NETGEAR®

User Manual

WiFi 6 AX1800/AX3200 Dual Band Wireless Access Point

Models
WAX202
WAX206

December 2021
202-12234-02

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134, USA

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

Do not use this device outdoors.

Applicable to 6 GHz devices only: Only use the device indoors. The operation of 6 GHz devices is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-12234-02	December 2021	We added the following sections: Specify a PPTP or L2TP Internet connection that uses a login [router mode] on page 49 Use WPS to connect to the WiFi network on page 67 (and subsections) Manage the SIP application-level gateway [router mode] on page 75 Block specific applications and services from the Internet [router mode] on page 82 (and subsections) Schedule blocking [router mode] on page 86 Set up security event email notifications on page 88 Static routes [router mode] on page 99 (and subsections) Bridge port and VLAN tag groups [router mode] on page 103 (and subsections) Improve network connections with Universal Plug and Play [router mode] on page 106 Traffic meter [router mode] on page 139 (and subsections) Check your Internet bandwidth on page 148 Set up the AP as a WiFi Bridge to another AP or WiFi router on page 169 Manage the WPS settings on page 172
		We added the following chapter: Port Forwarding and Port Triggering [Router Mode] on page 174
		We revised the information in the following sections: Connect the AP to a routing device and log in for the first time on page 28 Connect the AP to a modem and log in for the first time on page 32 How the operation mode affects how you can reach the device UI on page 35 Log in to the AP after you complete the initial log-in process on page 38 Routing features enabled in router mode on page 41 What to do if you get a browser security warning on page 42 Display, send, or clear the logs on page 125 Specify which activities the AP logs on page 126 Change the WiFi throughput mode on model WAX206 on page 158 Set up the AP as a WiFi Bridge to another AP or WiFi router on page 169 Check or manually start the PPPoE, PPTP, or L2TP connection [router mode] on page 200 Factory Default Settings and Technical Specifications on page 206
		We changed *local browser UI* to *device UI*. We changed http://www.routerlogin.net in to routerlogin.net. We made multiple minor changes.
202-12234-01	July 2021	We added model WAX206.
202-12211-01	July 2021	First publication for model WAX202.

Contents

Chapter 5 Manually Set Up Internet Settings [Router Mode]

Chapter 6 Basic WiFi and Radio Features

Chapter 7 Security, Firewall, and Access Rules

Chapter 8 Network Settings

Chapter 9 Maintain and Monitor

Chapter 10 Advanced WiFi and Radio Features

1

Introduction

This manual is for the following NETGEAR WiFi 6 Dual Band Wireless Access Point models:

- **WAX202**: WiFi 6 AX1800 Dual Band Wireless Access Point
- **WAX206**: WiFi 6 AX3200 Dual Band Wireless Access Point

Models WAX202 and WAX206, in this manual referred to as the AP, support 802.11ax high performance WiFi connectivity and dual-band concurrent operation at 2.4 GHz and 5 GHz. The AP is designed to function standalone in a small office network or home network.

You can use the AP in router mode with its router features enabled, directly connected to the Internet, for example through a modem. You can also use the AP in access point (AP) mode, connected to a device that provides routing functions in your network. In AP mode, the routing features of the AP are not required so they are masked out in the AP's local browser interface (UI).

The chapter contains the following sections:

Note: For more information about the topics that are covered in this manual, visit the support website at netgear.com/support/.

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. You can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this manual, you might need to update the firmware.

Note: In this manual, *WiFi network* means the same as SSID (service set identifier or WiFi network name). That is, when we refer to a WiFi network we mean an individual SSID.

Additional documentation

The following documents are available at netgear.com/support/download/:

- Installation guide
- Data sheet

Unique features for each model

The following table shows the main differences between model WAX202 and model WAX206:

Table 1. Model WAX202 and model WAX206 main differences

Feature	Model WAX202	Model WAX206
WAN (Internet) port speed	1 Gbps	2.5 Gbps
Number of Gigabit LAN ports	3	4
Approximate combined throughput	1800 Mbps total: 600 Mbps at 2.4 GHz 1200 Mbps at 5 GHz	3200 Mbps total: 800 Mbps at 2.4 GHz 2400 Mbps at 5 GHz.
Maximum number of supported WiFi clients	64	128
Maximum number of concurrent devices	40	60

Position the AP

Consider how you want to position the AP. Place it where you want to add WiFi, positioned so the WiFi range of the AP provides an optimal coverage area for your WiFi devices.

The WiFi range or coverage area can vary significantly depending on the physical placement of your AP. For example, the thickness and number of walls that the WiFi signal passes through can limit the range.

Additionally, other WiFi access points in and around your office or home might affect your AP's signal. WiFi access points can be routers, repeaters, WiFi range extenders, and any other devices that emit WiFi signals.

Tips for positioning your AP:

- Place your AP so that you can connect it with an Ethernet cable to your router, modem, or Ethernet outlet and within reach of an AC power outlet.
- Place the AP near the center of the area where your computers and other devices operate, and within a line of sight to your WiFi devices.
- Place the AP in an elevated location, minimizing the number of walls and ceilings between the AP and your WiFi client devices.
- Place the AP away from electrical devices like these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - Base of a cordless phone
  - 2.4 GHz and 5.8 GHz cordless phones
- Place the AP away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
  - Solid metal door
  - Aluminum studs
  - Fish tanks
  - Mirrors
  - Brick
  - Concrete

If other access points are nearby, consider using different radio frequency channels to reduce interference (see Change the channel for a radio on page 155).

Safety instructions and warnings for an indoor access point

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions:

- This product is designed for indoor use only in a temperature-controlled and humidity-controlled environment. Note the following:
  - For more information about the environment in which this product must operate, see the environmental specifications in the appendix or the data sheet.
  - If you want to connect the product over an Ethernet cable to a device located outdoors, the outdoor device must be properly grounded and surge protected, and you must install an Ethernet surge protector inline between the indoor product and the outdoor device. Failure to do so can damage the product.
  - Before connecting the product to outdoor cables or wired outdoor devices, see https://kb.netgear.com/000057103 for additional safety and warranty information.

  Failure to follow these guidelines can result in damage to your NETGEAR product, which might not be covered by NETGEAR's warranty, to the extent permissible by applicable law.
- Do not service the product except as explained in your product documentation. Some devices should never be opened.
- If any of the following conditions occur, unplug the product from its power source, and then replace the part or contact your trained service provider:
  - Depending on your product, the power adapter, power adapter cable, power adapter plug, or PoE Ethernet cable is damaged.
  - An object fell into the product.
  - The product was exposed to water.
  - The product was dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep the product away from radiators and heat sources. Also, do not block cooling vents.

- Do not spill food or liquids on your product components, and never operate the product in a wet environment. If the product gets wet, see the appropriate section in your troubleshooting guide, or contact your trained service provider.
- Do not push any objects into the openings of your product. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- If applicable to your product, allow the product to cool before removing covers or touching internal components.
- Be sure that devices that are attached over Ethernet cables are electrically rated to operate with the power available in your location.
- Depending on your product, use only the supplied power adapter or an Ethernet cable that provides PoE.
  If your product uses a power adapter:
  - If you were not provided with a power adapter, contact your local NETGEAR reseller.
  - The power adapter must be rated for the product and for the voltage and current marked on the product electrical ratings label.
- To help prevent electric shock, plug any system and peripheral power cables into properly grounded power outlets.
- If applicable to your product, the peripheral power cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a three-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables, power adapter cables, and PoE Ethernet cables carefully. Route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power adapters, power adapter cables, or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local and national wiring rules.

2

Hardware Overview Model WAX202

The NETGEAR WiFi 6 AX1800 Dual Band Access Point Model WAX202 is an indoor, standalone AP that supports a combined throughput of 1.8 Gbps (600 Mbps at 2.4 GHz and 1200 Mbps at 5 GHz).

The Gigabit WAN port lets you connect the AP to a modem, gateway, router, or Ethernet outlet for Internet connectivity.

Use the three Gigabit LAN ports to connect network devices through an Ethernet cable directly to the AP.

The chapter contains the following sections:

Note: In this chapter, we refer to the access point as the AP.

Front panel with LEDs

The seven status LEDs are located on the front panel of the AP. From top to bottom, the front panel contains the Power LED, Internet LED, LAN LEDs 1–3, 2.4 GHz WLAN LED, and 5 GHz WLAN LED.

Figure 1. Front panel with LEDs, model WAX202

Table 2. LED descriptions, model WAX202

LED	Description
Power	**Solid green**: The AP is ready. **Blinking amber**: The AP is starting, the firmware is being updated, or the AP was reset to factory default settings. **Off**: Power is not supplied to the AP.
Internet	**Solid green**: An Internet connection is established. **Off**: No Internet connection exists, for example, because no cable is inserted in the WAN port.

Table 2. LED descriptions, model WAX202 (Continued)

LED	Description
LAN 1–3 1	**Solid green**: The LAN port functions at 1 Gbps speed and is connected to a device that is turned on. **Blinking green**: The LAN port is sending or receiving traffic at 1 Gbps speed. **Solid amber**: The LAN port functions at 10 or 100 Mbps speed and is connected to a device that is turned on. **Blinking amber**: The LAN port is sending or receiving traffic at 10 or 100 Mbps speed. **Off**: The LAN port is not connected to a device or the device to which the LAN port is connected is not turned on.
2.4 GHz WLAN 2.4GHz	**Solid green**: The 2.4 GHz radio is operating without clients. **Solid blue**: The 2.4 GHz radio is operating with clients but is not transmitting or receiving data. **Blinking blue**: The 2.4 GHz radio is operating with clients and is transmitting or receiving data. **Off**: The 2.4 GHz radio is off. For more information, see One or both WLAN LEDs are off on page 194.
5 GHz WLAN 5GHz	**Solid green**: The 5 GHz radio is operating without clients. **Solid blue**: The 5 GHz radio is operating with clients but is not transmitting or receiving data. **Blinking blue**: The 5 GHz radio is operating with clients and is transmitting or receiving data. **Off**: The 5 GHz radio is off. For more information, see One or both WLAN LEDs are off on page 194.

Back panel

The back panel of the AP provides Gigabit Ethernet ports, a Reset button, and a DC power connector.

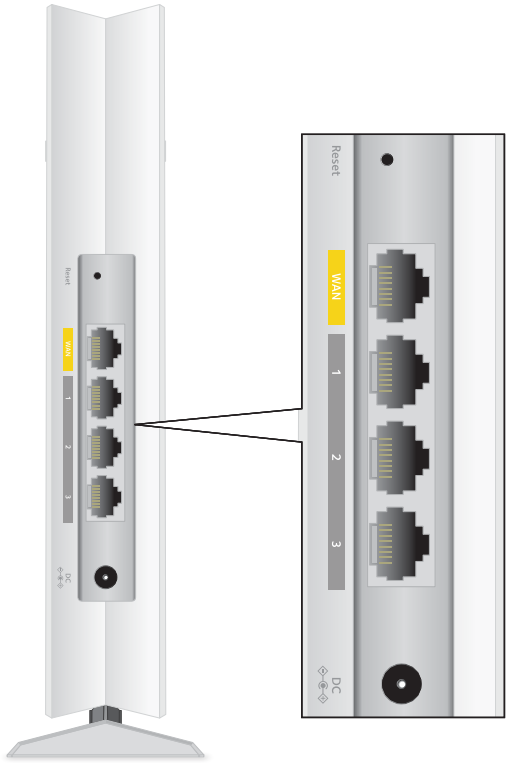

Figure 2. Back panel, model WAX202

Viewed from top to bottom, the back panel of model WAX202 contains the following components:

- **Reset button**. Press the **Reset** button to reset the AP to factory default settings. For more information, see Use the Reset button to return the AP to factory defaults on page 121.
- **WAN port**. One Gigabit (1 Gbps) Ethernet port with a yellow label that functions as a WAN (Internet) port to connect the AP to a modem, a router, or an Ethernet wall outlet that provides Internet service:
  - **Connect to a modem**: Connect the WAN port directly to a broadband, cable, or DSL device that is a modem. The modem must provide an Internet connection to the AP. For more information about this setup, in which the AP must function

in router mode, see Connect the AP to a modem and log in for the first time on page 32.

- **Connect to a router**: Connect the WAN port directly to a broadband, cable, or DSL device that is a router (for example, the device also provides WiFi), to another router in your network, or to a switch or hub that is connected to the router. For more information about this setup, in which the AP must function in AP mode, see Connect the AP to a routing device and log in for the first time on page 28.
- **Connect to an Ethernet wall outlet with Internet service**: Connect the WAN port directly to your Ethernet wall outlet. If you want to set up a WiFi 6 hotspot on an existing network, see Connect the AP to a routing device and log in for the first time on page 28. If you want to set up a private WiFi 6 network, see Connect the AP to a modem and log in for the first time on page 32.

- **LAN ports 1 through 3**: Three Gigabit Ethernet RJ-45 LAN ports numbered LAN 1 through LAN 3 to connect the AP to Ethernet devices such as a computer, printer, and switch.
- **DC power connector**: Connect the power adapter that came in the product package to the DC power connector.

AP label

The AP label on the bottom panel of the AP shows the default login information, default WiFi network name (SSID), default WiFi passphrase, serial number and MAC address of the AP, and other information.

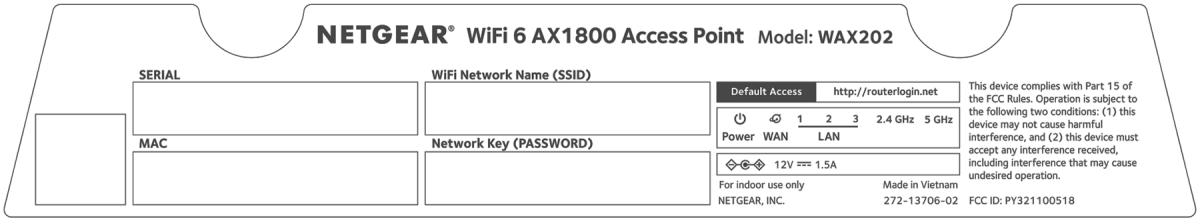

Figure 3. AP label, model WAX202

3

Hardware Overview Model WAX206

The NETGEAR WiFi 6 AX3200 Dual Band Access Point Model WAX206 is an indoor, standalone AP that supports a combined throughput of 3.2 Gbps (800 Mbps at 2.4 GHz and 2400 Mbps at 5 GHz).

The 2.5 Gbps WAN port lets you connect the AP to a modem, gateway, router, or Ethernet outlet for Internet connectivity.

IMPORTANT: The AP can provide an Internet connection with a speed of up to 2.4 Gbps to high-speed clients on the 5 GHz radio. To achieve this Internet speed, the AP's 2.5 Gbps WAN port must be connected to a 2.5 Gbps modem, gateway, router, or Ethernet outlet that supports 2.5 Gbps Internet service, using a Cat5E or higher-rated Ethernet cable.

Use the four Gigabit LAN ports to connect network devices through an Ethernet cable directly to the AP.

The chapter contains the following sections:

Note: In this chapter, we refer to the access point as the AP.

Front panel with LEDs

The seven status LEDs are located on the front panel of the AP. From top to bottom, the front panel contains the Power LED, Internet LED, LAN LEDs 1–4, 2.4 GHz WLAN LED, and 5 GHz WLAN LED.

Figure 4. Front panel with LEDs, model WAX206

Table 3. LED descriptions, model WAX206

LED	Description
Power	**Solid green**: The AP is ready. **Blinking amber**: The AP is starting, the firmware is being updated, or the AP was reset to factory default settings. **Off**: Power is not supplied to the AP.
Internet	**Solid green**: An Internet connection is established. **Off**: No Internet connection exists, for example, because no cable is inserted in the WAN port.

Table 3. LED descriptions, model WAX206 (Continued)

LED	Description
LAN 1–4 1	**Solid green**: The LAN port functions at 1 Gbps speed and is connected to a device that is turned on. **Blinking green**: The LAN port is sending or receiving traffic at 1 Gbps speed. **Solid amber**: The LAN port functions at 10 or 100 Mbps speed and is connected to a device that is turned on. **Blinking amber**: The LAN port is sending or receiving traffic at 10 or 100 Mbps speed. **Off**: The LAN port is not connected to a device or the device to which the LAN port is connected is not turned on.
2.4 GHz WLAN 2.4GHz	**Solid green**: The 2.4 GHz radio is operating without clients. **Solid blue**: The 2.4 GHz radio is operating with clients but is not transmitting or receiving data. **Blinking blue**: The 2.4 GHz radio is operating with clients and is transmitting or receiving data. **Off**: The 2.4 GHz radio is off. For more information, see One or both WLAN LEDs are off on page 194.
5 GHz WLAN 5GHz	**Solid green**: The 5 GHz radio is operating without clients. **Solid blue**: The 5 GHz radio is operating with clients but is not transmitting or receiving data. **Blinking blue**: The 5 GHz radio is operating with clients and is transmitting or receiving data. **Off**: The 5 GHz radio is off. For more information, see One or both WLAN LEDs are off on page 194.

Back panel

The back panel of the AP provides Gigabit Ethernet ports, a Reset button, and a DC power connector.

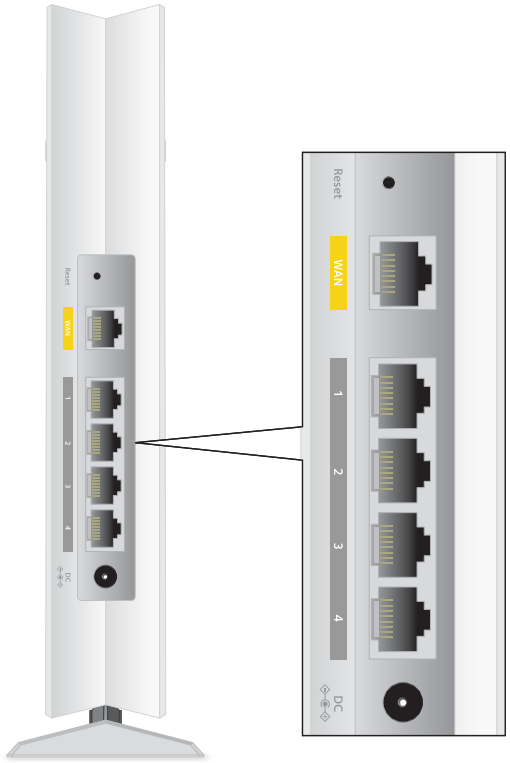

Figure 5. Back panel, model WAX206

Viewed from top to bottom, the back panel of model WAX206 contains the following components:

- **Reset button**. Press the **Reset** button to reset the AP to factory default settings. For more information, see Use the Reset button to return the AP to factory defaults on page 121.
- **WAN port**. One 2.5 Gbps Ethernet port with a yellow label that functions as a WAN (Internet) port to connect the AP to a modem, a router, or an Ethernet wall outlet that provides Internet service:
  - **Connect to a modem**: Connect the WAN port directly to a broadband, cable, or DSL device that is a modem. The modem must provide an Internet connection to the AP. For more information about this setup, in which the AP must function

in router mode, see Connect the AP to a modem and log in for the first time on page 32.

- **Connect to a router**: Connect the WAN port directly to a broadband, cable, or DSL device that is a router (for example, the device also provides WiFi), to another router in your network, or to a switch or hub that is connected to the router. For more information about this setup, in which the AP must function in AP mode, see Connect the AP to a routing device and log in for the first time on page 28.
- **Connect to an Ethernet wall outlet with Internet service**: Connect the WAN port directly to your Ethernet wall outlet. If you want to set up a WiFi 6 hotspot on an existing network, see Connect the AP to a routing device and log in for the first time on page 28. If you want to set up a private WiFi 6 network, see Connect the AP to a modem and log in for the first time on page 32.

- **LAN ports 1 through 4**: Four Gigabit (1 Gbps) Ethernet RJ-45 LAN ports numbered LAN 1 through LAN 4 to connect the AP to Ethernet devices such as a computer, printer, and switch.
- **DC power connector**: Connect the power adapter that came in the product package to the DC power connector.

AP label

The AP label on the bottom panel of the AP shows the default login information, default WiFi network name (SSID), default WiFi passphrase, serial number and MAC address of the AP, and other information.

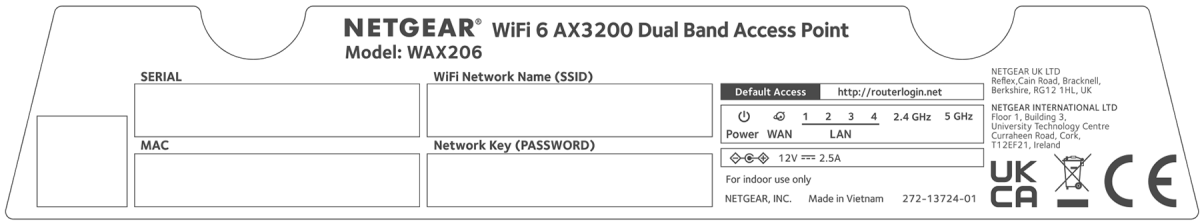

Figure 6. AP label, model, model WAX206

4

Installation and Initial Login

This chapter describes how you can install and access the AP in your network and log in to the local browser user interface (UI).

Depending on how you want to set up the AP in your environment, you can select the operation mode as AP mode or router mode. The AP setup options and their associated operation modes are also described in this chapter.

The chapter contains the following sections:

Note: In this chapter, we refer to the access point as the AP.

What WiFi setup do you want?

Use the following table to determine the type of WiFi setup that you want and the section that you must follow for your setup.

Table 4. What WiFi setup do you want?

What you have	What you want	Operation mode	Follow section
Broadband, cable, or DSL device with WiFi (router)	Add WiFi 6 to your home or office	AP mode	Connect the AP to a routing device and log in for the first time on page 28
Broadband, cable, or DSL device without WiFi (modem only)	Add WiFi 6 and a wired network to your home or office.	Router mode	Connect the AP to a modem and log in for the first time on page 32
Ethernet wall outlet with Internet service	Set up a WiFi 6 hotspot on an existing network.	AP mode	Connect the AP to a routing device and log in for the first time on page 28
	Set up a private WiFi 6 network.	Router mode	Connect the AP to a modem and log in for the first time on page 32

Note: By default, the operation mode is router mode. If you want to use AP mode, you can change the operation mode when you log in for the first time, as described in Connect the AP to a modem and log in for the first time on page 32.

For more information about AP mode and router mode, see About AP mode and router mode on page 26.

About AP mode and router mode

The AP is designed primarily to function as an access point, but can operate as a lightweight router behind another router to create an independent network segment. Your network and the WiFi setup that you want determine the operation mode that you must use for the AP.

Depending on your setup (see What WiFi setup do you want? on page 26), you can either change the operation mode to AP mode during the initial login procedure or keep the operation mode as router mode.

These are the differences between the operation modes:

- **AP mode**: The AP functions as a WiFi 6 access point and can support LAN clients through its LAN ports. The AP receives its IP address settings from a routing device in your network. The AP passes on the IP address settings from the routing device to its clients so that Internet access is provided.
  If you want to use AP mode, during the initial log-in process, change the operation mode from router mode to AP mode, as described in Connect the AP to a routing device and log in for the first time on page 28. If you already completed the initial log-in process, see Change the operation mode to AP mode or router mode on page 144.

  Note: In AP mode, the AP does not require routing features, so they are masked out in the device UI. For example, routing features such as NAT filtering and the DHCP server are disabled so that they do not interfere with the routing device in your network. For more information about the features that are enabled in router mode but not required in AP mode, see Routing features enabled in router mode on page 41.

- **Router mode**: The AP functions as both a lightweight router and WiFi 6 access point, and can support LAN clients through its LAN ports. Because the AP is connected to your modem, the AP receives its IP address settings from your Internet service provider (ISP). The AP delivers IP address settings to its clients so that Internet access is provided.
  If you want to use router mode, follow the initial log-in process as described in Connect the AP to a modem and log in for the first time on page 32.

Setup with an Ethernet wall outlet

If you have an Ethernet wall outlet that provides an Internet connection, you can connect the WAN port to the wall outlet and follow one of these procedures:

- **Set up a WiFi 6 hotspot on an existing network**: Follow the procedure that is described in Connect the AP to a routing device and log in for the first time on page 28 because the AP must operate in AP mode.
- **Set up a private WiFi 6 network**: Follow the procedure that is described in Connect the AP to a modem and log in for the first time on page 32 because the AP must operate in router mode.

Connect the AP to a routing device and log in for the first time

Use this procedure for the setups that are described in the following table:

Table 5. WiFi setups behind a routing device with the AP functioning in AP mode

What you have	What you want
Broadband, cable, or DSL device with WiFi (router)	Add WiFi 6 to your home or office
Gateway or regular router in your network	Add WiFi 6 to your home or office
Ethernet wall outlet with Internet service	Set up a WiFi 6 hotspot on an existing network.

You can also connect the AP to a switch or hub that is connected to one of the devices described in the previous table.

It is not common, but if your network includes an independent DHCP server, connect the AP to a switch or hub that is connected to the DHCP server.

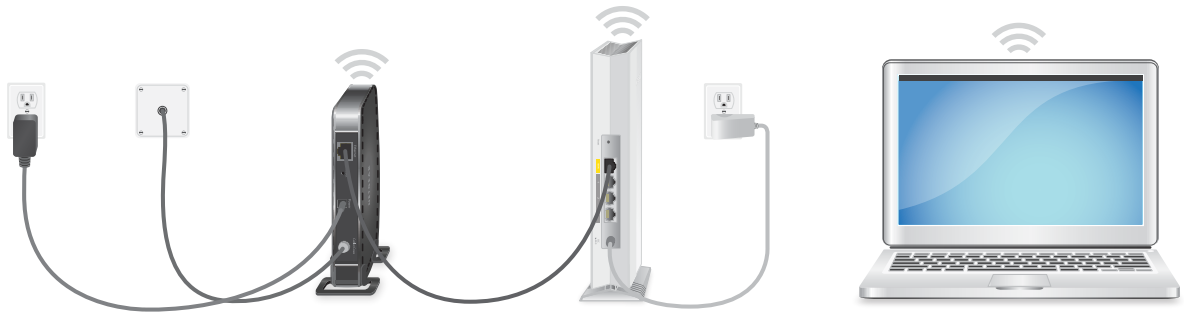

Figure 7. Connect the AP to a broadband, cable, or DSL router

Figure 8. Connect the AP to an Ethernet wall outlet with Internet service

IMPORTANT: Model WAX206 can provide an Internet connection with a speed of up to 2.4 Gbps to high-speed clients on the 5 GHz radio. To achieve this Internet speed, the AP's 2.5 Gbps WAN port must be connected to a 2.5 Gbps gateway, router, or Ethernet outlet that supports 2.5 Gbps Internet service, using a Cat5E or higher-rated Ethernet cable.

In the following procedure, we refer to the broadband, cable, or DSL router, the gateway or regular router, or the Ethernet wall outlet as the *routing device*.

To connect the AP to a routing device and log in to the device UI for the first time:

1. Connect an Ethernet cable to the yellow Internet port on the AP.
2. Connect the other end of the cable to a LAN port on your routing device.
3. Power on the AP.
   The Power LED blinks amber.
4. Wait about two minutes for the startup process to complete.
   The startup process is complete when the following happens:
   - The Power LED turns solid green.
   - The 2.4 GHz WLAN and 5 GHz WLAN LEDs light solid green.
5. Log in to the AP by using *one* of the following methods:
   - **Connect over WiFi**: On a WiFi-enabled computer or mobile device, find and connect to the AP's WiFi network (SSID).
     The default SSID and WiFi password (network key) are printed on the AP label.
   - **Connect over Ethernet directly to the AP**: Using an Ethernet cable, connect the LAN port on your computer directly to one of the LANs port on the AP.
6. Launch a web browser and enter **routerlogin.net** in the address field.
   You can also use **routerlogin.com**, **aplogin.net**, or **aplogin.com**.
   The Setup Wizard starts.
   Note the following:
   - Your browser might display a security warning because of the self-signed certificate on the AP, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
   - If the Setup Wizard still does not start, see You cannot log in to the AP [router mode] on page 195.
7. Follow the prompts.

Note: If the AP does not connect to the Internet, check the connection between the AP and your routing device.

While you follow the prompts, you must do the following:

a. **Select AP mode**: Because you are connecting the AP to a routing device, you must select AP mode (that is, select the **Access Point Mode** button).

b. **Set a new admin password**: You must set a new admin password (the local device password) and set answers to two security questions (you can choose the questions).

c. **Set a new WiFi network name (SSID) and WiFi password**: You can set a new WiFi network name (SSID) and WiFi password for the Wireless 1 network. This SSID and WiFi password replace the default SSID and WiFi password that are printed on the AP label.

d. **Update the firmware**: You can update the firmware (if new firmware is available).

At the end of the Setup Wizard process, your settings are saved and the AP is reconfigured in AP mode, and is assigned a new IP address by your routing device. The AP restarts.

Your WiFi-enabled computer or mobile device might be disconnected.

8. If your WiFi connection was terminated, reconnect to the AP.

   If you set a new WiFi network name (SSID) and WiFi password during the Setup Wizard process, use your new SSID and WiFi password to reconnect.

   The Local Device Login page displays.

9. If the Local Device Login page does not display, type **routerlogin.net** in the address field of your browser.

   If you experience connectivity problems, see You cannot log in to the AP [AP mode] on page 196.

10. Log in to the device UI again by entering your new local device password.

    This is the password that you set during the Setup Wizard process.

    The BASIC Home page displays. You can now configure and monitor the AP. In AP mode, the routing functions of the AP are masked out in the device UI.

11. Find the new IP address of the AP in the device UI by doing the following:

    a. Select **ADVANCED > ADVANCED Home**.
    The ADVANCED Home page of the AP displays. The LAN Port pane shows the IP address that is now assigned to the AP.

    b. Save the LAN IP address of the AP for later use.

You must use this IP address if you plan to connect to the same network as the AP but *not directly* to the AP network. For example, use this IP address if you connect over the LAN to the AP.
If you are directly connected to the AP over a WiFi connection or Ethernet connection to one of the LAN ports, you still can use **routerlogin.net**.

12. If you are using the AP in a country other than the U.S. or Canada (where the region is set and you cannot change it), set the country or region where you are using the AP by doing the following:
    a. Select **Advanced > Advanced Setup > Wireless Settings**.
    b. From the **Region** menu, select the country or region where you are using the AP.

       Note: Make sure that the country is set to the location where the device is operating. You are responsible for complying with the local, regional, and national regulations for channels, power levels, and frequency ranges.

    c. Click the **Apply** button.
       Your settings are saved and the AP is configured for the new country or region. Do not close the browser page. If you are connected over WiFi, your connection might be terminated.
    d. If you want to continue to configure the AP, reconnect to the AP (if you were connected over WiFi and your connection was terminated) and log back in to the device UI by entering your local device password.
       The BASIC Home page displays.
       The Home page displays various panes that let you see the status of your AP at a glance. You can now configure and monitor the AP.

Connect the AP to a modem and log in for the first time

Use this procedure for the setups that are described in the following table:

Table 6. WiFi setups behind a modem with the AP functioning in router mode

What you have	What you want
Broadband, cable, or DSL device without WiFi (modem only)	Add WiFi 6 and a wired network to your home or office.
Ethernet wall outlet with Internet service	Set up a private WiFi 6 network.

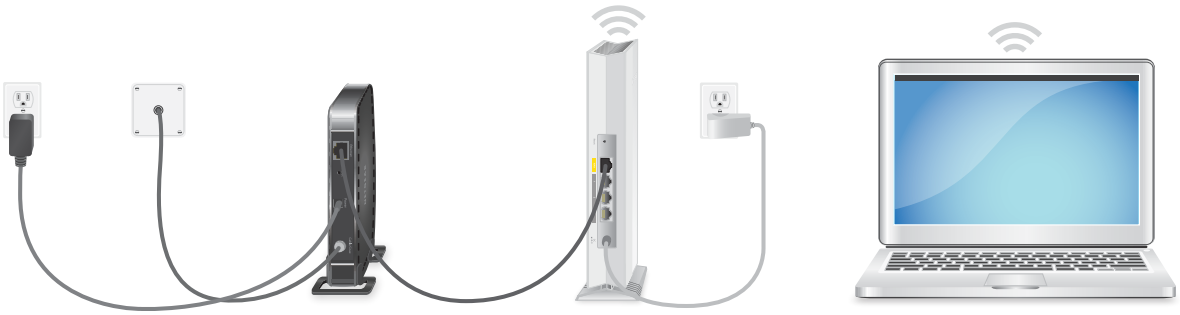

Figure 9. Connect the AP to your modem

Figure 10. Connect the AP to an Ethernet wall outlet with Internet service

When you set up the AP and connect it to your modem, the following applies, depending on the type of WAN connection your modem uses:

- **Dynamic DHCP**: If the type of WAN connection is dynamic DHCP, the AP automatically receives an IP address from your Internet service provider (ISP) and you do not need to provide any IP address information. This type of WAN connection is the most common.

- **PPPoE, PPTP, L2TP, or static IP address**: If the type of WAN connection is PPPoE, PPTP, or L2TP, or your Internet connection requires a static IP address, you must follow the prompts during the setup process and provide the required information for the Internet connection.

If you are not sure which type of WAN connection your Internet service uses, or if you do not have the required information, we recommend that you contact your ISP before you start the following procedure.

IMPORTANT: Model WAX206 can provide an Internet connection with a speed of up to 2.4 Gbps to high-speed clients on the 5 GHz radio. To achieve this Internet speed, the AP's 2.5 Gbps WAN port must be connected to a 2.5 Gbps modem or Ethernet outlet that supports 2.5 Gbps Internet service, using a Cat5E or higher-rated Ethernet cable.

To connect the AP to a modem and log in to the device UI for the first time:

1. Unplug your modem's power, leaving the modem connected to the wall jack for your Internet service.
2. If the modem uses a battery backup, remove the battery.
3. Connect the Ethernet cable to the yellow WAN port on the AP.
4. Connect the other end of the cable to a LAN port on your modem.
5. If the modem uses a battery backup, put the battery back in.
6. Plug in and turn on the modem.
7. Power on the AP.
   The Power LED blinks amber.
8. Wait about two minutes for the startup process to complete.
   The startup process is complete when the following happens:
   - The Power LED turns solid green.
   - The 2.4 GHz WLAN and 5 GHz WLAN LEDs light solid green.
9. Log in to the AP by using *one* of the following methods:
   - **Connect over WiFi**: On a WiFi-enabled computer or mobile device, find and connect to the AP's WiFi network (SSID).
     The default SSID and WiFi password (network key) are printed on the AP label.
   - **Connect over Ethernet directly to the AP**: Using an Ethernet cable, connect the LAN port on your computer directly to any of the LANs port on the AP.
10. Launch a web browser and enter **routerlogin.net** in the address field.

You can also use **routerlogin.com**, **aplogin.net**, or **aplogin.com**.

The Setup Wizard starts.

Note the following:

- Your browser might display a security warning because of the self-signed certificate on the AP, which is expected behavior. You can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
- If the Setup Wizard still does not start, see You cannot log in to the AP [router mode] on page 195.

11. Follow the prompts.

    While you follow the prompts, you must do the following:

    a. **Provide Internet settings that are assigned by your ISP**: If the WAN connection is PPPoE, PPTP, or L2TP, or your Internet connection requires a static IP address, provide the required information when you are prompted to do.
    If the AP does not connect to the Internet, see one of the following sections:

    - Check the Internet WAN IP address [router mode] on page 198
    - Check or manually start the PPPoE, PPTP, or L2TP connection [router mode] on page 200
    - Troubleshoot your Internet connection [router mode] on page 201

    b. **Select router mode**: Because you are connecting the AP to a modem, you must select router mode (that is, keep the **Router Mode** button selected).

    c. **Set a new admin password**: You must set a new admin password (the local device password) and set answers to two security questions (you can choose the questions).

    d. **Set a new WiFi network name (SSID) and WiFi password**: You can set a new WiFi network name (SSID) and WiFi password for the Wireless 1 network. This SSID and WiFi password replace the default SSID and WiFi password that are printed on the AP label.

    e. **Update the firmware**: You can update the firmware (if new firmware is available).

    At the end of the Setup Wizard process, the AP restarts. Do not close the browser page.

    Your WiFi-enabled computer or mobile device might be disconnected.

12. If your WiFi connection was terminated, reconnect to the AP.

    If you set a new WiFi network name (SSID) and WiFi password during the Setup Wizard process, use your new SSID and WiFi password to reconnect.

The Local Device Login page displays.

13. Log in again to the device UI by entering your new local device password.
    This is the password that you set during the Setup Wizard process.

    The BASIC Home page displays.

    The Home page displays various panes that let you see the status of your AP at a glance. You can now configure and monitor the AP.

14. If you are using the AP in a country other than the U.S. or Canada (where the region is set and you cannot change it), set the country or region where you are using the AP by doing the following:
    a. Select **Advanced > Advanced Setup > Wireless Settings**.
    b. From the **Region** menu, select the country or region where you are using the AP.

       Note: Make sure that the country is set to the location where the device is operating. You are responsible for complying with the local, regional, and national regulations for channels, power levels, and frequency ranges.

    c. Click the **Apply** button.
       Your settings are saved and the AP is configured for the new country or region. If you are connected over WiFi, your connection might be terminated.
    d. If you want to continue to configure the AP, reconnect to the AP (if you were connected over WiFi and your connection was terminated) and log back in to the device UI by entering your local device password.

How the operation mode affects how you can reach the device UI

The operation mode affects how you can reach the AP device UI:

- **Router mode**: Enter **routerlogin.net** in the address field of your browser. (You can also use **routerlogin.com**, **aplogin.net**, or **aplogin.com**.)
  In router mode, you always connect directly to the AP, whether use you a WiFi connection or a wired connection to a LAN port on the AP.
- **AP mode**: The method to reach the device UI depends on how you connect to the AP:
  - **Directly connected**: If you are directly connected over a WiFi connection or a wired connection to a LAN port on the AP, enter **routerlogin.net** in the address

field of your browser. (You can also use **routerlogin.com**, **aplogin.net**, or **aplogin.com**.)
One exception exists: If you assigned a static IP address to the AP, you must use *that* IP address to reach the device UI.

- **Connected over your LAN**: If you are connected to the same LAN that the AP is connected to but not directly to the AP, in the address field of your browser, enter the IP address that your existing router or DHCP server assigned to the AP. For more information, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
  Example 1: Your computer and AP are connected to a switch that is connected to your existing router, which assigns an IP address to your computer and AP. You must use the IP address that is assigned to the AP.
  Example 2: Your mobile device is connected to another access point in your network. *That* access point is connected to the same switch that the WAX202 or WAX206 AP is connected to, and the switch is connected to your existing router. You must use the IP address that is assigned to the WAX202 or WAX206 AP.

Find the IP address of the AP when you cannot use routerlogin.net

Under the following circumstances, when the AP is operating in AP mode, you cannot use **routerlogin.net** (or **routerlogin.com**, **aplogin.net**, or **aplogin.com**) to log in to the AP:

- Your computer or mobile device is not directly connected to the AP network even if it is on the same LAN as the AP. (For more information, see How the operation mode affects how you can reach the device UI on page 35.)
- Your computer or mobile device *is* directly connected to the AP, but the AP is using a static IP address.

  Note: If the AP can reach its DNS server only over the Internet (for example, the IP address of the DNS server is 8.8.8.8), you cannot use **routerlogin.net**. However, if the DNS server is the IP address of the router to which the AP connects but the router's Internet connection is down, you *can* use **routerlogin.net** because the AP can still reach the router.

- Your network includes another NETGEAR device that is also accessible by using **routerlogin.net**. In such a situation, if you use **routerlogin.net**, you might log in to the AP or you might log in to the other NETGEAR device, depending on your network situation.

In these situations, use the IP address that was assigned to the AP by your router during the setup process (see Connect the AP to a routing device and log in for the first time on page 28) to log in to the device UI of the AP.

If you do not know the IP address that was assigned to the AP, use *one* of the following options to find the IP address of the AP:

- Only if the AP is connected to the Internet, do one of the following:
  - **Option 1. Temporarily connect directly and log in**: Temporarily connect a computer directly either through an Ethernet cable or over WiFi or a mobile device over WiFi to the AP and do the following:
    1. Launch a web browser and enter **routerlogin.net** in the address field.
       The Local Device Login page displays.
       If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
    2. Enter the AP local device password.
       The local device password is the one that you specified. The local device password is case-sensitive.
       The BASIC Home page displays.
    3. Select **ADVANCED**.
       The ADVANCED Home page displays
    4. In the LAN Port pane, click the **CONNECTION STATUS** button.
       The IP Address field displays the IP address that is assigned to the AP.

  - **Option 2. Temporarily connect directly and ping the AP**: Temporarily connect a computer or mobile device directly through an Ethernet cable or over WiFi to the AP and send a ping to **www.routerlogin.net**.
    How to send a ping depends on your computer or mobile device.
    On your computer or mobile device, the field with the ping results displays the IP address that is assigned to the AP.

- Regardless of whether the AP is connected to the Internet, do one of the following:
  - **Option 1. Access your modem or existing router**: Access the DHCP server information of your modem or existing router to see the devices that are connected to it, including the AP. The IP address that is assigned to the AP is listed.
  - **Option 2. Use an IP scanner**: Use an IP scanner application (they are available free of charge on the Internet) in the network of your existing router. The IP scanner results include the IP address that is assigned to the AP.

If you made a direct connection to the AP, you can now terminate that connection. Connect your computer or mobile device to the same network as the AP, and use the discovered IP address to log in to the AP.

Log in to the AP after you complete the initial log-in process

After you complete the initial log-in process, the AP is ready for use and you can change the settings and monitor the traffic.

Note: You can use any of the following domain names to log in to the AP device UI: **routerlogin.net**, **routerlogin.com**, **aplogin.net**, and **aplogin.com**. The procedures in this manual use **routerlogin.net**. For information about exceptions to using these domain names, see How the operation mode affects how you can reach the device UI on page 35.

To log in to the AP's device UI after you complete the initial log-in process:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

The Device Status page displays various panes that let you see the status of your AP at a glance. You can now configure and monitor the AP.

Change the language

By default, the language of the device UI is set as Auto. You can change the language.

To change the language:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. In the upper right corner, select a language from the menu.
   The page refreshes with the language that you selected.

Connect a wired or WiFi device to the AP's network after installation

After you install the AP in your network (see Connect the AP to a routing device and log in for the first time on page 28 or Connect the AP to a modem and log in for the first time on page 32), you can connect devices to the AP's LAN through Ethernet cables or to the AP's WiFi network over a WiFi connection.

If the device that you are trying to connect is set up to use a static IP address, change the settings of your device so that it uses Dynamic Host Configuration Protocol (DHCP) and can receive an IP address through or from the AP.

Note: Connecting to the AP's network is not the same as connecting to the device UI to view or manage the AP's settings. For information about logging in to the AP device UI, see Log in to the AP after you complete the initial log-in process on page 38.

Join a WiFi network on the AP

You can manually add a WiFi device such as a WiFi-enabled computer, tablet, or smartphone to a WiFi network of the AP.

On the WiFi device that you want to connect to the AP, use the software application that manages your WiFi connections.

Note: By default, the AP's Wireless 1 network is enabled but the Wireless 2 and Wireless 3 networks are disabled.

To connect a device to a WiFi network on the AP:

1. Make sure that the AP is receiving power (its Power LED is solid green) and is connected to the Internet (the Internet LED is solid green), and that the 2.4 GHz and 5 GHz WLAN LEDs are solid green).
2. On the WiFi device, open the software application that manages your WiFi connections.

   This application scans for all WiFi networks in your area.
3. Look for one of the AP's WiFi networks and select it.

   For the Wireless 1 network, if you set a new SSID during the initial log-in process, use *that* SSID. If you did not set a new SSID, use the default SSID that is printed on the AP label.
4. Enter the WiFi password for WiFi access.

   For the Wireless 1 network, if you set a new WiFi password (network key) during the initial log-in process, use *that* WiFi password. If you did not set a new WiFi password, use the default WiFi password that is printed on the AP label.
5. Click the **Connect** button.

   The device connects to the WiFi network of the AP.

Connect to the AP through an Ethernet cable

You can connect a computer or other LAN device such as a switch to the AP using an Ethernet cable and join the AP's local area network (LAN).

To connect a computer or LAN device to the AP with an Ethernet cable:

1. Make sure that the AP is receiving power and is connected to the Internet (both its Power LED and Internet LED are solid green).
2. Connect an Ethernet cable to an Ethernet port on the computer or LAN device.
3. Connect the other end of the Ethernet cable to one of the LAN ports on the AP.

   You can use any of the LAN ports on the AP.

   Note: You can also connect the computer to a switch or hub that is connected to one of the LAN ports on the AP.

   The AP LAN LED for the port to which you attached the device lights solid green. Your computer or LAN device connects to the local area network (LAN).

Routing features enabled in router mode

The AP can function in router mode (its default operation mode) or in AP mode.

When the AP is in router mode, the following routing features are enabled in the device UI:

- Internet settings, including an IP address issued through dynamic DHCP (the default setting), an IP address issued through PPPoE, L2TP, or PPTP, or a manually specified static IP address.
- WAN settings, including routing services such as NAT.
- LAN settings, including a DHCP server.
- The option to block services and applications.
- The option to set up port forwarding and port triggering
- The option to set up static routes.
- Universal Plug and Play (UPnP).
- The option to enable the traffic meter.

Note: In AP mode, these features are not required because they can be provided by the routing device to which the AP connects. Therefore, in AP mode, these features are masked out in the device UI.

What to do if you get a browser security warning

When you enter **routerlogin.net** (or **routerlogin.com**, **aplogin.net**, or **aplogin.com**) in the address field of your browser, a security warning might display because of the self-signed certificate on the device. This is expected behavior. You can proceed, or add an exception for the security warning.

To proceed with a security warning or add an exception for a security warning:

- **Google Chrome**: Click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the domain name or IP address of the device.
- **Apple Safari**: Click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
- **Mozilla Firefox**: Click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Edge**: Select **Details > Go on to the webpage**.
- **Microsoft Internet Explorer**: Click the **Continue to this website (not recommended)** link.

5

Manually Set Up Internet Settings [Router Mode]

This chapter describes how you can manually set up the Internet connection for your AP in router mode (the default operation mode).

Note: In AP mode, the Internet settings that are described in this chapter are not required because they can be provided by the routing device to which the AP connects. Therefore, in AP mode, these Internet settings are masked out in the device UI.

Usually, the quickest way to set up the Internet connection is to allow the Setup Wizard to detect the Internet connection when you go through the initial log-in process. After initial setup, you can use the Setup Wizard at any time. If you prefer to specify the Internet setup yourself, you can enter the WAN IP address settings instead of using the Setup Wizard.

This chapter contains the following sections:

Note: In this chapter, we refer to the access point as the AP.

Use the Setup Wizard [router mode]

In most situations, you do not need use the Setup Wizard in the device UI. In some situations, you might want to use the Setup Wizard to redetect your Internet settings.

After the initial setup and login procedure (see Installation and Initial Login on page 25), if AP is in router mode, you can use the Setup Wizard to redetect your Internet settings. Using the Setup Wizard in the device UI is much easier than resetting your AP to factory default settings and going through the initial login procedure.

Note: The Setup Wizard is not required if the AP is operating in AP mode and is therefore masked out in the device UI.

The Setup Wizard detects your Internet setting through the AP's network connection to your modem, gateway, or Ethernet outlet with Internet connection. The Setup Wizard detects the WAN IP address assigned by your Internet service provider (ISP), and automatically adjusts the settings for your AP to access the Internet.

To use the Setup Wizard:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Setup Wizard**.

   The Setup Wizard page displays.

5. Select the **Yes** radio button.
6. Click the **Next** button.

   The Setup Wizard searches your Internet connection for servers and protocols to determine your Internet configuration. When the AP connects to the Internet, you are prompted to change the local device password (also referred to as the admin password).

Manually set up the AP Internet connection [router mode]

If the AP is in router mode, you can view or change the AP's Internet connection settings.

Note: The information in the following sections is not required if the AP is operating in AP mode. In AP mode, the Internet settings can be provided by the routing device to which the AP connects. Therefore, in AP mode, these Internet settings are masked out in the device UI.

Specify a dynamic or fixed WAN IP address Internet connection without a login [router mode]

Usually, the quickest way to set up a dynamic or fixed Internet connection is to allow the Setup Wizard to detect the Internet connection when you go through the initial log-in process as described in Connect the AP to a modem and log in for the first time on page 32 or, *after* initial setup, in Use the Setup Wizard [router mode] on page 44.

After you install the AP and it is in router mode, you can manually specify the dynamic or fixed Internet connection or change it. (These dynamic and fixed IP settings are not required if the AP is operating in AP mode.)

For this procedure, use the settings that your Internet service provider (ISP) gave you. If you are not sure, contact your ISP.

To specify or view the settings for a WAN Internet connection that uses a dynamic or fixed IP address and that does not require a login:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **BASIC > Internet**.
   The Internet Setup page displays.
5. Select the **No** radio button.
   This is the default setting.
6. If your Internet connection requires an account name (sometimes referred to as a host name), enter it in the **Account Name** field.
   The account name is the same as the device name, which, by default, is the model number of your AP.
7. If your Internet connection requires a domain name, enter it in the **Domain Name (if Required)** field.
   For the other sections on this page, the default settings usually work, but you can change them.
8. Select an Internet IP Address radio button:
   - **Get Dynamically from ISP**: Your ISP uses DHCP to automatically assign an IP address and related settings to the AP.
   - **Use Static IP Address**: Enter the static IP address, IP subnet mask, and gateway IP address that your ISP assigned to the AP. The gateway is the ISP router to which the AP connects.
9. Select a Domain Name Server (DNS) Address radio button:
   - **Get Automatically from ISP**: Your ISP uses DHCP to assign DNS servers to the AP.
   - **Use These DNS Servers**: If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If IP addresses for a second and a third DNS server are available, enter them also.
10. Specify which MAC address to use for the Internet connection.
    A MAC address is a unique 12-digit hexadecimal number that identifies each network device. A device's MAC address always stays the same. It does not change the way an IP address can.
    - **Use Default Address**: Use the default AP MAC address that displays on the Dashboard page and is on the AP label.
    - **Use Computer MAC Address**: The AP captures and uses the MAC address of the computer that you are now using to change the settings. Sometimes an ISP allows the MAC address of a particular computer only.
    - **Use This MAC Address**: Enter a MAC address that must be used. Sometimes an ISP allows the MAC address of a particular computer only.

11. If your ISP gave you a vendor class identifier (VCI) string, enter it in the **Vendor Class Identifier String (option 60)** field.

    If your ISP did not give you a VCI string, leave this field blank.

12. If your ISP gave you a client identifier (client ID) string, enter it in the **Client Identifier String (option 61)** field.

    If your ISP did not give you a client ID string, leave this field blank.

13. Click the **Apply** button.

    Your settings are saved.

14. Click the **Test** button to test your Internet connection.

    If the NETGEAR website does not display within one minute, see one of the following sections:

    - Check the Internet WAN IP address [router mode] on page 198
    - Troubleshoot your Internet connection [router mode] on page 201

Specify a PPPoE Internet connection that uses a login [router mode]

Usually, the quickest way to set up a PPPoE Internet connection is to allow the Setup Wizard to detect the Internet connection when you go through the initial log-in process as described in Connect the AP to a modem and log in for the first time on page 32 or, *after* initial setup, in Use the Setup Wizard [router mode] on page 44.

After you install the AP and it is in router mode, you can manually specify the PPPoE Internet connection or change it. (These PPPoE settings are not required if the AP is operating in AP mode.)

For this procedure, use the settings that your Internet service provider (ISP) gave you. If you are not sure, contact your ISP.

To specify or view the settings for an ISP Internet connection that uses PPPoE and that requires a login:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **BASIC > Internet**.
   The Internet Setup page displays.
5. Select the **Yes** radio button.
   The settings on the page change.
6. From the **Internet Service Provider** menu, select **PPPoE** as the encapsulation method.
7. In the **Login** field, enter the login name that your ISP gave you.
   This login name is often an email address.
8. In the **Password** field, enter the password that you use to log in to your Internet service.
9. If your ISP requires a service name, type it in the **Service Name (if Required)** field.
10. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
11. If you select **Dial on Demand** from the **Connection Mode** menu, in the **Idle Timeout** field, enter the number of minutes until the Internet login times out
    This time is how long the AP keeps the Internet connection active when no one on the network is using the Internet connection. A value of 0 (zero) means never log out. The default is 5 minutes.
12. Select an Internet IP Address radio button:
    - **Get Dynamically from ISP**: Your ISP uses DHCP to automatically assign an IP address and related settings to the AP.
    - **Use Static IP Address**: Enter the static IP address that your ISP assigned to you.
13. Select a Domain Name Server (DNS) Address radio button:
    - **Get Automatically from ISP**: Your ISP uses DHCP to assign DNS servers to the AP.
    - **Use These DNS Servers**: If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
14. Specify which MAC address to use for the Internet connection.

A MAC address is a unique 12-digit hexadecimal number that identifies each network device. A device's MAC address always stays the same. It does not change the way an IP address can.

- **Use Default Address**: Use the default AP MAC address that displays on the Dashboard page and is on the AP label.
- **Use Computer MAC Address**: The AP captures and uses the MAC address of the computer that you are now using to change the settings. Sometimes an ISP allows the MAC address of a particular computer only.
- **Use This MAC Address**: Enter a MAC address that must be used. Sometimes an ISP allows the MAC address of a particular computer only.

15. Click the **Apply** button.
    Your settings are saved.
16. Click the **Test** button to test your Internet connection.
    If the NETGEAR website does not display within one minute, see one of the following sections:
    - Check or manually start the PPPoE, PPTP, or L2TP connection [router mode] on page 200
    - Troubleshoot your Internet connection [router mode] on page 201

Specify a PPTP or L2TP Internet connection that uses a login [router mode]

Usually, the quickest way to set up a PPTP or L2TP Internet connection is to allow the Setup Wizard to detect the Internet connection when you go through the initial log-in process as described in Connect the AP to a modem and log in for the first time on page 32 or, *after* initial setup, in Use the Setup Wizard [router mode] on page 44.

After you install the AP and it is in router mode, you can manually specify the PPTP or L2TP Internet connection or change it. (These PPTP and L2TP settings are not required if the AP is operating in AP mode.)

For this procedure, use the settings that your Internet service provider (ISP) gave you. If you are not sure, contact your ISP.

To specify or view the settings for an ISP Internet connection that uses PPTP or L2TP and that requires a login:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **BASIC > Internet**.

   The Internet Setup page displays.

5. Select the **Yes** radio button.

   The settings on the page change.

6. From the **Internet Service Provider** menu, select **PPTP** or **L2TP** as the encapsulation method.
7. In the **Login** field, enter the login name that your ISP gave you.

   This login name is often an email address.

8. In the **Password** field, enter the password that you use to log in to your Internet service.
9. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
10. If you select **Dial on Demand** from the **Connection Mode** menu, in the **Idle Timeout** field, enter the number of minutes until the Internet login times out

    This time is how long the router keeps the Internet connection active when no one on the network is using the Internet connection. A value of 0 (zero) means never log out. The default is 5 minutes.

11. If your ISP gave you fixed IP addresses and a connection ID or name, enter them in the **My IP Address**, **IP Subnet Mask**, **Server Address**, **Gateway IP Address**, and **Connection ID/Name** fields.

    If your ISP did not give you an IP addresses, a connection ID, or name, leave these fields blank. The connection ID or name applies to a PPTP service only.

12. Select a Domain Name Server (DNS) Address radio button:

    - **Get Automatically from ISP**. Your ISP uses DHCP to assign DNS servers to the AP.
    - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

13. Select a Router MAC Address radio button:

    A MAC address is a unique 12-digit hexadecimal number that identifies each network device. A device's MAC address always stays the same. It does not change the way an IP address can.

    - **Use Default Address**. Use the default AP MAC address that displays on the Dashboard page and is on the AP label.
    - **Use Computer MAC Address**. The AP captures and uses the MAC address of the computer that you are now using to change the settings. Sometimes an ISP allows the MAC address of a particular computer only.
    - **Use This MAC Address**. Enter a MAC address that must be used. Sometimes an ISP allows the MAC address of a particular computer only.

14. Click the **Apply** button.

    Your settings are saved.

15. Click the **Test** button to test your Internet connection.

    If the NETGEAR website does not display within one minute, see one of the following sections:

    - Check or manually start the PPPoE, PPTP, or L2TP connection [router mode] on page 200
    - Troubleshoot your Internet connection [router mode] on page 201

6

Basic WiFi and Radio Features

This chapter describes how you can manage the basic WiFi and radio settings of the AP. For information about the advanced WiFi and radio settings, see Advanced WiFi and Radio Features on page 149.

Note: If you want to change the WiFi network settings, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

The chapter includes the following sections:

Note: In this chapter, we refer to the access point as the AP.

Set up or change an open or secure WiFi network

The AP has three WiFi networks (Wireless 1, Wireless 2, and Wireless 3). By default, the Wireless 1 network is enabled and the other two WiFi networks are disabled. The default security is WPA2-Personal [AES].

Table 7. WiFi networks

WiFi network	Default status	Default SSID	Default WiFi password
Wireless 1	Enabled	Unique, see label.	Unique, see label.
Wireless 2	Disabled	NETGEARXXXXXX-2	Unique, see label (same password as Wireless 1).
Wireless 3	Disabled	NETGEARXXXXXX-3	Unique, see label (same password as Wireless 1).

In the previous table, XXXXXX represents the last six digits of the MAC address of the AP. (A MAC address is a unique 12-digit hexadecimal number that identifies each network device.) The default SSID and WiFi password (network key) for the Wireless 1 network are printed on the AP label. During the initial login, you are prompted to change the default SSID and WiFi password for the Wireless 1 network.

Note: If you change the WiFi password for the Wireless 1 network, the default WiFi password for the Wireless 2 network and Wireless 3 network does not change and is still the password that is printed on the AP label.

For each WiFi network, the AP simultaneously supports the 2.4 GHz band for 802.11b/g/n/ax devices and the 5 GHz band for 802.11a/n/ac/ax devices.

For the 2.4 GHz band, the default WiFi throughput mode is 600 Mbps (model WAX202) or 800 Mbps (model WAX206). For the 5 GHz band, it is 1200 Mbps (model WAX202) or 2400 Mbps (model WAX206). You can change (lower) the WiFi throughput mode (see Change the WiFi throughput mode on model WAX202 on page 157).

You can view or change the WiFi settings and WiFi security for the Wireless 1 network, and you can enable and set up the Wireless 2 and Wireless 3 networks.

Note: For security, we recommend that you do change the names of the default SSIDs and the default WiFi passwords.

To set up or change an open or secure WiFi network:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **BASIC > Wireless**.

   The Wireless Network page displays.

   For information about SSID isolation, see Manage SSID isolation for all WiFi networks on page 65.
5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
6. To enable the selected WiFi network, select the **Enable** radio button.

   By default this radio button is selected for the Wireless 1 network but the **Disable** radio button is selected for the Wireless 2 and Wireless 3 networks.
7. To change the name of the SSID, in the **Name (SSID)** field, enter a 32-character (maximum), case-sensitive name.

   The SSID (service set identifier) is the WiFi network name. If you did not change the SSID, the default SSID displays, in which XXXXXX represents the last six digits of the MAC address of the AP:
   - **Wireless 1**: If you did not change the default SSID, the SSID *is* the default SSID that is printed on the AP label.
   - **Wireless 2**: NETGEARXXXXXX-2

- **Wireless 3**: NETGEARXXXXXX-3

8. To set up or change the AP WiFi security for the selected WiFi network, select the type of security from the **Security Options** menu, and configure the settings as described in the following table.

Setting	Description
None	An open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use an open WiFi network but configure WiFi security. However, an open network might be appropriate for a WiFi hotspot.
WPA2 Personal [AES]	This option, which is the same as WPA2-PSK, is the default setting and uses AES encryption. This type of security enables only WiFi devices that support WPA2 or WPA3 to join the WiFi network. WPA2 provides a secure connection but some legacy WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select **WPA-Personal [TKIP] + WPA2-Personal [AES]** authentication. In the **Password (Network Key)** field, enter a phrase of 8 to 63 characters or 64 hexadecimal digits. To join the WiFi network, a user must enter this password. To view the password in clear text, click the **eye** icon.
WPA-Personal [TKIP] + WPA2-Personal [AES]	This option, which is the same as WPA2-PSK/WPA-PSK, enables WiFi devices that support either WPA, WPA2, or WPA3 to join the WiFi network. This option uses AES and TKIP encryption. WPA-PSK (which uses TKIP) is less secure than WPA2-PSK (which uses AES) and limits the speed of WiFi devices to 54 Mbps. In the **Password (Network Key)** field, enter a phrase of 8 to 63 characters or 64 hexadecimal digits. To join the WiFi network, a user must enter this password. To view the password in clear text, click the **eye** icon.

(Continued)

Setting	Description
WPA/WPA2 Enterprise	This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For more information, see Set up WPA and WPA2 Enterprise WiFi security with a RADIUS server on page 58).
WPA3- Personal	This option, which is the same as WPA3, is the most secure personal authentication option. WPA3 uses SAE encryption and enables only WiFi devices that support WPA3 to join the WiFi network. WPA3 provides a secure connection but some legacy WiFi devices do not detect WPA3 and support only WPA2. If your network also includes WPA2 devices, select **WPA2 Personal [AES]** authentication. In the **Password (Network Key)** field, enter a phrase of 8 to 63 characters. To join the WiFi network, a user must enter this password. To view the password in clear text, click the **eye** icon.

9. To change the radio band or additional security for the selected WiFi network, configure the settings that are described in the following table.

Setting	Description
Band	Select a radio button for a single band **(2.4 GHz** or **5 GHz**) or keep the default selection, which is the **Both** radio button, to enable the WiFi network to broadcast on both radio bands.
Enable SSID Broadcast	By default, the AP broadcasts its SSID so that WiFi clients can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast, clear the **Enable SSID Broadcast** check box. Turning off the SSID broadcast provides additional WiFi security, but users must know the SSID to be able to join the WiFi network.

(Continued)

Setting	Description
Client isolation	For the Wireless 1 network, client isolation is disabled and you cannot change it. For the Wireless 2 and Wireless 3 networks, by default, client isolation is enabled, and the **Enable** radio button is selected. To allow communication between WiFi clients that are associated with the same SSID or different SSIDs on the AP, select the **Disable** radio button.
Allow access to wired ports and Router GUI	For the Wireless 1 network, access to wired ports and the device UI is enabled and you cannot change it. For the Wireless 2 and Wireless 3 networks, by default, the **Disable** radio button is selected to prevent WiFi clients from reaching devices that are connected to the wired ports (LAN ports) of the AP and from accessing the device UI. To allow communication between WiFi clients and devices that are connected to the wired ports and access to the device UI, select the **Enable** radio button.

10. Click the **Apply** button.

    Your settings are saved.

    If you connected over WiFi to the network and you changed the SSID, you are disconnected from the network.

11. Make sure that you can reconnect over WiFi to the network with its new settings.

    If you cannot connect over WiFi, check the following:

    - Are you using the correct network name (SSID) and password?
    - If your computer or device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your WiFi-enabled computer or mobile device to match the current settings for your network.
    - If your computer or device is connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the AP provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
    - Does your computer or device display as an attached device? (See Display the devices currently on the AP network and change device information on page 137.) If it does, it is connected to the network.

Set up WPA and WPA2 Enterprise WiFi security with a RADIUS server

Enterprise security requires that your AP can connect to a Remote Authentication Dial In User Service (RADIUS) server. RADIUS is an enterprise-level method for centralized authentication, authorization, and accounting (AAA) management.

RADIUS security is generally used in a company setting rather than in a small office or home office.

To enable the AP to provide WPA and WPA2 enterprise WiFi security, the WiFi network must be able to reach a RADIUS server.

To configure WPA and WPA2 enterprise security:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **BASIC > Wireless**.

   The Wireless Network page displays.
5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
6. From the **Security Options** menu, select the **WPA/WPA2 Enterprise** radio button.

   The WPA and WPA2 Enterprise settings display.

7. From the **WPA Mode** menu, select the enterprise mode:
   - **WPA2 [AES]**: WPA2 provides a secure connection for WPA2 and WPA3 devices but some older WiFi devices do not detect WPA2 and support only WPA. If your WiFi network includes such older devices, select **WPA [TKIP] + WPA2 [AES]** security.
   - **WPA [TKIP] +WPA2 [AES]**: This type of security enables WiFi devices that support either WPA, WPA2, or WPA3 to join the WiFi network. This is the default mode.
8. In the **RADIUS Server IP Address** field, enter the IPv4 address of the RADIUS server to which the WiFi network can connect.
9. In the **RADIUS Server Port** field, enter the number of the port on the AP that is used to access the RADIUS server for authentication.
   The default port number is 1812.
10. In the **RADIUS Server Shared Secret** field, enter the RADIUS password that is used between the AP and the RADIUS server during authentication of a WiFi client.
    To view the RADIUS password in clear text, click the **eye** icon.
11. Click the **Apply** button.
    Your settings are saved.
12. Make sure that you can reconnect over WiFi to the network with its new security settings.
    If you cannot connect over WiFi, check the following:
    - Are you using the correct network name (SSID) and password?
    - If your computer or device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your WiFi-enabled computer or mobile device to match the current settings for your network.
    - If your computer or device is connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the AP provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
    - Does your computer or device display as an attached device? (See Display the devices currently on the AP network and change device information on page 137.) If it does, it is connected to the network.

Enable or disable a WiFi network

The AP comes with its Wireless 1 network enabled and its Wireless 2 and Wireless 3 networks disabled. You can enable or disable each of these WiFi networks.

Note: You can set up a schedule to turn the AP's WiFi radios (2.4 GHz, 5 GHz, or both) on and off. See Add a WiFi schedule for a radio on page 163. For information about turning off the radios entirely, see Enable or disable a WiFi radio on page 66.

To disable or enable a WiFi network:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **BASIC > Wireless**.

   The Wireless Network page displays.
5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
6. Select a Wireless Network radio button:
   - **Enable**: Enables the WiFi network. By default, the Wireless 2 and Wireless 3 networks are disabled, but you can enable them.
   - **Disable**: Disables the WiFi network. By default, the Wireless 1 network is enabled, but you can disable it.

7. Click the **Apply** button.
   Your settings are saved.

Broadcast or hide the SSID for a WiFi network

By default, a WiFi network (SSID) broadcasts its network name (also referred to as the SSID) so that WiFi clients can display the SSID in their scanned network lists. For additional security, you can turn off the SSID broadcast and hide the SSID. Then, anyone who wants to join this WiFi network must type the SSID instead of selecting it from a list on a computer or mobile device.

To broadcast or hide the network name for a WiFi network:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **BASIC > Wireless**.
   The Wireless Network page displays.

5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).

6. Broadcast or hide the SSID:
   - **Broadcast the SSID**: Select the **Enable SSID Broadcast** check box.
   - **Hide the SSID**: Clear the **Enable SSID Broadcast** check box.
7. Click the **Apply** button.
   Your settings are saved.

Manage client isolation for clients of the Wireless 2 or Wireless 3 network

Client isolation is disabled for the Wireless 1 network so that clients on that network can communicate with each other. You cannot change this setting for the Wireless 1 network. For the Wireless 2 and Wireless 3 networks, client isolation is also disabled by default, but you *can* enable it as an added security measure. If enabled, none of the WiFi clients on the same WiFi network can communicate with each other. However, these WiFi clients can still communicate with each other over the Internet.

To manage client isolation for the Wireless 2 or Wireless 3 network:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.

4. Select **BASIC > Wireless**.
   The Wireless Network page displays.
5. Select the WiFi network (**Wireless 2** or **Wireless 3**).
6. Select a Client Isolation radio button:
   - **Enable**: All WiFi clients are isolated. WiFi clients that are connected to the same WiFi network are prevented from communicating with each other. (Communication over the Internet remains possible.)
   - **Disable**: WiFi clients that are connected to the same WiFi network are allowed to communicate with each other.
7. Click the **Apply** button.
   Your settings are saved.

Manage access to LAN ports and the device UI

For the Wireless 2 and Wireless 3 networks, you can enable or disable WiFi client access to devices connected to the AP LAN ports and to the device UI to manage the AP. For example, if you connect a printer to LAN port 2 and a server to LAN port 3, you can enable or disable access to the printer and server from the WiFi clients connected to the Wireless 2 and Wireless 3 networks.

Access to LAN ports depends on the WiFi network that the clients are connected to and whether you enabled access:

- **Wireless 1**: WiFi clients that are connected to the Wireless 1 network can access devices that are connected to the LAN ports of the AP. For the Wireless 1 network, you cannot disable this access. Clients of the Wireless 1 network also can access the device UI.
- **Wireless 2 or Wireless 3**: You can enable or disable access to the LAN ports and device UI for either or both of these WiFi networks. By default, such access is disabled. (If devices that are connected to the LAN ports are set up for communication over the Internet, WiFi clients of the Wireless 2 or Wireless 3 network might still be able to reach these devices.)

To enable or disable LAN port and device UI access for the Wireless 2 or Wireless 3 network:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **BASIC > Wireless**.
   The Wireless Network page displays.
5. Select the **Wireless 2** or **Wireless 3** button.
   The settings for the Wireless 2 or Wireless 3 network display.
6. Scroll down to Allow access to wired ports and Router GUI and select a radio button:
   - **Enable**: WiFi clients on the selected network can access devices connected to the LAN ports and can access the device UI.
   - **Disable**: WiFi clients on the selected network cannot access devices connected to the LAN ports or the device UI. (If devices that are connected to the LAN ports are set up for communication over the Internet, WiFi clients might still be able to reach these devices.)
7. Click the **Apply** button.
   Your settings are saved.

Manage SSID isolation for *all* WiFi networks

SSID isolation means that WiFi clients associated with different WiFi networks on the AP cannot communicate with each other. For example, a client connected to the Wireless 1 network cannot communicate with a client connected to the Wireless 2 network. The WiFi clients can still communicate with each other over the Internet. SSID isolation is the default setting for the AP and provides an added security measure. You can disable SSID isolation.

To manage SSID isolation for all WiFi networks:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **BASIC > Wireless**.

   The Wireless Network page displays.
5. Select an SSID Isolation radio button:
   - **Enable**: WiFi clients that are connected to different SSIDs cannot communicate with each other. This is the default setting. (Communication over the Internet is possible.)
   - **Disable**: WiFi clients that are connected to different SSIDs can communicate with each other.

6. Click the **Apply** button.
   Your settings are saved.

Enable or disable a WiFi radio

The AP has internal WiFi radios that broadcast signals in the 2.4 GHz and 5 GHz bands. By default, they are on so that you can connect over WiFi to the AP. When both WiFi radios are off, you can still use an Ethernet cable for a LAN connection to the AP.

You can also turn a WiFi radio on and off based on a schedule (see Add a WiFi schedule for a radio on page 163).

IMPORTANT: If you enabled the smart connect feature, you can only enable or disable both radios simultaneously. That means that you cannot enable or disable each radio individually.

To enable or disable a WiFi radio:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
   The Wireless Settings page displays.

5. Do one of the following:
   - **2.4 GHz radio**: To change the settings for the 2.4 GHz radio, scroll down to the Advanced Wireless Settings (2.4 GHz b/g/n/ax) section.
   - **5 GHz radio**: To change the settings for the 5 GHz radio, scroll down to the Advanced Wireless Settings (5 GHz 802.11a/n/ac/ax) section.

   Note: If you enabled the smart connect feature, the page presents a single option in the Advanced Wireless Settings (2.4 GHz b/g/n/ax & 5 GHz 802.11a/n/ac/ax) section. In that situation, enabling or disabling applies to both radios simultaneously. If the smart connect feature is disabled, you can enable or disable each radio individually.

6. Turn off or turn on the radio:
   - **Turn off the radio**: Clear the **Enable Wireless Router Radio** check box.
   - **Turn on the radio**: Select the **Enable Wireless Router Radio** check box.

7. Click the **Apply** button.
   Your settings are saved.

   If you turn off a radio, the associated 2.4 GHz or 5 GHz WLAN LED turns off.

Use WPS to connect to the WiFi network

WPS (Wi-Fi Protected Setup) lets you connect a computer or mobile device to the AP's Wireless 1 network without entering the WiFi network passphrase or key. Instead, you use a software push button or enter a PIN to connect.

If you use the software push button method, the computer or device that you are trying to connect must provide either a physical push button or a software push button. If you use the PIN method, you must know the PIN of the computer or device that you are trying to connect.

WPS supports WPA and WPA2 WiFi security. If your WiFi network is open (no WiFi security is set, which is not the default setting), connecting with WPS automatically sets WPA + WPA2 WiFi security on the WiFi network and generates a random passphrase. You can view this passphrase (see Set up or change an open or secure WiFi network on page 53).

Use WPS with the software push button method in the device UI

For you to use the software push button method to connect a WiFi device to the AP's Wireless 1 network, the WiFi device that you are trying to connect must provide either a physical push button or a software push button. You can use this method to let a WiFi device join the Wireless 1 network only (not another WiFi network on the AP).

You can use WPS with the push button method by pressing the software push button in the AP's device UI, as described in the following procedure.

To join the AP's Wireless 1 network using WPS with the push button method in the device UI:

1. Check the WPS instructions for the WiFi device that you want to connect to the Wireless 1 network.
2. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
3. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
4. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
5. Select **ADVANCED > WPS Wizard**.

   The Add WPS Client page displays and shows a description of the WPS method.
6. Click the **Next** button.

   By default, the **Push Button (recommended)** radio button is selected.
7. Click the button (that is, the green icon) onscreen.

8. Within two minutes, press the physical push button or a software push button on the WiFi device, or follow the WPS instructions that came with the device.

   The WPS process automatically sets up the device with the WiFi passphrase and connects the device to the Wireless 1 network of the AP.

9. To verify that the WiFi device is connected to the AP's Wireless 1 network, select **BASIC > Attached Devices**.

   The WiFi device displays on the page.

Use WPS with the PIN method

To use the PIN method to connect a WiFi device to the AP's Wireless 1 network, you must know the PIN of the WiFi device that you are trying to connect.

To join the AP's Wireless 1 network using WPS with the PIN method:

1. Get the PIN of the WiFi device that you want to connect to the Wireless 1 network.
2. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
3. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

4. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

5. Select **ADVANCED > WPS Wizard**.

   The Add WPS Client page displays and shows a description of the WPS method.

6. Click the **Next** button.

The Add WPS Client page adjusts.

The **Push Button (recommended)** radio button is selected by default.

7. Select the **PIN Number** radio button.
8. In the **Enter Client's PIN** field, enter the PIN number of the WiFi device.
9. Click the **Next** button.

   For four minutes, the AP attempts to find the WiFi device (that is, the client) that you want to join the AP's Wireless 1 network.

10. Within four minutes, go to the WiFi device and use its WPS software to join the network without entering a password.

    The WPS process automatically sets up the device with the WiFi passphrase and connects the device to the Wireless 1 network of the AP.

11. To verify that the WiFi device is connected to the AP's Wireless 1 network, select **BASIC > Attached Devices**.

    The WiFi device displays on the page.

7

Security, Firewall, and Access Rules

The AP comes with a built-in firewall that helps to protect your network from unwanted intrusions *from* the Internet and lets you control access *to* the Internet. You can also set up access rules for wired and WiFi devices. Such rules determine if a device can access or is blocked from accessing the AP network.

This chapter includes the following sections:

Note: In this chapter, we refer to the access point as the AP.

Firewall WAN settings [router mode]

If the AP is in router mode, the basic firewall settings let you manage these settings:

- Port scan protection
- Denial of service (DoS) protection
- Whether the AP can respond to a ping from the Internet (WAN) port
- DMZ server
- IGMP proxying
- NAT filtering
- Application-level gateway (ALG) for the Session Initiation Protocol (SIP)

For information about the MTU size, which is another basic firewall setting, see Change the MTU size [router mode] on page 108.

Note: The information in the following sections is not required if the AP is operating in AP mode. In AP mode, the firewall WAN settings can be provided by the routing device to which the AP connects. Therefore, in AP mode, the firewall WAN settings are masked out in the device UI.

Enable or disable responses to a ping from the Internet [router mode]

You can enable the AP to respond to a ping to its WAN (Internet) port. This feature allows your AP to be discovered. Enable this feature only as a diagnostic tool or for a specific reason.

To change the default WAN security settings:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. Enable or disable the AP from responding to a ping on its Internet (WAN) port:
   - **Enable**: Select the **Respond to Ping on Internet Port** check box.
   - **Disable**: Clear the **Respond to Ping on Internet Port** check box.
     By default, the check box is cleared and the AP does not respond to a ping on its WAN (Internet) port.
6. Click the **Apply** button.
   Your settings are saved.

Enable or disable IGMP proxying [router mode]

IGMP proxying allows a computer or mobile device on the AP network to receive multicast traffic from the Internet. If you do not need this feature, leave it disabled, which is the default setting.

To enable IGMP proxying:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. Enable or disable the AP to serve as an IGMP proxy device:
   - **Enable**: Clear the **Disable IGMP Proxying** check box.
   - **Disable**: Select the **Disable IGMP Proxying** check box.

By default, the check box is selected and IGMP proxying is disabled.

6. Click the **Apply** button.
   Your settings are saved.

Set up a default DMZ server [router mode]

A default DMZ server is helpful when you are using some Internet services and videoconferencing applications that are incompatible with Network Address Translation (NAT). The AP is programmed to recognize some of these applications and to work correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if the IP address for that computer is entered as the default DMZ server.

WARNING: DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

To set up a default DMZ server:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. Select the **Default DMZ Server** check box.
6. Enter the LAN IP address of the computer that must function as the DMZ server.
7. Click the **Apply** button.
   Your settings are saved.

Manage NAT filtering [router mode]

Network Address Translation (NAT) determines how the AP processes inbound traffic. Secured NAT protects computers on the LAN from attacks from the Internet but might prevent some Internet services, point-to-point applications, or multimedia applications from working. Open NAT provides a much less secured firewall but allows almost all Internet applications to work. Secured NAT is the default setting.

To change the default NAT filtering settings:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.

   The WAN Setup page displays.
5. Select a NAT Filtering radio button:

   - **Secured**: Provides a secured firewall to protect the computers on the LAN from attacks from the Internet but might prevent some Internet services, point-to-point applications, or multimedia applications from functioning. By default, the Secured radio button is selected.
   - **Open**: Provides a much less secured firewall but allows almost all Internet applications to function.
6. Click the **Apply** button.

   Your settings are saved.

Manage the SIP application-level gateway [router mode]

The application-level gateway (ALG) for the Session Initiation Protocol (SIP) is enabled by default for enhanced address and port translation. However, some types of VoIP and

video traffic might not work well when the SIP ALG is enabled. For this reason, the AP provides the option to disable the SIP ALG.

To change the default SIP ALG setting:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. To disable the SIP ALG, select the **Disable SIP ALG** check box.
   The SIP ALG is enabled by default.
6. Click the **Apply** button.
   Your settings are saved.

Network access control lists

You can use access control to block or allow device access to your network. An access control list (ACL) functions with the MAC addresses of wired and WiFi devices that can either access your entire network or are blocked from accessing your entire network.

The AP can detect the MAC addresses of devices that are connected to the network and list the MAC addresses of devices that were connected to the network.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of a device. If you cannot see the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses of devices that are connected to the AP on the Access Control page of the device UI (see Enable and manage network access control on page 77).

Enable and manage network access control

When you enable access control, you select whether new devices are allowed to access the AP network or are blocked. By default, currently connected devices are allowed to access the network, but you can block these devices. You can also view information about connected devices.

To set up network access control and view information about connected devices:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.

   The Access Control page displays.
5. Select the **Turn on Access Control** check box.

   You must select this check box before you can specify an access rule and use the **Allow all new devices to connect** and **Block all new devices from connecting** buttons. When the **Turn on Access Control** check box is cleared, all devices are allowed to connect, even if a device is in the list of blocked devices.
6. Click the **Apply** button.

   Your settings are saved.
7. Select an access rule for new devices that are not currently connected:

- **Allow all new devices to connect**: A new device can access your network. You do not need to enter the MAC address. We recommend that you leave this radio button selected.
- **Block all new devices from connecting**: Before a new device can access your network, you must enter its MAC address in the allowed list. For more information, see Add, remove, or change a device on the allowed list on page 78.

The access rule does not affect previously blocked or allowed devices. It applies only to devices joining your network in the future after you apply these settings.

8. To manage future access for currently connected devices, do the following:
   - **Allow your current device**: If you blocked all new devices, you can allow the device that you are currently using to continue to access the network. Select the check box next to your device in the table, and click the **Allow** button.
   - **Allow or block a device**: To change the allow or block settings for a device that is currently connected, select the check box next to the device in the table, and click either the **Allow** button or the **Block** button.
   - **Change the device name that is displayed**: To change the displayed name for a device that is currently connected, do the following:
     a. Select the check box next to the device in the table.
     b. Click the **Edit** button.
        The Edit Allowed Device or Edit Blocked Device page displays.
     c. In the **Device Name** field, change the name.
     d. Click the **Apply** button.
        The Access Control page displays again.
9. Click the **Apply** button.
   Your settings are saved.
10. To refresh the information in the table with currently connected devices, click the **Refresh** button.
    The table shows the status of the device (allowed or blocked from future sessions), device name, IP address, MAC address, and type of connection to the AP.

Add, remove, or change a device on the allowed list

If you set up an access list that blocks all new devices from accessing your network (see Enable and manage network access control on page 77), you must set up an allowed list that defines which WiFi and wired devices are allowed to access your entire network.

You do so by adding the MAC addresses of these devices to the allowed list. You can also change or remove a device from the allowed list.

To add, remove, or change a device on the allowed list:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.
   The Access Control page displays.
5. If the table with allowed devices does not display, click the **View list of allowed devices not currently connected to the network** link.
   A table displays the detected device name, MAC address, and connection type of the devices that are not connected but allowed to access the network.
6. To add a device to the allowed list, do the following:
   a. Click the **Add** button.
      The Add Allowed Device page displays.
   b. Enter the MAC address and device name for the device that you want to allow.
   c. Click the **Apply** button.
      The device is added to the allowed list. The Access Control page displays again.

7. To remove a device from the allowed list, do the following:
   a. Select the check box for the device.
   b. Click the **Remove from the list** button.
      The device is removed from the allowed list.

8. To change the MAC address or name for a device on the allowed list, do the following:
   a. Select the check box for the device.
   b. Click the **Edit** button.
      The Edited Allowed Device page displays.
   c. Change the MAC address, device name, or both.
   d. Click the **Apply** button.
      The Access Control page displays again.

9. Click the **Apply** button.
   Your settings are saved.

Add, remove, or change a device on the blocked list

If you set up an access list that allows all new devices to access your network (see Enable and manage network access control on page 77) but you want to block some devices, you must set up a blocked list that defines which WiFi and wired devices are blocked from accessing your network. You do so by adding the MAC addresses of these devices to the blocked list. You can also change or remove a device from the blocked list.

To add, remove, or change a device on the blocked list:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.
   The Access Control page displays.
5. Click the **View list of blocked devices not currently connected to the network** link.
   A table displays the detected device name, MAC address, and connection type of the devices that are not connected and are blocked from accessing the network.
6. To add a device to the blocked list, do the following:
   a. Click the **Add** button.
      The Add Blocked Device page displays.
   b. Enter the MAC address and device name for the device that you want to block.
   c. Click the **Apply** button.
      The device is added to the blocked list. The Access Control page displays again.
7. To remove a device from the blocked list, do the following:
   a. Select the check box for the device.
   b. Click the **Remove from the list** button.
      The device is removed from the blocked list.
8. To change the MAC address or name for a device on the blocked list, do the following:
   a. Select the check box for the device.
   b. Click the **Edit** button.
      The Edited Blocked Device page displays.
   c. Change the MAC address, device name, or both.
   d. Click the **Apply** button.
      The Access Control page displays again.

9. Click the **Apply** button.
   Your settings are saved.

Block specific applications and services from the Internet [router mode]

If the AP is in router mode, you can add service blocking rules to prevent access from your LAN to specific services and applications on the Internet. In addition, you can specify if a blocking rule applies to one user, a range of users, or all users on your LAN. The AP lists many default services and applications that you can use in blocking rules. You can also add a service blocking rule for a custom service or application.

Add a service blocking rule for a predefined service or application [router mode]

If the AP is in router mode, it lists many predefined services and applications that you can use in outbound rules.

You can add a service blocking rule to prevent access to a specific predefined service or application on the Internet.

To add a service blocking rule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Security > Block Services**.
   The Block Services page displays.

5. In the Services Blocking section, specify how the AP applies outbound rules:

- **Per Schedule**. Use service blocking according to a schedule that you set. For more information, see Schedule blocking [router mode] on page 86.
- **Always**. Use service blocking continuously.

6. Click the **Add** button.
   The Block Services Setup page displays.
7. From the **Service Type** menu, select the service or application to be covered by this rule.
   The **Protocol**, **Starting Port**, and **Ending Port** fields are automatically populated when you select the service or application.

   Note: If the service or application does not display in the list, you can add it by selecting **User Defined** from the **Service Type** menu (see Add a service blocking rule for a custom service or application [router mode] on page 83).
8. Specify which devices on your LAN are affected by the rule, based on their IP addresses:
   - **Only This IP Address**. Enter the required IP address in the fields to apply the rule to a single device on your LAN.
   - **IP Address Range**. Enter the required start and end IP addresses in the fields to apply the rule to a range of devices.
   - **All IP Addresses**. All computers and devices on your LAN are covered by this rule.
     By default, the **All IP Addresses** radio button is selected.
9. Click the **Add** button.
   The new rule is added to the Service Table on the Block Services page.

Add a service blocking rule for a custom service or application [router mode]

If the AP is in router mode, it lists many predefined services and applications that you can use in outbound rules.

If a service or application is not predefined, you can add a service blocking rule for a custom service or application.

To add service blocking rule for a custom service or application:

1. Find out which protocol and port number or range of numbers the service or application uses.

   You can usually find this information by contacting the publisher of the service or application or through online user or news groups.

2. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
3. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

4. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

5. Select **ADVANCED > Security > Block Services**.

   The Block Services page displays.

6. The first time that you add an outbound firewall rule, in the Services Blocking section, specify how the AP applies outbound rules:

   - **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see Schedule blocking [router mode] on page 86.
   - **Always**. Use keyword blocking continuously.

7. Click the **Add** button.

   The Blocking Services Setup page displays.

8. From the **Service Type** menu, select **User Defined**.
9. Specify a new service blocking rule by selecting a protocol, defining the ports, and defining a name:

   - **Protocol**. From the menu, select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.
   - **Starting Port**. In the field, enter the start port in the range from 1 to 65535 for the service or application.
   - **Ending Port**. In the field, enter the end port in the range from 1 to 65535 for the service or application.

- **Service Type/User Defined**. In the field, enter the name of the custom service or application.

10. Specify which devices on your LAN are affected by the rule, based on their IP addresses:
    - **Only This IP Address**. Enter the required address in the fields to apply the rule to a single device on your LAN.
    - **IP Address Range**. Enter the required addresses in the start and end fields to apply the rule to a range of devices.
    - **All IP Addresses**. All computers and devices on your LAN are covered by this rule.
      By default, the **All IP Addresses** radio button is selected.
11. Click the **Add** button.
    The new rule is added to the Service Table on the Block Services page.

Change a service blocking rule [router mode]

If the AP is in router mode, you can change an existing service blocking rule.

To change a service blocking rule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Services**.
   The Block Services page displays.
5. In the Service Table, select the radio button for the rule.
6. Click the **Edit** button.
   The Block Services Setup page displays.

7. Change the settings.

   For more information about the settings, see Add a service blocking rule for a custom service or application [router mode] on page 83.

8. Click the **Apply** button.

   Your settings are saved. The modified rule displays in the Service Table on the Block Services page.

Remove a service blocking rule [router mode]

If the AP is in router mode, you can remove a service blocking rule that you no longer need.

To remove a service blocking rule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Security > Block Services**.

   The Block Services page displays.

5. In the Service Table, select the radio button for the rule.
6. Click the **Delete** button.

   The rule is removed from the Service Table. Custom rules are deleted.

Schedule blocking [router mode]

If the AP is in router mode, you can set up a schedule that you can apply to Internet application and service blocking.

The schedule can specify the days and times that the feature is active. After you set up the schedule, if you want it to become active, you must apply it to Internet application and service blocking (see Block specific applications and services from the Internet [router mode] on page 82). Without a schedule, you can only enable or disable this feature. By default, no schedule is set.

To set up a schedule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > Schedule**.
   The Schedule page displays.
5. Set up the schedule for blocking:
   - **Days to Block**. Select the check box for each day that you want to block access or specify that blocking occurs on every day by selecting the **Every Day** check box.
     By default, the **Every Day** check box is selected.
   - **Time of Day to Block**. Select a start and end time for blocking in 24-hour format or select the **All Day** check box for 24-hour blocking.
     By default, the **All Day** check box is selected.
6. Click the **Apply** button.
   Your settings are saved.

Set up security event email notifications

The AP can email you its activity logs. The log records activity and security events.

To set up email notifications:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > E-mail**.
   The E-mail page displays.
5. Select the **Turn E-mail Notification On** check box.
6. In the **Primary E-mail Address** field, type the email address to which logs and alerts are to be sent.
   This email address is also used for the From address. If this field is blank, log and alert messages are not sent.
7. In the **Your Outgoing Mail Server** field, enter the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com).
   You might be able to find this information in the configuration window of your email program. If you leave this field blank, log and alert messages are not sent.

8. In the **Outgoing Mail Server Port Number** field, enter the port number that the mail server uses.

   If you do not know the port number, leave the default port number, which is 25.

9. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box, and do the following:
   a. In the **User Name** field, type the user name for the outgoing email server.
   b. In the **Password** field, type the password for the outgoing email server.

10. To send logs based on a schedule, from the **Send logs according to this schedule** menu, select the schedule type and specify the associated settings if applicable:

    - **When log is full**. The AP sends log messages when the log is full.
    - **Hourly**. The AP sends log messages hourly.
    - **Daily**. The AP sends log messages daily at the time that you specify. From the **Time** menu, select the time, and select the **AM** or **PM** radio button.
    - **Weekly**. The AP sends log messages weekly at the day and time that you specify. From the **Day** menu, select the day of the week. From the **Time** menu, select the time, and select the **AM** or **PM** radio button.

    The default selection from the menu is **None**.

11. Click the **Apply** button.

    Your settings are saved.

    Logs are sent automatically according to the schedule that you set. If the log fills before the specified time, it is sent. After the log is sent, it is cleared from the AP memory. If the AP cannot email the log and the log buffer fills, the AP overwrites the log.

8

Network Settings

This chapter describes how you can manage various LAN and WAN network settings of the AP.

The chapter includes the following sections:

Note: In this chapter, we refer to the access point as the AP.

LAN IP address settings [router mode]

If the AP is in router mode, the LAN subnet defines the LAN IP address settings for the AP, including the IP address at which you can access the AP over the device UI, the DHCP IP address settings, and the Router Information Protocol (RIP) settings.

Note: The information in the following sections is not required if the AP is operating in AP mode. In AP mode, the LAN IP settings can be provided by the routing device to which the AP connects. Therefore, in AP mode, the LAN IP settings are masked out in the device UI.

Change the LAN IP address and subnet settings [router mode]

If the AP is in router mode, it uses private IP addresses on the LAN side and functions as a DHCP server. The AP's LAN IP configuration is as follows:

- **LAN IP address**: 192.168.1.1 (if the AP is in router mode, this is the same as www.routerlogin.net, routerlogin.com, aplogin.net, and aplogin.com)
- **Subnet mask**: 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. The IP address and subnet mask identify which addresses are local to a specific device and which must be reached through a gateway or router. If you need a specific IP subnet that one or more devices on the network use, or if competing subnets use the same IP scheme, you can change the LAN IP address settings.

Note: If you change the default LAN IP address settings, the IP address range for the default DHCP server also changes (see Manage the DHCP server address pool [router mode] on page 92).

To change the LAN IP address and subnet settings:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup page displays.

5. In the **IP Address** fields, enter the new LAN IP address.

   The LAN IP address at which you can access the device UI of the AP also changes, but the domain names routerlogin.net and routerlogin.com are adjusted to the new LAN IP address.

6. In the **IP Subnet Mask** fields, enter the new LAN subnet mask.

   The LAN IP subnet mask at which you can access the device UI of the AP also changes.

7. Click the **Apply** button.

   Your settings are saved.

   If you changed the LAN IP address settings of the LAN subnet, you might be disconnected from the device UI. If you are disconnected, reconnect by closing your browser, relaunching it, and logging in to the AP at its new LAN IP address, or use routerlogin.net, routerlogin.com, aplogin.net, or aplogin.com

Manage the DHCP server address pool [router mode]

If the AP is in router mode, it functions as a Dynamic Host Configuration Protocol (DHCP) server. The AP assigns IP, DNS server, and default gateway addresses to all computers and mobile devices that are connected to its LAN subnet.

These addresses are part of the same IP address subnet as the AP's LAN IP address. By default, the DHCP address pool for the LAN subnet is 192.168.1.2 through 192.168.1.254.

The AP delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range that you define
- Subnet mask
- Gateway IP address
- DNS server IP address

To change the DHCP pool of IP addresses that the AP assigns:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup page displays.
5. Make sure that the **Use Router as DHCP Server** check box is selected.

   This check box is selected by default.
6. Specify the range of IP addresses that the router assigns for the LAN subnet:
   - In the **Starting IP Address** field, enter the lowest number in the range. This IP address must be in the same LAN subnet.
   - In the **Ending IP Address** field, enter the number at the end of the range of IP addresses. This IP address must be in the same LAN subnet.
7. To change the DHCP lease time, from the **DHCP Lease Time** menu, select a period from 1 hour to 24 hours.

   By default, the period is 24 hours. When the lease time expires, the DHCP server releases the IP address, and a DHCP client must reconnect to get a new (or the same) IP address from the DHCP server.
8. Click the **Apply** button.

   Your settings are saved.

Disable the DHCP server [router mode]

If the AP is in router mode, you can use another device on your network as the DHCP server or specify the network settings of all your computers.

Note: If you disable the DHCP server and do not specify another DHCP server or no other DHCP server is available on your network, you must set your computer IP addresses manually so that they can reach the AP.

To disable the DHCP server:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Clear the **Use Router as DHCP Server** check box.
6. Click the **Apply** button.
   Your settings are saved.

Manage the Router Information Protocol settings [router mode]

If the AP is in router mode, Router Information Protocol (RIP) lets the AP exchange routing information with other routers. By default, RIP is enabled in both directions (in and out) without a particular RIP version.

To manage the RIP settings:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup**.
   The LAN Setup page displays.

5. From the **RIP Direction** menu, select the RIP direction:

   - **Both**: The AP broadcasts its routing table periodically and incorporates information that it receives. This is the default setting.
   - **In Only**: The AP incorporates the RIP information that it receives but does not broadcast its routing table.
   - **Out Only**: The AP broadcasts its routing table periodically but does not incorporate the RIP information that it receives.

6. From the **RIP Version** menu, select the RIP version:

   - **Disabled**: The RIP version is disabled. This is the default setting.
   - **RIP-1**: This format is universally supported. It is adequate for most networks, unless you are using an unusual network setup.
   - **RIP-2B**: This format carries more information than RIP-1, sends the routing data in RIP-2 format, and uses subnet broadcasting.
   - **RIP-2M**: This format carries more information than RIP-1, sends the routing data in RIP-2 format, and uses multicasting.

7. Click the **Apply** button.
   Your settings are saved.

Change the AP network device name

The default network device name of the AP is the model number of the AP.

This device name displays in, for example, a file manager when you browse your network.

To change the AP network device name:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > Device Name**.
   The Device Name page displays.
5. Type a new name in the **Device Name** field.
   You can type up to 15 alphanumeric characters.
6. Click the **Apply** button.
   Your settings are saved.

Reserved LAN IP addresses [router mode]

If the AP is in router mode, you can specify a reserved IP address for a device on the LAN subnet. Each time such a device accesses the AP's DHCP server, the device receives the same IP address.

Note: The information in the following sections is not required if the AP is operating in AP mode. In AP mode, reserved LAN IP addresses can be provided by the routing device to which the AP connects. Therefore, in AP mode, the reserved LAN IP address settings are masked out in the device UI.

Reserve a LAN IP address [router mode]

You can assign a reserved IP address for a device such as a computer or server that requires permanent IP settings.

To reserve an IP address:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Below the Address Reservation table, click the **Add** button.
   The Address Reservation page displays.
6. Either select the radio button for an attached device that displays in the table or specify the reserved IP address settings in the following fields:
   - **IP Address**: Enter the IP address to assign to the computer or device. Enter an IP address in the AP's LAN subnet, such as 192.168.1.x.
   - **MAC Address**: Enter the MAC address of the computer or device.

- **Device Name**: Enter the name of the computer or device.

7. Click the **Add** button.
   The reserved address is entered into the Address Reservation table on the LAN Setup page.

   The reserved address is not assigned until the next time the computer or device contacts the AP's DHCP server. Reboot the computer or device, or access its IP configuration and force a DHCP release and renew.

Change a reserved LAN IP address entry [router mode]

If the AP is in router mode, you can change an existing reserved LAN IP address entry.

To change a reserved LAN IP address entry:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Setup > LAN Setup**.
   The LAN Setup page displays.

5. In the Address Reservation table, select the radio button for the reserved address.
6. Click the **Edit** button.
   The Address Reservation page displays.

7. Change the settings.
8. Click the **Apply** button.
   Your settings are saved.

Remove a reserved LAN IP address entry [router mode]

If the AP is in router mode, you can remove a reserved LAN IP address entry that you no longer need.

To remove a reserved LAN IP address entry:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
   The LAN Setup page displays.
5. In the Address Reservation table, select the radio button for the reserved address.
6. Click the **Delete** button.
   The IP address entry is removed.

Static routes [router mode]

If the AP is in router mode, the AP can support IPv4 static routes. Static routes can provide detailed routing information to your AP. Typically, you do not need to add static routes. You must configure static routes only for unusual cases such as when you use multiple routers or multiple IP subnets on your network.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through an ADSL modem to an ISP.
- You use an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.158.
- Your company's network address is 203.0.113.0.

When you first configured your AP, two implicit static routes were created. A default route was created with your ISP as the gateway and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 203.0.113.0 network, your AP forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case, you must define a static route, instructing your router that 203.0.113.0 is accessed through the ISDN router at 192.168.1.158. Here is an example:

- Through the destination IP address and IP subnet mask, specify that this static route applies to all 203.0.113.x addresses.
- Through the gateway IP address, specify that all traffic for these addresses is forwarded to the ISDN router at 192.168.1.158.
- A metric value of 2 works fine because the ISDN router is on the LAN.

Add an IPv4 static route [router mode]

If the AP is in router mode, it supports static routes.

You can add an IPv4 static route to a destination IP address and specify the subnet mask, gateway IP address, and metric.

To add an IPv4 static route:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.
5. Click the **Add** button.
   The Static Routed page adjusts.
6. In the **Route Name** field, enter a name for the route.

The name is for identification purposes.

7. To make the route private, select the **Private** check box.
   A private static route is not reported in RIP messages.
8. To prevent the route from becoming active after you click the **Apply** button, clear the **Active** check box.
   In some situations, you might want to set up a static route but keep it disabled until a later time. By default, the **Active** check box is selected and a route becomes active after you click the **Apply** button.
9. Enter the route IP address and metric settings in the following fields:
   - **Destination IP Address**. Enter the IP address for the final destination of the route.
   - **IP Subnet Mask**. Enter the IP subnet mask for the final destination of the route. If the destination is a single host, enter **255.255.255.255**.
   - **Gateway IP Address**. Enter the IP address of the gateway.
     The IP address of the gateway must be on the AP LAN subnet.
   - **Metric**. Enter a number from 2 through 15.
     This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to **2**.
10. Click the **Apply** button.
    Your settings are saved. The static route is added to the table on the Static Routes page.

Change an IPv4 static route [router mode]

If the AP is in router mode, it supports static routes.

You can change an existing IPv4 static route.

To change an IPv4 static route:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.
5. In the Static Routes table, select the radio button for the route.
6. Click the **Edit** button.
   The Static Routes page adjusts.
7. Change the settings for the route.
   For more information about the settings, see Add an IPv4 static route [router mode] on page 100.
8. Click the **Apply** button.
   The route settings are updated in the table on the Static Routes page.

Remove an IPv4 static route

If the AP is in router mode, it supports static routes.

You can remove an existing IPv4 static route that you no longer need.

To remove an IPv4 static route:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.

5. In the Static Routes table, select the radio button for the route.
6. Click the **Delete** button.
   The route is removed from the table on the Static Routes page.

Bridge port and VLAN tag groups [router mode]

If the AP is in router mode, some devices, such as an Internet Protocol television (IPTV), cannot function behind the AP's Network Address Translation (NAT) service or firewall. Based on what your Internet service provider (ISP) requires, for the device to connect to the ISP's network directly, you can enable a bridge either between the device and the AP's Internet (WAN) port or between the device and a VLAN tag group.

Also, some ISPs might require the AP to send VLAN packets for the Internet connection. This requirement is common for ISP fiber connections.

Note: If your ISP provides directions on how to set up a bridge port or VLAN tag group for IPTV, Internet service, or both, follow those directions.

Set up a bridge for a port group [router mode]

If the AP is in router mode and a device such as an IPTV is connected to a LAN port or WiFi network, your ISP might require you to set up a bridge for a port group for the AP's Internet (WAN) port.

A bridge with a port group allows packets that are sent between a device such as an IPTV and the AP Internet (WAN) port to circumvent the AP's NAT service, which otherwise could drop the packets.

CAUTION: Unless you are comfortable with advanced network configurations, be sure to follow the directions of your ISP. Incorrect configuration might cause the Internet connection of the AP to go down.

To set up a bridge for a port group:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.

   The VLAN / Bridge Settings page displays.

5. Select the **Enable VLAN / Bridge group** check box.

   The page expands.

6. Select the **By bridge group** radio button.

   The page adjusts.

7. Select the check box for the LAN port (**Port 1**, **Port 2**, or **Port 3**, or, for model WAX206 only, **Port 4**) or WiFi network (**Wireless1**, **Wireless2**, or **Wireless2**) to which the device that must circumvent the AP's NAT service is connected.

   You must select at least one LAN port or one WiFi network. You can select more than one LAN port and WiFi network.

8. If the port group must use a VLAN, select the **Enable VLAN ID** check box and enter the VLAN ID.

   If your ISP did not tell you to use a VLAN, leave the check box cleared.

   By default, the VLAN ID for the port group is 10, but the VLAN is disabled. VLAN 10 includes all LAN ports, WiFi networks, and the WAN port as members.

9. Click the **Apply** button.

   Your settings are saved. You might need to reconnect to the AP.

Set up a bridge for a VLAN tag group [router mode]

If the AP is in router mode and a device such as an IPTV is connected to a LAN port or WiFi network, your ISP might require you to set up a bridge for a VLAN tag group for the AP's Internet (WAN) port.

If you are subscribed to an IPTV service, the ISP might require you to use VLAN tags on the AP to distinguish between the Internet traffic and the IPTV traffic. A bridge with a VLAN tag group allows packets that are sent between the IPTV device and the AP Internet (WAN) port to circumvent the AP's NAT service, which otherwise could drop the packets.

The AP includes a default VLAN tag group with the name Internet, with VLAN ID 10, and with all LAN ports, WiFi networks, and the WAN port as members. If you enable the bridge for a VLAN tag group, this default VLAN tag group is also enabled. To allow one or more devices to send and receive traffic over a separate VLAN, you can add custom VLAN tag groups, and assign a VLAN ID, priority value, and one or more ports, wireless network, or both to each VLAN tag group.

CAUTION: Unless you are comfortable with advanced network configurations, be sure to follow the directions of your ISP. Incorrect configuration might cause the Internet connection of the AP to go down.

To set up a bridge for a VLAN tag group and enable the new VLAN tag group:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.
   The VLAN / Bridge Settings page displays.
5. Select the **Enable VLAN / Bridge group** check box.
   The page expands.
6. Select the **By VLAN tag group** radio button.
   The page adjusts and the default VLAN tag group displays.
7. To add a custom VLAN tag group, do the following:
   a. Click the **Add** button.
      The Add VLAN Rule page displays.
   b. Specify the settings in the following fields:
      - **Name**. Enter a name for the VLAN tag group.
        The name is for identification purposes.

- **VLAN ID**. Enter an ID from 1 to 4094.
- **Priority**. Enter a value from 0 to 7.

c. Select the check box for the LAN port (**Port 1**, **Port 2**, or **Port 3**, or, for model WAX206 only, **Port 4**) or WiFi network (**Wireless1**, **Wireless2**, or **Wireless2**) to which the device that must circumvent the AP's NAT service is connected. You must select at least one LAN port or one WiFi network. You can select more than one LAN port and WiFi network.

8. Click the **Apply** button.
   The new VLAN tag group is added . The VLAN / Bridge Settings page display again.
9. To enable the bridge using the new VLAN tag group, do the following:
   a. Select the **Enable VLAN / Bridge group** check box again.
   The page expands.
   b. Select the **By VLAN tag group** radio button.
   The page adjusts and the default VLAN tag group and new VLAN tag group display.
   c. Select the radio button for the new VLAN tag group.
   d. Click the **Apply** button.
   Your settings are saved. You might need to reconnect to the AP.

Improve network connections with Universal Plug and Play [router mode]

Universal Plug and Play (UPnP) helps devices such as Internet appliances and computers access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If the AP is in router mode and you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance, you can enable UPnP. If you enable UPnP, make sure that the devices in your network are safe and none are affected with malware.

To manage Universal Plug and Play:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > UPnP**.

   The UPnP page displays.

5. Select the **Turn UPnP On** check box.

   By default, this check box is cleared and UPnP is disabled. If you select the **Turn UPnP On** check box, a device can automatically control the resources of the AP. For example, a device can control port forwarding on the AP.

6. Enter the advertisement period in minutes.

   The advertisement period specifies how often the AP broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points detect current device status at the expense of more network traffic. Longer durations can compromise the freshness of the device status but can significantly reduce network traffic.

7. Enter the advertisement time to live in hops.

   The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

8. Click the **Apply** button.

   If the AP is in router mode, the UPnP Portmap Table displays the IP address of each UPnP device that is accessing the AP and which ports (internal and external) that device opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

9. If the AP is in router mode, to refresh the information in the UPnP Portmap table, click the **Refresh** button.

Change the MTU size [router mode]

If the AP is in router mode, you can change the maximum transmission unit (MTU).

The MTU is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path uses a lower MTU setting than the other devices, the data packets must be split or "fragmented" to accommodate the device with the smallest MTU.

The best MTU setting for router equipment is often the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU of the AP unchanged unless one of these situations occurs:

- You experience problems connecting to your ISP or other Internet service, and the technical support of the ISP recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open, or displays only part of a web page
  - Yahoo email
  - MSN portal
- You use VPN and experience severe performance problems.
- You used a program to optimize MTU for performance reasons and now you are experiencing connectivity or performance problems.

WARNING: An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

To change the MTU size:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. In the **MTU Size** field, enter a value from 616 to 1500.
   The default size is 1500 bytes.
6. Click the **Apply** button.
   Your settings are saved.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

Table 8. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.

9

Maintain and Monitor

This chapter describes how you can maintain the AP by changing the password for local login and by managing the firmware, configuration file, and logs. The chapter also describes how you can monitor the AP and its network traffic.

The chapter includes the following sections:

Note: In this chapter, we refer to the access point as the AP.

Update the firmware

From time to time, or as needed, NETGEAR makes new firmware (software) available.

You can log in to the AP and let the AP check if new firmware is available, or you can manually upload a specific firmware version to your AP.

Depending on how you are connected to the AP, we recommend the following firmware update methods:

- **WiFi connection from a computer or mobile device**: If you are connected over WiFi to the AP, we recommend that you let the AP check the Internet to see if new firmware is available. See Let the AP check for new firmware and update the firmware on page 111.
  If you let the AP check for new firmware and new firmware is available, it is downloaded directly to the AP.

  Note: If you want to load a particular firmware version (but not necessarily the latest firmware version), you must manually update the firmware (see below). In that situation, we recommend that you use a wired connection to the AP.

- **Wired connection from a computer**: If you are connected over an Ethernet cable to a LAN port on the AP or over a LAN connection to the same network as the AP, we recommend that you manually update the firmware. See Manually check for new firmware and update the firmware on page 112.
  With the manual update mode, if new firmware is available, or you want to load a particular firmware version (but not necessarily the latest firmware version), you must download it to your computer and then upload it to your AP.

Let the AP check for new firmware and update the firmware

You can let the AP check the Internet to see if new firmware is available. If it is, you can update the firmware.

To let the AP check for new firmware and update the firmware:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Administration > Firmware Update**.
   The Firmware Update page displays.

5. Click the **Check** button.
   The AP finds new firmware information if any is available and displays a message asking if you want to download and install it.

6. Click the **Yes** button.
   The AP locates and downloads the firmware and begins the update.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes restarting and the Power LED turns solid green.

   A progress bar might show the progress of the firmware update process. The firmware update process takes several minutes. When the update is complete, your AP restarts.

   Read the new firmware release notes to find out if you must reconfigure the AP after updating.

7. To verify that the AP runs the new firmware version, log back in to the AP.
   The firmware version is stated in the Firmware Version field at the top right of the BASIC Home page.

Manually check for new firmware and update the firmware

To download new firmware and update the AP:

1. Visit netgear.com/support/download/ and locate the support page for the router.
2. If available, download the new firmware to your computer or mobile device.

3. Read the new firmware release notes to determine whether you must reconfigure the router after updating.
4. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
5. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
6. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
7. Select **ADVANCED > Administration > Firmware Update**.

   The Firmware Update page displays.
8. Locate and select the firmware file on your computer or mobile device:
   a. Click the **Browse** button.
   b. Navigate to and select the firmware file.
      The file ends in `.img`.
9. Click the **Upload** button.

   A warning pop-up window displays.
10. Click the **OK** button.

    WARNING: To avoid the risk of corrupting the firmware, do not interrupt the upload. For example, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes restarting and the Power LED turns solid green.

A progress bar might show the progress of the firmware upload process. The firmware upload process takes several minutes. When the upload is complete, your AP restarts.

11. To verify that the AP runs the new firmware version, log back in to the AP.
    The firmware version is stated in the Firmware Version field at the top right of the BASIC Home page.

Enable the AP to automatically update the firmware

You can let the AP check for new firmware and automatically update the firmware if new firmware is available.

To let the AP check for new firmware and automatically update the firmware:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Firmware Update**.
   The Firmware Update page displays.
5. In the Router Auto Firmware Update section, select the **Enable** radio button.
   By default, the **Disable** radio button is selected.
6. Click the **Apply** button.
   Your settings are saved.

Back up or restore the settings

The configuration settings of the AP are stored within the AP in a configuration file. You can back up (save) this file to your computer or restore it.

Back up the AP settings

You can save a copy of the current configuration settings.

To back up the AP's configuration file:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.
   The Backup Settings page displays.
5. Click the **Back Up** button.
6. Choose a location to store the file on your computer.
   The backup file ends in `.cfg`.
7. Follow the directions of your browser to save the file.

Restore the AP settings

If you backed up the configuration file, you can restore the configuration settings from this file.

To restore configuration settings that you backed up:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.
   The Backup Settings page displays.
5. Click the **Browse** button and navigate to and select the saved configuration file.
   The backup file ends in `.cfg`.
6. Click the **Restore** button.
   A warning pop-up window displays.
7. Click the **OK** button.
   The configuration is uploaded to the AP. When the restoration is complete, the AP reboots. This process takes about two minutes.

WARNING: To avoid the risk of corrupting the firmware, do not interrupt the restoration. For example, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes restarting and the Power LED turns solid green.

Change the local device password

During the initial log-in process, when you followed the prompts of the Setup Wizard, you specified the local device password (also referred to as the admin password). This is the password that you use to log in to the device UI of the AP with the user name admin. You can change this password again.

We recommend that your password meets the following conditions:

- Contains 8 to 32 characters
- Contains no more than two identical characters in a row

In addition, we recommend that your password meets at least three of the following four conditions:

- At least one uppercase character
- At least one lowercase character
- At least one number
- At least one special character, such as the following characters:
  @ # $ % ^ & * ( ) !

To change the password for the user name admin for login to the device UI of the AP:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Administration > Set Password**.

   The Set Password page displays.

5. Enter the current password.
6. Enter the new password twice.

   For information about password recovery, see Change the password recovery questions for the local device password on page 118.

7. Click the **Apply** button.

   Your settings are saved.

Change the password recovery questions for the local device password

During the initial log-in process, when you followed the prompts of the Setup Wizard, you set up recovery for the local device password (also referred to as the admin password). This is the password that you use to log in locally to the AP with the user name admin.

If you forget this password, you can recover access to the device UI by resetting the password and specifying a new password. The recovery process is supported in the Chrome, Safari, Firefox, and Internet Explorer browsers.

You can change the password recovery questions.

To change the password recovery questions:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Set Password**.
   The Set Password page displays.
5. Make sure that the **Enable Password Reset** check box is selected.
   This check box is selected by default.
6. Select two security questions and provide answers to them.
7. Click the **Apply** button.
   Your settings are saved.

Recover device UI access after login failures

When you use the Setup Wizard for the initial log-in process, you customize the local device password and set up password recovery. If three local login failures occur, you can try to recover access to the device UI and set a new password. This recovery process is supported in the Chrome, Safari, Internet Explorer, and Firefox browsers.

To recover access and set a new local device password:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter your local device password.
   If you enter an incorrect password three times, you are prompted to enter the serial number of the AP.
   The serial number is on the AP label.
4. Enter the serial number of the AP.
5. Click the **Continue** button.
   The page that displays prompts you for the answers to your security questions.
6. Enter the saved answers to your security questions.
7. Click the **Continue** button.
   The Access Point/Router Password Reset page displays.
8. Enter a new password and confirm it.
9. Select two security questions and provide answers to them.
10. Click the **Next** button.
    The page that displays confirms that you successfully reset the admin password.
11. Click the **Login Again** button.
    A login window displays.
12. With your new password, log in to the AP.

Factory default settings

Under some circumstances (for example, if you lost track of the changes that you made to the AP settings or you move the AP to a different network), you might want to erase the configuration and reset the AP to factory default settings.

If the AP is operating in AP mode and you do not know the current IP address of the AP, first try to use an IP scanner application to detect the IP address. (IP scanner applications are available on the Internet free of charge.) If you still cannot find the current IP address of the AP, reset the AP to factory default settings.

Note: If the AP is in router mode, you can always access the AP by using routerlogin.net, routerlogin.com, aplogin.net, or aplogin.com (all of which are the same as IP address 192.168.1.1).

To reset the AP to factory default settings, you can use either the **Reset** button on the back of the AP or the Erase function in the device UI. However, if you cannot find the IP address or lost the password to access the AP and cannot recover it, you must use the **Reset** button.

After you reset the AP to factory default settings, the AP is in router mode, the login URL is routerlogin.net, and the DHCP server is enabled. For a list of factory default settings, see Technical specifications model WAX202 on page 209 or Technical specifications model WAX206 on page 211.

Use the Reset button to return the AP to factory defaults

The **Reset** button on the back panel of the AP lets you return the AP to factory default settings.

After you return the AP to factory default settings, you must go through the initial login process again (see Connect the AP to a modem and log in for the first time on page 32 or Connect the AP to a routing device and log in for the first time on page 28).

CAUTION: The following process erases all settings that you configured in the AP.

To reset the AP to factory default settings using the Reset button:

1. On the back of the AP, locate the recessed **Reset** button.
   For more information, see Back panel on page 18.
2. Insert a device such as a straightened paper clip into the opening.
3. Press the **Reset** button for 10 seconds or until the Power LED starts blinking amber.

When the Power LED starts blinking amber, the configuration is reset to factory default settings. When the reset is complete, the AP reboots. This process takes about two minutes.

WARNING: To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, if you are connected to the AP's device UI, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes restarting and the Power LED turns solid green.

Use the device UI to return the AP to factory defaults

You can use the device UI to return the AP to factory default settings.

After you return the AP to factory default settings, you must go through the initial log-in process again (see Connect the AP to a modem and log in for the first time on page 32 or Connect the AP to a routing device and log in for the first time on page 28).

CAUTION: The following process erases all settings that you configured in the AP.

To erase the settings:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.

The Backup Settings page displays.

5. Click the **Erase** button.
   A warning page displays.
6. Click the **Yes** button.
   The configuration is reset to factory default settings. When the reset is complete, the AP reboots. This process takes about two minutes.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, do not close the browser, click a link, or load a new page. Do not turn off the AP. Wait until the AP finishes restarting and the Power LED turns solid green.

Time and Network Time Protocol server

By default, the AP receives its time settings from a NETGEAR Network Time Protocol (NTP) server. You can change to another NTP server or set the time zone and daylight saving time manually.

Manually set the time zone and adjust the daylight saving time

The AP might detect the time zone automatically or you might need to adjust the time zone and daylight saving time settings. When the AP synchronizes its clock with a Network Time Protocol (NTP) server, the AP detects the date and time. If the AP does not detect the correct date and time, you might need to manually set the time zone and adjust the daylight saving time setting.

To manually set the time zone and adjust the daylight saving time setting:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Administration > NTP Settings**.

   The NTP Settings page displays.

5. From the **Time Zone** menu, select the time zone for the area in which the AP operates.
6. If the AP is in an area that observes daylight saving time, select the **Automatically adjust for daylight saving times** check box.
7. Click the **Apply** button.

   Your settings are saved.

   When the AP connects over the Internet to an NTP server, the date and time that display on the page are adjusted according to your settings.

Change the Network Time Protocol server

By default, the AP uses the NETGEAR NTP server to synchronize the network time. You can change the Network Time Protocol (NTP) server to your preferred NTP server.

To change the NTP server to your preferred NTP server:

1. Connect your computer or mobile device to the AP in one of the following ways:

   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Administration > NTP Settings**.

   The NTP Settings page displays. The page also displays the current date and time. By default, the **Use default NETGEAR NTP server** radio button is selected.

5. Select the **Set your preferred NTP server** radio button.
6. Enter the NTP server domain name or IP address in the **Primary NTP server** field.
7. Click the **Apply** button.

   Your settings are saved.

   When the AP connects over the Internet to the new NTP server, the date and time that display on the page might be adjusted.

Logs

The logs are a detailed record of many activities that occur on the AP. You can manage which activities are logged.

Display, send, or clear the logs

The logs displays information about the operation and networks of the AP. You can send the logs by email or clear the logs.

To display, send, or clear the logs:

1. Connect your computer or mobile device to the AP in one of the following ways:

   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Administration > Logs**.

   The Logs page displays.

5. To send the logs by email, click the **Send Log** button.

   The AP sends the logs to the email address that you specified for email notifications (see Set up security event email notifications on page 88).

6. To refresh the log entries onscreen, click the **Refresh** button.
7. To clear the log entries, click the **Clear Log** button.

Specify which activities the AP logs

You can specify which activities the AP logs. These activities display in the log.

To manage which activities are logged:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

The local device password is the one that you set. The local device password is case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Administration > Logs**.
   The Logs page displays.
5. Select the check boxes that correspond to the activities that you want to be logged.
   Some activities do not apply if the AP is in AP mode.

   By default, the following check boxes are selected:

   - Attempted access to blocked services
   - Connections to the Web-based interface of this Router
     (A log entry is created when someone makes a connection to the device UI of the AP).
   - Router operation (startup, get time, etc)
   - Known DoS attacks and Port Scans
   - Port Forwarding / Port Triggering
   - Wireless access
     (A log entry is created when someone connects to a WiFi network on the AP.)
   - Turn off wireless signal by schedule
     (A log entry is created when a radio is turned on or off because of a WiFi schedule.)
6. Clear the check boxes that correspond to the activities that you do not want to be logged.
7. Click the **Apply** button.
   Your settings are saved.

Status and statistics

You can view information about the AP and its ports and the status of the Internet connection and WiFi network. In addition, you can view traffic statistics for the various ports.

Display information about the Internet port, AP, and WiFi settings [router mode]

If the AP is in router mode, you can display information about the AP, the WAN and LAN IP addresses, and the WiFi networks in each radio band.

To display information about the AP and the IP and WiFi settings if the AP is in router mode:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED**.

   The ADVANCED Home page displays.

   The color in the heading of each of the panes uses the following coding:

   - **Green circle**: The settings are fine and no problems exist. For a WiFi network, a green circle displays if the network is enabled and secured.
   - **Red circle**: Settings are disabled, a problem exists, or the connection is down. For a WiFi network, a red circle displays if the network is disabled.

   The following tables describe the fields in the panes on the Advanced Home page.

Field	Description
Router Information	
Hardware Version	The AP hardware version, which is the model number.
Firmware Version	The AP firmware version. If you update the firmware, the version changes (see Update the firmware on page 111).
GUI Language Version	The AP language version for the device UI.
Operation Mode	The operation mode is Router. For more information about the changing the operation mode, see Change the operation mode to AP mode or router mode on page 144.
CPU Load	The usage load on the CPUs
Memory Usage (Used/Total)	The RAM memory that is being used and the available memory.
Flash Usage (Used/Total)	The flash memory that is being used and the available memory.
System Uptime	The time elapsed since the AP was last restarted.
LAN Port (This is a subsection in the Router Information pane)	
MAC Address	The single MAC address that applies to all four AP LAN ports combined.
IP Address	The IP address that applies to all four AP LAN ports. For more information, see Change the LAN IP address and subnet settings [router mode] on page 91.
DHCP Server	If the AP is in router mode, this field displays if the DHCP server of the AP is enabled (the default setting in router mode) or disabled (see Disable the DHCP server [router mode] on page 94).
IP Subnet Mask	The IP subnet mask that applies to all four AP LAN ports. For more information, see Change the LAN IP address and subnet settings [router mode] on page 91.
DHCP Lease Time	The DHCP lease time. For more information, see Manage the DHCP server address pool [router mode] on page 92.

Field	Description
Internet Port To change these settings, see, Use the Setup Wizard [router mode] on page 44 or Manually set up the AP Internet connection [router mode] on page 45.	
MAC Address	The MAC address that applies to the AP WAN (Internet) port.

(Continued)

Field	Description
IP Address	The WAN IP address that the AP receives from your ISP (through your modem) or the WAN IP address that you manually configured.
Connection	The type of Internet connection that the AP uses, which can be DHCP (the default setting), Static IP, or PPPoE.
IP Subnet Mask	The IP subnet mask that the AP uses.
Domain Name Server	The IP address of the Domain Name System (DNS) server that the AP uses.
WAN Preference	This field shows *Internet Port* and the speed of the connection.

Field	Description
Wireless Settings (2.4 GHz) or **Wireless Settings (5.0 GHz)** These settings display for each WiFi network and each band. To change these settings, see Basic WiFi and Radio Features on page 52 and Advanced WiFi and Radio Features on page 149.	
Name	The name of the SSID (see Set up or change an open or secure WiFi network on page 53).
Region	The country and region in which the AP is being used (see Change the region of operation on page 150).
Channel	The channel that the radio uses (see Change the channel for a radio on page 155).
Mode	The WiFi throughput mode that the radio uses (see Change the WiFi throughput mode on model WAX202 on page 157).
Wireless AP	Displays if the WiFi network is enabled (see Set up or change an open or secure WiFi network on page 53 or Enable or disable a WiFi network on page 60).

(Continued)

Field	Description
Broadcast Name	Displays if the WiFi network broadcasts its SSID (see Broadcast or hide the SSID for a WiFi network on page 61).
Wi-Fi Protected Setup	This setting applies to the Wireless 1 network only. Displays if WPS is enabled. **Note**: If you either set up open security for the Wireless 1 network or disable the WiFi radios, WPS is disabled.

Display information about the LAN port, AP, and WiFi settings [AP mode]

If the AP is operating in AP mode, you can display information about the AP, the LAN IP addresses, and the WiFi networks in each radio band.

To display information about the AP and the IP and WiFi settings if the AP is operating in AP mode:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED**.

The ADVANCED Home page displays.

The color in the heading of each of the panes uses the following coding:

- **Green circle**: The settings are fine and no problems exist. For a WiFi network, a green circle displays if the network is enabled and secured.
- **Red circle**: Settings are disabled, a problem exists, or the connection is down. For a WiFi network, a red circle displays if the network is disabled.

The following tables describe the fields in the panes on the Advanced Home page.

Field	Description
Router Information	
Hardware Version	The AP hardware version, which is the model number WAX204.
Firmware Version	The AP firmware version. If you update the firmware, the version changes (see Update the firmware on page 111).
GUI Language Version	The AP language version for the device UI.
Operation Mode	The operation mode is AP. For more information about the changing the operation mode, see Change the operation mode to AP mode or router mode on page 144.
CPU Load	The usage load on the CPUs
Memory Usage (Used/Total)	The RAM memory that is being used and the available memory.
Flash Usage (Used/Total)	The flash memory that is being used and the available memory.
System Uptime	The time elapsed since the AP was last restarted.

Field	Description
LAN Port You cannot change these settings when the AP operates in AP mode.	
MAC Address	The MAC address that applies to the AP WAN (Internet) port.
DHCP	Displays if the DHCP client of the AP is enabled.
IP Address	The LAN IP address that the AP receives from an existing router in your network or the static (fixed) IP address that you manually configured.
IP Subnet Mask	The IP subnet mask that the AP uses.

(Continued)

Field	Description
Gateway IP Address	The IP address of the gateway to which the AP connects to the Internet.
Domain Name Server	The IP address of the Domain Name System (DNS) server that the AP uses.

Field	Description
Wireless Settings (2.4 GHz) or **Wireless Settings (5.0 GHz)** These settings display for each WiFi network and each band. To change these settings, see Basic WiFi and Radio Features on page 52 and Advanced WiFi and Radio Features on page 149.	
Name	The name of the SSID (see Set up or change an open or secure WiFi network on page 53).
Region	The country and region in which the AP is being used (see Change the region of operation on page 150).
Channel	The channel that the radio uses (see Change the channel for a radio on page 155).
Mode	The WiFi throughput mode that the radio uses (see Change the WiFi throughput mode for a radio on page 156).
Wireless AP	Displays if the WiFi network is enabled (see Set up or change an open or secure WiFi network on page 53 or Enable or disable a WiFi network on page 60).

(Continued)

Field	Description
Broadcast Name	Displays if the WiFi network broadcasts its SSID (see Broadcast or hide the SSID for a WiFi network on page 61).
Wi-Fi Protected Setup	This setting applies to the Wireless 1 network only. Displays if WPS is enabled. **Note**: If you either set up open security for the Wireless 1 network or disable the WiFi radios, WPS is disabled.

Check the Internet connection status

To check the Internet connection status:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED**.

   The ADVANCED Home page displays.
5. In the Internet Port pane (in router mode) or in the LAN Port pane (in AP mode), click the **CONNECTION STATUS** button.

The Connection Status pop-up window displays.

The information that displays depends on whether the AP is in router mode (the default operation mode) or AP mode and on the type of Internet connection.

When the AP receives an IP address dynamically (which is the most common type of connection), the following information displays:

- **IP Address**: The IP address that is assigned to the AP.
  In AP mode, the IP address is a LAN IP address. In router mode, the IP address is a WAN IP address.
- **Subnet Mask**: The subnet mask that is assigned to the AP.
- **Default Gateway**: The IP address for the default gateway that the AP communicates with.
  In AP mode, the IP address is a LAN IP address. In router mode, the IP address is a WAN IP address.
- **DHCP Server**: The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration to the AP.
  In AP mode, the IP address is a LAN IP address. In router mode, the IP address is a WAN IP address.
- **DNS Server**: The IP address of the Domain Name Service server that provides translation of network names to IP addresses.
  In AP mode, the IP address is a LAN IP address. In router mode, the IP address is a WAN IP address.
- **Lease Obtained**: The date and time when the DHCP IP address lease was obtained.
- **Lease Expires**: The date and time that the DHCP IP address lease expires.

6. When the AP receives an IP address dynamically, you can perform the following actions:
   - **Release the IP address**: Click the **Release** button to terminate the DHCP IP address, that is, terminate the Internet connection.
   - **Renew the IP address**: Click the **Renew** button to renew the DHCP IP address, that is, renew the Internet connection.

Display the Internet port statistics

To display the Internet port statistics:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED**.
   The ADVANCED Home page displays.
5. In the Internet Port pane (in router mode) or in the LAN Port pane (in AP mode), click the **Show Statistics** button.
   A pop-up window displays, showing the following information:
   - **System Up Time**: The time elapsed since the AP was last restarted.
   - **Port**: The statistics for the WAN (Internet) port, LAN (Ethernet) ports, and WLANs. For each port, the window displays the following information:
     - **Status**: The link status of the port.
     - **TxPkts**: The number of packets transmitted on this port since reset or manual clear.
     - **RxPkts**: The number of packets received on this port since reset or manual clear.
     - **Collisions**: The number of collisions on this port since reset or manual clear.

- **Tx B/s**: The current transmission (outbound) bandwidth used on the WAN and LAN ports.
- **Rx B/s**: The current reception (inbound) bandwidth used on the WAN and LAN ports.
- **Up Time**: The time elapsed since this port acquired the link.

6. To manage the polling, do one of the following:
   - To change the polling frequency, which is the interval at which the statistics are updated in this window, enter a time in seconds in the **Poll Interval** field and click the **Set Interval** button.
   - To stop the polling, click the **Stop** button.

Display the devices currently on the AP network and change device information

You can display the active wired and WiFi devices in the AP network. If you do not recognize a WiFi device, it might be an intruder.

If the AP is in router mode, you can also display the VPN devices in the AP network.

To display the attached wired, WiFi, and VPN devices or to change device information:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

The local device password is the one that you set. The local device password is case-sensitive.

The BASIC Home page displays.

4. Select **BASIC > Attached Devices**.
   The Attached Devices page displays:

   - Wired devices are connected to the AP with Ethernet cables. WiFi devices are connected to the AP through the WiFi network, in either the 2.4 GHz band or the 5 GHz band.
   - If you enabled access control (see Enable and manage network access control on page 77), the page displays the access control status of the device in the network.

   The following tables describe the fields on the Attached Devices page.

Field	Description
Status	If access control is enabled (see Enable and manage network access control on page 77), the access control status of the device in the network (Allowed or Blocked).
Connection Type	For WiFi devices, the connection type information shows the radio (2.4 GHz or 5 GHz) and WiFi network (Wireless 1, Wireless 2, or Wireless 3) to which the device is connected. For LAN devices, the connection type is always Wired.
Device Name, including device model and device type icon	The device name, if detected. This field also displays the device model, if detected, and device type icon. This information is for display only. You can change the information that displays (see Step 5).
IP Address	The IP address that is assigned to the device when it joined the AP network. This address can change when a device is disconnected and rejoins the network.
MAC Address	The MAC address of the device.

5. To change the information that displays for a device or the QoS priority, do the following:
   a. Select the check box for the device for which you want to change the information or priority.
   b. Click the **Edit** button.
      The Edit Device page displays.
   c. In the **Device Model** field, specify a model.
   d. In the **Device Name** field, specify a name.

e. From the **Device Type** menu, select a type.
The device type displays as a device icon on the Attached Devices page.

f. Click the **Apply** button.
Your settings are saved. The Attached Devices page displays again.

6. To refresh the information onscreen, click the **Refresh** button.
The information onscreen is updated.

Traffic meter [router mode]

If the AP is in router mode, you can enable traffic metering to monitor the volume of Internet traffic that passes through the AP's Internet (WAN) port. With the traffic meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

Start the traffic meter without traffic restrictions [router mode]

If the AP is in router mode, you can monitor the traffic volume without setting a limit on the volume or connection time.

To start or restart the traffic meter without configuring traffic volume or connection time restrictions:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
The Local Device Login page displays.
If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
The local device password is the one that you set. The local device password is case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.
The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.

By default, no traffic limit is specified and the traffic volume or connection time is not controlled.

6. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
7. To start the traffic counter immediately, click the **Restart Counter Now** button.
8. Click the **Apply** button.

   Your settings are saved.

   The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics [router mode] on page 143.

Restrict Internet traffic by volume [router mode]

If the AP is in router mode, you can record and restrict the traffic by volume in MB. This is useful when your ISP measures your traffic volume.

To record and restrict the Internet traffic by volume:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Traffic Meter**.

   The Traffic Meter page displays.

5. Select the **Enable Traffic Meter** check box.
6. Select the **Traffic volume control by** radio button.
7. From the corresponding menu, select an option:
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.

8. In the **Monthly Limit** field, enter how many MBytes (MB) per month are allowed.
9. If your ISP charges you for extra data volume when you make a new connection, enter the extra data volume in MB in the **Round up data volume for each connection by** field.
10. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
11. In the Traffic Control section, enter a value in MB to specify when the AP issues a warning message before the monthly limit in MB is reached.

    This setting is optional. The AP issues a warning when the balance falls below the number of MB that you enter. By default, the value is 0 and no warning message is issued.

12. Select one or more of the following actions to occur when the limit is reached:

    - **Turn the Internet LED to blinking green and blue**. This setting is optional. When the traffic limit is reached, the Internet LED alternates between green and blue.
    - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.

13. Click the **Apply** button.

    Your settings are saved.

    The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics [router mode] on page 143.

Restrict Internet traffic by connection time [router mode]

If the AP is in router mode, you can record and restrict the traffic by connection time. This is useful when your ISP measures your connection time.

The AP must be connected to the Internet for you to be able to restrict Internet traffic by connection time.

To record and restrict the Internet traffic by connection time:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Traffic Meter**.

   The Traffic Meter page displays.

5. Select the **Enable Traffic Meter** check box.
6. Select the **Connection time control** radio button.

   The AP must be connected to the Internet for you to be able to select the **Connection time control** radio button.

7. In the **Monthly Limit** field, enter how many hours per month are allowed.

   The AP must be connected to the Internet for you to be able to enter information in the **Monthly Limit** field.

8. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
9. In the Traffic Control section, enter a period in minutes to specify when the AP issues a warning message before the monthly limit in hours is reached.

   This setting is optional. The AP issues a warning when the balance falls under the number of minutes that you enter. By default, the value is 0 and no warning message is issued.

10. Select one or more of the following actions to occur when the limit is reached:

    - **Turn the Internet LED to blinking green and blue**. This setting is optional. When the traffic limit is reached, the Internet LED alternates between green and blue.
    - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.

11. Click the **Apply** button.

    Your settings are saved.

    The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics [router mode] on page 143.

View the Internet traffic volume and statistics [router mode]

If the AP is in router mode and you enabled the traffic meter (see Start the traffic meter without traffic restrictions [router mode] on page 139), you can view the Internet traffic volume and statistics.

To view the Internet traffic volume and statistics shown by the traffic meter:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.

   The Traffic Meter page displays.
5. Scroll down to the Internet Traffic Statistics section.

   The Internet Traffic Statistics section displays when the traffic counter was started and what the traffic balance is. The table displays information about the connection time and traffic volume in MB.
6. To refresh the information onscreen, click the **Refresh** button.

   The information is updated.
7. To display more information about the data traffic and to change the polling interval, click the **Traffic Status** button.

   The Traffic Status pop-up windows displays.

Unblock the traffic meter after the traffic limit is reached [router mode]

If the AP is in router mode and you configured the traffic meter to disconnect and disable the Internet connection after the traffic limit is reached, you cannot access the Internet until you unblock the traffic meter.

CAUTION: If your ISP set a traffic limit, your ISP might charge you for the overage traffic.

To unblock the traffic meter:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.
   The Traffic Meter page displays.
5. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.
6. Click the **Apply** button.
   Your settings are saved.

Change the operation mode to AP mode or router mode

By default, the AP's operation mode is router mode. However, if a device in your network already provides routing functions and you do not need the AP's routing functions, you can change the operation mode to AP mode. For more information about the operation

mode that is associated with each network setup, see What WiFi setup do you want? on page 26.

You can use the AP in either operation mode:

- **AP mode**: The AP functions as a WiFi 6 access point and can support LAN clients through its LAN ports. The AP receives its IP address settings from a routing device in your network. The AP passes on the IP address settings from the routing device to its clients so that Internet access is provided.

  Note: In AP mode, the AP does not require routing features, so they are masked out in the device UI. For example, routing features such as NAT filtering and the DHCP server are disabled so that they do not interfere with the routing device in your network. For more information about the features that are enabled in router mode but not required in AP mode, see Routing features enabled in router mode on page 41.

- **Router mode**: The AP functions as both a lightweight router and WiFi 6 access point, and can support LAN clients through its LAN ports. Because the AP is connected to your modem, the AP receives its IP address settings from your Internet service provider (ISP). The AP delivers IP address settings to its clients so that Internet access is provided.

To change the operation mode:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Router / AP Mode**.
   The Router / AP Mode page displays.

5. Specify the operation mode by doing one of the following:

   - **Router mode**: Select the **Router Mode** radio button.
     The page adjusts to provide information and the following options:

     - To manually change the Internet settings before you change the operation mode, click the **Internet Setup** button. For more information, see Manually set up the AP Internet connection [router mode] on page 45.
     - To change the WiFi settings before you change the operation mode, click the **Wireless Setup** button. For more information, see Set up or change an open or secure WiFi network on page 53.

   - **AP mode**: Select the **AP Mode** radio button.
     The page adjusts to provide information and the following options:

     - Although you can configure a fixed IP address, we recommend that you leave the **Get dynamically from existing access point/router** button selected to let the AP get an IP address dynamically from the existing router in your network.
       To configure a static IP address, click the **Use fixed IP Address (not recommended)** button, and in the fields that display below the **Learn more** button, change the IP address information.
     - To change the device name before you change the operation mode, click the **Edit** button.
     - To change the WiFi settings before you change the operation mode, click the **Wireless Setup** button. For more information, see Set up or change an open or secure WiFi network on page 53.

6. Click the **Apply** button.
   Your settings are saved and the AP is reconfigured in the new operation mode.

Disable LED blinking or turn off LEDs

The LEDs on the front panel of the AP indicate activities and behavior. By default, the Internet LED, LAN LED, and WLAN LEDs blink when the AP detects data traffic. You can disable LED blinking for data traffic, or turn off all LEDs except the Power LED.

To disable LED blinking or turn off the LEDs:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > LED Control Settings**.
   The LED Control Settings page displays.
   By default, the first radio button is selected, which allows standard LED behavior.
   For more information about LEDs, see Front panel with LEDs on page 16.
5. Select a radio button:
   - **Disable blinking on Internet LED, LAN LED, Wireless LED when data traffic is detected**
   - **Turn off all LEDs except Power LED**
6. Click the **Apply** button.
   Your settings are saved.

Check your Internet bandwidth

You can use Ookla Speedtest to detect your Internet bandwidth.

To check your Internet bandwidth using a speed test:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **BASIC > Speed Test**.
   The Speed Test page displays.
5. Click the **Test Speed** button.
   After a short time, your Internet's download and upload speeds display.

10

Advanced WiFi and Radio Features

This chapter describes how you can manage the advanced WiFi and radio features of the AP. For information about the basic WiFi and radio settings, see Basic WiFi and Radio Features on page 52.

Note: If you want to change the WiFi network settings, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

The chapter includes the following sections:

- Change the region of operation
- Manage 802.11ax and enable or disable OFDMA for a radio
- Enable or disable smart connect for the AP
- Enable or disable 20/40 MHz coexistence for the 2.4 GHz radio
- Change the channel for a radio
- Change the WiFi throughput mode for a radio
- Change the CTS/RTS threshold and preamble mode for a radio
- Change the transmission output power for a radio
- Add a WiFi schedule for a radio
- Enable or disable MU-MIMO
- Enable or disable explicit beamforming
- Enable or disable PMF
- Set up the AP as a WiFi Bridge to another AP or WiFi router
- Manage the WPS settings

Note: In this chapter, we refer to the access point as the AP.

Change the region of operation

You can change the region of operation, which is the region in which you operate the AP. For some countries such as North America, you cannot change the region because it is preset.

Note: Make sure the country is set to the location where the device is operating. You are responsible for complying within the local, regional, and national regulations set for channels, power levels, and frequency ranges.

WARNING: It might not be legal to operate the AP in a region other than the regions listed in the menu. If your country or region is not listed, check with your local government agency.

To change the region of operation:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays.
5. From the **Region** menu, select the region in which the AP must operate.
6. Click the **Apply** button.

Your settings are saved. The AP restarts with the settings for the new region.

Manage 802.11ax and enable or disable OFDMA for a radio

If 802.11ax (11AX) WiFi is enabled (which it is by default), you can enable Orthogonal Frequency-Division Multiple-Access (OFDMA) for the 5 GHz band. For model WAX202 only, you can also enable OFDMA for the 2.4 GHz band. By default, OFDMA is disabled on both radio bands, even when 11AX WiFi is enabled.

OFDMA allows data transmission signals to be split into smaller signals. The AP sends these small signals directly to individual devices in your network. Because multiple devices can be served in the same transmission window, the AP does not need to wait for WiFi access for every packet. This method of communication increases network speed and efficiency.

Note the following about OFDMA:

- Enable OFDMA if your network includes many Internet of things (IoT) devices.
- After you enable OFDMA, if you notice that some of your devices do not function as expected, disable OFDMA to see if the devices function fine.
- If your network includes many older devices, you might want to keep OFDMA disabled.

We recommend that you keep 11AX enabled.

To manage 11AX for both radios and enable or disable OFDMA for an individual radio:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
   The Wireless Settings page displays.
5. Select or clear the **Enable 11AX** check box.
   Selecting this check box enables 11AX for both radio bands. If you disable 11AX, you cannot enable OFDMA for either radio band.
6. If 11AX is enabled, select or clear the **Enable OFDMA in 5GHz** check box.
   Selecting this check box enables OFDMA in the 5 GHz radio band.
7. For model WAX202 only: If 11AX is enabled, select or clear the **Enable OFDMA in 2.4GHz** check box.
   Selecting this check box enables OFDMA in the 2.4 GHz radio band.
8. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Enable or disable smart connect for the AP

Smart connect automatically selects the fastest WiFi band for a WiFi client device that is connected to the AP. By default, smart connect is disabled. (During initial login, or when you ran the Setup Wizard, you might have enabled smart connect.)

When smart connect is enabled, it applies to all WiFi networks on the AP. For each individual WiFi network, the 2.4 GHz and 5 GHz bands use the same WiFi network name (SSID) and network key (WiFi password). That means that when you connect to a WiFi network on the AP, you see only *one* SSID, which connects to both bands of the WiFi network.

Note: If smart connect is enabled and the SSID and passwords for the 2.4 GHz and 5 GHz bands do not match, the WiFi settings for 2.4 GHz band overwrite the WiFi settings for the 5 GHz band.

If the smart connect feature is enabled, in addition to the SSID and network key, the following WiFi settings apply to both radios simultaneously, which means that you cannot configure these settings for each radio individually:

- Enabling or disabling the WiFi radios
- Changing the CTS/RTS threshold and preamble mode for the radios
- Changing the transmission output power for the radios
- Adding a WiFi schedule for the radios

To enable or disable smart connect:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays.
5. Select or clear the **Enable smart connect** check box.

   Selecting this check box enables smart connect and clearing this check box disables smart connect.

   By default, smart connect is disabled (unless you enabled it during initial login) and the check box is cleared.
6. Click the **Apply** button.

Your settings are saved. The radios restart and WiFi clients might need to reconnect.

Enable or disable 20/40 MHz coexistence for the 2.4 GHz radio

20/40 coexistence allows a 20 MHz and 40 MHz channel width to be supported simultaneously. By default, 20/40 MHz coexistence is enabled on the 2.4 GHz radio to prevent interference between WiFi networks in your environment at the expense of the WiFi speed. If no other WiFi networks are present in your environment, you can disable 20/40 MHz coexistence to increase the WiFi speed on the 2.4 GHz radio to the maximum supported speed for the WiFi mode.

20/40 MHz coexistence does not apply to the 5 GHz radio.

To enable or disable 20/40 MHz coexistence for the 2.4 GHz radio:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
   The Wireless Settings page displays.
5. Select or clear the **Enable 20/40 MHz co-existence 2.4 GHz** check box.

Selecting this check box enables 20/40 MHz coexistence and clearing this check box enables 20/40 MHz coexistence.
By default, 20/40 MHz coexistence is enabled and the check box is selected.

6. Click the **Apply** button.
   Your settings are saved. The 2.4 GHz radio restarts and WiFi clients might need to reconnect.

Change the channel for a radio

The available WiFi channels and frequencies depend on the region or country and the radio. For the 2.4 GHz radio, the default is Auto, which means that the radio automatically selects the most suitable channel. When you select a particular channel, the channel selection becomes static, which means that the AP uses only that channel until you change the channel setting again. For the 5 GHz radio, the default channel depends on the region.

Note: You do not need to change the WiFi channel unless you experience interference (which is indicated by lost connections).

Note: If you use multiple WiFi access points in your network, or your AP is close to another one, reduce interference by selecting different channels for adjacent access points. We recommend a channel spacing of four channels between adjacent access points (for example, for 2.4 GHz radios, use channels 1 and 5, or 6 and 10).

To change the channel for a radio:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays.

5. From the **2.4 GHz channel** or **5 GHz channel** menu, select a channel.

   For the 2.4 GHz radio, the default is Auto, which means that the radio automatically selects the most suitable channel. When you select a particular channel, the channel selection becomes static. For the 5 GHz radio, the default channel depends on the region.

6. Click the **Apply** button.

   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the WiFi throughput mode for a radio

By default, all types of WiFi clients can access a WiFi network on the AP. The AP supports WiFi throughput modes 802.11ax, 802.11ac, 802.11a, 802.11n, 802.11g, and 802.11b. You can change the WiFi throughput mode for a radio to better suit your WiFi environment. However, in doing so, you might limit the speed that some WiFi clients are capable of.

With the exception of some legacy throughput modes, each throughput mode is associated with a channel width, such as HT20 or HT80, and a quadrature amplitude modulation (QAM) mode, such as 256 QAM or 1024 QAM.

Change the WiFi throughput mode on model WAX202

To change the WiFi throughput mode for a radio on model WAX202:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
   The Wireless Settings page displays.
5. From the **Mode** menu for a radio, select the WiFi throughput mode:
   - **2.4 GHz mode**: Select one of the following WiFi throughput modes for the 2.4 GHz radio:
     - **Up to 54 Mbps (11g)**: Legacy mode. This mode allows 802.11ax, 802.11n, 802.11g, 802.11b, devices to join the network but limits 802.11ax and 802.11n devices to functioning at up to 54 Mbps.
     - **Up to 286 Mbps (11ax, HT20, 1024-QAM)**: Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11ax and 802.11n devices to functioning at up to 286 Mbps. This mode supports a 20 MHz–wide channel and 1024 quadrature amplitude modulation (QAM).
     - **Up to 573 Mbps (11ax, HT40, 1024-QAM)**: Performance mode. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network

and allows 802.11ax devices to function at up to 573 Mbps. This mode is the default mode.
This mode supports a 40 MHz–wide channel and 1024 QAM.

- **5 GHz mode**: Select one of the following WiFi throughput modes for the 5 GHz radio:
  - **Up to 286 Mbps (11ax, HT20, 1024-QAM)**: Legacy mode. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the network but limits 802.11ax, 802.11ac, and 802.11n devices to functioning at up to 286 Mbps.
    This mode supports a 20 MHz–wide channel and 1024 QAM.
  - **Up to 573 Mbps (11ax, HT40, 1024-QAM)**: Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the network but limits 802.11ax and 802.11ac devices to functioning at up to 573 Mbps.
    This mode supports a 40 MHz–wide channel and 1024 QAM.
  - **Up to 1200 Mbps (80 MHz) (11ax, HT80, 1024-QAM)**: Performance mode. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the network and allows 802.11ax and 802.11ac devices to function at up to 1200 Mbps. This mode is the default mode.
    This mode supports a 80 MHz–wide channel and 1024 QAM.

6. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the WiFi throughput mode on model WAX206

To change the WiFi throughput mode for a radio on model WAX206:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
   The Wireless Settings page displays.

5. From the **Mode** menu for a radio, select the WiFi throughput mode:

   - **2.4 GHz mode**: Select one of the following WiFi throughput modes for the 2.4 GHz radio:

     - **Up to 54 Mbps (11g)**: Legacy mode. This mode allows 802.11n, 802.11g, and 802.11b, devices to join the network but limits 802.11n devices to functioning at up to 54 Mbps.
     - **Up to 346 Mbps (11ng, HT20, 256-QAM)**: Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11ng devices to functioning at up to 346 Mbps.
       This mode supports a 20 MHz–wide channel and 256 quadrature amplitude modulation (QAM).
     - **Up to 800 Mbps (11ng, HT40, 256-QAM)**: Performance mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11ng devices to function at their maximum speed. This mode is the default mode.
       This mode supports a 40 MHz–wide channel and 256 QAM.

   - **5 GHz mode**: Select one of the following WiFi throughput modes for the 5 GHz radio:

     - **Up to 573 Mbps (11ax, HT20, 1024-QAM)**: Legacy mode. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the network but limits 802.11ax and 802.11ac devices to functioning at up to 573 Mbps.
       This mode supports a 20 MHz–wide channel and 1024 QAM.
     - **Up to 1147 Mbps (11ax, HT40, 1024-QAM)**: Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the network but limits 802.11ax devices to functioning at up to 1147 Mbps.

This mode supports a 40 MHz–wide channel and 1024 QAM.

- **Up to 2400 Mbps (80 MHz) (11ax, HT80, 1024-QAM)**: Performance mode. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the network and allows 802.11ax and 802.11ac devices to function at up to 2400 Mbps. This mode is the default mode.
  This mode supports a 80 MHz–wide channel and 1024 QAM.

6. Click the **Apply** button.
   Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

Change the CTS/RTS threshold and preamble mode for a radio

For most WiFi networks, the CTS/RTS threshold and preamble mode work fine and we recommend that you do not change the settings. (In general, these settings are intended for WiFi testing.)

CAUTION: Do not change these settings unless directed by NETGEAR support or unless you are sure what the consequences are. Incorrect settings might disable the WiFi function of a radio unexpectedly.

IMPORTANT: If you enabled the smart connect feature, the CTS/RTS threshold and preamble mode apply to both radios. That means that you cannot change the CTS/RTS threshold and preamble mode for each radio individually.

To change the CTS/RTS threshold and preamble mode for a radio:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays.

5. Do one of the following:

   - **2.4 GHz radio**: To change the settings for the 2.4 GHz radio, scroll down to the Advanced Wireless Settings (2.4 GHz/b/g/n/ax) section.
   - **5 GHz radio**: To change the settings for the 5 GHz radio, scroll down to the Advanced Wireless Settings (5 GHz 802.11a/n/ac/ax) section.

   Note: If you enabled the smart connect feature, the page presents a single option only in the Advanced Wireless Settings (2.4 GHz/b/g/n/ax & 5 GHz 802.11a/n/ac/ax) section. In that situation, any change in the CTS/RTS threshold or preamble mode applies to both radios simultaneously. If the smart connect feature is disabled, you can change the CTS/RTS threshold and preamble mode for each radio individually.

6. In the **CTS/RTS threshold (1-2347)** field, enter a value from 1 to 2437.

   The default value is 2347.

7. Form the **Preamble Mode** menu, select the preamble mode:

   - **Automatic**: The automatic option (which is the default option) lets the AP process both long and short preambles.
   - **Long Preamble**: A long transmit preamble might provide a more reliable connection or a slightly longer range.
   - **Short Preamble**: A short transmit preamble might give better performance.

   CAUTION: Incorrect settings might disable the WiFi function for the selected radio unexpectedly.

8. Click the **Apply** button.

   Your settings are saved.

Change the transmission output power for a radio

By default, the transmission output power of the AP is set at the maximum. If two or more APs are operating in the same area and on the same channel, interference can occur. In such a situation, you might want to decrease the transmission output power for one or both radios. Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.

IMPORTANT: If you enabled the smart connect feature, any change in the transmission output power applies to both radios. That means that you cannot change the transmission output power for each radio individually.

To change the transmission output power for a radio:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays.

5. Do one of the following:
   - **2.4 GHz radio**: To change the settings for the 2.4 GHz radio, scroll down to the Advanced Wireless Settings (2.4 GHz/b/g/n/ax) section.
   - **5 GHz radio**: To change the settings for the 5 GHz radio, scroll down to the Advanced Wireless Settings (5 GHz 802.11a/n/ac/ax) section.

   Note: If you enabled the smart connect feature, the page presents a single option in the Advanced Wireless Settings (2.4 GHz/b/g/n/ax & 5 GHz 802.11a/n/ac/ax) section. In that situation, any change in the transmission output power applies to both radios simultaneously. If the smart connect feature is disabled, you can change the transmission output power for each radio individually.

6. From the **Transmit Power Control** menu , select **100%**, **75%**, **50%**, or **25%**.
   The default setting is 100%.
7. Click the **Apply** button.
   Your settings are saved. The radio restarts and WiFi clients might need to reconnect.

Add a WiFi schedule for a radio

You can use this feature to turn off the WiFi signal from a radio at times when you do not need a WiFi connection. For example, you might turn it off at night, for the weekend, or for a holiday. You can add multiple schedules but only a single schedule can be active for each radio.

Note: You can add a WiFi schedule only if the AP is connected to the Internet and synchronizes its internal clock with a time server on the Internet. For more information about whether the AP synchronizes its clock, see Time and Network Time Protocol server on page 123.

IMPORTANT: If the smart connect feature is enabled (by default, it is not, unless you enabled it during initial login), you can add a WiFi schedule that applies to both radios. That means that you cannot add a WiFi schedule for each radio individually.

To add a WiFi schedule for a radio:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays. The lower part of the page is called the Advanced Wireless Settings page. (As you scroll down on the page, the page name changes.)
5. Do one of the following:
   - **2.4 GHz radio**: To change the settings for the 2.4 GHz radio, scroll down to the Advanced Wireless Settings (2.4 GHz b/g/n/ax) section.
   - **5 GHz radio**: To change the settings for the 5 GHz radio, scroll down to the Advanced Wireless Settings (5 GHz 802.11a/n/ac/ax) section.

   Note: If the smart connect feature is enabled (by default, it is not, unless you enabled it during initial login), the page presents a single option in the Advanced Wireless Settings (2.4 GHz b/g/n/ax & 5 GHz 802.11a/n/ac/ax) section. In that situation, setting up or changing a WiFi schedule applies to both radios simultaneously. If the smart connect feature is disabled, you can set up or change a WiFi schedule for each radio individually.
6. Click the **Add a new period** button.

The settings display for specifying when you want to turn off the WiFi signal.

7. Select times from the **Start** and **End** menus to set up a period to turn off the WiFi signal for the selected radio.

   The start time and end time cannot be identical, even if they fall on different days. For example, if you start the schedule at 12:00 midnight, you cannot end it on another day at 12:00 midnight but you *can* end it at 11:30 p.m. or 12:30 a.m.

8. Specify the pattern by selecting either the **Daily** radio button for a daily recurrence (the default setting) or the **Select Days** radio button for recurrence on specific days of the week, and then select the check boxes for the days.
9. Click the **Apply** button.

   Your settings are saved, the Advanced Wireless Settings page displays again, and the new schedule shows in the table for the selected radio.

10. To enable a schedule immediately, do the following above the table,
    a. In the table, select the radio button for the schedule.
       The radio button for the schedule also lets you select the schedule if you want to change (edit) or delete it.
    b. Select the **Turn off wireless signal by schedule** check box.

11. Click the **Apply** button.

    Your settings are saved and the schedule becomes active. The WiFi signal is turned off according to the schedule that you added.

Enable or disable MU-MIMO

Multiuser multiple input, multiple output (MU-MIMO) improves performance when multiple MU-MIMO-capable WiFi clients transfer data at the same time. WiFi clients must support MU-MIMO. This feature is enabled by default, but you can disable it.

Note: When MU-MIMO is enabled, Tx beamforming is automatically enabled and you cannot disable it.

To enable or disable MU-MIMO:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
   The Wireless Settings page displays.
5. Scroll down the bottom of the page.
6. Select or clear the **Enable MU-MIMO** check box.
   Selecting this check box enables MU-MIMO. By default, MU-MIMO is enabled.
7. Click the **Apply** button.
   Your settings are saved. The radios restart and WiFi clients might need to reconnect.

Enable or disable explicit beamforming

Explicit beamforming (which is the same as Tx beamforming) lets the AP actively track WiFi clients and direct power to the AP antenna closest to the client.

With this technique, the AP uses information about the WiFi communication link with clients to improve signal transmission to the clients. Explicit beamforming provides better reception, range, and throughput while minimizing interference.

Explicit beamforming functions whether or not the client supports beamforming.

Note: When MU-MIMO is enabled, explicit beamforming is automatically enabled and you cannot disable it.

To enable or disable explicit beamforming when MU-MIMO is disabled:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays.
5. Scroll down the bottom of the page.
6. Select or clear the **Enable Tx Beamforming** check box.

   Selecting this check box enables explicit beamforming. (Tx beamforming is another term for explicit beamforming.)
   By default, MU-MIMO is enabled, and therefore explicit beamforming is also enabled. If MU-MIMO is disabled, explicit beamforming is automatically enabled, but you can disable it.
7. Click the **Apply** button.

   Your settings are saved. The radios restart and WiFi clients might need to reconnect.

Enable or disable PMF

Protected Management Frames (PMF), according to the 802.11w standard, is a security feature that protects unicast and multicast management frames from being intercepted and changed for malicious purposes. PMF, which is enabled by default, requires devices on the AP WiFi networks to support PMF. However, you can disable PMF, for example, if your network includes many legacy WiFi clients that do not support PMF.

To enable or disable PMF:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays.
5. Scroll down the bottom of the page.
6. Select or clear the **Disable PMF** check box.

   Selecting this check box disables PMF. By default, PMF is enabled and the check box is cleared.
7. Click the **Apply** button.

   Your settings are saved. The radios restart and WiFi clients might need to reconnect.

Set up the AP as a WiFi Bridge to another AP or WiFi router

You can use the AP as a *WiFi bridge* with a WiFi connection (which forms the actual *bridge*) to another access point or WiFi router that has a wired Internet connection. In this section, we are referring to the access point or WiFi router with the wired Internet connection as the *base*. Using the WiFi connection between the base and the WiFi bridge, the base provides Internet access to the clients of the WiFi bridge.

The base does not require any special configuration because the WiFi bridge connects to an existing SSID as a WiFi client of the base, just like any other WiFi clients of the base.

With this setup, if the WiFi connection between the base and the WiFi bridge is at the fast 802.11ax speed, capable clients at the base and the WiFi bridge can communicate with each other at 802.11ax speed. If you use a model WAX206 AP as the base (that model has a 2.5 Gbps WAN port) together with an Internet service provider (ISP) connection that is very fast, capable clients of the WiFi bridge can also enjoy very fast Internet.

Note: High WiFi speeds that are possible *within* your network do not necessarily apply to your Internet traffic. The speed of your Internet traffic depends on the speed of your ISP connection and the speed that is supported by the equipment between your AP and your Internet connection (for example, your modem).

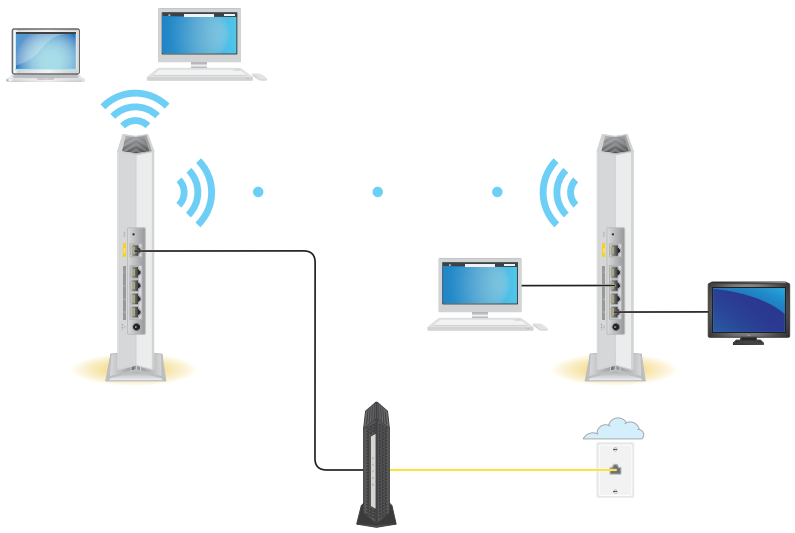

Figure 11. Base and WiFi bridge between two APs

In the previous sample figure, which uses two model WAX206 APs, the AP on the left functions as the base with a wired Internet connection over a modem. The base can support both wired and WiFi clients. The AP on the right functions as the WiFi bridge, has a WiFi connection the base, and can support wired clients only.

Note: A model WAX202 or WAX206 AP that functions as a WiFi bridge can support wired clients over its Ethernet ports. The WiFi bridge functions as a WiFi client of the base, but the WiFi bridge itself cannot not support WiFi clients.

Setting up a WiFi bridge with two WAX202 or WAX206 APs (or between a WAX202 AP and a WAX206 AP) offers the following benefits:

- Allow wired clients of both the WiFi bridge and the base to take advantage of the high WiFi speed (802.11ax) connection between the WiFi bridge and the base.
- Connect multiple clients such as a NAS, Smart TV, NeoTV, and Blu-ray player using a high-speed (802.11ax) WiFi connection.

As an example of a WiFi bridge setup, you could install the base in the office in which your Internet connection (your modem) is located. Then set up the WiFi bridge in a different room or floor. If you use a home office, you could use another room such as one where your home entertainment center is located. Cable the WiFi bridge to your Smart TV, NeoTV, or Blu-ray player to allow these clients to use the WiFi bridge's 802.11ax WiFi connection to the base in the office.

To set up a model WAX202 or WAX206 AP as a WiFi bridge to another access point or WiFi router that provides the wired Internet connection and that functions as the base:

1. Make a note of the WiFi settings of the base that provides the wired Internet connection.

   You must know the SSID, WiFi security mode, WiFi password, and operating frequency (either 2.4 GHz or 5 GHz).

2. Connect your computer or mobile device to the AP in one of the following ways:

   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

3. Launch a web browser and enter **routerlogin.net** in the address field.

   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

4. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Router / AP / Bridge Mode**.

   The Router / AP / Bridge Mode page displays.

6. Select the **Bridge Mode** radio button.

   The page adjusts.

7. Click the **Setup bridge mode wireless settings** button.

   The Wireless Settings pop-up window displays.

8. Enter the WiFi settings that the base is providing:
   a. From the **Choose a Wireless Network** menu, select the WiFi band that the base is using.
   b. In the **Name (SSID)** field, type the WiFi network name (SSID) that the base is providing and to which you want to connect the WiFi bridge as a client.
   c. In the Security Options section, select the radio button for the WiFi security that the base is using for the SSID.
   d. In the **Password (Network Key)** field, type the passphrase (WiFi password) that the base is using for the SSID.

9. Click the **Apply** button.

   Your settings are saved. The pop-up window closes.

10. To change the device name of the WiFi bridge, enter a new name in the **Device Name** field.

    By default, the device name is the AP model. If you use two APs of the same model and you want to distinguish the names, you could, for example, change the name to *WiFi bridge* or something similar.

11. To let the WiFi bridge dynamically get an IP address and DNS addresses from the base, leave the **Get IP Address Dynamically** and **Get DNS Server Address Dynamically** check boxes selected.

    We recommend that you leave the **Get IP Address Dynamically** and **Get DNS Server Address Dynamically** check boxes selected. However, if you are sure that

you must use a static IP address, use an IP address from the LAN IP address pool of the base. To specify a static IP address for the AP that functions as the WiFi bridge, do the following:

a. Clear the **Get IP Address Dynamically** check box.
   The **Get DNS Server Address Dynamically** check box is automatically cleared.

b. Enter all static IP address information and, if applicable, static DNS address information.

12. Click the **Apply** button.
    Your settings are saved. The WiFi bridge restarts with a new IP address.

13. To reconnect to the device UI of the WiFi Bridge, close your browser, make a wired connection to the WiFi bridge, launch a web browser, and enter **routerlogin.net** in the address field.
    For more information about making a wired connection, see Connect to the AP through an Ethernet cable on page 41.

Manage the WPS settings

Wi-Fi Protected Setup (WPS) lets you join the WiFi network without typing the WiFi password. By default, the existing WiFi settings are kept when a device joins an SSID using WPS, which is what we recommend. However, you can change this setting so that the next time that a WiFi device uses WPS to connect to an SSID, the WiFi settings change to an automatically generated random SSID and passphrase.

That means that for each AP WiFi network individually, a WiFi device that uses WPS to connect to the WiFi network causes the SSID and passphrase to change for *that* WiFi network. For information about viewing the automatically generated random SSID and passphrase, see Set up or change an open or secure WiFi network on page 53.

Note: If you enabled the smart connect feature, you cannot change the WPS settings.

To manage the WPS settings:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)

2. Launch a web browser and enter **routerlogin.net** in the address field.

Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.

The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings page displays. The lower part of the page is called the Advanced Wireless Settings page. (As you scroll down on the page, the page name changes.).

5. Select or clear the **Keep Existing Wireless Settings** check box.

   Selecting this check box enables an existing SSID and passphrase to be kept when a device joins the SSID using WPS. Clearing this check box causes an existing SSID and passphrase to be changed when a device joins the SSID using WPS.

   By default, the existing WiFi settings are kept when a device joins an SSID using WPS, and the check box is selected.

   Note: We recommend that you leave the **Keep Existing Wireless Settings** check box selected. Clear the check box *only* if you want to allow the WPS process to change SSIDs and passphrases.

   WARNING: If you clear the **Keep Existing Wireless Settings** check box, the SSID and passphrase for a WiFi network that accepts a device using WPS are automatically generated and other WiFi devices that are already connected to that WiFi network might be disconnected.

6. Click the **Apply** button.

   Your settings are saved.

11

Port Forwarding and Port Triggering [Router Mode]

As an advanced function of the AP firewall, you can use port forwarding and port triggering to set up port traffic rules for Internet services and applications. These rules apply specifically to ports. You need networking knowledge to set up port traffic rules.

Note: In AP mode, the port forwarding and port triggering settings that are described in this chapter are not required because they can be provided by the routing device to which the AP connects. Therefore, in AP mode, these port forwarding and port triggering settings are masked out in the local browser

This chapter includes the following sections:

Note: In this chapter, we refer to the access point as the AP.

Port forwarding to a local server for services and applications [router mode]

If the AP is in router mode, and if a server is part of your network, you can allow certain types of incoming traffic to reach the server. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

The AP can forward incoming traffic with specific protocols to computers on your local network. You can specify the servers for applications and you can also specify a default DMZ server to which the AP forwards all other incoming protocols (see Set up a default DMZ server [router mode] on page 74).

Forward incoming traffic for a default service or application [router mode]

If the AP is in router mode, you can forward traffic for a default service or application to a computer on your network.

To forward incoming traffic for a default service or application:

1. Decide which type of service, application, or game you want to provide.
2. Find the local IP address of the computer on your network that will provide the service.

   The server computer must always receive the same IP address. To specify this setting, use the reserved IP address feature (see Reserved LAN IP addresses [router mode] on page 97).
3. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
4. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
5. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
6. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

The Port Forwarding / Port Triggering page displays.

7. Make sure that the **Port Forwarding** radio button is selected.
8. From the **Service Name** menu, select the service or application.

   If the service or application that you want to add is not in the list, create a port forwarding rule with a custom service or application (see Add a port forwarding rule for a custom service or application [router mode] on page 176).

9. In the **Server IP Address** field, enter the LAN IP address of the computer or server that must provide the service or that runs the application.
10. Click the **Add** button.

    Your settings are saved and the rule is added to the table.

11. To sort the table by internal IP addresses, click the **Arrange By Internal IP** button.

Add a port forwarding rule for a custom service or application [router mode]

If the AP is in router mode, it lists default services and applications that you can use in port forwarding rules. If the service or application is not predefined, you can add a port forwarding rule with a custom service or application.

To add a port forwarding rule with a custom service or application:

1. Find out which port number or range of numbers the service or application uses.

   You can usually find this information by contacting the publisher of the service or application or through user groups or news groups.

2. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
3. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

4. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

The Port Forwarding / Port Triggering page displays.

6. Make sure that the **Port Forwarding** radio button is selected.
7. Click the **Add Custom Service** button.
   The Ports - Custom Services page opens.
8. Set up a new port forwarding rule for a custom service or application by specifying the following settings:
   - **Service Name**. Enter the name of the custom service or application.
   - **Service Type**. Select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.
   - **External port range**. If the service or application uses a single port, enter the port number in the **External port range** field. If the service or application uses a range or ranges of ports, specify the range in the **External port range** field. Specify one range by using a hyphen between the port numbers. Specify multiple ranges by separating the ranges with commas.
   - **Internal port range**. Specify the internal port or ports by one of these methods:
     - If the external and internal port or ports are identical, leave the **Use the same port range for Internal port** check box selected.
     - If the service or application uses a range or ranges of ports, clear the check box and specify the range in the **Internal port range** field. Specify one range by using a hyphen between the port numbers. Specify multiple ranges by separating the ranges with commas.
   - **Internal IP address**. Either enter an IP address in the **Internal IP address** field or select the radio button for a currently attached device that is listed in the table.
9. Click the **Apply** button.
   Your settings are saved. The rule is added to the table on the Port Forwarding / Port Triggering page.
10. To sort the table by internal IP addresses, click the **Arrange By Internal IP** button.

Change a port forwarding rule [router mode]

If the AP is in router mode, you can change an existing port forwarding rule.

To change a port forwarding rule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Make sure that the **Port Forwarding** radio button is selected.
6. In the table, select the radio button for the service or application name.
7. Click the **Edit Service** button.
   The Ports - Custom Services page displays.
8. Change the settings.
   For information about the settings, see Add a port forwarding rule for a custom service or application [router mode] on page 176.
9. Click the **Apply** button.
   Your settings are saved. The changed rule displays in the table on the Port Forwarding / Port Triggering page.

Remove a port forwarding rule [router mode]

If the AP is in router mode, you can remove a port forwarding rule that you no longer need.

To remove a port forwarding rule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.
5. Make sure that the **Port Forwarding** radio button is selected.
6. In the table, select the radio button for the service or application name.
7. Click the **Delete Service** button.

   The rule is removed from the table.

   A default rule remains available in the **Service Name** menu. A custom rule is removed. If you want to reinstate the custom rule, you must redefine it.

How the AP implements a port forwarding rule [router mode]

The following sequence shows the effects of a port forwarding rule:

1. When you enter the URL www.example.com in your browser, the browser sends a web page request message with the following destination information:
   - **Destination address**. The IP address of www.example.com, which is the address of your AP.
   - **Destination port number**. 80, which is the standard port number for a web server process.
2. The AP receives the message and finds your port forwarding rule for incoming port 80 traffic.
3. The AP changes the destination IP address in the message to, for example, 192.168.1.123 and sends the message to that computer.
4. Your web server at IP address 192.168.1.123 receives the request and sends a reply message to your AP.
5. Your AP performs Network Address Translation (NAT) on the source IP address and sends the reply through the Internet to the computer or mobile device that sent the web page request.

Application example: Make a local web server public [router mode]

If the AP is in router mode and you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

To make a local web server public:

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.

   In this example, your AP always assigns your web server an IP address of 192.168.1.33.
2. On the Port Forwarding / Port Triggering page, configure the AP to forward the HTTP service to the local address of your web server at 192.168.1.33.

   HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and specify that name on the Dynamic DNS page of the AP.

Dynamic DNS makes it much easier to access a server from the Internet because you can enter the name in the web browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

Port triggering for services and applications [router mode]

If the AP is in router mode, port triggering can function as a dynamic extension of port forwarding that is useful in these cases:

- An application must use port forwarding to more than one local computer (but not simultaneously).
- An application must open incoming ports that are different from the outgoing port.

With port triggering, the AP monitors traffic to the Internet from an outbound "trigger" port that you specify. For outbound traffic from that port, the AP saves the IP address of the computer that sent the traffic. The AP temporarily opens the incoming port or ports that you specify in your rule and forwards that incoming traffic to that destination.

Port forwarding creates a static mapping of a port number or range of ports to a single local computer. Port triggering can dynamically open ports to any computer when needed and close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance, we recommend that you do not disable Universal Plug-N-Play (UPnP, see Improve network connections with Universal Plug and Play [router mode] on page 106).

Add a port triggering rule and enable port triggering [router mode]

The AP does not provide default services and applications for port triggering rules. You must define a custom service or application for each port triggering rule. The AP must be in router mode.

To add a port triggering rule and enable port triggering:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
   The port triggering settings display.
6. Click the **Add Service** button.
   The Port Triggering - Services page displays.
7. Set up a new port triggering rule with a custom service or application by specifying the following settings:
   - **Service Name**. Enter the name of the custom service or application.
   - **Service User**. From the **Service User** menu, select **Any**, or select **Single address** and enter the IP address of one computer:
     - **Any**. This is the default setting and allows any computer on the Internet to use this service.
     - **Single address**. Restricts the service to a particular computer. Enter the IP address in the fields that become available with this selection from the menu.
   - **Service Type**. Select the protocol (**TCP** or **UDP**) that is associated with the service or application.
   - **Triggering Port**. Enter the number of the outbound traffic port that must open the inbound port or ports.
8. Set up the inbound connection by specifying the following settings:
   - **Service Type**. Select the protocol (**TCP** or **UDP**) that is associated with the inbound connection. If you are unsure, select **TCP/UDP**.
   - **Starting Port**. Enter the start port number for the inbound connection.
   - **Ending Port**. Enter the end port number for the inbound connection.

9. To enable port triggering, scroll up and clear the **Disable Port Triggering** check box.

   By default, the **Disable Port Triggering** check box is selected and port triggering is disabled.

10. Click the **Apply** button.

    Your settings are saved, the rule is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page, and port triggering is enabled.

Disable or change a port triggering rule [router mode]

If the AP is in router mode, you can disable or change an existing port triggering rule.

To disable or change a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

5. Select the **Port Triggering** radio button.

   The port triggering settings display.

6. To disable the rule, in the Port Triggering Portmap Table, clear the **Enable** check box.
7. To change the rule, do the following:
   a. In the Port Triggering Portmap Table, select the radio button for the service or application name.
   b. Click the **Edit Service** button.
      The Port Triggering - Services page displays.
   c. Change the settings.

For information about the settings, see Add a port triggering rule and enable port triggering [router mode] on page 181.

8. Click the **Apply** button.

   Your settings are saved. If you changed the rule, the new settings display in the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Remove a port triggering rule [router mode]

If the AP is in router mode, you can remove a port triggering rule that you no longer need.

To remove a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

5. Select the **Port Triggering** radio button.

   The port triggering settings display.

6. In the Port Triggering Portmap Table, select the radio button for the service or application name.
7. Click the **Delete Service** button.

   The rule is removed from the Port Triggering Portmap Table. If you want to reinstate the rule, you must redefine it.

Specify the time-out for port triggering [router mode]

The time-out period for port triggering controls how long the inbound ports stay open when the AP detects no activity. (The AP must be in router mode.) A time-out period is required because the AP cannot detect when the service or application terminates.

To specify the time-out for port triggering:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
   The port triggering settings display.
6. In the **Port Triggering Time-out** field, enter a value up to 9999 minutes.
   The default setting is 20 minutes.
7. Click the **Apply** button.
   Your settings are saved.

Enable or disable port triggering [router mode]

If the AP is in router mode and you add one or more port triggering rules, you can enable or disable port triggering. If you disable port triggering, the rules are not removed.

To enable or disable port triggering:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

The Local Device Login page displays.

If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.

3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.

5. Select the **Port Triggering** radio button.
   The port triggering settings display.

6. Clear or select the **Disable Port Triggering** check box.
   If this check box is cleared, port triggering is enabled for all rules that are individually enabled. If the check box is selected (the default setting), the AP does not apply port triggering rules, even if individual port triggering rules are enabled.

7. Click the **Apply** button.
   Your settings are saved.

Application example: Port triggering for Internet Relay Chat [router mode]

Some application servers, such as FTP and IRC servers, send replies to multiple port numbers. Using port triggering (if the AP is in router mode), you can tell the AP to open more incoming ports when a particular outgoing port starts a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the AP, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer."

The following sequence shows the effects of this port triggering rule:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your AP.

3. Your AP creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your AP stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and observing the destination port number of 6667, your AP creates another session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your AP using the NAT-assigned source port (for example, port 33333) as the destination port and also sends an "identify" message to your AP with destination port 113.
6. When your AP receives the incoming message to destination port 33333, it checks its session table to see if a session is active for port number 33333. Finding an active session, the AP restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your AP receives the incoming message to destination port 113, it checks its session table and finds an active session for port 113 associated with your computer. The AP replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.
8. When you finish your chat session, your AP eventually senses a period of inactivity in the communications. The AP then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

12

Diagnostics and Troubleshooting

This chapter provides information to help you diagnose and solve problems you might experience with the AP. If you do not find the solution here, visit the NETGEAR support site at netgear.com/support for more product and contact information.

The chapter contains the following sections:

Note: In this chapter, we refer to the access point as the AP.

Reboot the AP from the device UI

You or NETGEAR technical support can reboot the AP from its device UI, either locally or remotely, for example, if the AP seems to be unstable or is not operating normally.

To reboot the AP from the device UI:

1. Connect your computer or mobile device to the AP in one of the following ways:
   - Connect directly to the AP's WiFi network or LAN. (Applies to the AP in either operation mode.)
   - Connect to the same network that the AP is connected to. (Applies only if the AP is operating in AP mode.)
2. Launch a web browser and enter **routerlogin.net** in the address field.
   Instead, if you are connected to same network as the AP, enter the LAN IP address that is assigned to the AP. For information about finding the IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
   The Local Device Login page displays.
   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED**.
   The ADVANCED Home page displays.
5. In the Router Information pane, click the **REBOOT** button.
   A pop-up warning window displays.
6. Click the **Yes** button.
   The AP restarts.

Quick tips for troubleshooting

Many common problems can be resolved by following our tips for troubleshooting.

Restart your AP network if the AP is in router mode

If the AP is in router mode and you must restart your network, follow this sequence:

1. Disconnect the AP from your broadband, cable, or DSL device, or from your Ethernet outlet.
2. If your device is a modem, turn off and unplug the modem.
3. Turn off the AP.
4. If your device is a modem, plug in the modem and turn it on. Wait two minutes.
5. Reconnect the AP to your broadband, cable, or DSL device, or to your Ethernet outlet.
6. Turn on the AP and wait two minutes.

Restart your AP if it is operating in AP mode

If the AP is operating in AP mode and you must restart it, follow this sequence:

1. Turn off the AP.
2. Turn on the AP and wait two minutes.

Check the Ethernet cable connections

Make sure that the Ethernet cables are connected correctly and securely plugged in:

- If the AP is operating in router mode (the default operation mode), make sure that you connect the yellow WAN (Internet) port on the AP through an Ethernet cable to a LAN port on your broadband, cable, or DSL device (a modem), or to your Ethernet wall outlet.
- If the AP is operating in AP mode, make sure that you connect the yellow WAN (Internet) port on the AP through an Ethernet cable to a LAN port on your broadband, cable, or DSL device (a router), to your wall Ethernet outlet, to another existing router in your network, or to a switch or hub that is located between the AP and the router.
- For any computer or device that you connect directly through an Ethernet cable to the AP, make sure that you connect the Ethernet cable from the computer or device to one of the LANs port on the AP.

Check the WiFi settings of your computer or mobile device

If you connect over WiFi to the AP, make sure that the WiFi settings on your computer or mobile device and the AP match exactly. If you did not change the SSID for the Wireless 1 network, use the AP's default SSID that is printed on the AP label. If you did not change the passphrase (also referred to as the network key or WiFi password), use the unique default passphrase that is also printed on the AP label. The default security is WPA2-Personal [AES].

Note: If you set up an access control list (ACL) on the AP, depending on the type of ACL, you might need to add each computer or mobile device to the ACL (see Enable and manage network access control on page 77).

The AP provides three WiFi networks (Wireless 1, Wireless 2, and Wireless 3). By default, the Wireless 1 network is enabled and the other two WiFi networks are disabled. If the Wireless 2 and Wireless 3 networks are enabled and you did not change the default settings, you can access these networks as follows:

- **Wireless 2**: The default SSID is NETGEARXXXXXX-2, in which XXXXXX represents the last six characters of the AP's MAC address, and the default password is the default password for the Wireless 1 network, as printed on the AP label.
- **Wireless 3**: The default SSID is NETGEARXXXXXX-3, in which XXXXXX represents the last six characters of the AP's MAC address, and the default password is the default password for the Wireless 1 network, as printed on the AP label.

Check the DHCP network settings of your computer or mobile device

Make sure that the network settings of the computer or mobile device with which you want to connect to the AP are correct:

- **Router mode**: If the AP is operating in router mode (the default operation mode), make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the AP. If you are using the default addressing scheme, your device's address is in the range of 192.168.1.2 to 192.168.1.254.
- **AP mode**: If the AP is operating in AP mode, the LAN subnet to which your computer or device connects depends on the type of connection to the AP:
  - **Directly connected**: If you are directly connected over WiFi or an Ethernet cable to the AP network, make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the AP. If you are using the

default addressing scheme, your device's address is in the range of 192.168.1.2 to 192.168.1.254.

- **Connected to the same network but not directly connected**: If you are not directly connected to the AP, make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the existing network router to which the AP is connected.

Most computers and mobile devices function as DHCP clients. If your computer or mobile device does not, enable its DHCP client so that is can obtain an IP address automatically using DHCP.

Standard LED behavior when the AP is powered on

After you turn on power to the AP, verify that the following sequence of events occurs:

1. When power is first applied, verify that the Power LED is blinking amber.
2. After about two minutes, verify the following:
   - The Power LED is solid green.
   - The Internet LED is solid green.
   - The 2.4 GHz WLAN LED is solid green, solid blue, or blinking blue.
   - The 5 GHz WLAN LED is solid green, solid blue, or blinking blue.
   - If a LAN device is connected to one of the LAN ports of the AP, the LAN LED is solid or blinking green, or solid or blinking amber, depending on the speed of the connection.

   You can use the LEDs on the front panel of the AP for troubleshooting (see Troubleshoot with the LEDs on page 192)

Troubleshoot with the LEDs

You can troubleshoot by checking the LEDs.

Power LED is off

This could occur for a number of reasons. Check the following:

- Make sure that the power adapter is securely connected to your AP and securely connected to a working power outlet.
- Make sure that you are using the power adapter that NETGEAR supplied for this product.

Power LED does not turn green

When you turn on the AP, the Power LED blinks amber for about two minutes, after which it lights solid green.

When the AP is upgrading firmware, the Power LED blinks amber temporarily and finally lights solid green.

If the LED stays blinking amber five minutes after startup, or blinks amber at any other time (not including a firmware upgrade), this indicates a problem with the AP. In that situation, do the following:

- Restart the AP to see if it recovers. If the problem occurs again, try one more time.
- If the AP does not recover, press and hold the **Reset** button on the back to return the AP to its factory default settings. For more information, see Use the Reset button to return the AP to factory defaults on page 121. If the problem occurs again, try one more time.

If the error persists, a hardware problem might be the cause. Contact NETGEAR technical support at netgear.com/support/.

WAN (Internet) LED remains off [router mode]

If the AP is in router mode and the WAN (Internet) LED remains off, the AP did not get an Internet connection. Check the following:

- Make sure that the Ethernet cable connection is secure at the yellow WAN port (do *not* use a LAN port for this connection) of the AP and at an Ethernet port on the broadband, cable, or DSL device (a modem) or at your Ethernet wall outlet.
- Make sure that power is turned on to the connected broadband, cable, or DSL device. When you connect the AP's WAN port to a broadband, cable, or DSL device, use the cable that was supplied with the device. This cable can be a standard straight-through Ethernet cable or an Ethernet crossover cable.
- If the type of WAN connection of your broadband, cable, or DSL device is PPPoE, PPTP, or L2TP or requires a static IP address, make sure that you configured the Internet settings correctly.

For more information, see Specify a PPPoE Internet connection that uses a login [router mode] on page 47, Specify a PPTP or L2TP Internet connection that uses a login [router mode] on page 49,or Specify a dynamic or fixed WAN IP address Internet connection without a login [router mode] on page 45.

- Make sure that you completed the initial log-in process. For more information, see Connect the AP to a modem and log in for the first time on page 32 or, if you are connected to the device UI, see Use the Setup Wizard [router mode] on page 44.
- Make sure that your Internet service provider (ISP) is not experiencing an Internet outage.

WAN (Internet) LED remains off [AP mode]

If the AP is in AP mode and the WAN (Internet) LED remains off, the AP did not get an Internet connection. Check the following:

- Make sure that the Ethernet cable connection is secure at the yellow WAN port (do *not* use a LAN port for this connection) of the AP and at an Ethernet port on your broadband, cable, or DSL device (a router), another network router, a switch or hub that is connected to the router, or your Ethernet wall outlet. In AP mode, do not connect the cable directly to a device that functions as a modem.
- Make sure that power is turned on to the connected broadband, cable, or DSL device or other network router and that the device is connected to the Internet.
  When you connect the AP's WAN port to your broadband, cable, or DSL device or other network router, use a standard straight-through Ethernet cable or an Ethernet crossover cable.
- Make sure that you completed the initial log-in process. For more information, see Connect the AP to a routing device and log in for the first time on page 28.
- If the broadband, cable, or DSL device (a router) or other network router to which the AP is connected does not function as a DHCP server (this is very unusual), make sure that another DHCP server in the network is active. The AP functions as a DHCP client and must receive an IP address from a network router or a DHCP server.
- Make sure that your Internet service provider (ISP) is not experiencing an Internet outage.

One or both WLAN LEDs are off

If the 2.4 GHz WLAN LED, the 5 GHz WLAN LED, or both WLAN LEDs remains off, check to see if the radios on the AP are disabled (see Enable or disable a WiFi radio on page 66). By default, both radios are enabled and the WLAN LEDs light solid green without clients, solid blue with clients, and blinking blue while processing client ttraffic.

Also, check to see if a WiFi schedule turned off one or off both radios (see Add a WiFi schedule for a radio on page 163).

A LAN LED is off while a device is connected

If a LAN LED remains off while a powered-on device is connected, check these items:

- Make sure that the Ethernet cable connectors are securely plugged in at the AP and the network device.
- Make sure that the connected network device is actually turned on.
- Make sure that you are using the correct Ethernet cable. Use a standard Category 5 Ethernet patch cable. If the network device incorporates Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

You cannot log in to the AP

If you are unable to log in to the AP's device UI from a computer or mobile device, troubleshooting depends on whether the AP is in router mode or AP mode.

You cannot log in to the AP [router mode]

If the AP is in router mode and you are unable to log in to its device UI from a computer or mobile device on the AP network, check the following:

- Make sure that the yellow WAN port on the AP is connected to the Internet through your broadband, cable, or DSL device (a modem) or your Ethernet wall outlet. The WAN (Internet) LED must light solid green or blinking green.
- Make sure that the computer or mobile device that you are using is connected to the AP.
- Check the Ethernet or WiFi connection between your computer or mobile device and the AP:
  - **Connect over Ethernet directly to the AP**: If you connect the LAN port on your computer directly to the AP, check the Ethernet cable between the computer and the LAN port on the AP. (Do not connect your computer to the yellow WAN port on the AP.)
  - **Connect over WiFi**: If you are using a WiFi-enabled computer or mobile device, check the WiFi connection between the computer or device and the AP. If you did not change the SSID and WiFi password for the Wireless 1 network, the default SSID and WiFi password are printed on the AP label.

Make sure that you are using the Wireless 1 network. By default, the Wireless 2 and Wireless 3 networks do not allow access to the device UI. For more information, see Manage access to LAN ports and the device UI on page 63.)

- Make sure that you are using the correct login information.
  Use the user name **admin** and your customized local device password, also referred to as the admin password. When you used the Setup Wizard for the initial log-in process on the AP, you customized the local device password. The user name and password are case-sensitive. Make sure that Caps Lock is off when you enter this information.
- Make sure that you log in using **routerlogin.net** (which, in router mode, is the same as routerlogin.com and IP address 192.168.1.1).
- Make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the AP. If you are using the default addressing scheme, your device's address is in the range of 192.168.1.2 to 192.168.1.254. Most computers and mobile devices function as DHCP clients. If your computer or mobile device does not, enable its DHCP client so that is can obtain an IP address automatically using DHCP.

  Note: Some versions of Windows and Mac OS generate and assign an IP address if a device cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the device to the AP and reboot your device.

- Try quitting the browser and launching it again.
- Clear your browsing data.
- Make sure that Java, JavaScript, or ActiveX is enabled in your browser. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.

You cannot log in to the AP [AP mode]

If the AP is operating in AP mode and you are unable to log in to its device UI from a computer or mobile device, check the following:

- Make sure that the yellow WAN port on the AP is connected to the Internet through your broadband, cable, or DSL device (a router), another network router, a switch or hub that is connected to the router, or your Ethernet wall outlet. The WAN (Internet) LED must light solid green or blinking green.
- Make sure that the computer or mobile device that you are using is connected to the AP or the same network as the AP.

- Check the Ethernet or WiFi connection between your computer or mobile device and the AP:
  - **Connect over Ethernet directly to the AP**: If you connect the LAN port on your computer directly to the AP, check the Ethernet cable between the computer and the LAN port on the AP. (Do not connect your computer to the yellow WAN port on the AP.)
  - **Connect over WiFi**: If you are using a WiFi-enabled computer or mobile device, check the WiFi connection between the computer or device and the AP. If you did not change the SSID and WiFi password for the Wireless 1 network, the default SSID and WiFi password are printed on the AP label.
    Make sure that you are using the Wireless 1 network. By default, the Wireless 2 and Wireless 3 networks do not allow access to the device UI. For more information, see Manage access to LAN ports and the device UI on page 63.)

  Note: Connect over Ethernet to the same network: After you completed the initial login-process, if you connect your computer to the same network as the AP, check the Ethernet cable between your computer and the LAN port on either the network router or the switch or hub.

- Make sure that you are using the correct login information.
  Use the user name **admin** and your customized local device password, also referred to as the admin password. When you used the Setup Wizard for the initial log-in process on the AP, you customized the local device password. The user name and password are case-sensitive. Make sure that Caps Lock is off when you enter this information.
- If the AP's IP address was changed and you cannot log in using **routerlogin.net** but you do not know the current IP address, see Find the IP address of the AP when you cannot use routerlogin.net on page 36.
- Make sure that the IP address of your computer or mobile device is on the correct LAN subnet. Most computers and mobile devices function as DHCP clients. If your computer or mobile device does not, enable its DHCP client so that is can obtain an IP address automatically using DHCP. The LAN subnet to which your computer or device connects depends on the type of connection to the AP:
  - **Directly connected**: If you are directly connected over WiFi or an Ethernet cable to the AP network, make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the AP. If you are using the default addressing scheme, your device's address is in the range of 192.168.1.2 to 192.168.1.254.
  - **Connected to the same network but not directly connected**: If you are not directly connected to the AP, make sure that the IP address of your computer or

mobile device is on the same subnet as the LAN subnet of the existing network router to which the AP is connected.

Note: Some versions of Windows and Mac OS generate and assign an IP address if a device cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the device to the AP and reboot your device.

- Try quitting the browser and launching it again.
- Clear your browsing data.
- Make sure that Java, JavaScript, or ActiveX is enabled in your browser. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.

You cannot access the Internet [router mode]

If the AP is in router mode and you can log in to the AP's device UI but cannot get an Internet connection, check if the AP can obtain an IP address from your Internet service provider (ISP).

Check the Internet WAN IP address [router mode]

If the AP is in router mode, unless your ISP provides a fixed IP address, the AP requests an IP address from your ISP. You can determine whether the request was successful.

To check the Internet WAN IP address:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.

   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.

   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED**.

The ADVANCED Home page displays.

5. In the Internet Port pane, click the **CONNECTION STATUS** button.
   The Connection Status pop-up window displays.

   Note: The information that displays depends on the type of Internet connection. If the Internet connection is PPPoE, PPTP, or L2TP, other information might display than if the Internet connection is an IP address that the ISP assigns dynamically (the most common situation).

6. Check to see that a valid IP address is shown in the IP address field.
   If 0.0.0.0 is shown, the AP did not obtain an IP address from your ISP.

If the AP cannot obtain an IP address from the ISP, you might need to force your modem to recognize the AP by restarting your network. For more information, see Restart your AP network if the AP is in router mode on page 190.

If the AP is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your ISP might require a login program. Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account as the account name (see Manually set up the AP Internet connection [router mode] on page 45).
- If your ISP allows only one Ethernet MAC address to connect to Internet and checks for your registered computer's MAC address, do one of the following:
  - Inform your ISP that you bought a new network device and ask them to use the AP's MAC address.
  - Configure the AP to clone your registered computer's MAC address.

If the AP obtained an IP address, but your computer or mobile device does not load any web pages from the Internet, it might be for one or more of the following reasons:

- Your computer or mobile device might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the AP's configuration, reboot your computer or mobile device, and verify the DNS address. You can configure your computer or mobile device manually with DNS addresses, as explained in your operating system documentation.

- The AP might not be configured as the TCP/IP gateway on your computer ore mobile device.
  If your computer or mobile device obtains its information from the AP by DHCP, reboot the computer or mobile device and verify the gateway address.
- You might be running login software that is no longer needed.
  If your ISP provided a program to log you in to the Internet, you might no longer need to run that software after installing your AP.

Check or manually start the PPPoE, PPTP, or L2TP connection [router mode]

If the AP is in router mode and your ISP uses a PPPoE, PPTP, or L2TP connection, you can check or manually start the connection.

To check or manually start the connection:

1. Launch a web browser from a computer or mobile device that is connected to a WiFi network or LAN port on the AP.
2. Enter **routerlogin.net** in the address field.
   The Local Device Login page displays.

   If your browser displays a security warning, you can proceed, or add an exception for the security warning. For more information, see What to do if you get a browser security warning on page 42.
3. Enter the AP local device password.
   The local device password is the one that you set. The local device password is case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED**.
   The ADVANCED Home page displays.
5. In the Internet Port pane, click the **CONNECTION STATUS** button.
   The Connection Status pop-up window displays.
6. Check the information to see if your connection is up and working.
   If the AP is not connected, click the **Connect** button.

   The AP continues to attempt to connect indefinitely.

   If you cannot connect after several minutes, the AP might be set up with an incorrect login name, password, or service name, or your ISP might be experiencing a provisioning problem.

Note: Unless you connect manually, the AP does not authenticate using PPPoE, PPTP, or L2TP until data is transmitted to the network.

Troubleshoot your Internet connection [router mode]

If the AP is in router mode and can obtain an IP address, but your computer or mobile device is unable to load any web pages from the Internet, check the following:

- Your Internet service provider (ISP) might be experiencing a temporary Internet outage.
- If you can log in to the AP's device UI but you cannot get an Internet connection, the AP might not be able to obtain an IP address from your ISP (see You cannot access the Internet [router mode] on page 198).
- The traffic meter is enabled, and the limit was reached.
  By configuring the traffic meter not to block Internet access when the traffic limit is reached, you can resume Internet access (see Unblock the traffic meter after the traffic limit is reached [router mode] on page 144). If your ISP sets a usage limit, they might charge you for the overage.
- Your computer or mobile device might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.
  Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the AP's configuration, restart your computer or mobile device.
  (Alternatively, you can configure your computer or mobile device manually with a DNS address, as explained in the documentation for your computer or mobile device.)
- The AP might not be configured as the default gateway on your computer or mobile device.
  Reboot the computer or mobile device and verify that the AP address is listed by your computer or mobile device as the default gateway address.
- You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet, you might no longer need to run that software after installing the AP.

Troubleshoot the WiFi connectivity

If you are experiencing trouble connecting over WiFi to the AP, try to isolate the problem:

- Make sure that the WiFi settings in your WiFi device and AP match exactly.
  For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the AP and WiFi device must match exactly. If you did not change the SSID for the Wireless 1 network, use the AP's default SSID that is printed on the AP label. If you did not change the passphrase (also referred to as network key or WiFi password), use the unique default passphrase that is also printed on the AP label.

  Note: If you set up an access control list (ACL) on the AP, depending on the type of ACL, you might need to add each computer or mobile device to the ACL (see Enable and manage network access control on page 77).

  The AP provides three WiFi networks (Wireless 1, Wireless 2, and Wireless 3). By default, the Wireless 1 network is enabled and the other two WiFi networks are disabled. If the Wireless 2 and Wireless 3 networks are enabled and you did not change the default settings, you can access these networks as follows:

  - **Wireless 2**: The default SSID is NETGEARXXXXXX-2, in which XXXXXX represents the last six characters of the AP's MAC address, and the default password is the default password for the Wireless 1 network, as printed on the AP label.
  - **Wireless 3**: The default SSID is NETGEARXXXXXX-3, in which XXXXXX represents the last six characters of the AP's MAC address, and the default password is the default password for the Wireless 1 network, as printed on the AP label.

  Note: To access the device UI of the AP, make sure that you are using the Wireless 1 network. By default, the Wireless 2 and Wireless 3 networks do not allow access to the device UI. For more information, see Manage access to LAN ports and the device UI on page 63.

- Does the WiFi device that you are using find your WiFi network?
  If not, check the WLAN LEDs on the AP. If a WLAN LED is off, the associated WiFi radio is probably off too. For more information about the WiFi radios, see Enable or disable a WiFi radio on page 66.
- If you disabled the AP's SSID broadcast, your WiFi network is hidden and does not display in your WiFi client's scanning list. (By default, SSID broadcast is enabled.) For more information, see Broadcast or hide the SSID for a WiFi network on page 61.

- Does your WiFi device support the security that you are using for your WiFi network? For information about changing the WiFi security, see Set up or change an open or secure WiFi network on page 53.

  Note: If you want to change the WiFi network settings, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

If your WiFi device finds your network but the signal strength is weak, check these conditions:

- Is your AP too far from your WiFi device or too close? Place your WiFi device near the AP but at least 6 feet (1.8 meters) away and see whether the signal strength improves.
- Are objects between the AP and your WiFi device blocking the WiFi signal? For more information, see Position the AP on page 11.

Changes are not saved

If the AP does not save the changes that you make through the device UI, do the following:

- When entering configuration settings, always click the **Apply** button before moving to another page or tab, or your changes are lost.
- If the page in the device UI displays a **Refresh** button, click it. It is possible that the changes occurred, but the old settings might be in the web browser's cache.

Troubleshoot your network using the ping utility of your computer or mobile device

Most network devices and routers contain a ping utility that can send an echo request packet to a device that you select. The device then responds with an echo reply. You can troubleshoot a network using the ping utility in your computer or mobile device.

Test the LAN path from a Windows-based computer to the AP

You can ping the AP from a Windows-based computer to verify that the path to your AP is set up correctly. You can use a WiFi or wired connection to the AP, which can be in router mode or AP mode.

To ping the AP from a Windows-based computer:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the AP, as in this example:

   ping www.routerlogin.net

3. Click the **OK** button.

   You see a message like this one:

   ```
   Pinging <IP address > with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

If the path is not functioning correctly, check to see if the following is correct:

- Correct LAN subnet?
  Verify that the IP addresses and LAN subnet for the AP and your computer are correct. For more information, see Check the DHCP network settings of your computer or mobile device on page 191.
- Correct physical connections?
  If you are using a wired connection to the AP, make sure that the Ethernet port on your computer is connected to a LAN port on the AP.
  If the AP and computer are connected through a switch or hub, make sure that the link LEDs are lit for the switch ports that are connected to the AP and computer.
- Correct software?
  If you are using a wired connection to the AP, verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

Test the path from a Windows-based computer to a remote device [router mode]

For this task, the AP must be in router mode.

To test the path from a Windows-based computer that is connected to the AP to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run window, type

   ping -n 10 *<IP address>*

   in which *<IP address>* is the IP address of a remote device such as your ISP DNS server.

   If the path is functioning correctly, messages display that are similar to those shown in Test the LAN path from a Windows-based computer to the AP on page 204.

3. If you do not receive replies, check the following:

   - The AP is listed as the default gateway for your computer. If DHCP assigns the IP configuration of your computers, this information is not visible in your computer Network Control Panel. Verify that the IP address of the AP is listed as the default gateway.
   - The network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
   - Your modem is connected and functioning.
   - If your ISP assigned a host name to your registered computer, use that host name as the account name (see Manually set up the AP Internet connection [router mode] on page 45).
   - Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.
     Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If your ISP does this, configure your router to “clone” or “spoof” the MAC address from the authorized computer.

A

Factory Default Settings and Technical Specifications

This appendix includes the following sections:

Note: In this appendix, we refer to the access point as the AP.

Factory default settings

You can reset the AP to the factory default settings, which are shown in the following table.

For more information about resetting the AP to its factory settings, see Factory default settings on page 121.

Table 9. WAX202 AP and WAX206 AP factory default settings

Feature	Default Setting
Login to the device UI	
Login URL	Secure HTTP (HTTPS) with routerlogin.net, routerlogin.com, aplogin.net, or aplogin.com (all of which are the same as IP address 192.168.1.1) If the AP is operating in AP mode and does not get an IP address from a DHCP server in your network, the IP address is 192.168.1.1.
Local login user name	admin (case-sensitive, nonconfigurable)
Local device password	password However, for normal use, you do not need to enter this default password anywhere. When you log in for the first time, you must specify a unique local device password.
Operation modes	
Router mode	Enabled by default.
AP mode	Disabled by default.
DHCP settings	
DHCP client	Enabled as a WAN client in router mode. (LAN client in AP mode.)
DHCP server	Enabled in router mode. (Disabled in AP mode.)
WiFi networks and radios	
WiFi communication	Enabled for Wireless 1 network Disabled for Wireless 2 and Wireless 3 networks
SSID names	Wireless 1 default network: A unique name that is printed on the AP label Wireless 2 optional network: NETGEARXXXXXX-2 Wireless 3 optional network: NETGEARXXXXXX-3 For the Wireless 2 and Wireless 3 default SSIDs, XXXXXX represents the last six digits of the MAC address of the AP:
Security for the default Wireless 1 network	WPA2 Personal [AES] The default WiFi passphrase is a unique passphrase that is printed on the AP label.
Security for the optional Wireless 2 and Wireless 3 networks	WPA2 Personal [AES] The default WiFi passphrase is the same default passphrase of the Wireless 1 network. This passphrase is printed on the AP label.

Table 9. WAX202 AP and WAX206 AP factory default settings (Continued)

Feature	Default Setting
Country/region	North America: United States Europe: Europe Other continents: Varies by region
Channel	2.4 GHz: Auto. The available channels depend on the region. 5 GHz: The default channel and available channels depend on the region.
WiFi throughput mode model WAX202	Up to 600 Mbps at 2.4 GHz Up to 1200 Mbps at 5 GHz Throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, affect the data throughput rate.
WiFi throughput mode model WAX206	Up to 800 Mbps at 2.4 GHz Up to 2400 Mbps at 5 GHz Throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, affect the data throughput rate.
SSID broadcast	Enabled (applies to each single network)
Client isolation	Disabled for the Wireless 1 network Enabled for the Wireless 2 and Wireless 3 networks
Access to wired ports	Enabled for the Wireless 1 network Disabled for the Wireless 2 and Wireless 3 networks
SSID isolation	Enabled (applies to all networks together)
CTS/RTS threshold	2347
Preamble mode	Long Preamble
Radio transmission power	100%
802.11ax (11AX)	Enabled
OFDMA	Disabled
Smart connect	Disabled
20/40 MHz coexistence	Enabled (applies to the 2.4 GHz radio only)
MU-MIMO	Enabled
Tx beamforming	Enabled
PMF	Enabled (configurable for the 5 GHz radio only; not configurable for the 2.4 GHz radio)
WPS	
WPS capability	Enabled

Table 9. WAX202 AP and WAX206 AP factory default settings (Continued)

Feature	Default Setting
Security and other features	
Access control	Disabled and no access control lists (ACLs) configured
Block services	None in router mode (the feature does not apply to AP mode)
Port Scan and DoS Protection	Enabled in router mode (the feature does not apply to AP mode)
Respond to Ping on Internet Port	Disabled in router mode (the feature does not apply to AP mode)
DMZ server	None in router mode (the feature does not apply to AP mode)
IGMP proxying	Disabled in router mode (the feature does not apply to AP mode)
NAT filtering	Secured in router mode (the feature does not apply to AP mode)
SIP ALG	Enabled in router mode (the feature does not apply to AP mode)
Port forwarding and port triggering	Disabled in router mode (the feature does not apply to AP mode)
Traffic meter	Disabled in router mode (the feature does not apply to AP mode)
UPnP	Enabled in router mode (the feature does not apply to AP mode)
Static routes	None in router mode (the feature does not apply to AP mode)

Technical specifications model WAX202

The following table shows the technical specifications for model WAX202. For more information, see the product data sheet, which you can download by visiting netgear.com/support/download/.

Table 10. WAX202 AP specifications

Feature	Description
Power adapter	12V, 1.5A (18W) The plug is localized to the country of sale. Power consumption 17W maximum
Dimensions (L x W x H)	6.7 x 2.5 x 9.5 in. (170 x 63 x 242 mm)
Weight	1.1 lb (497 g)

Table 10. WAX202 AP specifications (Continued)

Feature	Description
Operating temperature	32°F to 104°F (0°C to 40°C)
Operating humidity	10 to 90% maximum relative humidity, noncondensing
Storage temperature	–4°F to 158°F (–20°C to 70°C)
Storage humidity	5 to 95% maximum relative humidity, noncondensing
WAN (Internet)	One 10/100/1000BASE-T Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X)
LAN	Three 10/100/1000BASE-T Ethernet (RJ-45) ports with Auto Uplink (Auto MDI-X)
Protocols for Internet connections	IP, PPPoE, L2TP, PPTP
WiFi standards	IEEE 802.11ax IEEE 802.11ac IEEE 802.11n 2.0 IEEE 802.11g IEEE 802.11b IEEE 802.11a
Radio bands	2.4 GHz and 5 GHz, concurrent operation
Maximum theoretical WiFi throughput	Up to 600 Mbps at 2.4 GHz Up to 1200 Mbps at 5 GHz Throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, affect the data throughput rate.
Maximum number of supported clients	The AP can support a maximum of 64 WiFi clients: In a WiFi network, the actual number of clients might be limited by the amount of WiFi traffic that is generated by each client.
Maximum number of concurrent devices	The AP can support a maximum of 40 concurrent devices.
Operating frequency range 2.4 GHz band	US: 2.412–2.462 GHz Europe: 2.412–2.472 GHz Australia: 2.412–2.472 GHz
Operating frequency range 5 GHz band	US: 5.180–5.240 + 5.745–5.825 GHz Europe: 5.180–5.700 GHz Australia: 5.180–5.320 + 5.500–5.825 GHz
802.11 security	WPA2 Personal [AES] WPA-Personal [TKIP] + WPA2-Personal [AES] WPA/WPA2 Enterprise WPA3- Personal
Safety certification	CB IEC60950-1 CE LVD EN62368-1

Technical specifications model WAX206

The following table shows the technical specifications for model WAX206. For more information, see the product data sheet, which you can download by visiting netgear.com/support/download/.

Table 11. WAX206 AP specifications

Feature	Description
Power adapter	12V, 2.5A (30W) The plug is localized to the country of sale. Power consumption 20W maximum
Dimensions (L x W x H)	6.7 x 2.5 x 9.5 in. (170 x 63 x 242 mm)
Weight	1.1 lb (497 g)
Operating temperature	32°F to 104°F (0°C to 40°C)
Operating humidity	10 to 90% maximum relative humidity, noncondensing
Storage temperature	–4°F to 158°F (–20°C to 70°C)
Storage humidity	5 to 95% maximum relative humidity, noncondensing
WAN (Internet)	One 2.5GBASE-T Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X)
LAN	Four 10/100/1000BASE-T Ethernet (RJ-45) ports with Auto Uplink (Auto MDI-X)
Protocols for Internet connections	IP, PPPoE, L2TP, PPTP
WiFi standards	IEEE 802.11ax IEEE 802.11ac IEEE 802.11n 2.0 IEEE 802.11g IEEE 802.11b IEEE 802.11a
Radio bands	2.4 GHz and 5 GHz, concurrent operation
Maximum theoretical WiFi throughput	Up to 800 Mbps at 2.4 GHz Up to 2400 Mbps at 5 GHz Throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, affect the data throughput rate.
Maximum number of supported WiFi clients	The AP can support a maximum of 128 WiFi clients: In a WiFi network, the actual number of clients might be limited by the amount of WiFi traffic that is generated by each client.
Maximum number of concurrent devices	The AP can support a maximum of 60 concurrent devices.

Table 11. WAX206 AP specifications (Continued)

Feature	Description
Operating frequency range 2.4 GHz band	US: 2.412–2.462 GHz Europe: 2.412–2.472 GHz Australia: 2.412–2.472 GHz
Operating frequency range 5 GHz band	US: 5.180–5.240 + 5.745–5.825 GHz Europe: 5.180–5.700 GHz Australia: 5.180–5.320 + 5.500–5.825 GHz
802.11 security	WPA2 Personal [AES] WPA-Personal [TKIP] + WPA2-Personal [AES] WPA/WPA2 Enterprise WPA3- Personal
Safety certification	CB IEC60950-1 CE LVD EN62368-1