as the router controller in a Mesh network with the WAP6807. If your router does not support Zyxel MPro Mesh, your WAP6807 will automatically become an AP controller.

Note: You can configure the controller in WAP6807's Mesh network with the MPro Mesh app.

CHAPTER 9

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](#)
- [WAP6807 Web Configurator Access and Login](#)
- [Internet Access](#)
- [Resetting the WAP6807 to its Factory Defaults](#)
- [WiFi Problems](#)
- [MPro Mesh Problems](#)
- [MPro Mesh App Problems](#)
- [Daisy Chain Problems](#)

9.1 Power, Hardware Connections, and LEDs

[The WAP6807 does not turn on. None of the LEDs turn on.](#)

- Make sure the WAP6807 is plugged in to an appropriate power source. Make sure the power source is turned on.
- Check if the power button is pressed.
- Disconnect and re-connect the WAP6807.
- Remove the WAP6807 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.
- If the problem continues, contact the vendor.

[LED FAQ](#)

For **POWER** LED:

- How do I know my WAP6807 is in Repeater mode?
A: Your **POWER** LED is steady green.
- How do I know my WAP6807 is booting?
A: Your **POWER** LED is blinking green.

- How do I know my WAP6807 is in AP mode?
A: Your **POWER** LED is solid amber.
- How do I know my WAP6807 failed to join the WiFi network?
A: Your **POWER** LED is steady red.

For **LINK** LED:

- How do I know my WAP6807 is too close to the controller (Zyxel MPro Mesh Router in **Scenario 1** and WAP6807-1 in **Scenario 2**)?
A: Your **LINK** LED is steady amber.
- How do I know my WAP6807 is too far from the controller (Zyxel MPro Mesh Router in **Scenario 1** and WAP6807-1 in **Scenario 2**)?
A: Your **LINK** LED is steady red.

One of the LEDs does not behave as expected.

- Make sure you understand the normal behavior of the LED, see [Table 13 on page 27](#) and [Table 15 on page 29](#) for more information.
- Check the hardware connections. See the Quick Start Guide.
- Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- Disconnect and re-connect the WAP6807.
- If the problem continues, contact the vendor.

9.2 WAP6807 Web Configurator Access and Login

I forgot the password.

- The default password is in the device label.
- If the default password does not work, you have to reset the device to its factory defaults. See [Section 9.4 on page 89](#).

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

- Make sure you are using the correct address. The default web address (URL) of the WAP6807 in Repeater mode is **192.168.1.5**.
If the WAP6807 is in AP mode, check for the web address the connected router assigns to your device.
- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 2.1 on page 17](#).

- Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
- Reset the device to its factory defaults, and try to access the WAP6807 with the default address.
- If the problem continues, contact the network administrator or vendor.

I can see the [Login](#) screen, but I cannot log in to the WAP6807.

- Make sure you have entered the password correctly. The default password is in the device label.
- This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- Disconnect and re-connect the WAP6807.
- If the problem continues, you have to reset the device to its factory defaults. See [Section 9.4 on page 89](#).

9.3 Internet Access

I cannot access the Internet.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 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 WAP6807.
- Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- If the problem continues, contact the network administrator or vendor.

I cannot access the Internet anymore. I had access to the Internet (with the WAP6807), but my Internet connection is not available anymore.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 2.1 on page 17](#).
- Make sure you're not blocked from the Internet in the app.
- Reboot the WAP6807.
- If the problem continues, contact the network administrator or vendor.

The Internet connection is slow or intermittent.

- There might be a lot of traffic on the network. Look at the LEDs, and check [Section 2.1 on page 17](#). If the WAP6807 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- Check the signal strength. If the signal strength is low, try moving the WAP6807 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).
- Reboot the WAP6807.
- If the problem continues, contact the network administrator or vendor.

9.4 Resetting the WAP6807 to its Factory Defaults

If you reset the WAP6807, you lose all of the changes you have made. The WAP6807 re-loads its default settings, and the password resets to the back-label default key. You have to make all of your changes again.

[I want to reset my WAP6807 to the factory defaults.](#)

- You can back up the configuration you made before resetting the WAP6807.

To reset the WAP6807,

- Make sure the power LED is on.
- Press the **RESET** button for longer than 5 seconds, the Power LED begins to blink, to set the WAP6807 back to its factory-default configuration.

OR

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

- If the WAP6807 restarts automatically, wait for the WAP6807 to finish restarting, and log in to the Web Configurator. The password is in the device label.

If the WAP6807 does not restart automatically, disconnect and reconnect the WAP6807. Then, follow the directions above again.

- You can upload a previously saved configuration file from your computer to the WAP6807 after resetting the device.

9.5 WiFi Problems

[I cannot access the WAP6807 using WiFi.](#)

- Make sure the WAP6807 is working in AP or Repeater mode and the wireless LAN is enabled on the WAP6807.
- Make sure the wireless adapter on the wireless client is working properly.

- Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the WAP6807.
- Make sure your computer (with a wireless adapter installed) is within the transmission range of the WAP6807.
- Check that both the WAP6807 and your wireless station are using the same wireless and wireless security settings.

9.6 MPro Mesh Problems

I cannot trigger MPro Mesh on the WAP6807 successfully.

- You should see **Current EasyMesh Role: Controller** or **Current EasyMesh Role: Agent** in the **WiFi Configuration** screen after you set up your WAP6807 in a mesh network. If you see **Current EasyMesh Role: Not Configured**, it means your WAP6807 failed to join the mesh network.

This might happen if your router does not support Zyxel MPro Mesh. In this case, manually change the SSID and key of the WAP6807's wireless network so that they are the same as your router.

9.7 MPro Mesh App Problems

I cannot use the MPro Mesh app to manage my wireless network.

- Make sure you connect your mobile device to the controller (Zyxel MPro Mesh Router in [Section 3.6.1 on page 27](#) and WAP6807-1 in [Section 3.6.2 on page 28](#)) in order to manage the wireless network.
- Make sure you use the controller's SSID and key when logging in with the app.

9.8 Daisy Chain Problems

I cannot add another extender to my daisy chain network.

- Check your device mode. The mode of your WAP6807 will affect how you add another extender to your network. For more information on modes and how to set your device in AP or Repeater mode, see [Section 1.2 on page 10](#).
- If you are using the WPS PBC (Push Button Configuration) method, make sure you press the WPS button in the right way. For more information on adding extenders using WPS button, see [Section 2.4.1 on page 20](#).

- If you are using the MPro Mesh app for adding extenders to your network, make sure you choose the right scenario.

With MPro Mesh Router, follow the steps in [Section 3.6.1 on page 27](#) to add extenders to your network.

With non-MPro Mesh Router, follow the steps in [Section 3.6.2 on page 28](#) to add extenders to your network.

APPENDIX A

Wireless LANs

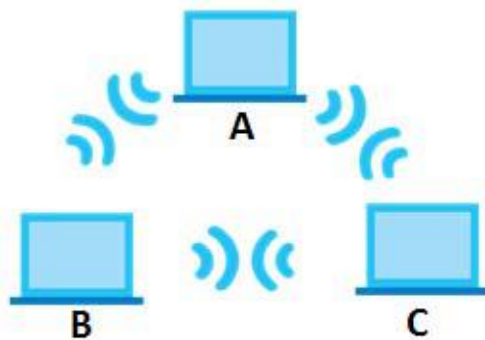
Wireless LAN Topologies

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

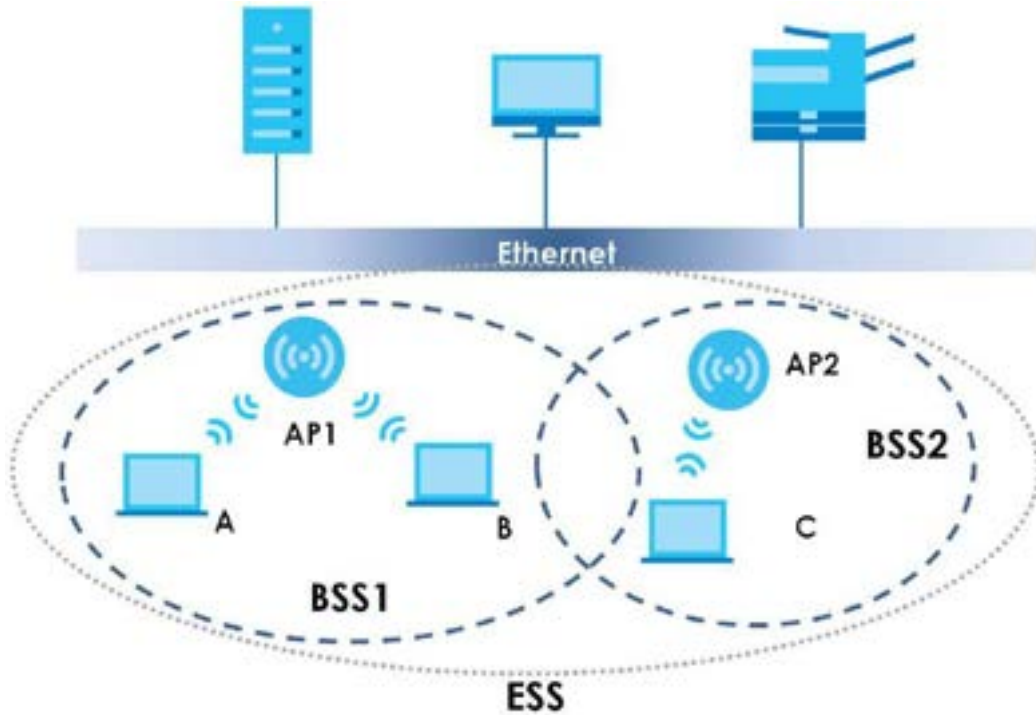


ESS

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

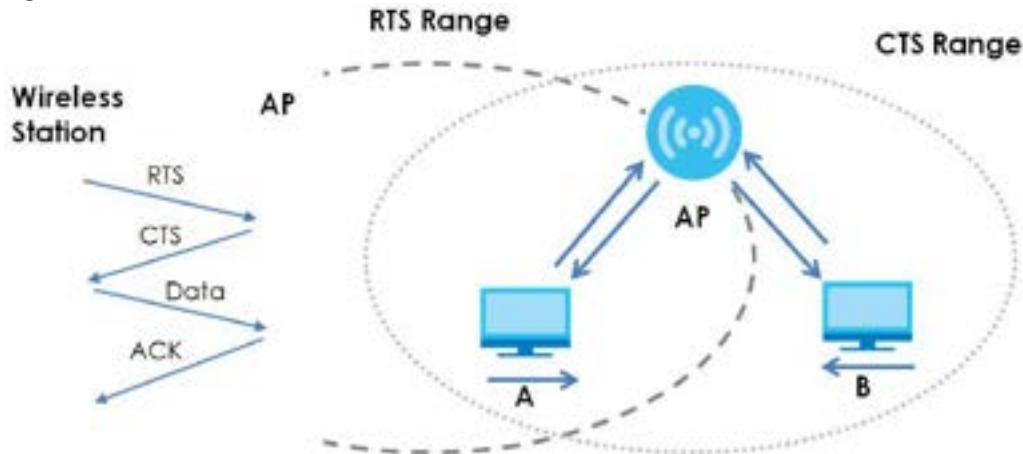
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 34 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 WAP6807 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the WAP6807 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your WAP6807.

Table 35 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 WAP6807 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 36 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

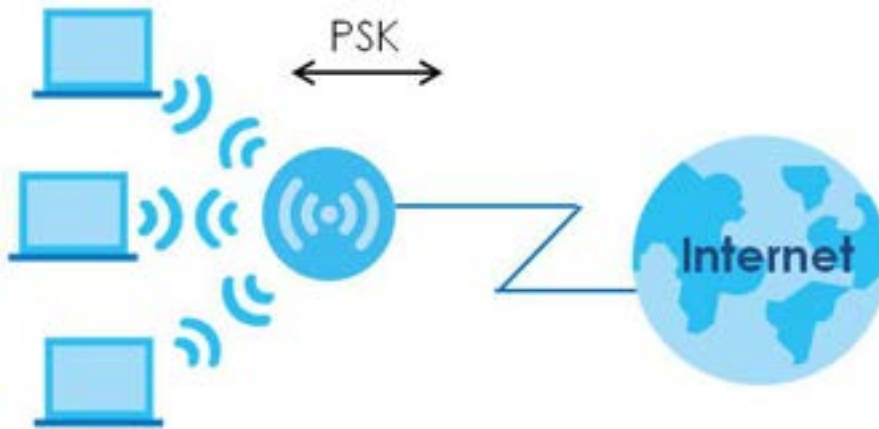


WPA(2)-PSK Application Example

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 1 dB 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 <https://www.zyxel.com/homepage.shtml> and also https://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.
- <https://www.zyxel.com/cn/zh/>

India

- Zyxel Technology India Pvt Ltd.
- <https://www.zyxel.com/in/en/>

Kazakhstan

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

Korea

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

Malaysia

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

Pakistan

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

- Zyxel Thailand Co., Ltd.
- <https://www.zyxel.com/th/th/>

Vietnam

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

Europe

Belarus

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

Belgium

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

- <https://www.zyxel.com/be/fr/>

Bulgaria

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

Czech Republic

- Zyxel Communications Czech s.r.o
- <https://www.zyxel.com/cz/cs/>

Denmark

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da/>

Estonia

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

Finland

- Zyxel Communications
- <https://www.zyxel.com/fi/fi/>

France

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

Germany

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

Hungary

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

Italy

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

Latvia

- Zyxel Latvia
- <https://www.zyxel.com/lv/lv/>

Lithuania

- Zyxel Lithuania
- <https://www.zyxel.com/lt/lt/>

Netherlands

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

Norway

- Zyxel Communications
- <https://www.zyxel.com/no/no/>

Poland

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

Romania

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

Russia

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

Slovakia

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

Spain

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

Sweden

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

Switzerland

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

Turkey

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

UK

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

Ukraine

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

South America

Argentina

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Brazil

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

Colombia

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Ecuador

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

South America

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Middle East

Israel

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

Middle East

- Zyxel Communications Corporation
- <https://www.zyxel.com/me/en/>

North America

USA

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

Oceania

Australia

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

Africa

South Africa

- Nology (Pty) Ltd.
- <https://www.zyxel.com/za/en/>

APPENDIX C

Legal Information

Copyright

Copyright © 2021 by Zyxel and/or its affiliates.

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

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

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

Regulatory Notice and Statement

EUROPEAN UNION and United Kingdom



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

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

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU 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 20 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 97.72 mW,
 - The bands 5,150 MHz to 5,350 MHz is 195.88 mW,
 - The 5,470 MHz to 5,725 MHz is 918.33 mW.

Български (Bulgarian)	<p>С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.</p> <p>National Restrictions</p> <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)	<p>Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.</p> <p>National Restrictions</p> <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 Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/EU.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/EU.
Italiano (Italian)	<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 deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ftigijiet 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 adaptor 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.)

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、食物或其他不適合的材料。
- 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。
- 如果更換不正確的電池型式，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 at www.zyxel.com to receive e-mail notices of firmware upgrades and related information.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses.

(For ZNET UG) To request the source code covered under these licenses, please go to: https://www.zyxel.com/form/gpl_oss_software_notice.shtml

(For ZCOM UG) To request the source code covered under these licenses, please go to: <https://service-provider.zyxel.com/global/en/gpl-oss->

software-notice

Index

A

Advanced Encryption Standard
See AES.

AES [99](#)

antenna

directional [102](#)

gain [102](#)

omni-directional [102](#)

AP (access point) [93](#)

B

backup configuration [62](#)

C

CA [97](#)

Certificate Authority
See CA.

certifications [111](#)

viewing [113](#)

channel [66](#), [93](#)

interference [93](#)

configuration

backup [62](#)

reset factory defaults [63](#)

restore [63](#)

contact information [103](#)

copyright [109](#)

CTS (Clear to Send) [94](#)

customer support [103](#)

D

daisy chain [11](#), [15](#)

disclaimer [109](#)

dynamic WEP key exchange [98](#)

E

EAP Authentication [97](#)

encryption [99](#)

ESS [92](#)

Extended Service Set, See ESS [92](#)

F

firmware upgrade

screen [61](#)

firmware upload [63](#)

file extension

using HTTP

firmware version [49](#), [50](#), [58](#)

fragmentation threshold [94](#)

G

General wireless LAN screen [68](#)

H

hidden node [93](#)

I

IBSS [92](#)

IEEE 802.11g [95](#)

Independent Basic Service Set
See IBSS [92](#)

initialization vector (IV) [99](#)

L

language [64](#)

Log [58](#)

M

MAC OS X [53](#)

Message Integrity Check (MIC) [99](#)

Microsoft Windows [51](#)

P

Pairwise Master Key (PMK) [99](#), [101](#)

PIN

configuration [79](#)

PSK [99](#)

push button

configuration [79](#)

Q

Quality of Service (QoS) [71](#)

R

RADIUS [96](#)

message types [96](#)

messages [96](#)

shared secret key [97](#)

Reset button [22](#)

Reset the device [22](#)

restore configuration [63](#)

Roaming [69](#)

RTS (Request To Send) [94](#)

threshold [93](#), [94](#)

S

security

PBC [79](#)

PIN [79](#)

Service Set [72](#), [73](#)

Service Set IDentity. See SSID.

SSID [66](#)

system [60](#)

system password

screen [61](#)

T

Temporal Key Integrity Protocol (TKIP) [99](#)

Time setting [60](#)

W

warranty [113](#)

note [113](#)

Web Configurator

how to access [47](#)

Overview [47](#)

Wi-Fi Protected Access [98](#)

wireless channel [89](#)

wireless client WPA supplicants [100](#)

wireless LAN [89](#)

Wireless network

basic guidelines [66](#)

channel [66](#)

example [65](#)

overview [65](#)

security [66](#)

SSID [66](#)

Wireless security [66](#)

wireless security [95](#)

troubleshooting [89](#)

Wireless tutorial [39](#)

WLAN

interference [93](#)

security parameters [79](#)

WPA [98](#)

- key caching [100](#)
- pre-authentication [100](#)
- user authentication [99](#)
- vs WPA-PSK [99](#)
- wireless client supplicant [100](#)
- with RADIUS application example [100](#)
- WPA2 [98](#)
 - user authentication [99](#)
 - vs WPA2-PSK [99](#)
 - wireless client supplicant [100](#)
 - with RADIUS application example [100](#)
- WPA2-Pre-Shared Key [98](#)
- WPA2-PSK [98, 99](#)
 - application example [101](#)
- WPA-PSK [99](#)
 - application example [101](#)
- WPS [20](#)
- WPS button [20](#)