

NETGEAR®

User Manual

WiFi 6 AX1800 Dual Band Wireless Access Point

Model WAX204

November 2020
202-12147-01

NETGEAR, Inc.

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

Support and Community

Visit [netgear.com/support](https://www.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.

Trademarks

© NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-12147-01	November 2020	First publication.

Contents

Chapter 1 Hardware Overview

- Top panel with LEDs.....11
- Back panel with ports, buttons, and a power connector.....13
- Position the antennas for best WiFi performance.....14
- Access point label.....14

Chapter 2 Installation and Initial Log-in

- About router mode and access point mode.....16
- Routing features enabled only in router mode.....16
- Set up the access point and complete the initial log-in process...17
 - Connect the access point to a modem and log in for the first time.....18
 - Connect the access point to a router and log in for the first time.....22
- Get a registration key.....26
- Find the IP address of the access point when you cannot use routerlogin.net.....27
- Find the IP address of the access point with the NETGEAR Insight mobile app.....29
- Log in to the access point after initial setup.....30
- Change the language.....31
- Connect a wired or WiFi device to the access point’s network after installation.....32
 - Connect to the access point through an Ethernet cable.....32
 - Use Wi-Fi Protected Setup to join the WiFi network.....33
 - Manually join the WiFi network.....33

Chapter 3 Manually Set Up Internet Settings

- Use the Setup Wizard.....36
- Manually set up the access point Internet connection [router mode].....37
 - Specify a dynamic or fixed WAN IP address Internet connection without a login [router mode].....37
 - Specify a PPPoE Internet connection that uses a login [router mode].....39

Specify a PPTP or L2TP Internet connection that uses a login [router mode].....	41
IPv6 Internet connections and IPv6 addresses [router mode].....	43
Use Auto Detect for an IPv6 Internet connection [router mode].....	44
Use Auto Config for an IPv6 Internet connection [router mode].....	46
Set up an IPv6 6to4 tunnel Internet connection [router mode].	48
Set up an IPv6 6rd Internet connection [router mode].....	49
Set up an IPv6 passthrough Internet connection [router mode].....	51
Set up an IPv6 fixed Internet connection [router mode].....	52
Set up an IPv6 DHCP Internet connection [router mode].....	54
Set up an IPv6 PPPoE Internet connection [router mode].....	56

Chapter 4 Basic WiFi and Radio Features

Set up or change an open or secure WiFi network.....	59
Configure WPA and WPA2 Enterprise WiFi security with a RADIUS server.....	63
Enable or disable a WiFi network.....	65
Hide or broadcast the SSID for a WiFi network.....	66
Manage client isolation for clients of the Wireless 2 or Wireless 3 network.....	67
Manage access to LAN ports for clients of the Wireless 2 or Wireless 3 network.....	68
Manage SSID isolation for all WiFi networks.....	69
Enable or disable a WiFi radio.....	70
Use WPS to connect to the WiFi network.....	72
Use WPS with the push button method.....	72
Use WPS with the PIN method.....	73

Chapter 5 Security, Firewall, and Access Rules

Firewall WAN settings [router mode].....	76
Manage port scan protection and denial of service protection [router mode].....	76
Set up a default DMZ server [router mode].....	77
Manage IGMP proxying [router mode].....	78
Manage NAT filtering [router mode].....	79
Manage the SIP application-level gateway [router mode].....	80
Network access control lists.....	81
Enable and manage network access control.....	81
Add, remove or change a device on the the allowed list.....	83
Add, remove or change a device on the blocked list.....	84
Block specific Internet sites [router mode].....	86

- Set up keyword and domain blocking [router mode].....86
- Remove a keyword or domain from the blocked list [router mode].....88
- Remove all keywords and domains from the blocked list [router mode].....89
- Block specific applications and services from the Internet [router mode].....89
 - Add a service blocking rule for a predefined service or application [router mode].....90
 - Add a service blocking rule for a custom service or application [router mode].....91
 - Change a service blocking rule [router mode].....93
 - Remove a service blocking rule [router mode].....94
- Assign a trusted device [router mode].....95
- Schedule blocking [router mode].....96
- Set up security event email notifications.....97

Chapter 6 Optimize Performance

- Enable QoS and automatically set the Internet bandwidth.....100
- Enable QoS and manually set the Internet bandwidth.....101
- Enable or disable the automatic update of the Performance Optimization Database.....102
- Manage WiFi Multimedia (WMM) for a radio.....103
- Improve network connections with Universal Plug and Play [router mode].....105
- Change the priority for a connected device [router mode].....106

Chapter 7 Network Settings

- LAN IP address settings [router mode].....109
 - Change the LAN IP address and subnet settings [router mode].....109
 - Manage the DHCP server address pool [router mode].....110
 - Disable the DHCP server [router mode].....112
 - Manage the Router Information Protocol settings [router mode].....113
- Change the access point network device name.....114
- Reserved LAN IP addresses [router mode].....115
 - Reserve a LAN IP address [router mode].....115
 - Change a reserved LAN IP address [router mode].....116
 - Remove a reserved LAN IP address entry [router mode].....117
- Static routes.....118
 - Add an IPv4 static route.....118
 - Change an IPv4 static route.....120
 - Remove an IPv4 static route.....121

Bridge port and VLAN tag groups [router mode].....121
Set up a bridge for a port group [router mode].....122
Set up a bridge for a VLAN tag group [router mode].....123
Change the MTU size [router mode].....125

Chapter 8 Maintain and Monitor

Update the firmware.....129
Let the access point check for new firmware and update the
firmware.....129
Manually check for new firmware and update the firmware...131
Back up or restore the settings.....133
Back up the access point settings.....133
Restore the access point settings.....134
Change the local device password.....135
Change the password recovery questions for the local device
password.....136
Recover the local device admin password.....137
Factory default settings.....138
Use the dual-function Reset button to return to factory
defaults.....138
Use the local browser UI to return to factory defaults.....140
Time and Network Time Protocol server.....142
Manually set the time zone and adjust the daylight saving
time.....142
Change the Network Time Protocol server.....143
Logs.....144
Specify which activities the access point logs.....144
View, send, or clear the logs.....145
Status and statistics.....146
Display information about the Internet port, access point, and
WiFi settings [router mode].....146
Display information about the LAN port, access point, and WiFi
settings [access point mode].....149
Check the Internet connection status.....151
Display the Internet port statistics.....153
Display the devices currently on the access point network and
change device information.....154
Traffic meter [router mode].....157
Start the traffic meter without traffic restrictions [router mode].158
Restrict Internet traffic by volume [router mode].....159
Restrict Internet traffic by connection time [router mode].....160
View the Internet traffic volume and statistics [router mode].162
Unblock the traffic meter after the traffic limit is reached [router
mode].....163

Change the system mode to access point mode or to router mode.....164
Disable LED blinking or turn off LEDs.....166

Chapter 9 Dynamic DNS [Router Mode]

About Dynamic DNS [router mode].....168
Set up a new Dynamic DNS account [router mode].....168
Use an existing Dynamic DNS account [router mode].....169
Change the Dynamic DNS account settings [router mode].....171

Chapter 10 VPN Client [Router Mode]

About setting up the access point as a VPN client [router mode].173
Enable the VPN client in the access point and connect to a VPN server [router mode].....174
Disconnect the access point from the VPN server [router mode].176

Chapter 11 VPN Server and Service with OpenVPN [Router Mode]

Enable and configure OpenVPN and VPN client access on the access point [router mode].....178
OpenVPN client utility and VPN configuration files [router mode].....179
 Install OpenVPN on a Windows-based computer [router mode].....180
 Install OpenVPN on a Mac [router mode].....181
 Install OpenVPN on an iOS device [router mode].....182
 Install OpenVPN on an Android device [router mode].....183
About setting up an OpenVPN connection [router mode].....184
About VPN access to your network or Internet service at your office or home [router mode].....185
Use a VPN tunnel to remotely access your Internet service [router mode].....186

Chapter 12 Advanced WiFi and Radio Features

Change the region of operation.....188
Manage 802.11ax and enable or disable OFDMA for a radio....189
Enable or disable smart connect for the access point.....190
Enable or disable 20/40 MHz coexistence for the 2.4 GHz radio.192
Change the channel for a radio.....193
Change the WiFi throughput mode for a radio.....194
Change the transmission output power for a radio.....196
Add a WiFi schedule for a radio.....197
Enable or disable MU-MIMO.....199
Enable or disable explicit beamforming.....200
Enable or disable PMF.....201

Set up access point as a WiFi Bridge to another device.....202
Change the CTS/RTS threshold and preamble mode for a radio.205

Chapter 13 Port Forwarding and Port Triggering [Router Mode]

Port forwarding to a local server for services and applications [router mode].....208
 Forward incoming traffic for a default service or application [router mode].....208
 Add a port forwarding rule for a custom service or application [router mode].....209
 Change a port forwarding rule [router mode].....211
 Remove a port forwarding rule [router mode].....212
 How the access point implements a port forwarding rule [router mode].....213
 Application example: Make a local web server public [router mode].....213
Port triggering for services and applications [router mode].....214
 Add a port triggering rule [router mode].....214
 Change a port triggering rule [router mode].....216
 Remove a port triggering rule [router mode].....217
 Specify the time-out for port triggering [router mode].....218
 Disable port triggering [router mode].....219
 Application example: Port triggering for Internet Relay Chat [router mode].....220

Chapter 14 Diagnostics and Troubleshooting

Reboot the access point from the local browser UI.....222
Quick tips for troubleshooting.....223
 Restart your access point network if in router mode.....223
 Restart your access point when in access point mode.....223
 Check the Ethernet cable connections.....223
 Check the WiFi settings of your computer or mobile device..223
 Check the DHCP network settings of your computer or mobile device.....224
Standard LED behavior when the access point is powered on...225
Troubleshoot with the LEDs.....225
 Power LED is off.....225
 Power LED does not turn green.....226
 Internet LED is solid amber or off [router mode].....226
 Internet LED is solid amber or off [access point mode].....227
 WiFi LED is Off.....227
 The LAN LED is off while a device is connected.....228
You cannot log in to the access point.....228
 You cannot log in to the access point [router mode].....228

You cannot log in to the access point [access point mode].....	229
You cannot access the Internet [router mode].....	231
Check the Internet WAN IP address [router mode].....	231
Check or manually start the PPPoE connection [router mode].....	233
Troubleshoot Internet browsing.....	234
Troubleshoot the WiFi connectivity.....	235
Changes are not saved.....	236
Troubleshoot your network using the ping utility of your computer or mobile device.....	236
Test the LAN path from a Windows-based computer to the access point.....	237
Test the path from a Windows-based computer to a remote device [router mode].....	238

Appendix A Factory Default Settings and Technical Specifications

Factory default settings.....	240
Technical specifications.....	242

Appendix B Positioning and Wall-Mounting

Position the access point.....	245
Wall-mount the access point.....	246

1

Hardware Overview

The WiFi 6 AX1800 Dual Band Wireless Access Point Model WAX204, in this manual referred to as the access point, supports 802.11ax high performance WiFi connectivity and dual-band concurrent operation at 2.4 GHz and 5 GHz with a combined throughput of 1.8 Gbps (600 Mbps at 2.4 GHz and 1200 Mbps at 5 GHz). The access point is designed to function standalone in a small office network or home network.

You can use the access point in its default router mode with its router features enabled, directly connected to the Internet, for example through a modem. You can also use the access point in access point mode with its router features disabled, connected to an existing router in your network.

The chapter contains the following sections:

- [Top panel with LEDs](#)
- [Back panel with ports, buttons, and a power connector](#)
- [Position the antennas for best WiFi performance](#)
- [Access point label](#)

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.

Top panel with LEDs






The five status LEDs are located on the top panel of the access point. From left to right, the top panel contains the Power LED, Internet LED, WiFi LED, LAN LED, and WPS LED.



Figure 1. Top panel with LEDs

WiFi 6 AX1800 Dual Band Wireless Access Point WAX204

Table 1. LED descriptions

LED	Description
	<p>Solid green. The access point is ready.</p> <p>Solid amber. The access point is starting or upgrading firmware.</p> <p>Blinking amber. The access point was reset to factory default settings and is restarting. For more information about resetting the access point to factory default settings, see Factory default settings on page 138.</p> <p>Blinking red. The firmware is corrupted and the access point cannot start. For more information, see Power LED does not turn green on page 226.</p> <p>Off. Power is not supplied to the access point.</p>
	<p>Solid green. An Internet connection is established.</p> <p>Blinking green. The Internet port is sending or receiving traffic.</p> <p>Solid amber. The access point cannot get an Internet connection. For more information, see Internet LED is solid amber or off [router mode] on page 226 (router mode is the default system mode) or Internet LED is solid amber or off [access point mode] on page 227.</p> <p>Blinking alternating green and amber. If the traffic meter is enabled, the traffic limit is reached. For more information, see Unblock the traffic meter after the traffic limit is reached [router mode] on page 163.</p> <p>Off. No Internet connection exists, for example, because no cable is inserted in the Internet port.</p>
	<p>Solid green. One or both WiFi radios are operating.</p> <p>Blinking green. One or both WiFi radios are sending or receiving traffic.</p> <p>Off. Both WiFi radios are off. For more information, see WiFi LED is Off on page 227.</p>
	<p>Solid green. One or more LAN ports are connected to powered-up devices.</p> <p>Blinking green. One or more LAN ports are sending or receiving traffic.</p> <p>Solid amber. One or more LAN ports function at 10 or 100 Mbps speed and are connected to powered-up devices.</p> <p>Blinking amber. One or more LAN ports are sending or receiving traffic at 10 or 100 Mbps speed.</p> <p>Off. None of the LAN ports is connected to a device.</p>
	<p>Solid green. WPS is available.</p> <p>Blinking green. The WPS button was pressed. For two minutes, the access point attempts to find the WiFi device (that is, the client) that can join the access point Wireless 1 network. For more information, see Use Wi-Fi Protected Setup to join the WiFi network on page 33.</p> <p>Off. WPS is disabled.</p>

Back panel with ports, buttons, and a power connector

The back panel of the access point provides ports, buttons, and a DC power connector.



Figure 2. Back panel

Viewed from left to right, the back panel contains the following components:

- **WPS button.** Press the **WPS** button to join the access point's WiFi network without typing the WiFi password. For more information, see [Use Wi-Fi Protected Setup to join the WiFi network](#) on page 33.
- **Internet port.** One Internet (WAN) port (yellow) to connect the access point to a modem or existing router in your network:
 - **Connect to a modem.** Connect the Internet port directly to a modem. The modem must provide an Internet connection to the access point. For more information about this setup, in which the access point must function in its default router mode, see [Connect the access point to a modem and log in for the first time](#) on page 18.
 - **Connect to a router.** Connect the Internet port directly to a 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 access point must function in access point mode, see [Connect the access point to a router and log in for the first time](#) on page 22.

- **LAN ports 1 through 4.** Four Gigabit Ethernet RJ-45 LAN ports numbered LAN 1 through LAN 4 to connect the access point to Ethernet devices such as a computer and a switch.
- **Reset button.** Press the **Reset** button to reset the access point to factory default settings. For more information, see [Use the dual-function Reset button to return to factory defaults](#) on page 138.
- **DC power connector.** Connect the power adapter that came in the product package to the DC power connector.

Position the antennas for best WiFi performance

You can swivel the three access point antennas in any direction. For best WiFi performance, we recommend that you experiment with various antenna positions. For example, you could position the center antenna vertically and aim the other two antennas outward at 45-degree angles.

Access point label

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

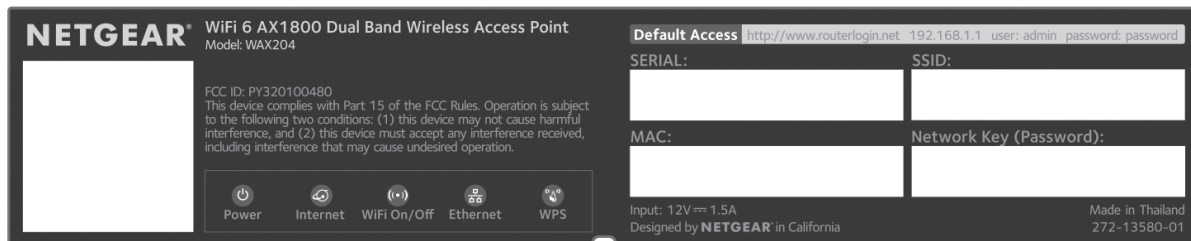


Figure 3. Access point label

2

Installation and Initial Log-in

This chapter describes how you can install and access the access point in your network and go through the initial log-in process. By default, the access point is in router mode. You can also change the mode to access point mode.

IMPORTANT: To obtain full and unlimited access to access point, you must register the access point. You can do so by accessing your NETGEAR account and obtaining a registration key. However, the easiest way to register your access point is to connect it to the Internet, go through the initial log-in process, also referred to as single sign-on (SSO), and log in with a NETGEAR account. (You can create an account during the log-in process.)

Note: When you log in to the access point, you connect to the local browser user interface (UI).

The chapter contains the following sections:

- [About router mode and access point mode](#)
- [Routing features enabled only in router mode](#)
- [Set up the access point and complete the initial log-in process](#)
- [Get a registration key](#)
- [Find the IP address of the access point when you cannot use routerlogin.net](#)
- [Find the IP address of the access point with the NETGEAR Insight mobile app](#)
- [Log in to the access point after initial setup](#)
- [Change the language](#)
- [Connect a wired or WiFi device to the access point's network after installation](#)

About router mode and access point mode

Before you set up the access point, decide whether you will use the access point in its default router mode or in access point mode:

- **Router mode.** By default, the access point is in router mode so that you can connect it directly to a modem such as a cable or DSL modem. In router mode, the access point functions as both a router for Internet access and a WiFi access point. The access point receives its IP address settings from your Internet service provider (ISP) and delivers IP address settings to its WiFi and LAN clients.
- **Access point mode.** You can also connect the access point to an existing router in your network and, after you log in, change the system mode to access point mode. The router must support a DHCP server, or another DHCP server must be present in the network, so that an IP address is assigned to the access point and its clients and Internet access is provided. Another option is to assign the access point and its clients static IP addresses, but using DHCP is easier. In access point mode, the access point functions as a WiFi access point only and its router functions are disabled. For example, routing services such as NAT and the DHCP server are disabled.

For more information about the routing features, see [Routing features enabled only in router mode](#) on page 16.

Routing features enabled only in router mode

The access point can function in router mode (its default system mode) or in access point mode.

The following routing features are enabled in router mode but disabled in access point mode:

- Internet settings, including an IP address issued through dynamic DHCP (the default setting), a manually specified static IP address, an IP address issued through PPPoE, L2TP, or PPTP, and various ways to implement an IPv6 address.
- WAN settings, including routing services such as NAT.
- LAN settings, including a DHCP server.
- QoS settings.

- Internet security settings, including the option to block sites and services, and the option to set up port forwarding and port triggering rules.
- VPN service and VPN client.
- Internet traffic meter.
- Bridge port and VLAN tag groups.
- Changing the priority for an attached device.

For information about changing the system mode after initial setup, [Change the system mode to access point mode or to router mode](#) on page 164.

The system mode affects how you can reach the access point local browser UI:

- **Router mode.** Enter **http://www.routerlogin.net** in the address field of your browser.
In router mode, you always connect directly to the access point.
- **Access point mode.** The method to reach the local browser UI depends on how you connect to the access point:
 - **Directly connected.** Enter **http://www.routerlogin.net** in the address field of your browser.
One exception exists: If you assigned a static IP address to the access point, you must use *that* IP address to reach the local browser UI.
 - **Connected over your network.** In the address field of your browser, enter the IP address that your existing router or DHCP server assigned to the access point. For more information, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

Set up the access point and complete the initial log-in process

When you connect the access point to the Internet and complete the initial log-in process, also referred to as single sign-on (SSO), the following are required in most situations:

- **Default router mode.** The access point must be in its default router mode.
- **Internet connection.** The access point must connect to the Internet through a modem or through an existing router in your network.
- **Registration.** To get full and unlimited access to the local browser UI, you must log in with either a NETGEAR account or a registration key. If you do not have a NETGEAR account, you can create one during the initial log-in process. For information about getting a registration key, see [Get a registration key](#) on page 26.

Before you register the access point, you *can* access the local browser UI of the access point by using your new local device password (you must specify it during the initial log-in process), for either restricted access or full access for a limited time. Before you register the switch with your NETGEAR account, you can use one of the following options:

- **Access limited features.** Select the option to access a restricted menu of the local browser UI without time limitations. You can do so by using the local device password to get access to limited features such updating the firmware, uploading or downloading the configuration file, and restarting the access point.
- **Temporarily access all features.** Select the option to temporarily access the full menu of the local browser UI. You can do so by using the local device password, but you get full access *three times only*. During a temporary full access session, you can configure and manage all features and settings in the local browser UI.

Note: During a temporary access session, if the session is inactive for 60 minutes, you are automatically logged out from the local browser UI. However, the session still counts as one of three temporary access sessions.

For more information about connecting the access point to the Internet and completing the initial log-in process, see one of the following sections:

- [Connect the access point to a modem and log in for the first time](#) on page 18
- [Connect the access point to a router and log in for the first time](#) on page 22

Connect the access point to a modem and log in for the first time

When you set up the access point 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 access point 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, L2TP, or PPTP, or static IP address.** If the type of WAN connection is PPPoE, L2TP, or PPTP, 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.

Note: If you are not sure which type of WAN connection your Internet service uses, contact your ISP before you start the following procedure.



Figure 4. Connect the access point in default router mode to your modem

To connect the access point to a modem and log in to the local browser 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 Internet port on the access point.
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 access point and check to see that the LEDs light.

LED		Description
Power		When you turn on the access point, the Power LED lights solid red for about five seconds and then turns solid amber. After about 90 seconds, the Power LED lights solid green.
Internet		The Internet LED lights solid green or blinks green when the Internet connection is established. Note: The Internet connection is established after you access the local browser UI during the Setup Wizard process. If the Internet LED remains off or solid amber and does not turn solid green or blinking green, see Internet LED is solid amber or off [router mode] on page 226.
WiFi		The WiFi LED lights solid green or blinks green.

8. Log in to the access point by using *one* of the following methods:
 - **Connect over WiFi.** On a WiFi-enabled computer or mobile device, find and connect to the access point's WiFi network (SSID).
The default SSID and WiFi password (network key) are printed on the access point label.
 - **Connect over Ethernet directly to the access point.** Using an Ethernet cable, connect the LAN port on your computer directly to any of the four LANs port on the access point.

9. Launch a web browser and enter **http://www.routerlogin.net** in the address field.
The Setup Wizard starts.
If the Setup Wizard does not start, see [You cannot log in to the access point \[router mode\]](#) on page 228.

10. Follow the prompts.
Note the following:
 - **Trouble connecting to the Internet?** If the access point does not connect to the Internet, see [Troubleshoot Internet browsing](#) on page 234.
 - **WAN connection type.** If the WAN connection is PPPoE, L2TP, or PPTP, or your Internet connection requires a static IP address, during the Setup Wizard Process, provide the required information for the Internet connection when the Smart Setup Wizard prompts you for the information.
 - **New admin password.** During the Setup Wizard process, you must specify a new admin password (the local device password) and specify answers to two security questions (you can choose the questions).
 - **Firmware update.** During the Setup Wizard process, you can update the firmware (if new firmware is available). Depending on the configuration, the access point might need to restart, you might need to log in again to continue the Setup Wizard process, or you might need to do both.
 - **Browser security message.** During the Setup Wizard process, your browser will most likely display a security message. You can either ignore this message or install the security certificate. Consider the following examples:
 - **Google Chrome.** If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the IP address of the switch.
 - **Apple Safari.** If Apple Safari displays a *This connection is not private* message, 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.** If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Internet Explore.** If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link.
- **Microsoft Edge.** If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage.**

When the Setup Wizard is finished, the Register to unlock all features page displays.

11. Register the access point or select either restricted access or full access for a limited time to the local browser UI:

- **Register with a NETGEAR account.** Click the **Login In with Netgear account** button and follow the prompts. Either use your existing NETGEAR account or create a new free NETGEAR account.
- **Register with a registration key.** If you have a registration key (see [Get a registration key](#) on page 26), click the **Enter Registration Key** and enter the key.
- **Access limited features.** Click the **Skip Registration and Access Limited Features** button to get access to a restricted menu of the local browser UI without time limitations. (For more information, see [Set up the access point and complete the initial log-in process](#) on page 17.) The password that you must enter is your new local device password.
- **Temporarily access all features.** Click the **Skip Registration and Temporarily Access All Features** button to get access to the full menu of the local browser UI, but you get this access three times only. (For more information, see [Set up the access point and complete the initial log-in process](#) on page 17.) The password that you must enter is your new local device password.

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

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

The BASIC Home page displays.

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

Connect the access point to a router and log in for the first time

The easiest way to use the access point in access point mode is to connect it to an existing router in your network, either directly, or through a switch or hub (almost any router functions as a DHCP server). If your network includes an independent DHCP server, connect the access point to a switch or hub that is connected to the DHCP server.

Only after you complete the initial log-in process, can you change the system mode to access point mode.






Figure 5. Connect the access point to an existing router in your network

To connect the access point directly to an existing router in your network and log in to the local browser UI for the first time:

1. Connect an Ethernet cable to the yellow Internet port on the access point.
2. Connect the other end of the cable to a LAN port on your network router.
Your network router must support a DHCP server so that it assigns an IP address to the access point and its clients and provides Internet access.
3. Power on the access point and check to see that the LEDs light.

WiFi 6 AX1800 Dual Band Wireless Access Point WAX204

LED		Description
Power		When you turn on the access point, the Power LED lights solid red for about five seconds and then turns solid amber. After about 90 seconds, the Power LED lights solid green.
Internet		The Internet LED lights solid green or blinks green when the Internet connection is established. Note: The Internet connection is established after you access the local browser UI during the Setup Wizard process. If the Internet LED remains off or solid amber and does not turn solid green or blinking green, see Internet LED is solid amber or off [access point mode] on page 227.
WiFi		The WiFi LED lights solid green or blinks green.

- Log in to the access point by using *one* of the following methods:
 - Connect over WiFi.** On a WiFi-enabled computer or mobile device, find and connect to the access point's WiFi network (SSID). The default SSID and WiFi password (network key) are printed on the access point label.
 - Connect over Ethernet directly to the access point.** Using an Ethernet cable, connect the LAN port on your computer directly to any of the four LANs port on the access point.
- Launch a web browser and enter **<http://www.routerlogin.net>** in the address field. The Setup Wizard starts.
If the Setup Wizard does not start, see [You cannot log in to the access point \[access point mode\]](#) on page 229.
- Follow the prompts.
Note the following:
 - Trouble connecting to the Internet?** If the access point does not connect to the Internet, see [Troubleshoot Internet browsing](#) on page 234.
 - WAN connection type.** If the WAN connection is PPPoE, L2TP, or PPTP, or your Internet connection requires a static IP address, during the Setup Wizard Process, provide the required information for the Internet connection when the Smart Setup Wizard prompts you for the information.
 - New admin password.** During the Setup Wizard process, you must specify a new admin password (the local device password) and specify answers to two security questions (you can choose the questions).

- **Firmware update.** During the Setup Wizard process, you can update the firmware (if new firmware is available). Depending on the configuration, the access point might need to restart, you might need to log in again to continue the Setup Wizard process, or you might need to do both.
- **Browser security message.** During the Setup Wizard process, your browser will most likely display a security message. You can either ignore this message or install the security certificate. Consider the following examples:
 - **Google Chrome.** If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the IP address of the switch.
 - **Apple Safari.** If Apple Safari displays a *This connection is not private* message, 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.** If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
 - **Microsoft Internet Explore.** If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link.
 - **Microsoft Edge.** If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage**.

When the Setup Wizard is finished, the Register to unlock all features page displays.

7. Register the access point or select either restricted access or full access for a limited time to the local browser UI:
 - **Register with a NETGEAR account.** Click the **Login In with Netgear account** button and follow the prompts. Either use your existing NETGEAR account or create a new free NETGEAR account.
 - **Register with a registration key.** If you have a registration key (see [Get a registration key](#) on page 26), click the **Enter Registration Key** and enter the key.
 - **Access limited features.** Click the **Skip Registration and Access Limited Features** button to get access to a restricted menu of the local browser UI without time limitations. (For more information, see [Set up the access point and complete](#)

[the initial log-in process](#) on page 17.) The password that you must enter is your new local device password.

- **Temporarily access all features.** Click the **Skip Registration and Temporarily Access All Features** button to get access to the full menu of the local browser UI, but you get this access three times only. (For more information, see [Set up the access point and complete the initial log-in process](#) on page 17.) The password that you must enter is your new local device password.

8. Log in to the local browser UI again by entering your new local device password. This is the password that you specified during the Setup Wizard process. The BASIC Home page displays.
9. To change the system mode to access point mode, select **ADVANCED > Advanced Setup > Router / AP / Bridge Mode**, and continue with the following steps. The Router / AP / Bridge Mode page displays.
10. Select the **AP Mode** radio button.
We recommend that you leave the **Get dynamically from existing access point/router** button selected to let the access point get an IP address dynamically from the existing router in your network.
11. Click the **Apply** button, and in the pop-up window that displays, click the **OK** button. Your settings are saved and the access point is reconfigured in access point mode. The routing functions of the access point are disabled. Do not close the browser page.
12. Log back in to the access point.
For more information, see [Step 4](#).
If your browser web page does not show the login window, you might need to enter the new IP address of the access point in the address field. For more information, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
13. If your browser displays a security message again, see the information in [Step 6](#).
14. Find the new IP address of the access point in the local browser UI by doing the following:
 - a. Select **ADVANCED > ADVANCED Home**.
The ADVANCED Home page of the access point displays. The LAN Port pane shows the IP address that is now assigned to the access point.
 - b. Save the LAN IP address of the access point for later use.

You must use this IP address if you plan to connect to the same network as the access point but not directly to the access point network. If you are directly connected to the access point network, you can use <http://www.routerlogin.net>.

15. Clear the cache of your browser.

In access point mode, the access point functions with different IP address settings than in router mode. Clearing the cache of your browser might prevent website connectivity problems.

If you experience connectivity problems, see one of the following sections:

- [You cannot log in to the access point \[access point mode\]](#) on page 229
- [Troubleshoot Internet browsing](#) on page 234

Get a registration key

After you register the access point with NETGEAR, you can get a registration key to unlock full access to the local browser UI. When you enter the registration key to access the local browser UI, the access point can be connected to the Internet but does not need to be for you to configure the features.

This procedure describes how you can visit my.netgear.com, log in to your NETGEAR account, register the access point using its serial number, and get a registration key. If you do not have a free NETGEAR account, you can create one.

Note: You can also use the NETGEAR Insight app to get a registration key. For more information, visit kb.netgear.com/000061819/How-do-I-find-my-NETGEAR-registration-key.

To get a registration key:

1. From a computer or mobile device that is connected to the Internet, visit my.netgear.com.
2. Log in to your NETGEAR account.
If you do not have a free NETGEAR account, you can create one.
The My Products page displays.
3. From the menu on the left, select **Register a Product**.
The Register a Product page displays.
4. In the **Serial Number** field, enter the serial number of the access point.

The serial number consists of 13 digits. The serial number is printed on the access point label.

5. From the **Date Of Purchase** menu, select the date that you purchased the access point.
6. Click the **REGISTER** button.
The access point is registered with NETGEAR.
An confirmation email that includes the registration key is sent to your NETGEAR account email address.
7. If the My Products page does not display, click **My Product** from the menu.
8. Select the radio button for the newly registered access point.
9. Scroll down and click the **VIEW REGISTRATION KEY** button.
A pop-up window with the registration key displays.

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

Under the following circumstances, when the access point is in access point mode, you cannot use **http://www.routerlogin.net** to log in to the access point:

- Your computer or mobile device is not directly connected to the access point network even it is on the same network as the access point.
- Your computer or mobile device *is* directly connected to the access point, but the access point is using a static IP address.

Note: If the access point 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 **http://www.routerlogin.net**. However, if the DNS server is the IP address of the router to which the access point connects but the router's Internet connection is down, you *can* use **http://www.routerlogin.net** because the access point can still reach the router.

- Your network includes another NETGEAR device that is also accessible by using **http://www.routerlogin.net**. In such a situation, if you use **http://www.routerlogin.net**, you might log in to the access point 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 access point by your existing router during the setup process (see [Connect the access point to a router and log in for the first time](#) on page 22) to log in to the local browser UI of the access point.

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

- Only if the access point 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 access point and do the following:
 1. Open a web browser from a computer or mobile device that is directly connected to the access point network.
 2. Enter **http://www.routerlogin.net** in the address field.
 3. Click the **Login** button.
The NETGEAR Account Login page displays.
 4. Enter your registered email address and password and click the **Login** button.
The BASIC Home page displays.
 5. Select **ADVANCED**.
The ADVANCED Home page displays
 6. In the LAN Port pane, click the **CONNECTION STATUS** button.
The IP Address field displays the IP address that is assigned to the access point.
 - **Option 2. Temporarily connect directly and ping the access point.** Temporarily connect a computer or mobile device directly through an Ethernet cable or over WiFi to the access point and send a ping to **http://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 access point.
- Regardless of whether the access point is connected to the Internet, do one of the following:
 - **Option 1. Use the NETGEAR Insight mobile app.** To use the NETGEAR Insight mobile app to discover the IP address of the access point in your network, do the following:
 1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, and download and install the app.
 2. Connect your mobile device to the access point WiFi network.

3. Open the NETGEAR Insight mobile app.
4. Tap **LOG IN** to log in to your NETGEAR account, which is the same account that you logged into or created during the initial log-in process.
After you log in to your account, the IP address of the access point displays in the device list.

- **Option 2. 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 access point. The IP address that is assigned to the access point is listed.
- **Option 3. 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 access point.

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

Find the IP address of the access point with the NETGEAR Insight mobile app

The NETGEAR Insight mobile app lets you discover the access point in your network.

Note: Although you can use the NETGEAR Insight mobile app to register the access point, the access point is already registered automatically after the initial log-in process.

To use the NETGEAR Insight mobile app to discover the access point in your network:

1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, and download and install the app.
2. Connect your mobile device to the access point WiFi network.
3. Open the NETGEAR Insight mobile app.
4. Tap **LOG IN** to log in to your existing NETGEAR account, which is the same account that you logged into or created during the initial log-in process.
After you log in to your account, the IP address of the access point displays in the device list.
5. Save the IP address for future use.

Log in to the access point after initial setup

After initial setup, the access point is ready for use and you can change the settings and monitor the traffic.

When you enter the IP address that is assigned to the access point and you use http, the browser automatically redirects your request to https. If you did not yet install the access point's security certificate, your browser might display a security message. You can either ignore this message or install the security certificate. Consider the following examples:

- **Google Chrome.** If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the IP address of the switch.
- **Apple Safari.** If Apple Safari displays a *This connection is not private* message, 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.** If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
- **Microsoft Internet Explore.** If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link.
- **Microsoft Edge.** If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage**.

To log in to the access point's local browser UI after initial setup:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
A direct connection to the access point network, which is the most common type of setup, can be through WiFi or over Ethernet:
 - **WiFi.** A connection from a computer or mobile device to a WiFi network on the access point.
 - **Ethernet.** A connection from a computer over an Ethernet cable to one of the LAN ports on the access point, either with or without a switch or hub between the computer and the access point.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message, see the information in the introduction to this task.

3. Enter the access point 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.

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

Change the language

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

To change the language:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point's network after installation

After you install the access point in your network (see [Set up the access point and complete the initial log-in process](#) on page 17), you can connect devices to the access point's LAN through Ethernet cables or to the access point'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 access point.

Note: Connecting to the access point's network is not the same as connecting to the local browser UI to view or manage the access point's settings. For information about logging in to the access point local browser UI, see [Log in to the access point after initial setup](#) on page 30.

Connect to the access point through an Ethernet cable

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

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

1. Make sure that the access point is receiving power and is connected to the Internet (both its Power LED and Internet LED are lit).
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 access point.

You can use any of the four LAN ports on the access point.

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

Your computer or LAN device connects to the local area network (LAN). A message might display on your computer screen to notify you that an Ethernet cable is connected.

Use Wi-Fi Protected Setup to join the WiFi network

You can use Wi-Fi Protected Setup (WPS) to add a WiFi device such as a WiFi-enabled computer, tablet, or smartphone to the WiFi network of the access point.

WPS is a standard for easily adding computers and other devices to a home network while maintaining security. To use WPS (Push 'N' Connect), make sure that all WiFi devices to be connected to the network are Wi-Fi certified and support WPS. During the connection process, the client device gets the security settings from the access point so that every device in the network supports the same security settings.

To use WPS to connect a device to the WiFi network of the access point:

1. Make sure that the access point is receiving power (its Power LED is lit) and is connected to the Internet (its Internet LED is lit), and that the WiFi radios are on (its WiFi LED is lit).
2. Check the WPS instructions for your computer or WiFi device.
3. Press the **WPS** button on the access point for three seconds.
For more information, see [Back panel with ports, buttons, and a power connector](#) on page 13.
4. Within two minutes, press the **WPS** button on your 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 WiFi network of the access point.

Manually join the WiFi network

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

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

Note: By default, the access point's second and third WiFi network are disabled.

To connect a device manually to the WiFi network:

1. Make sure that the access point is receiving power (its Power LED is lit) and is connected to the Internet (its Internet LED is lit), and that the WiFi radios are on (its WiFi LED is lit).
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 the access point's network and select it.

If you did not change the default SSID, the default SSID is printed on the access point label. Otherwise, the SSID is the one that you specified during the initial log-in process.

For security, we recommend that you change the name of the default SSID.

4. Enter the WiFi password for WiFi access.

If you did not change the WiFi password (network key), the default WiFi password is printed on the access point label. Otherwise, the WiFi password is the one that you specified during the initial log-in process.

For security, we recommend that you change the default WiFi password.

5. Click the **Connect** button.

The device connects to the WiFi network of the access point.

3

Manually Set Up Internet Settings

Usually, the quickest way to set up the Internet connection is to allow the Setup Wizard to detect the Internet connection when go through the initial log-in procedure. After initial setup, you can use the Setup Wizard at any time.

If the access point is in router mode, you can specify the WAN (Internet) settings manually, including IPv6 settings. For information about changing the LAN settings if the access point is in router mode, see [LAN IP address settings \[router mode\]](#) on page 109.

This chapter contains the following sections:

- [Use the Setup Wizard](#)
- [Manually set up the access point Internet connection \[router mode\]](#)
- [IPv6 Internet connections and IPv6 addresses \[router mode\]](#)

Use the Setup Wizard

If the access point is in router mode, you can use the Setup Wizard to detect the WAN IP address that is issued by your Internet service provider (ISP) or an existing router in your network and automatically set up your access point. Unlike the Setup Wizard that runs when you go through the initial log-in procedure, you can start the Setup Wizard in the local browser UI any time.

For the Setup Wizard to detect the WAN IP address that is issued by your ISP, the access point must be connected to your modem with an Internet connection. You can also connect the access point to an existing router in your network and let the router assign an IP address to the access point.

To use the Setup Wizard:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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

The Setup Wizard page displays.

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

If you select the **No** radio button, you are taken to the WAN Setup page when you click the **Next** button. You can then set up the Internet connection manually. For more information, see [Manually set up the access point Internet connection \[router mode\]](#) on page 37.

6. Click the **Next** button.

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

Manually set up the access point Internet connection [router mode]

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

Note: The information in this section and subsections does not apply if the access point is in access point mode.

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

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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 WAX204.
 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.** Your ISP uses DHCP to automatically assign an IP address and related settings to the access point.
 - **Use Static IP Address.** Enter the static IP address, IP subnet mask, and gateway IP address that your ISP assigned to the access point. The gateway is the ISP router to which the access point 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 access point.
 - **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.
 10. Select a Router MAC Address radio button:
 - **Use Default Address.** Use the default access point MAC address that displays on the Dashboard page and is on the access point label.
 - **Use Computer MAC Address.** The access point 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. If your Internet configuration requires a specific VLAN ID, click the **VLAN/Bridge Settings** link.
For more information, see [Bridge port and VLAN tag groups \[router mode\]](#) on page 121.
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:
 - [You cannot access the Internet \[router mode\]](#) on page 231
 - [Troubleshoot Internet browsing](#) on page 234

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

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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 is how long the access point 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.** Your ISP uses DHCP to automatically assign an IP address and related settings to the access point.
 - **Use Static IP Address.** Enter the static IP address, IP subnet mask, and gateway IP address that your ISP assigned to the access point. The gateway is the ISP router to which the access point connects.
 13. Select a Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign DNS servers to the access point.
 - **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. Select a Router MAC Address radio button:
 - **Use Default Address.** Use the default access point MAC address that displays on the Dashboard page and is on the access point label.
 - **Use Computer MAC Address.** The access point 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. If your Internet configuration requires a specific VLAN ID, click the **VLAN/Bridge Settings** link.

For more information, see [Bridge port and VLAN tag groups \[router mode\]](#) on page 121.

16. Click the **Apply** button.

Your settings are saved.

17. 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:

- [You cannot access the Internet \[router mode\]](#) on page 231
- [Troubleshoot Internet browsing](#) on page 234

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

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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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. If your ISP requires a service name, type it in the **Service Name** 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 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.
12. If your ISP gave you fixed IP addresses and a connection ID or name, enter them in the **My IP Address**, **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.
13. Select a Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign DNS servers to the access point.
 - **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. Select a Router MAC Address radio button:
 - **Use Default Address.** Use the default access point MAC address that displays on the Dashboard page and is on the access point label.
 - **Use Computer MAC Address.** The access point 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:

- [You cannot access the Internet \[router mode\]](#) on page 231
- [Troubleshoot Internet browsing](#) on page 234

IPv6 Internet connections and IPv6 addresses [router mode]

The access point supports multiple types of IPv6 Internet connections. Which connection type you must use depends on your IPv6 ISP. Follow the directions that your IPv6 ISP gave you.

- If your ISP did not provide details, use the 6to4 tunnel connection type (see [Set up an IPv6 6to4 tunnel Internet connection \[router mode\]](#) on page 48).
- If you are not sure what type of IPv6 connection the access point uses, use the Auto Detect connection type, which lets the access point detect the IPv6 type that is in use (see [Use Auto Detect for an IPv6 Internet connection \[router mode\]](#) on page 44).
- If your Internet connection does not use pass-through, a fixed IP address, DHCP, 6rd, or PPPoE but is IPv6, use the Auto Config connection type, which lets the access point autoconfigure its IPv6 connection (see [Use Auto Config for an IPv6 Internet connection \[router mode\]](#) on page 46).

The access point supports the following IPv6 connection types:

- **Auto Detect.** For more information, see [Use Auto Detect for an IPv6 Internet connection \[router mode\]](#) on page 44.
- **Auto Config.** For more information, see [Use Auto Config for an IPv6 Internet connection \[router mode\]](#) on page 46.
- **6to4 tunnel.** For more information, see [Set up an IPv6 6to4 tunnel Internet connection \[router mode\]](#) on page 48.
- **Pass-through.** For more information, see [Set up an IPv6 passthrough Internet connection \[router mode\]](#) on page 51.
- **Fixed.** For more information, see [Set up an IPv6 fixed Internet connection \[router mode\]](#) on page 52.

- **DHCP.** For more information, see [Set up an IPv6 DHCP Internet connection \[router mode\]](#) on page 54.
- **6rd.** For more information, see [Set up an IPv6 6rd Internet connection \[router mode\]](#) on page 49.
- **PPPoE.** For more information, see [Set up an IPv6 PPPoE Internet connection \[router mode\]](#) on page 56.

When you enable IPv6 and select any connection type other than IPv6 pass-through, the access point starts the stateful packet inspection (SPI) firewall function on the WAN interface. This process is referred to as IPv6 filtering. The access point creates connection records and checks every inbound IPv6 packet. If the inbound packet is not destined for the access point itself and the access point does not expect to receive such a packet, or the packet is not in the connection record, the access point blocks this packet. This function works either in secured mode or in open mode. In secured mode, the access point inspects both TCP and UDP packets. In open mode, the access point inspects UDP packets only.

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. You can reduce any four-digit group of zeros within an IPv6 address to a single zero or omit it. The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

Use Auto Detect for an IPv6 Internet connection [router mode]

To set up an IPv6 Internet connection through autodetection:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **ADVANCED > Advanced Setup > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Detect**.
The page adjusts. The access point automatically detects the information in the following fields:
 - **Connection Type**. This field indicates the connection type that is detected.
 - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the access point's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
 - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the access point's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
6. In the LAN Setup section, select an IP Address Assignment radio button:
 - **Use DHCP Server**. This method passes more information to LAN devices but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config**. This is the default setting.

This setting specifies how the access point assigns IPv6 addresses to the devices on your home network (the LAN).
7. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the access point's LAN interface.
If you do not specify an ID here, the access point generates one automatically from its MAC address.
8. Select an IPv6 Filtering radio button:
 - **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
 - **Open**. In open mode, the router inspects UDP packets only.
9. Click the **Apply** button.

Your settings are saved.

Use Auto Config for an IPv6 Internet connection [router mode]

To set up an IPv6 Internet connection through autoconfiguration:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Auto Config**.

The page adjusts. The access point automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the access point's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the access point's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. (Optional) In the **DHCP User Class (if Required)** field, enter a host name.

Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.

7. (Optional) In the **DHCP Domain Name (if Required)** field, enter a domain name. You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.

8. Select an IPv6 Domain Name Server (DNS) Address radio button:

- **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
- **Use These DNS Servers.** If you know that your ISP requires specific servers, select this option. Enter the IPv6 address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

9. In the LAN Setup section, select an IP Address Assignment radio button:

- **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCPv6 client function.
- **Auto Config.** This is the default setting.

This setting specifies how the access point assigns IPv6 addresses to the devices on your home network (the LAN).

10. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the access point's LAN interface.

If you do not specify an ID here, the access point generates one automatically from its MAC address.

11. Select an IPv6 Filtering radio button:

- **Secured.** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open.** In open mode, the router inspects UDP packets only.

12. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 6to4 tunnel Internet connection [router mode]

The remote relay router is the router to which your router creates a 6to4 tunnel. Make sure that the IPv4 Internet connection is working before you apply the 6to4 tunnel settings for the IPv6 connection.

To set up an IPv6 Internet connection by using a 6to4 tunnel:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **6to4 Tunnel**.

The page adjusts. The access point automatically detects the information in the Router's IPv6 Address on LAN field. This field shows the IPv6 address that is acquired for the access point's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. Select a Remote 6to4 Relay Router radio button:

- **Auto.** Your access point uses any remote relay router that is available on the Internet. This is the default setting.
- **Static IP Address.** Enter the static IPv4 address of the remote relay router. Your IPv6 ISP usually provides this address.

7. Select an IPv6 Domain Name Server (DNS) Address radio button:

- **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
 - **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.
8. In the LAN Setup section, select an IP Address Assignment radio button:
- **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config.** This is the default setting.
- This setting specifies how the access point assigns IPv6 addresses to the devices on your home network (the LAN).
9. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the access point's LAN interface.
- If you do not specify an ID here, the access point generates one automatically from its MAC address.
10. Select an IPv6 Filtering radio button:
- **Secured.** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
 - **Open.** In open mode, the router inspects UDP packets only.
11. Click the **Apply** button.
- Your settings are saved.

Set up an IPv6 6rd Internet connection [router mode]

The 6rd protocol makes it possible to deploy IPv6 to sites using a service provider's IPv4 network. 6rd (also referred to as IPv6 rapid deployment) uses the service provider's own IPv6 address prefix. This limits the operational domain of 6rd to the service provider's network and is under direct control of the service provider. The IPv6 service provided is equivalent to native IPv6. The 6rd mechanism relies on an algorithmic mapping between the IPv6 and IPv4 addresses that are assigned for use within the service provider's network. This mapping allows for automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6rd.

With a 6rd tunnel configuration, the access point follows the RFC5969 standard, supporting two ways to establish a 6rd tunnel IPv6 WAN connection:

- **Auto Detect mode.** In IPv6 Auto Detect mode, when the access point receives option 212 from the DHCPv4 option, autodetect selects the IPv6 as 6rd tunnel setting (see

Use [Auto Detect for an IPv6 Internet connection \[router mode\]](#) on page 44). The access point uses the 6rd option information to establish the 6rd connection.

- **Manual mode.** Select **6rd Tunnel**. If the access point receives option 212, the fields are automatically completed. Otherwise, you must enter the 6rd settings.

To set up an IPv6 6rd Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **6rd Tunnel**.

The page adjusts. The access point automatically detects the information in the following sections:

- **6rd (IPv6 Rapid Development) Configuration.** The access point detects the service provider's IPv4 network and attempts to establish an IPv6 6rd tunnel connection. If the IPv4 network returns 6rd parameters to the access point, the page adjusts to display the correct settings in this section.

Note: If the access point does not automatically receive the 6rd parameters, you might need to enter them manually.

- **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the access point's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. Select an IPv6 Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
 - **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.
7. In the LAN Setup section, select an IP Address Assignment radio button:
 - **Use DHCP Server.** This method passes more information to devices on your LAN than the Auto Config method, but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config.** This method lets the access point assign IPv6 addresses to the devices on your the LAN. This is the default setting.

This setting specifies how the access point assigns IPv6 addresses to the devices on your home network (the LAN).
8. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the access point's LAN interface.

If you do not specify an ID here, the access point generates one automatically from its MAC address.
9. Select an IPv6 Filtering radio button:
 - **Secured.** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
 - **Open.** In open mode, the router inspects UDP packets only.
10. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 passthrough Internet connection [router mode]

In pass-through mode, the router works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The access point does not process any IPv6 header packets.

To set up a pass-through IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Pass Through**.

The page adjusts, but no additional fields display.

6. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 fixed Internet connection [router mode]

To set up a fixed IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **ADVANCED > Advanced Setup > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Fixed**.
The page adjusts.
6. In the WAN Setup section, specify the fixed IPv6 addresses for the WAN connection:
 - **IPv6 Address/Prefix Length**. The IPv6 address and prefix length of the access point's Internet (WAN) port.
 - **Default IPv6 Gateway**. The IPv6 address of the default IPv6 gateway for the access point's Internet (WAN) port.
 - **Primary DNS Server**. The primary DNS server that resolves IPv6 domain name records for the access point.
 - **Secondary DNS Server**. The secondary DNS server that resolves IPv6 domain name records for the access point.

Note: If you do not specify the DNS servers, the access point uses the DNS servers that are configured for the IPv4 Internet connection on the WAN Setup page. (See [Manually set up the access point Internet connection \[router mode\]](#) on page 37.)

7. In the LAN Setup section, select an IP Address Assignment radio button:
 - **Use DHCP Server**. This method passes more information to LAN devices but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config**. This is the default setting.

This setting specifies how the access point assigns IPv6 addresses to the devices on your home network (the LAN).
8. In the LAN Setup section, in the **IPv6 Address/Prefix Length** fields, specify the static IPv6 address and prefix length of the access point's LAN interface.
9. Select an IPv6 Filtering radio button:

- **Secured.** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open.** In open mode, the router inspects UDP packets only.

10. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 DHCP Internet connection [router mode]

To set up an IPv6 Internet connection with a DHCP server:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > IPv6**.

The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **DHCP**.

The page adjusts. The access point automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the access point's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the access point's LAN interface. The number after the slash (/) is the length

of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.

6. (Optional) In the **User Class (if Required)** field, enter a host name.
Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.
7. (Optional) In the **Domain Name (if Required)** field, enter a domain name.
You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.
8. Select an IPv6 Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
 - **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.
9. In the LAN Setup section, select an IP Address Assignment radio button:
 - **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config.** This is the default setting.

This setting specifies how the access point assigns IPv6 addresses to the devices on your home network (the LAN).
10. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the access point's LAN interface.
If you do not specify an ID here, the access point generates one automatically from its MAC address.
11. Select an IPv6 Filtering radio button:
 - **Secured.** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
 - **Open.** In open mode, the router inspects UDP packets only.
12. Click the **Apply** button.
Your settings are saved.

Set up an IPv6 PPPoE Internet connection [router mode]

To set up a PPPoE IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Advanced Setup > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **PPPoE**.
The page adjusts. The access point automatically detects the information in the following fields:
 - **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the access point's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
 - **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the access point's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
6. If already you set up your IPv4 ISP connection for PPPoE and want to use the same login information for IPv6, select the **Use the same Login information as IPv4 PPPoE check box** and go to [Step 8](#).

7. To manually configure the PPPoE settings for IPv6, specify the following settings:
 - **Login.** Enter the login name that your ISP gave you.
 - **Password.** Enter the password for the ISP connection.
 - **Service Name (if Required).** Enter a service name. If your ISP did not provide a service name, leave this field blank.

Note: The default setting of the **Connection Mode** menu is **Always On** to provide a steady IPv6 connection. The access point never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the access point attempts to reestablish the connection immediately after the PPPoE connection becomes available again.

8. Select an IPv6 Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
 - **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.

9. In the LAN Setup section, select an IP Address Assignment radio button:

- **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCv6 client function.
- **Auto Config.** This is the default setting.

This setting specifies how the access point assigns IPv6 addresses to the devices on your home network (the LAN).

10. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the access point's LAN interface.

If you do not specify an ID here, the access point generates one automatically from its MAC address.

11. Select an IPv6 Filtering radio button:

- **Secured.** In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open.** In open mode, the router inspects UDP packets only.

12. Click the **Apply** button.

Your settings are saved.

4

Basic WiFi and Radio Features

This chapter describes how you can manage the basic WiFi and radio settings of the access point. For information about the advanced WiFi and radio settings, see [Advanced WiFi and Radio Features](#) on page 187.

Tip: 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:

- [Set up or change an open or secure WiFi network](#)
- [Configure WPA and WPA2 Enterprise WiFi security with a RADIUS server](#)
- [Enable or disable a WiFi network](#)
- [Hide or broadcast the SSID for a WiFi network](#)
- [Manage client isolation for clients of the Wireless 2 or Wireless 3 network](#)
- [Manage access to LAN ports for clients of the Wireless 2 or Wireless 3 network](#)
- [Manage SSID isolation for all WiFi networks](#)
- [Enable or disable a WiFi radio](#)
- [Use WPS to connect to the WiFi network](#)

Set up or change an open or secure WiFi network

The access point 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. The default security is WPA2-Personal [AES].

Table 2. WiFi networks

WiFi network	Default status	Default SSID	Default WiFi password
Wireless 1	Enabled	NETGEARXXXXXX	Unique, see label.
Wireless 2	Disabled	NETGEARXXXXXX-2	sharedsecret
Wireless 3	Disabled	NETGEARXXXXXX-3	sharedsecret

In the previous table, XXXXXX represents the last six digits of the MAC address of the access point. The default SSID and WiFi password (network key) for the Wireless 1 network are printed on the access point label. If you changed the default SSID or WiFi password for the Wireless 1 network, use the ones that you specified.

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

For each WiFi network, the access point 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. For the 5 GHz band, it is 1200 Mbps. You can change (lower) the WiFi throughput mode (see [Change the WiFi throughput mode for a radio](#) on page 194).

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.

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

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **BASIC > Wireless**.
The Wireless Network page displays.
For information about SSID isolation, see [Manage SSID isolation for all WiFi networks](#) on page 69.
5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
6. To enable the selected WiFi network and set up or change the settings, configure the options that are described in the following table.
(For information about the WiFi security options, see [Step 7](#).)

Setting	Description
Wireless Network	Select the Enable radio button to enable the WiFi network or the Disable radio button to disable the WiFi network. By default, the Wireless 1 network is enabled and the other two WiFi networks are disabled.
Name (SSID)	The SSID (service set identifier) is the WiFi network name. If you do not change the SSID, the default SSID displays, in which XXXXXX represents the last six digits of the MAC address of the access point: Wireless 1. NETGEARXXXXXX Wireless 2. NETGEARXXXXXX-2 Wireless 3. NETGEARXXXXXX-3 The default SSID (for the Wireless 1 network) is also printed on the access point label (see Access point label on page 14). If you change the SSID, enter a 32-character (maximum), case-sensitive name in this field.
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.

(Continued)

Setting	Description
Enable SSID Broadcast	By default, the access point 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.
Client isolation	You cannot configure this setting for the Wireless 1 network. By default, client isolation is enabled for the WiFi network, 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 access point, select the Disable radio button.
Allow access to wired ports	You cannot configure this setting for the Wireless 1 network. By default, WiFi clients cannot reach devices that are connected to the wired ports (LAN ports) of the access point, and the Disable radio button is selected. To allow communication between WiFi clients and devices that are connected to the wired ports, select the Enable radio button.

- To set up or change the access point WiFi security for selected WiFi network, select and configure *one* of the options that are 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 <i>not</i> use an open WiFi network but configure WiFi security. However, an open network might be appropriate for a WiFi hotspot. Note: If you change the Wireless 1 network to an open network, WPS is disabled and the WPS LED turns off.
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 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.

(Continued)

Setting	Description
WPA-Personal [TKIP] + WPA2-Personal [AES]	<p>This option, which is the same as WPA2-PSK/WPA-PSK, enables WiFi devices that support either WPA2 or WPA to join the WiFi network. This option uses AES and TKIP encryption.</p> <p>WPA-PSK (which uses TKIP) is less secure than WPA2-PSK (which uses AES) and limits the speed of WiFi devices to 54 Mbps.</p> <p>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.</p>
WPA/WPA2 Enterprise	<p>This enterprise-level security uses RADIUS for centralized Authentication, Authorization, and Accounting (AAA) management. For more information, see Configure WPA and WPA2 Enterprise WiFi security with a RADIUS server on page 63).</p>
WPA3- Personal	<p>This option, which is the same as WPA3, is most secure personal authentication option. WPA3 uses SAE encryption and enables only WiFi devices that support WPA3 to join the WiFi network.</p> <p>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.</p> <p>In the Password (Network Key) field, enter a phrase of 8 to 127 characters or 128 hexadecimal digits. To join the WiFi network, a user must enter this password. To view the password in clear text, click the eye icon.</p>

- 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.

- Make sure that you can reconnect over WiFi to the network with its new settings. If you cannot connect over WiFi, check the following:
 - 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 access point provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
 - 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.

- Does your computer or device display as an attached device? (See [Display the devices currently on the access point network and change device information](#) on page 154.) If it does, it is connected to the network.
- Are you using the correct network name (SSID) and password?

Configure WPA and WPA2 Enterprise WiFi security with a RADIUS server

Remote Authentication Dial In User Service (RADIUS) is an enterprise-level method for centralized Authentication, Authorization, and Accounting (AAA) management. To enable the access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **BASIC > Wireless**.
The Wireless Network page displays.
5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
6. In the Security Options section, 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 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 or WPA2 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 that is used to access the RADIUS server for authentication.
The default port number is 1812.
10. In the **RADIUS Sever Shared Secret** field, enter the RADIUS password that is used between the access point 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:
 - 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 access point provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
 - 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.
 - Does your computer or device display as an attached device? (See [Display the devices currently on the access point network and change device information](#) on page 154.) If it does, it is connected to the network.
 - Are you using the correct network name (SSID) and password?

Enable or disable a WiFi network

You can temporarily disable a WiFi network (that is, an SSID) and you can reenble the WiFi network.

Note: For information about setting up a WiFi schedule that temporarily turns off a radio band (and, therefore, all WiFi networks that are active on that band), see [Add a WiFi schedule for a radio](#) on page 197. For information about turning off the radios entirely (and, therefore, all WiFi networks), see [Enable or disable a WiFi radio](#) on page 70.

To disable or enable a WiFi network:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **BASIC > Wireless**.
The Wireless Network page displays.
5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
6. Select one of following VAP radio buttons:
 - **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.

Hide or broadcast 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 detect the SSID in their scanned network lists. For additional security, you can turn off the SSID broadcast and hide the SSID so that users must know the SSID to be able to join the WiFi network.

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

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **BASIC > Wireless**.
The Wireless Network page displays.
5. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
6. Select or clear the **Enable SSID Broadcast** check box.
When you select the check box, the WiFi network broadcasts the SSID.
When you clear the check box, the WiFi network hides the SSID.

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

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

If client isolation is disabled for a WiFi network (SSID) on the access point, WiFi clients that are associated with that WiFi network can communicate with each other. This is the default setting for the Wireless 1 network and you cannot change the setting for the Wireless 1 network.

As an added security measure for the Wireless 2 and Wireless 3 networks, you can enable client isolation for all WiFi clients on the same WiFi network, preventing communication between WiFi clients that are associated with that WiFi network. Those WiFi clients can still communicate with each other over the Internet. This is the default setting for the Wireless 2 and Wireless 3 networks.

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

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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. That is, 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 for clients of the Wireless 2 or Wireless 3 network

You can manage whether WiFi clients can directly access devices that are connected to LAN ports of the access point. For example, if you connect a printer to LAN port 3 and a server to LAN port 4, WiFi clients might be able to access the printer and the server.

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

- **Wireless 1.** By default, WiFi clients that are connected to the Wireless 1 network can access devices that are connected to the LAN ports of the access point. For the Wireless 1 network, you cannot disable this type of access.
- **Wireless 2 or Wireless 3.** For the Wireless 2 and Wireless 3 networks independently, you can configure whether WiFi clients can access devices that are connected to the LAN ports. 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 specify whether WiFi clients of the Wireless 2 or Wireless 3 network can access devices that are connected to the LAN ports:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 select a radio button:
 - **Enable**. WiFi clients that are connected to the selected network can access devices that are connected to the LAN ports.
 - **Disable**. WiFi clients that are connected to the selected network cannot access devices that are connected to the LAN ports. (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

By default, as an added security measure, SSID isolation is enabled for all WiFi networks (SSIDs) on the access point, preventing communication between WiFi clients that are associated with different WiFi networks on the access point. Those WiFi clients can still communicate with each other over the Internet.

You can disable SSID isolation so that clients that are associated with different WiFi networks on the access point *can* communicate with each other.

To manage SSID isolation for all WiFi networks:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **BASIC > Wireless**.

The Wireless Network page displays.

5. Select an SSID Isolation radio button:

- **Enable.** All SSIDs are isolated. That is, WiFi clients that are connected to different SSIDs are prevented from communicating with each other. This is the default setting. (Communication over the Internet remains 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 access point 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 access point. When both WiFi radios are off, you can still use an Ethernet cable for a LAN connection to the access point. If you turn both WiFi radios off, WPS is also disabled.

You can also turn a WiFi radio on and off based on a schedule. (See [Add a WiFi schedule for a radio](#) on page 197.)

IMPORTANT: If the smart connect feature is enabled (which it is by default), 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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 (which it is by default), 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 both radios, the WiFi 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 access point's network without entering the WiFi network passphrase or key. Instead, you use a **WPS** button or enter a PIN to connect.

If you use the push button method, the computer or device that you are trying to connect must provide either a physical button or a software 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 59).

Use WPS with the push button method

For you to use the push button method to connect a WiFi device to the access point's WiFi network, the WiFi device that you are trying to connect must provide either a physical button or a software button. You can use the physical button and software button to let a WiFi device join only the main WiFi network, not the guest WiFi network.

To join the access point's main WiFi network using WPS with the push button method:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > WPS Wizard**.

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

5. Click the **Next** button.

By default, the **Push Button (recommended)** radio button is selected.

6. Either click the button onscreen or press the **WPS** button on the rear panel of the access point.

For two minutes, the access point attempts to find the WiFi device (that is, the client) that you want to join the access point's main WiFi network.

During this time, the WPS LED on the top panel of the access point blinks slowly.

7. Within two minutes, go to the WiFi device and press its **WPS** button to join the access point's main WiFi network without entering a password.

After the access point establishes a WPS connection, the WiFi LED lights and the Add WPS Client page displays a confirmation message.

8. To verify that the WiFi device is connected to the access point's WiFi network, select **BASIC > Attached Devices**.

The WiFi device displays onscreen.

Use WPS with the PIN method

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

To join the access point's WiFi network using WPS with the PIN method:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **ADVANCED > WPS Wizard**.
The Add WPS Client page displays and shows a description of the WPS method.
5. Click the **Next** button.
The Add WPS Client page adjusts.
The **Push Button (recommended)** radio button is selected by default.
6. Select the **PIN Number** radio button.
7. In the **Enter Clients' PIN** field, enter the PIN number of the WiFi device.
8. Click the **Next** button.
For four minutes, the access point attempts to find the WiFi device (that is, the client) that you want to join the access point's main WiFi network.
During this time, the WPS LED on the top panel of the access point blinks.
9. Within four minutes, go to the WiFi device and use its WPS software to join the network without entering a password.
After the access point establishes a WPS connection, the WiFi LED lights and the Add WPS Client page displays a confirmation message.
10. To verify that the WiFi device is connected to the access point's WiFi network, select **BASIC > Attached Devices**.
The WiFi device displays on the page.

5

Security, Firewall, and Access Rules

The access point 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.

This chapter includes the following sections:

- [Firewall WAN settings \[router mode\]](#)
- [Network access control lists](#)
- [Block specific Internet sites \[router mode\]](#)
- [Block specific applications and services from the Internet \[router mode\]](#)
- [Assign a trusted device \[router mode\]](#)
- [Schedule blocking \[router mode\]](#)
- [Set up security event email notifications](#)

Firewall WAN settings [router mode]

If the access point is in router mode, the basic firewall settings let you manage port scan protection and denial of service (DoS) protection, specify whether the access point can respond to a ping from the Internet (WAN) port, set up a DMZ server, and manage IGMP proxying, NAT filtering, and the 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 125.

Note: The information in this section and subsections does not apply if the access point is in access point mode.

Manage port scan protection and denial of service protection [router mode]

Port scan protection and denial of service (DoS) protection can protect your LAN against attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. By default, DoS protection is enabled and a port scan is rejected.

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

To change the default WAN security settings:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Setup > WAN Setup**.
The WAN Setup page displays.
5. To enable a port scan and disable DoS protection, select the **Disable Port Scan and DoS Protection** check box.
6. To enable the access point to respond to a ping on its Internet (WAN) port, select the **Respond to Ping on Internet Port** check box.
7. 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 access point 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.

The access point usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service or application for which you set up a port forwarding or port triggering rule (see [Port Forwarding and Port Triggering \[Router Mode\]](#) on page 207). Instead of discarding this traffic, you can direct the access point to forward the traffic to one computer on your network. This computer is called the default DMZ server.

To set up a default DMZ server:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 IGMP proxying [router mode]

IGMP proxying allows a computer or mobile device on the access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.

4. Select **ADVANCED > Setup > WAN Setup**.
The WAN Setup page displays.
5. Clear the **Disable IGMP Proxying** check box.
By default, this check box is selected and IGMP proxying is disabled.
6. Click the **Apply** button.
Your settings are saved.

Manage NAT filtering [router mode]

Network Address Translation (NAT) determines how the access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point 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 owns 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 access point on the Access Control page of the local browser UI (see [Enable and manage network access control](#) on page 81).

Enable and manage network access control

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

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

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **<http://www.routerlogin.net>** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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.** With this setting, if you add a new device, it can access your network. You do not need to enter its MAC address on this page. We recommend that you leave this radio button selected.
- **Block all new devices from connecting.** With this setting, if you add a new device, before it can access your network, you must enter its MAC address in the allowed list. For more information, see [Network access control lists](#) on page 81.

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 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::, and click either the **Allow** button or the **Block** button.
 - 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 access point.

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

If you set up an access list that blocks all new devices from accessing your network, 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Security > Access Control**.
The Access Control page displays.

5. 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 device 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 from accessing your network 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 allowed list.

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

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 device 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 Internet sites [router mode]

If the access point is in router mode, you can block keywords and domains (websites) to prevent certain types of HTTP traffic from accessing your network. Keyword and domain blocking does not work for HTTPS traffic.

By default, keyword blocking is disabled and no domains are blocked.

Note: The information in this section and subsections does not apply if the access point is in access point mode.

Set up keyword and domain blocking [router mode]

You can set up blocking of specific keywords and domains to occur continuously or according to a schedule.

To set up keyword and domain blocking:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **ADVANCED > Security > Block Sites**.
The Block Sites page displays.
5. Specify a keyword blocking option:
 - **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see [Schedule blocking \[router mode\]](#) on page 96.
 - **Always**. Use keyword blocking continuously.
6. In the **Type keyword or domain name here** field, enter a keyword or domain. Here are some sample entries:
 - Specify XXX to block <http://www.badstuff.com/xxx.html>.
 - Specify the domain suffix (for example, .com) if you want to block only sites with a domain suffix such as .com. In such a situation, sites with domain suffixes such as .edu and .gov are still allowed.
 - Enter a period (.) to block all Internet browsing access.
7. Click the **Add Keyword** button.
The keyword or domain is added to the **Block sites containing these keywords or domain names** field (which is also referred to as the blocked list).
8. To add more keywords or domains, repeat the previous two steps.
The keyword list supports up to 32 entries.
9. Click the **Apply** button.
Your settings are saved.

Remove a keyword or domain from the blocked list [router mode]

If you no longer need a keyword or domain on the blocked list, you can remove the keyword or domain.

To remove a keyword or domain from the blocked list:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Security > Block Sites**.
The Block Sites page displays.
5. In the **Block sites containing these keywords or domain names** field, select the keyword or domain.
6. Click the **Delete Keyword** button.
The keyword or domain is removed from the blocked list.
7. Click the **Apply** button.
Your settings are saved.

Remove all keywords and domains from the blocked list [router mode]

You can simultaneously remove all keywords and domains from the blocked list.

To remove all keywords and domains from the blocked list:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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

The Block Sites page displays.

5. Click the **Clear List** button.

All keywords and domains are removed from the blocked list.

6. Click the **Apply** button.

Your settings are saved.

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

If the access point 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 access point 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.

Note: The information in this section and subsections does not apply if the access point is in access point mode.

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

If the access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Security > Block Services**.
The Block Services page displays.
5. In the Services Blocking section, specify how the access point 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 96.
 - **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 91).
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 access point 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 the access point network.

3. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

4. Enter the access point 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.

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 access point 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 96.
- **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 access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 91.

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 access point 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 the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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.

Assign a trusted device [router mode]

If the access point is in router mode, you can exempt one trusted device from blocking and logging.

The device that you exempt must be assigned a fixed (static) IP address.

To assign a trusted device:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Security > Block Sites**.
The Block Sites page displays.
5. Scroll down and select the **Allow trusted IP address to visit blocked sites** check box.
6. In the **Trusted IP Address** field, enter the IP address of the trusted device.
The first three octets of the IP address (by default, 192.168.1) are automatically populated and depend on the IP address that is assigned to the DHCP server of the access point. For more information, see [Manage the DHCP server address pool \[router mode\]](#) on page 110.
7. Click the **Apply** button.
Your settings are saved.

Schedule blocking [router mode]

If the access point is in router mode, you can set up a schedule that you can apply to keyword and domain blocking, Internet service and application blocking, or both.

The schedule can specify the days and times that these features are active. After you set up the schedule, if you want it to become active, you must apply it to keyword and domain blocking (see [Set up keyword and domain blocking \[router mode\]](#) on page 86), Internet service and application blocking (see [Block specific applications and services from the Internet \[router mode\]](#) on page 89), or both. Without a schedule, you can only enable or disable these features. 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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

If the access point is in router mode, the access point can email you its logs of router activity. The log records activity and security events such as attempts to access blocked sites or services.

To set up email notifications:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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. To send email alerts over a secure connection, select the **Secure connection (use SSL)** check box.
10. 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.
11. To send alerts when someone attempts to visit a blocked site, select the **Send Alerts Immediately** check box.
Email alerts are sent immediately when someone attempts to visit a blocked site.
12. 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 access point sends log messages when the log is full.
 - **Hourly.** The access point sends log messages hourly.
 - **Daily.** The access point 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 access point 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.

13. 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 access point memory. If the access point cannot email the log and the log buffer fills, the access point overwrites the log.

6

Optimize Performance

This chapter describes how you can optimize the access point's performance and manage the traffic flows through the access point.

The chapter contains the following sections:

- [Enable QoS and automatically set the Internet bandwidth](#)
- [Enable QoS and manually set the Internet bandwidth](#)
- [Enable or disable the automatic update of the Performance Optimization Database](#)
- [Manage WiFi Multimedia \(WMM\) for a radio](#)
- [Improve network connections with Universal Plug and Play \[router mode\]](#)
- [Change the priority for a connected device \[router mode\]](#)

Enable QoS and automatically set the Internet bandwidth

You can enable QoS and let the access point automatically set its Internet download and upload bandwidth based on an automated speedtest. Although you can manually set the download and upload speed (see [Enable QoS and manually set the Internet bandwidth](#) on page 101), we recommend that you use the automatic method that is described in the following procedure.

To enable QoS and set the Internet download and upload bandwidth based on a speedtest:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **BASIC > Quality of Service**.

The QoS Setup page displays. By default, Quality of Service (QoS) is enabled, and the **Enable QoS** check box is selected.

5. Click the **Take A Speedtest** button.

The speed test checks the access point download and uplink bandwidth, sets the detected bandwidths, and displays the results on the page.

6. Click the **Apply** button.

Your settings are saved.

For information about bandwidth utilization by device and application, see [Display the devices currently on the access point network and change device information](#) on page 154.

Enable QoS and manually set the Internet bandwidth

If you enable QoS, we recommend that you use the automatic method to set the Internet download and upload speed for the access point (see [Enable QoS and automatically set the Internet bandwidth](#) on page 100). However, you can also manually set the Internet bandwidth.

Note the following about manual configuration:

- Do not set the bandwidth higher than the actual bandwidth because it causes dynamic QoS to become ineffective.
- If you set the bandwidth lower than the actual bandwidth, the access point underutilizes the available bandwidth.

To enable QoS and manually set the Internet download and upload bandwidth:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **BASIC > Quality of Service**.

The QoS Setup page displays. By default, Quality of Service (QoS) is enabled, and the **Enable QoS** check box is selected. By default, the **Let Speedtest detect my Internet bandwidth** radio button is selected.

5. To find out what bandwidths your Internet connection supports, click the **Take A Speedtest** button.

The speed test checks the access point download and uplink bandwidth, sets the detected bandwidths, and displays the results on the page.

6. Select the **I want to define my Internet bandwidth** radio button.

A pop-up windows displays.

7. Click the **OK** button.

The fields for manual configuration display.

8. In the **Download Speed (Mbps)** field, enter the Internet download speed in Mbps. You can use decimal numbers.

9. In the **Upload Speed (Mbps)** field, enter the Internet upload speed in Mbps. You can use decimal numbers.

10. Click the **Apply** button.

A pop-up windows displays.

11. Click the **OK** button.

Your settings are saved.

For information about bandwidth utilization by device and application, see [Display the devices currently on the access point network and change device information](#) on page 154.

Enable or disable the automatic update of the Performance Optimization Database

The access point uses a Performance Optimization Database that includes the most popular applications and services for the implementation of dynamic QoS. By default, the access point automatically updates this database. You can turn off this feature and manually update the database.

To enable or disable the automatic update of the Performance Optimization Database:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **BASIC > Quality of Service**.
The QoS Setup page displays.
In the Performance Optimization Database section, the version and release of the database are displayed.
5. Select or clear the **Automatically update performance optimization database** check box.
6. Click the **Apply** button.
Your settings are saved.
7. To immediately let the access point update the Performance Optimization Database if an update is available, click the **Update Now** button.

Manage WiFi Multimedia (WMM) for a radio

WiFi Multimedia (WMM) is a subset of the 802.11e standard. Time-dependent information such as video or audio is given higher priority than normal traffic. For WMM to function correctly, WiFi clients must also support WMM. By enabling WMM, you allow WMM to control upstream traffic flowing from WiFi devices to the access point and downstream

traffic flowing from the access point to WiFi devices. WMM defines the following four queues in decreasing order of priority:

- **Voice.** The highest priority queue with minimum delay, which makes it very suitable for applications such as VoIP and streaming media.
- **Video.** The second highest priority queue with low delay. Video applications are routed to this queue.
- **Best effort.** The medium priority queue with medium delay. Most standard IP applications use this queue.
- **Background.** The low priority queue with high throughput. Applications such as FTP that are not time-sensitive but require high throughput can use this queue.

By default, WMM is enabled for both radios, but you can disable WMM for one or both radios.

To disable WMM for one or both radios:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
 2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
 3. Enter the access point 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.
 4. Select **ADVANCED > Setup > QoS Setup**.
The QoS Setup page displays.
 5. Select the **WMM** tab.
The Quality of Service page displays.
 6. Clear the **Enable WMM (Wi-Fi multimedia) settings** check box for the radio to disable WMM, or clear both check boxes for both radios.
 7. Click the **Apply** button.
-

Your settings are saved. The radio or radios restart and WiFi clients might need to reconnect.

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 access point 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, keep UPnP enabled, which it is by default in router mode.

To manage Universal Plug and Play:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Advanced Setup > UPnP**.
The UPnP page displays.
5. Select the **Turn UPnP On** check box.
By default, this check box is selected. You can disable or enable UPnP for automatic configuration. If the **Turn UPnP On** check box is cleared, a device cannot automatically control the resources of the access point. For example, a device cannot control port forwarding on the access point.

6. Enter the advertisement period in minutes.

The advertisement period specifies how often the access point 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 access point is in router mode, the UPnP Portmap Table displays the IP address of each UPnP device that is accessing the access point 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 access point is in router mode, to refresh the information in the UPnP Portmap table, click the **Refresh** button.

Change the priority for a connected device [router mode]

If the access point is in router mode and you enabled QoS ([Enable QoS and automatically set the Internet bandwidth](#) on page 100 or [Enable QoS and manually set the Internet bandwidth](#) on page 101), the access point automatically assigns a priority to any device that connects to it. By default, an attached device receives a medium priority. However, the device with which you connect to the local browser UI of the access point receives a high priority. You can change the priority for an attached device so that it receives a different treatment in the access point network.

To change the priority for an attached device:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not

know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **BASIC > Attached Devices**.
The Attached Devices page displays.
5. Select the radio button for the device for which you want to change the priority.
6. Click the **Edit** button.
The Edit Device page displays.
7. Select one of the following Device Priority buttons: **Highest, High, Medium**, or **Low**.

Note: For information about changing display settings for the device, see [Display the devices currently on the access point network and change device information](#) on page 154.

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

7

Network Settings

This chapter describes how you can manage various network settings of the access point.

The chapter includes the following sections:

- [LAN IP address settings \[router mode\]](#)
- [Change the access point network device name](#)
- [Reserved LAN IP addresses \[router mode\]](#)
- [Static routes](#)
- [Bridge port and VLAN tag groups \[router mode\]](#)
- [Change the MTU size \[router mode\]](#)

LAN IP address settings [router mode]

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

Note: The information in this section and subsections does not apply if the access point is in access point mode.

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

If the access point is in router mode, it is preconfigured to use private IP addresses on the LAN side and to function as a DHCP server. The access point's LAN IP configuration is as follows:

- **LAN IP address.** 192.168.1.1 (if the access point is in router mode, this is the same as www.routerlogin.net)
- **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 110).

To change the LAN IP address and subnet settings:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **<http://www.routerlogin.net>** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 local browser UI of the access point also changes.

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

The LAN IP subnet mask at which you can access the local browser UI of the access point also changes.

7. Click the **Apply** button.

Your settings are saved.

If you changed the LAN IP address settings of the default LAN subnet, you are disconnected from the local browser UI.

To reconnect, close your browser, relaunch it, and log in to the access point at its new LAN IP address.

Manage the DHCP server address pool [router mode]

If the access point is in router mode, it functions as a Dynamic Host Configuration Protocol (DHCP) server. The access point 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 access point'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 access point 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 access point assigns:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point 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 access the access point.

To disable the DHCP server:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point is in router mode, Router Information Protocol (RIP) lets the access point 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 the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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

The LAN Setup page displays.

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

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

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 access point network device name

The default network device name of the access point is the model number (WAX204). This device name displays in, for example, a file manager when you browse your network.

To change the access point network device name:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point 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 access point's DHCP server, the device receives the same IP address.

Note: The information in this section and subsections does not apply if the access point is in access point mode.

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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point'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 access point'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 [router mode]

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

To change a reserved LAN IP address:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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

The access point supports IPv4 static routes. Static routes can provide detailed routing information to your access point. 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 access point, 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 access point 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

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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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.
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 access point 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

You can change an IPv4 static route.

To change an IPv4 static route:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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](#) on page 118.
8. Click the **Apply** button.
The route settings are updated in the table on the Static Routes page.

Remove an IPv4 static route

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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 access point is in router mode, some devices, such as an Internet Protocol television (IPTV), cannot function behind the access point'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 access point's Internet (WAN) port or between the device and a VLAN tag group.

Also, some ISPs might require the access point 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.

Note: The information in this section and subsections does not apply if the access point is in access point mode.

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

If the access point 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 access point's Internet (WAN) port.

A bridge with a port group allows packets that are sent between a device such as an IPTV and the access point Internet (WAN) port to circumvent the access point'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 access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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**, **Port 3**, or **Port 4**) or WiFi network (**Wireless1**, **Wireless2**, or **Wireless2**) to which the device that must circumvent the access point'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.
Your settings are saved. You might need to reconnect to the access point.

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

If the access point 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 access point's Internet (WAN) port.

If you are subscribed to an IPTV service, the ISP might require you to use VLAN tags on the access point 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 access point Internet (WAN) port to circumvent the access point's NAT service, which otherwise could drop the packets.

The access point 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 access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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:

- **ISP Profile.** This menu applies only to certain ISPs. If this option does not apply, the menu is set to Others.
- **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, Port 3, or Port 4**) or WiFi network (**Wireless1, Wireless2, or Wireless2**) to which the device that must circumvent the access point'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 access point.

Change the MTU size [router mode]

If the access point 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 access point 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.

Note: 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 3. 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.
1436	Used in PPTP environments or with VPN.

8

Maintain and Monitor

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

The chapter includes the following sections:

- [Update the firmware](#)
- [Back up or restore the settings](#)
- [Change the local device password](#)
- [Change the password recovery questions for the local device password](#)
- [Recover the local device admin password](#)
- [Factory default settings](#)
- [Time and Network Time Protocol server](#)
- [Logs](#)
- [Status and statistics](#)
- [Traffic meter \[router mode\]](#)
- [Change the system mode to access point mode or to router mode](#)
- [Disable LED blinking or turn off LEDs](#)

Update the firmware

From time to time, or as needed, NETGEAR makes new firmware (software) available. The firmware is stored in flash memory.

You can log in to the access point and check if new firmware is available, or you can manually load a specific firmware version to your access point.

Let the access point check for new firmware and update the firmware

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

Note: We recommend that you connect a computer to the access point using an Ethernet connection to update the firmware.

To let the access point check for new firmware and update the firmware:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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

5. Click the **Check** button.

The access point 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 access point 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 access point. Wait until the access point 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 access point restarts.

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

To verify that the access point runs the new firmware version, continue with the following steps:

7. Launch a web browser from a computer or mobile device that is connected to the access point network.

8. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

9. Enter the access point 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.

The version firmware is stated in the Firmware Version field at the top right of the page.

Manually check for new firmware and update the firmware

Note: We recommend that you connect a computer to the access point using an Ethernet connection to update the firmware.

To download new firmware manually and update the access point manually:

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. Launch a web browser from a computer or mobile device that is connected to the access point network.
5. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

6. Enter the access point 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.
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 access point. Wait until the access point 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 access point restarts.

To verify that the access point runs the new firmware version, continue with the following steps:

11. Launch a web browser from a computer or mobile device that is connected to the access point network.
12. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
13. Enter the access point 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.

The version firmware is stated in the Firmware Version field at the top right of the page.

Back up or restore the settings

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

Back up the access point settings

You can save a copy of the current configuration settings.

To back up the access point's configuration file:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point. When the restoration is complete, the access point 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 access point. Wait until the access point 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 access point 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 local login to the access point:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 136.
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 password 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 access point with the user name admin. If you forget this password, you can recover it. The recovery process is supported in the Internet Explorer, Firefox, Chrome, and Safari browsers.

You can change the password recovery questions.

To change the password recovery questions:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 the local device admin password

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

To recover your local device password:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter your local device password.
If you enter an incorrect password three times, you are prompted to enter the serial number of the access point.
The serial number is on the access point label.
4. Enter the serial number of the access point.
5. Click the **Continue** button.
A window displays prompts for the answers to your security questions.
6. Enter the saved answers to your security questions.
7. Click the **Continue** button.
A window displays your recovered password.

- Click the **Login again** button.
A login window displays.
- With your recovered password, log in to the access point.

Factory default settings

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

If the access point is in access point mode and you do not know the current IP address of the access point, first try to use the NETGEAR Insight mobile app or an IP scanner application to detect the IP address. If you still cannot find the current IP address of the access point, reset the access point to factory default settings.

Note: If the access point is in router mode, you can always access the access point by using <http://www.routerlogin.net>.

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

After you reset the access point to factory default settings, the access point is in router mode, the login URL is www.routerlogin.net, and the DHCP server is enabled. For a list of factory default settings, see [Technical specifications](#) on page 242.

Use the dual-function Reset button to return to factory defaults

Depending on how you long press the dual-function **Reset** button (for details, see the following procedure), this button lets you return the access point to factory default settings and either keep the registration status or reset it on the access point only:

- Reset to factory default settings but maintain the registration status.** Return the access point to factory default settings only. After you do so, you must go through the initial log-in process again (see [Set up the access point and complete the initial log-in process](#) on page 17), but you do not need to register the access point with NETGEAR and can use your local device password to log in to the local browser UI.
- Reset to factory default settings and reset the registration status.** Return the access point to factory default settings *and* reset the NETGEAR registration status

on the access point. This option can be useful if you want to register the access point under a different name or account.

This option requires two steps:

1. Contact NETGEAR support at netgear.com/support so that the NETGEAR registration status on the NETGEAR server can be reset.
2. Return the access point to factory default settings and reset the registration on the access point. After you do so, you must go through the initial log-in process again (see [Set up the access point and complete the initial log-in process](#) on page 17), which is then automatically followed by the single sign-on (SSO) process, which lets you reregister the access point with NETGEAR.

Note: If you reset the registration on the access point without contacting NETGEAR first, the access point is returned to factory default settings only, and the registration is not reset.

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

To reset the access point to factory default settings using the Reset button:

1. On the back of the access point, locate the recessed **Reset** button.
For more information, see [Back panel with ports, buttons, and a power connector](#) on page 13.
2. Insert a device such as a straightened paper clip into the opening.
3. Do one of the following:
 - **Reset to factory default settings but maintain the registration status.** Press the **Reset** button for more than 5 seconds *but less than 10 seconds*. (Do not press the button for more than 10 seconds!)
After you use this option, you must go through the initial log-in process again but you do *not* need to reregister access point with NETGEAR and can use your local device password to log in to the local browser UI.
 - **Reset to factory default settings and reset the registration status.** Press the **Reset** button for more than 10 seconds.
This option requires you to first contact NETGEAR support at netgear.com/support so that the NETGEAR registration status on the NETGEAR server can be reset. Then, you can use this option, go through the initial log-in process again, and reregister the access point with NETGEAR.

The Power LED turns red and the configuration is reset to factory default settings. When the reset is complete, the access point 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 access point's local browser UI, do not close the browser, click a link, or load a new page. Do not turn off the access point. Wait until the access point finishes restarting and the Power LED turns solid green.

Use the local browser UI to return to factory defaults

The local browser provides two reset options:

- **Reset to factory default settings but maintain the registration status.** Return the access point to factory default settings only. After you do so, you must go through the initial log-in process again (see [Set up the access point and complete the initial log-in process](#) on page 17), but you do not need to register the access point with NETGEAR and can use your local device password to log in to the local browser UI.
- **Reset to factory default settings and reset the registration status.** Return the access point to factory default settings *and* reset the NETGEAR registration status on the access point. This option can be useful if you want to register the access point under a different name or account.

This option requires two steps:

1. Contact NETGEAR support at netgear.com/support so that the NETGEAR registration status on the NETGEAR server can be reset.
2. Return the access point to factory default settings and reset the registration on the access point. After you do so, you must go through the initial log-in process again (see [Set up the access point and complete the initial log-in process](#) on page 17), which is then automatically followed by the single sign-on (SSO) process, which lets you reregister the access point with NETGEAR.

Note: If you reset the registration on the access point without contacting NETGEAR first, the access point is returned to factory default settings only, and the registration is not reset.

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

To erase the settings:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **<http://www.routerlogin.net>** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not

know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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

The Backup Settings page displays.

5. Select one of the following radio buttons:

- **Revert to factory default settings and unregister the device.**

This option requires you to first contact NETGEAR support at netgear.com/support so that the NETGEAR registration status on the NETGEAR server can be reset.

Then, you can use this option, go through the initial log-in process again, and reregister the access point with NETGEAR.

- **Revert to factory default settings.**

After you use this option, you must go through the initial log-in process again but you do *not* need to reregister access point with NETGEAR and can use your local device password to log in to the local browser UI.

6. Click the **Erase** button.

A warning page displays.

7. Click the **Yes** button.

The configuration is reset to factory default settings. When the reset is complete, the access point 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 access point. Wait until the access point finishes restarting and the Power LED turns solid green.

Time and Network Time Protocol server

By default, the access point 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 access point might detect the time zone automatically or you might need to adjust the time zone and daylight saving time settings. When the access point synchronizes its clock with a Network Time Protocol (NTP) server, the access point detects the correct date and time. If the access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 access point operates.
6. If the access point 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 access point 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 access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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

Logs

The log is a detailed record of the websites that users on your network accessed or attempted to access and many other access point actions. You can manage which activities are logged.

Specify which activities the access point logs

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

To manage which activities are logged:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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. By default, all check boxes are selected, and the following activities are logged:

- Attempted access to allowed sites
- Attempted access to blocked sites and services
- Connections to the local browser UI of the access point
- Router operations such as startup, getting the time, and so on
- Known DoS attacks and port scans

- Port forwarding and port triggering
 - WiFi access
 - Scheduled deactivation of the WiFi signal
 - VPN service
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.

View, send, or clear the logs

In addition to viewing the logs, you can send them by email, and clear them.

To view, send, or clear the logs:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Administration > Logs**.
The Logs page displays.
5. To send the logs by email, click the **Send Log** button.
The access point sends the logs to the email address that you specified for email notifications (see [Set up security event email notifications](#) on page 97).
6. To refresh the log entries onscreen, click the **Refresh** button.

7. To clear the log entries, click the **Clear Log** button.

Status and statistics

You can view information about the access point 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, access point, and WiFi settings [router mode]

If the access point is in router mode, you can display information about the access point, the IP addresses, and the WiFi settings for each radio.

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

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **ADVANCED**.
The ADVANCED Home page displays.

WiFi 6 AX1800 Dual Band Wireless Access Point WAX204

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 access point hardware version, which is the model number WAX204.
Firmware Version	The access point firmware version. If you update the firmware, the version changes (see Update the firmware on page 129).
GUI Language Version	The access point language version for the local browser UI.
Operation Mode	The operation mode is Router. For more information about the changing the operation mode, see Change the system mode to access point mode or to router mode on page 164.
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 access point 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 access point LAN ports combined.
IP Address	The IP address that applies to all four access point LAN ports. For more information, see Change the LAN IP address and subnet settings [router mode] on page 109.
DHCP Server	If the access point is in router mode, this field displays if the DHCP server of the access point is enabled (the default setting in router mode) or disabled (see Disable the DHCP server [router mode] on page 112).

(Continued)

Field	Description
IP Subnet Mask	The IP subnet mask that applies to all four access point LAN ports. For more information, see Change the LAN IP address and subnet settings [router mode] on page 109.
DHCP Lease Time	The DHCP lease time. For more information, see Manage the DHCP server address pool [router mode] on page 110.

Field	Description
-------	-------------

Internet Port

To change these settings, see, [Use the Setup Wizard](#) on page 36 or [Manually set up the access point Internet connection \[router mode\]](#) on page 37.

MAC Address	The MAC address that applies to the access point WAN (Internet) port.
IP Address	The WAN IP address that the access point receives from your ISP (through your modem) or the WAN IP address that you manually configured.
Connection	The type of Internet connection that the access point uses, which can be DHCP (the default setting), Static IP, PPPoE, PPTP, or L2TP.
IP Subnet Mask	The IP subnet mask that the access point uses.
Domain Name Server	The IP address of the Domain Name System (DNS) server that the access point uses.
WAN Preference	This field always shows Internet Port (1 Gbps).

Field	Description
-------	-------------

Wireless Settings (2.4GHz) or Wireless Settings (5GHz)

To change these settings, see [Basic WiFi and Radio Features](#) on page 58 and [Advanced WiFi and Radio Features](#) on page 187.

Name	The name of the SSID (see Set up or change an open or secure WiFi network on page 59).
Region	The country and region in which the access point is being used (see Change the region of operation on page 188).
Channel	The channel that the radio uses (see Change the channel for a radio on page 193).

(Continued)

Field	Description
Mode	The WiFi throughput mode that the radio uses (see Change the WiFi throughput mode for a radio on page 194).
Wireless AP	Displays if the WiFi network is enabled (see Set up or change an open or secure WiFi network on page 59 or Enable or disable a WiFi network on page 65).
Broadcast Name	Displays if the WiFi network broadcasts its SSID (see Hide or broadcast the SSID for a WiFi network on page 66).
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, access point, and WiFi settings [access point mode]

If the access point is in access point mode, you can display information about the LAN IP addresses, access point, and the WiFi settings for each radio.

To display information about the access point and the IP and WiFi settings if the access point is in access point mode:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point hardware version, which is the model number WAX204.
Firmware Version	The access point firmware version. If you update the firmware, the version changes (see Update the firmware on page 129).
GUI Language Version	The access point language version for the local browser UI.
Operation Mode	The operation mode is AP. For more information about the changing the operation mode, see Change the system mode to access point mode or to router mode on page 164.

Field	Description
LAN Port	
To change these settings, see Use the Setup Wizard on page 36.	
MAC Address	The MAC address that applies to the access point WAN (Internet) port.
DHCP	Displays if the DHCP client of the access point is enabled.
IP Address	The LAN IP address that the access point 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 access point uses.

(Continued)

Field	Description
Gateway IP Address	The IP address of the gateway to which the access point connects to the Internet.
Domain Name Server	The IP address of the Domain Name System (DNS) server that the access point uses.
Field	Description
Wireless Settings (2.4GHz) or Wireless Settings (5GHz)	
To change these settings, see Basic WiFi and Radio Features on page 58 and Advanced WiFi and Radio Features on page 187.	
Name	The name of the SSID (see Set up or change an open or secure WiFi network on page 59).
Region	The country and region in which the access point is being used (see Change the region of operation on page 188).
Channel	The channel that the radio uses (see Change the channel for a radio on page 193).
Mode	The WiFi throughput mode that the radio uses (see Change the WiFi throughput mode for a radio on page 194).
Wireless AP	Displays if the WiFi network is enabled (see Set up or change an open or secure WiFi network on page 59 or Enable or disable a WiFi network on page 65).
Broadcast Name	Displays if the WiFi network broadcasts its SSID (see Hide or broadcast the SSID for a WiFi network on page 66).
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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED**.

The ADVANCED Home page displays.

5. In the Internet Port pane (in router mode) or in the LAN Port pane (in access point mode), click the **CONNECTION STATUS** button.

The Connection Status pop-up window displays.

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

When the access point 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 access point.
In access point 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 access point.
- **Default Gateway.** The IP address for the default gateway that the access point communicates with.
In access point 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 access point.
In access point 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 access point 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 access point receives an IP address dynamically, you can perform the following actions:
- **Release.** Click the **Release** button to terminate the DHCP IP address, that is, terminate the Internet connection.
 - **Renew.** 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED**.
The ADVANCED Home page displays.
5. In the Internet Port pane (in router mode) or in the LAN Port pane (in access point mode), click the **Show Statistics** button.

A pop-up window displays, showing the following information:

- **System Up Time.** The time elapsed since the access point 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 entirely, click the **Stop** button.

Display the devices currently on the access point network and change device information

You can display the active wired and WiFi devices in the access point network. If you do not recognize a WiFi device, it might be an intruder.

If the access point is in router mode, you can also display the VPN devices in the access point network.

To display the attached wired, WiFi, and VPN devices or to change device information:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **BASIC > Attached Devices**.

The Attached Devices page displays:

- Wired devices are connected to the access point with Ethernet cables. WiFi devices are connected to the access point through the WiFi network, in either the 2.4 GHz band or the 5 GHz band. VPN devices are connected over a VPN tunnel to the access point.
- If you enabled access control (see [Enable and manage network access control](#) on page 81), the page displays the access control status of the device in the network.
- If you enabled QoS (see [Enable QoS and automatically set the Internet bandwidth](#) on page 100 or [Enable QoS and manually set the Internet bandwidth](#) on page 101), the page displays the detected download and upload speeds for the access point and the automatically assigned priority.

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 81), the access control status of the device in the network (Allowed or Blocked).
Priority	If QoS is enabled (see Enable QoS and automatically set the Internet bandwidth on page 100 or Enable QoS and manually set the Internet bandwidth on page 101), the priority that the access point assigned automatically to the device or that you changed manually (see Step 5 or see Change the priority for a connected device [router mode] on page 106).

(Continued)

Field	Description
Connection Type	For WiFi devices, the connection type information shows the radio 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 access point network. This address can change when a device is disconnected and rejoins the network. Note: If you enable access control or QoS, the IP address is displayed in the Device Name field.
Internet Download Speed by Device	If QoS is enabled (see Enable QoS and automatically set the Internet bandwidth on page 100 or Enable QoS and manually set the Internet bandwidth on page 101), the download speed in Mbps that the device uses.
Internet Upload Speed by Device	If QoS is enabled (see Enable QoS and automatically set the Internet bandwidth on page 100 or Enable QoS and manually set the Internet bandwidth on page 101), the upload speed in Mbps that the device uses.

The following information displays only if the access point is in router mode and supports VPN clients devices.

Field	Description
VPN Client Devices	
Device Name	The device name, if detected.
Remote IP Address	The IP address of the device at the other side of the VPN tunnel.

(Continued)

Field	Description
Local IP Address	The IP address that is assigned to the device when it joined the access point network. This address can change when a device is disconnected and rejoins the network.
Connection Time	The time that elapsed since the device connected to the access point.

5. To change the information that displays for a device or the QoS priority, do the following:
 - a. Select the radio button 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. If QoS is enabled (see [Enable QoS and automatically set the Internet bandwidth](#) on page 100 or [Enable QoS and manually set the Internet bandwidth](#) on page 101), select one of the following Device Priority buttons: **Highest**, **High**, **Medium**, or **Low**.
 - g. 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 access point is in router mode, you can enable traffic metering to monitor the volume of Internet traffic that passes through the access point'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.

Note: The information in this section and subsections does not apply if the access point is in access point mode.

Start the traffic meter without traffic restrictions [router mode]

If the access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 162.

Restrict Internet traffic by volume [router mode]

If the access point 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 the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point issues a warning message before the monthly limit in MB is reached.

This setting is optional. The access point 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 or amber.** This setting is optional. When the traffic limit is reached, the Internet LED alternates between green and amber.
- **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 162.

Restrict Internet traffic by connection time [router mode]

If the access point is in router mode, you can record and restrict the traffic by connection time. This is useful when your ISP measures your 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point 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 access point 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 access point issues a warning message before the monthly limit in hours is reached.

This setting is optional. The access point 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 or amber.** This setting is optional. When the traffic limit is reached, the Internet LED alternates between green and amber.
- **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 162.

View the Internet traffic volume and statistics [router mode]

If the access point is in router mode and you enabled the traffic meter (see [Start the traffic meter without traffic restrictions \[router mode\]](#) on page 158), 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 system mode to access point mode or to router mode

By default, the access point functions in router mode, that is, the system mode is router mode. You can connect the access point to a router, switch, or hub in your network and change the system mode to access point mode.

The access point can function in either of the following system modes:

- **Router mode.** By default, the access point functions in router mode with its router functionality enabled. When the access point is in router mode, you must connect the WAN (Internet) port of the access point to a LAN port on your Internet modem. For more information, see [Connect the access point to a modem and log in for the first time](#) on page 18.
- **Access point mode.** The access point can function in access point mode with its router functionality disabled. If the access point is in access point mode, you must connect the WAN (Internet) port of the access point to a LAN port on a router, switch, or hub in your network. For more information, see [Connect the access point to a router and log in for the first time](#) on page 22.

For information about the features that are enabled in router mode and disabled in access point mode, see [Routing features enabled only in router mode](#) on page 16.

To change the system mode to access point mode or back to router mode:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > Router / AP / Bridge Mode**.

The Router / AP / Bridge Mode page displays.

5. Specify the system mode by doing one of the following:

- **Router mode.** Select the **Router Mode** radio button to let the access point function in router mode.

The page adjusts to provide information. To change the WiFi settings before you change the system mode, click the **Wireless Setup** button. For more information, see [Set up or change an open or secure WiFi network](#) on page 59.

- **AP mode.** Select the **AP Mode** radio button to let the access point function in access point mode.

The page adjusts to provide information and the following options:

- To change the device name before you change the system mode, click the **Edit** button.
- To change the WiFi settings before you change the system mode, click the **Wireless Setup** button. For more information, see [Set up or change an open or secure WiFi network](#) on page 59.
- 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 access point 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 recommend)** button, and in the fields that display below the **Learn more** button, change the IP address information.

Note: For information about bridge mode, see [Set up access point as a WiFi Bridge to another device](#) on page 202.

6. Click the **Apply** button.

Your settings are saved and the access point is reconfigured in the new system mode.

Disable LED blinking or turn off LEDs

The LEDs on the top panel of the access point indicate activities and behavior. By default, the Internet LED, LAN LED, and WiFi LED blink when the access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 [Top panel with LEDs](#) on page 11.

5. To disable blinking, select the **Disable blinking on Internet LED, LAN LED, Wireless LED when data traffic is detected** radio button.
6. To turn off all LEDs except the Power LED, select the **Turn off all LEDs except Power LED** radio button.
7. Click the **Apply** button.
Your settings are saved.

9

Dynamic DNS [Router Mode]

If the access point is in router mode, with Dynamic DNS (DDNS), you can use the Internet and a domain name to access a storage device that is attached to the access point when you are not in your office or home. If you know the IP address of the access point (and the IP address did not change), you can also access the storage device by using the IP address. If you use OpenVPN software to set up VPN tunnels, the access point requires an account with a Dynamic DNS service.

This chapter contains the following sections:

- [About Dynamic DNS \[router mode\]](#)
- [Set up a new Dynamic DNS account \[router mode\]](#)
- [Use an existing Dynamic DNS account \[router mode\]](#)
- [Change the Dynamic DNS account settings \[router mode\]](#)

For information about using DDNS if you set up the access point as a VPN server with OpenView, see [About setting up an OpenVPN connection \[router mode\]](#) on page 184.

Note: The information in this chapter does not apply if the access point is in access point mode.

About Dynamic DNS [router mode]

Internet service providers (ISPs) assign IP addresses to identify each Internet account. Most ISPs use dynamically assigned IP addresses. This means that the IP address can change at any time. You can use the IP address to access your network remotely, but most people do not know what their IP address is or when this address changes.

To make it easier to connect to a storage device that is connected to your access point or to set up a VPN tunnel to the access point, you can get a free account with a Dynamic DNS (DDNS) service that lets you use a domain name to access your office or home network. To use this account, you must set up the access point to use DDNS. Then the access point notifies the DDNS service provider whenever its IP address changes. When you access your DDNS account, the service finds the current IP address of your home network and automatically connects you.

The access point must be in router mode. However (and this is very unusual), if your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the DDNS service does not work because private addresses are not routed on the Internet.

Set up a new Dynamic DNS account [router mode]

NETGEAR offers you the opportunity to set up and register for a free Dynamic DNS account.

To set up Dynamic DNS and register for a free NETGEAR account:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **<http://www.routerlogin.net>** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

The Dynamic DNS page displays.

5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select **NETGEAR**.
7. Select the **No** radio button.
8. In the **Host Name** field, enter the name that you want to use for your URL.
The host name is also called the domain name. Your free URL includes the host name that you specify and ends with mynetgear.com. For example, enter *MyName.mynetgear.com*.
9. In the **Email** field, enter the email address that you want to use for your account.
10. In the **Password** field, enter the password that you want to use for your account.
The password must contain between 6 and 32 characters.
11. Click the **Register** button.
12. Follow the onscreen instructions to register for your NETGEAR Dynamic DNS service.

Use an existing Dynamic DNS account [router mode]

If you already created a Dynamic DNS (DDNS) account with NETGEAR, No-IP, or Dyn, you can set up the access point to use your account.

To set up DDNS if you already created an account:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select your provider.
7. Select the **Yes** radio button.
8. In the **Host Name** field, enter the host name (sometimes called the domain name) for your account.
9. Depending on the type of account, specify your user name or email address:
 - For a No-IP or Dyn account, in the **User Name** field, enter the user name for your account.
 - For a NETGEAR account, in the **Email** field, enter the email address for your account.
10. In the **Password** field, enter the password for your DDNS account.
11. Click the **Apply** button.
Your settings are saved.
12. To verify that your DDNS service is enabled in the access point, click the **Show Status** button.
A pop-window displays the DDNS status.

Change the Dynamic DNS account settings [router mode]

You can change the settings for your Dynamic DNS (DDNS) account.

To your DDNS account settings:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

The Dynamic DNS page displays.

5. Change your DDNS account settings as necessary.

6. Click the **Apply** button.

Your settings are saved.

10

VPN Client [Router Mode]

If the access point is in router mode, you can use it as a VPN client (as opposed to a VPN server) to let devices on the access point's network securely access an *external* network using virtual private networking (VPN). This chapter describes how to set up the access point as a VPN client and use VPN access.

Note: For you to be able to use the access point as a VPN client, you must obtain a third-party license for VPN server access. The local browser UI includes a link to a third-party VPN service (PureVPN) so that you can obtain a license.

For information about using the router as a VPN server, see [VPN Server and Service with OpenVPN \[Router Mode\]](#) on page 177.

This chapter includes the following sections:

- [About setting up the access point as a VPN client \[router mode\]](#)
- [Enable the VPN client in the access point and connect to a VPN server \[router mode\]](#)
- [Disconnect the access point from the VPN server \[router mode\]](#)

About setting up the access point as a VPN client [router mode]

In addition to using a virtual private network (VPN) to securely access your own network over the Internet when you are not home (see [VPN Server and Service with OpenVPN \[Router Mode\]](#) on page 177), you can also set up the access point as a VPN *client* to let devices on the access point's network securely access an *external* network, while protecting your own network identity and preventing a distributed denial-of-service (DDoS) attack. An external network can be a business network behind a firewall or an Internet service that might not be accessible from your geographical location without using a VPN server in another country.

Similar to using the access point as a VPN server, this type of VPN access is also called a client-to-gateway tunnel, but in this situation the access point functions as the *client* and an external gateway (that is not on the access point's network) functions as the VPN server.

A VPN creates a secure, encrypted tunnel over the Internet between your access point and a VPN server. The VPN client on the access point redirects the Internet connection so that the access point first connects to a VPN server (which could be in another country) and then to the Internet. All devices that are connected to your access point are assigned new IP addresses from the VPN server, which hides the actual location of your access point and the devices that are connected to it. After the VPN connection is established, you use your web browser and any apps as you would normally do.

Note: The access point comes with a predefined commercial VPN service provider called PureVPN. To use the VPN client feature in the access point, you need a license from this provider. However, if you want to use a free VPN service on a device on your access point's network, you can download the service's VPN client on your device and establish a connection to the free VPN server. Such a connection serves only that individual device, not all devices on the access point's network.

To use the VPN client feature, the access point must be in router mode and you must log in to the access point, enable the access point's VPN client, and establish a connection to an external VPN server (see [Enable the VPN client in the access point and connect to a VPN server \[router mode\]](#) on page 174).

Enable the VPN client in the access point and connect to a VPN server [router mode]

The access point comes with a commercial VPN service provider (HideMyAss) predefined. To use the VPN client feature in the access point, you need a license from the HideMyAss server provider.

You must enable the VPN client in the router before you can select one of two predefined VPN services and establish a connection to the VPN server.

To enable the VPN client in the router and connect to a VPN server:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
4. Select **BASIC > VPN Client**.
The VPN Client page displays.
5. Select the **Enable VPN Client** check box.
The VPN settings on the page becomes available.
6. If you do not have a VPN license or a predefined VPN service, do the following:
 - a. From the **VPN Server** menu, select a VPN provider.
 - b. Click the **Buy a License** button.
A provider web page opens that lets you choose a price plan and purchase a license.

- c. Follow the instructions on the web page.
- d. When you obtain a license, save your user name and password for the VPN service.

For more information about VPN service, click the **Help Center** button.

7. From the **VPN Server** menu, select a VPN provider.
8. From the **VPN Protocol** menu, select **UDP** or **TCP**.
UDP functions without error correction in transmission, so it is faster, but less reliable.
TCP functions with error correction in transmission, so it is more reliable, but slower.
9. From the **Country** menu, select the country in which you want to use the VPN server.
10. From the **City** menu, select the city in which you want to use the VPN server, or leave the Any City selection, which is the default.
11. In the **Username** field, enter the user name for authentication with the VPN server.
12. In the **Password** field, enter the password for authentication with the VPN server.
13. Click the **Connect** button.

Your settings are saved and the access point attempts to connect to the VPN server.

When the access point is connected to the VPN server, the **Connect** button changes into the **Disconnect** button, allowing you to terminate the VPN connection.

The Status field at the top of the page displays the status of the VPN connection, which you can be one of the following:

- **Connecting.** The access point is attempting to connect to the VPN server.
- **Connected.** The access point is connected to the VPN server.
- **Disconnected.** The access point is connected to the VPN server.
- **Error.** The connection to the VPN server failed.

If you experience difficulty in establishing a VPN connection, click the **Show Logs** link and see if any log messages provide helpful information. For more information about the logs, see [Logs](#) on page 144.

Disconnect the access point from the VPN server [router mode]

To disconnect the router from the VPN server and terminate the VPN connection:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

4. Select **BASIC > VPN Client**.

The VPN Client page displays.

5. Click the **Disconnect** button.

The VPN connection is terminated.

When the access point is disconnected from the VPN server, the **Disconnect** button changes into the **Connect** button, allowing you to reestablish the VPN connection.

11

VPN Server and Service with OpenVPN [Router Mode]

If the access point is in router mode, you can use OpenVPN software to set up VPN connections and remotely access an office or site at which the access point is installed. In such a situation, the access point functions as a VPN server.

This chapter describes how to set up OpenVPN on the access point and on a computer or mobile device and how to initiate a VPN connection to the access point, using OpenVPN.

The chapter includes the following sections:

- [Enable and configure OpenVPN and VPN client access on the access point \[router mode\]](#)
- [OpenVPN client utility and VPN configuration files \[router mode\]](#)
- [About setting up an OpenVPN connection \[router mode\]](#)
- [About VPN access to your network or Internet service at your office or home \[router mode\]](#)
- [Use a VPN tunnel to remotely access your Internet service \[router mode\]](#)

Note: The information in this chapter does not apply if the access point is in access point mode.

Enable and configure OpenVPN and VPN client access on the access point [router mode]

If the access point is in router mode, you can configure OpenVPN and VPN client access on the access point.

You must enable OpenVPN and specify the OpenVPN service settings on the access point before remote clients can access the access point with a VPN connection using OpenVPN software.

Note: Make sure that remote clients install their VPN configuration files after you configure OpenVPN on the access point. If you make changes to the OpenVPN configuration on the access point, the VPN configuration files that the remote clients use might change, requiring the remote clients to download and install the new VPN configuration files.

To enable and configure OpenVPN on the access point:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
The VPN Service page displays.
5. Select the **Enable VPN Service** check box.

We recommend that you use the default TUN mode and TAP mode settings. However, if you know that you need other settings, you can change the TUN mode and TAP mode settings by doing the following:

- To change the TUN mode service type, select the **UDP** or **TCP** radio button
- To change the TUN mode service port, type the port number that you want to use in the field.
The default port number is 12973.
- To change the TAP mode service type, select the **UDP** or **TCP** radio button.
- To change the TAP mode service port, type the port number that you want to use in the field.
The default port number is 12974.

6. Specify how VPN client connections can be used on the access point by selecting one of the following radio buttons:

- **Auto.** The access point automatically uses the VPN service only for necessary access, that is, the access point allows access to sites and services that would not be accessible without a VPN connection. This is the default selection. However, if some sites or services are not accessible to the VPN client, or if a user cannot access some sites on the Internet, select another radio button.
- **All sites on the Internet & Home Network.** The VPN client can access the Internet and all sites and services on the access point network, that is, behind the access point firewall. Accessing the Internet remotely through a VPN connection might be slower than accessing the Internet directly.
- **Home Network only.** The VPN client can access all sites and services on the access point network, that is, behind the access point firewall, but cannot access the Internet.

7. Click the **Apply** button.

Your settings are saved. OpenVPN service is enabled on the access point.

Users must install and set up OpenVPN software on their computer or mobile device before they can establish a VPN connection to the access point.

OpenVPN client utility and VPN configuration files [router mode]

To establish a VPN connection to the access point using OpenVPN software, a remote client must install both OpenVPN client software and the access point VPN configuration

files on their computer or mobile device. A remote client can install this software on a Windows computer, Mac computer, iOS device, and Android device.

Install OpenVPN on a Windows-based computer [router mode]

To download and install the OpenVPN client utility and the access point's VPN configuration files on a Windows-based computer:

1. Visit openvpn.net/index.php/download/community-downloads.html, download the OpenVPN client utility for a Windows-based computer, and install it on the Windows-based computer.

You might need administrative privileges to install the OpenVPN client utility.

2. Launch a web browser from a computer or mobile device that is connected to the access point network.

3. Enter **<http://www.routerlogin.net>** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

4. Enter the access point 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.

5. Select **ADVANCED > Advanced Setup > VPN Service**.

The VPN Service page displays.

6. Make sure that the **Enable VPN Service** check box is selected.

For more information, see [Enable and configure OpenVPN and VPN client access on the access point \[router mode\]](#) on page 178.

7. In the OpenVPN configuration package download section, click the **For Windows** button, and download the access point's VPN configuration files.

8. Unzip the configuration files and copy them to the folder in which the OpenVPN client utility is installed.

9. Modify the VPN interface name to NETGEAR-VPN by doing the following:
 - a. In Windows, open Network Connection or Network and Sharing Center. The network connection information displays.
 - b. In the local area connection list, find the local area connection with the device name TAP-Windows Adapter.
 - c. Change the name of the associated local area connection to **NETGEAR-VPN**. Make sure that you change the name of the local area connection, *not* the device name (TAP-Windows Adapter).

If you do not change the local area connection name, the VPN connection to the access point will fail.

The computer is now ready for you to set up a VPN connection to the access point.

For more information about using OpenVPN on a Windows-based computer, visit openvpn.net/community-resources/how-to/#quick.

Install OpenVPN on a Mac [router mode]

To download and install the OpenVPN client utility and the access point's VPN configuration files on a Mac:

1. Visit tunnelblick.net, download the OpenVPN client utility for a Mac, and install it on the Mac.

You might need administrative privileges to install the OpenVPN client utility.

2. Launch a web browser from a computer or mobile device that is connected to the access point network.
3. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

4. Enter the access point 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.

5. Select **ADVANCED > Advanced Setup > VPN Service**.

The VPN Service page displays.

6. Make sure that the **Enable VPN Service** check box is selected.

For more information, see [Enable and configure OpenVPN and VPN client access on the access point \[router mode\]](#) on page 178.

7. In the OpenVPN configuration package download section, click the **For Mac OS X** button, and download the access point's VPN configuration files.

8. Unzip the configuration files and copy them to the folder in which the OpenVPN client utility is installed.

The Mac is now ready for you to set up a VPN connection to the access point.

For more information about using OpenVPN on a Mac, visit openvpn.net/vpn-server-resources/installation-guide-for-openvpn-connect-client-on-macos/.

Install OpenVPN on an iOS device [router mode]

To download and install the OpenVPN client utility and the access point's VPN configuration files on an iOS device:

1. On your iOS device, visit the Apple app store and download and install the OpenVPN Connect app.
2. Launch a web browser from the iOS device or a computer, either of which must be connected to the access point network.
3. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

4. Enter the access point user name and local device password.

The user name is **admin**. The local device password is the one that you specified. The user name and local device password are case-sensitive.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VPN Service**.

The VPN Service page displays.

6. Make sure that the **Enable VPN Service** check box is selected.

For more information, see [Enable and configure OpenVPN and VPN client access on the access point \[router mode\]](#) on page 178.

7. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the access point's VPN configuration files to your iOS device or computer.

If you download the configuration files to a computer, unzip the configuration files that you downloaded and send the files to your iOS device.

The configuration files include the .ovpn file.

8. On your iOS device, open the .ovpn file, select the OpenVPN Connect app, and import the .ovpn file.

Your iOS device is now ready to for you to set up a VPN connection to the access point.

For more information about using OpenVPN on an iOS device, visit vpngate.net/en/howto_openvpn.aspx#ios.

Install OpenVPN on an Android device [router mode]

To download and install the OpenVPN client utility and the access point's VPN configuration files on an Android device:

1. On your Android device, visit the Google Play Store and download and install the OpenVPN Connect app.
2. Launch a web browser from the Android device or a computer, either of which must be connected to the access point network.
3. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

4. Enter the access point 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.

5. Select **ADVANCED > Advanced Setup > VPN Service**.

The VPN Service page displays.

6. Make sure that the **Enable VPN Service** check box is selected.

For more information, see [Enable and configure OpenVPN and VPN client access on the access point \[router mode\]](#) on page 178.

7. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the access point's VPN configuration files to your Android device or computer.

If you download the configuration files to a computer, unzip the configuration files that you downloaded and send the files to your Android device.

The configuration files include the `.ovpn` file.

8. On your Android device, start the OpenVPN Connect app, and search for and import the `.ovpn` file.

Your Android device is now ready for you to set up a VPN connection to the access point.

For more information about using OpenVPN on an Android device, visit vpngate.net/en/howto_openvpn.aspx#android.

About setting up an OpenVPN connection [router mode]

The type of virtual private network (VPN) access in which remote users access a protected network is called a client-to-gateway tunnel. The computer is the client, and the access point is the gateway. To enable users to access the access point over a VPN connection, the access point must be in router mode, and you must enable and configure OpenVPN service on the access point. Remote users must install and run OpenVPN client software on their computer or mobile device.

OpenVPN requires a static IP address or DDNS service on the access point to enable a remote client such as a computer or mobile device to connect with the access point. (If the access point uses a static WAN IP address that never changes, OpenVPN can use that IP address to connect to the network over a VPN connection.)

If the access point does not use a static WAN IP address, you can use a DDNS service for the access point and register for an account with a host name (also referred to as a domain name). A remote client such as a computer or mobile device can use that host name to connect with the access point and access the network over a VPN connection. For more information, see [About Dynamic DNS \[router mode\]](#) on page 168.

About VPN access to your network or Internet service at your office or home [router mode]

When you are away from your office or home and you access the Internet, you usually use a local Internet service provider. For example, at a coffee shop you might be given a code that lets you use the coffee shop's Internet service account to surf the web.

The access point lets you use a VPN connection to access your own Internet service when you are away from your office or home. You might want to do this if you travel to a geographic location that does not support all the Internet services that you use at your office or home. For example, your Netflix account might work at home but not in a different country.

For information about the types of VPN client connections that the access point supports, see [Enable and configure OpenVPN and VPN client access on the access point \[router mode\]](#) on page 178. In addition to access to your office or home network, you can either allow or block VPN client Internet access through your office or home network.

For the VPN tunnel to work, the LAN where your VPN client computer is connected must use a different LAN IP address scheme from that of the LAN of the access point at your office or home. If both networks use the same LAN IP address scheme, when the VPN tunnel is established, you cannot access the access point network at your office or home with the OpenVPN software.

The default LAN IP address scheme for the access point is 192.168.1.x. The most common IP schemes are 192.x.x.x, 172.x.x.x, and 10.x.x.x. If you experience a conflict while you are not at your office or home, consider asking someone else at your office or home to change the access point IP address scheme for your office or home network (see [LAN IP address settings \[router mode\]](#) on page 109).

Use a VPN tunnel to remotely access your Internet service [router mode]

Before you leave the location with your Internet service (for example, your office or home), make sure that you do the following:

- Set up VPN client access to your office or home network for the type of computer or mobile device that you intend to use as a VPN client and allow VPN client *Internet* access through your office or home network (see [Enable and configure OpenVPN and VPN client access on the access point \[router mode\]](#) on page 178).
- Download and install OpenVPN client software on the computer or mobile device that you intend to use as a VPN client and download and install the access point's VPN configuration files (see [OpenVPN client utility and VPN configuration files \[router mode\]](#) on page 179).

To remotely access your Internet service:

1. On your computer, launch the OpenVPN application.
2. Right-click the icon and select **Connect**.
Depending on the operating system on your computer or mobile client, you might have to do something else to make a VPN connection.
3. Enter the OpenVPN password for VPN access.
This is the password that you set up when you installed and configured OpenVPN client software on your computer or mobile device
4. When the VPN connection is established, launch your web browser.

12

Advanced WiFi and Radio Features

This chapter describes how you can manage the advanced WiFi and radio features of the access point. For information about the basic WiFi and radio settings, see [Basic WiFi and Radio Features](#) on page 58.

Tip: If you want to change the settings of the access point's WiFi network, 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 access point](#)
- [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 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 access point as a WiFi Bridge to another device](#)
- [Change the CTS/RTS threshold and preamble mode for a radio](#)

Change the region of operation

You can change the region of operation, which is region in which you operate the access point. 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 access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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. From the **Region** menu, select the region in which the access point must operate.
6. Click the **Apply** button.
Your settings are saved. The access point 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 each radio band independently. 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 access point sends these small signals directly to individual devices in your network. Because multiple devices can be served in the same transmission window, the access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **<http://www.routerlogin.net>** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 **Enable 11AX** check box.

Selecting this check box enables 11AX for both radio bands and clearing this check box disables 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 2.4GHz** check box.

Selecting this check box enables OFDMA in the 2.4 GHz radio band and clearing this check box disables OFDMA in the 2.4 GHz radio band.

7. 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 and clearing this check box disables OFDMA in the 5 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 access point

Smart connect automatically selects the fastest WiFi band for a WiFi client device that is connected to the access point. This feature is enabled by default and applies on all WiFi networks on the access point.

When smart connect is enabled, the 2.4 GHz and 5 GHz bands for a WiFi network use the same WiFi network name (SSID) and network key (password). That means that when you connect to the access point using that WiFi network 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 **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 enabled and the check box is selected.
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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 **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 disables 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. For the 5 GHz radio, the default channel depends on the region. When you select a particular channel, the channel selection becomes static.

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 access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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. 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. For the 5 GHz radio, the default channel depends on the region. When you select a particular channel, the channel selection becomes static.
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 access point, that is, the WiFi throughput modes on the access point support 802.11ax, 802.11ac, 802.11a, 802.11n, 802.11g and 802.11b clients. 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.

To change the WiFi throughput mode for a radio:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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. 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 802.1ax, 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 802.1ax, 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 600 Mbps (11ax, HT40, 1024-QAM).** Performance mode. This mode allows 802.1ax, 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11ax devices to function at up to 600 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 transmission output power for a radio

By default, the transmission output power of the access point is set at the maximum. If two or more access points 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 the smart connect feature is enabled (which it is by default), 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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 (which it is by default), 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 access point is connected to the Internet and synchronizes its internal clock with a time server on the Internet. For more information about whether the access point synchronizes its clock, see [Time and Network Time Protocol server](#) on page 142.

IMPORTANT: If the smart connect feature is enabled (which it is by default), 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 (which it is by default), 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 to turn off the WiFi signal display.

7. Use the menus, radio buttons, and check boxes to set up a period during which you want to turn off the WiFi signal for the selected radio and specify whether the schedule is recurrent.

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. 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.

- To enable a schedule immediately, do the following above the table,
 - In the table, select the radio button for the schedule.
If the table includes a single schedule only, the radio button for the schedule is already selected.
The radio button for the schedule also lets you select the schedule if you want to change (edit) or delete it.
 - Select the **Turn off wireless signal by schedule** check box.
- 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

Multuser 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:

- Launch a web browser from a computer or mobile device that is connected to the access point network.
- Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
- Enter the access point 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.

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 **Enable MU-MIMO** check box.

Selecting this check box enables MU-MIMO and clearing this check box disables MU-MIMO.

By default, MU-MIMO is enabled and the **Enable MU-MIMO** 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 explicit beamforming

Explicit beamforming (which is the same as Tx beamforming) lets the access point actively track WiFi clients and direct power to the access point antenna closest to the client.

With this technique, the access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 **Enable Tx Beamforming** check box.

Selecting this check box enables explicit beamforming and clearing this check box disables 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.

6. 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 access point 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. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **<http://www.routerlogin.net>** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 **Disable PMF** check box.

Selecting this check box disables PMF and clearing this check box enables PMF. By default, PMF is enabled 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.

Set up access point as a WiFi Bridge to another device

You can use the access point as a WiFi bridge and connect multiple devices with WiFi, for example, at the faster 802.11ax speed. The access point that functions as the bridge must connect over WiFi to another WAX204 access point, WiFi router, or access point (AP) that provides Internet access. In this way, the access point that functions as the bridge receives Internet access over a *WiFi bridge* from the device that is connected to the Internet.

You can also connect the access point in router mode to the modem and use the other WAX204 access point, WiFi router or AP as a WiFi bridge (assuming that the WiFi router or AP is capable of functioning as a WiFi bridge).

Setting up a WiFi bridge with two WAX204 access points offers the following benefits:

- Take advantage of high WiFi speeds (802.11ax) for WiFi devices connected to either side of the WiFi bridge.
- Connect multiple devices such as a NAS, Smart TV, NeoTV, and Blu-ray player using a high-speed (802.11ax) WiFi link.

Note: The Internet (WAN) and LAN ports of the WAX204 access point support gigabit speed. That means that speeds over 1 GB can be achieved only between the access point and its connected devices, but not for traffic to and from the Internet.

As an example of a WiFi bridge, you could install the first access point in the office in which your Internet connection is located. Then set up the second access point as a WiFi bridge and place it 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 access point that functions as a WiFi bridge to your Smart TV, NeoTV, or Blu-ray player, and use its 802.11ax WiFi connection to the first access point.

The access point that is connected to the modem does not require any special setup because the access point that functions as a WiFi bridge connects to an existing SSID as a WiFi client, just like any other WiFi clients.

To set up the access point as a WiFi bridge to a device that provides the Internet connection:

1. Make a note of the WiFi settings of the other access point, WiFi router, or AP that is connected to the modem.

You must know the SSID, WiFi security mode, WiFi password, and operating frequency (either 2.4 GHz or 5 GHz).

2. Launch a web browser from a computer or mobile device that is connected to the access point network.

3. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

4. Enter the access point 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.

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 of the WAX204 access point, WiFi router, or AP that is connected to the modem (that is, the *other* device):
 - a. From the **Choose a Wireless Network** menu, select the WiFi band that the other device is using.
 - b. In the **Name (SSID)** field, type the WiFi network name (SSID) that the other device is using.
 - c. In the Security Options section, select the radio button for the WiFi security that the other device is using.
 - d. In the **Password (Network Key)** field, type the passphrase (WiFi password) that the other device is using for the SSID to which you want to connect the access point.
9. Click the **Apply** button.
Your settings are saved. The pop-up window closes.
10. To change the device name of the access point, enter a new name in the **Device Name** field.
By default, the device name is the access point model (WAX204). If you use two WAX204 access points and you want to distinguish the names, you could, for example, change the name to *WiFi bridge* or something similar.
11. To let the access point that functions as the WiFi bridge get an IP address and DNS addresses dynamically from the other WAX204 access point, WiFi router, or AP that is connected to the modem, 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 WAX204 access point, WiFi router, or AP that is connected to the modem. To specify a static IP address for the access point 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 access point restarts with a new IP address.

13. To reconnect, close your browser, relaunch it, and log in to the access point by entering **http://www.routerlogin.net**.

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 the smart connect feature is enabled (which it is by default), 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. Launch a web browser from a computer or mobile device that is connected to the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 (which it is by default), 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. From the **Preamble Mode** menu, select **Automatic**, **Long Preamble**, or **Short Preamble**.

The default setting is Automatic.

CAUTION: Incorrect settings might disable the WiFi function for the selected radio unexpectedly.

8. Click the **Apply** button.

Your settings are saved.

13

Port Forwarding and Port Triggering [Router Mode]

As an advanced function of the access point 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: The information in this chapter does not apply if the access point is in access point mode.

This chapter includes the following sections:

- [Port forwarding to a local server for services and applications \[router mode\]](#)
- [Port triggering for services and applications \[router mode\]](#)

Port forwarding to a local server for services and applications [router mode]

If the access point 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 access point 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 access point forwards all other incoming protocols (see [Set up a default DMZ server \[router mode\]](#) on page 77).

Note: The information in this section and subsections does not apply if the access point is in access point mode.

Forward incoming traffic for a default service or application [router mode]

If the access point 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 115).

3. Launch a web browser from a computer or mobile device that is connected to the access point network.

4. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

5. Enter the access point 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.
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 209).
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 access point 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 the access point network.
3. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not

know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

4. Enter the access point 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.
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 access point 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 the access point network.

2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 209.

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 access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point 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 access point.
 - **Destination port number.** 80, which is the standard port number for a web server process.
2. The access point receives the message and finds your port forwarding rule for incoming port 80 traffic.
3. The access point 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 access point.
5. Your access point 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 access point 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 access point always assigns your web server an IP address of 192.168.1.33.
2. On the Port Forwarding / Port Triggering page, configure the access point 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 access point.

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 access point 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 access point monitors traffic to the Internet from an outbound “trigger” port that you specify. For outbound traffic from that port, the access point saves the IP address of the computer that sent the traffic. The access point 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 105).

Note: The information in this section and subsections does not apply if the access point is in access point mode.

Add a port triggering rule [router mode]

The access point 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 access point must be in router mode.

To add a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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. Click the **Apply** button.

Your settings are saved and the rule is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Change a port triggering rule [router mode]

If the access point is in router mode, you can change an existing port triggering rule.

To change a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 **Edit Service** button.
The Port Triggering - Services page displays.
8. Change the settings.
For information about the settings, see [Add a port triggering rule \[router mode\]](#) on page 214.
9. Click the **Apply** button.
Your settings are saved. The changed rule displays in the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Remove a port triggering rule [router mode]

If the access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point detects no activity. (The access point must be in router mode.) A time-out period is required because the access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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.

Disable port triggering [router mode]

If the access point is in router mode, port triggering is enabled by default. You can disable port triggering temporarily without removing any port triggering rules.

To disable port triggering:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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. Select the **Disable Port Triggering** check box.
If this check box is selected, the access point does not apply port triggering rules even if you specified them.
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 access point is in router mode), you can tell the access point 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 access point, "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 access point.
3. Your access point creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your access point 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 access point creates another session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your access point using the NAT-assigned source port (for example, port 33333) as the destination port and also sends an "identify" message to your access point with destination port 113.
6. When your access point 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 access point restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your access point 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 access point 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 access point eventually senses a period of inactivity in the communications. The access point then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

14

Diagnosics and Troubleshooting

This chapter provides information to help you diagnose and solve problems you might experience with the access point. 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:

- [Reboot the access point from the local browser UI](#)
- [Quick tips for troubleshooting](#)
- [Standard LED behavior when the access point is powered on](#)
- [Troubleshoot with the LEDs](#)
- [You cannot log in to the access point](#)
- [You cannot access the Internet \[router mode\]](#)
- [Troubleshoot Internet browsing](#)
- [Troubleshoot the WiFi connectivity](#)
- [Changes are not saved](#)
- [Troubleshoot your network using the ping utility of your computer or mobile device](#)

Reboot the access point from the local browser UI

You or NETGEAR technical support can reboot the access point from its local browser UI, either locally or remotely, for example, if the access point seems to be unstable or is not operating normally.

To reboot the access point from the local browser UI:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.
If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
A login window displays.
If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.
3. Enter the access point 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.
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 access point restarts.

Quick tips for troubleshooting

Many common problems can be resolved by following our tips for troubleshooting.

Restart your access point network if in router mode

If the access point is in router mode and you must restart your network, follow this sequence:

1. Turn off and unplug the modem.
2. Turn off the access point.
3. Plug in the modem and turn it on. Wait two minutes.
4. Turn on the access point and wait two minutes.

Restart your access point when in access point mode

If the access point is in access point mode and you must restart it, follow this sequence:

1. Turn off the access point.
2. Turn on the access point and wait two minutes.

Check the Ethernet cable connections

Make sure that the Ethernet cables are connected correctly and securely plugged in:

- If the access point is in router mode (the default system mode), make sure that you connect the yellow Internet port on the access point through an Ethernet cable to a LAN port on your modem.
- If the access point is in access point mode, make sure that you connect the yellow Internet port on the access point through an Ethernet cable to a LAN port on the existing router in your network or to a switch or hub that is located between the access point and the router.
- For any computer or device that you connect directly through an Ethernet cable to the access point, make sure that you connect the Ethernet cable from the computer or device to one of the four LANs port on the access point.

Check the WiFi settings of your computer or mobile device

If you connect over WiFi to the access point, make sure that the WiFi settings on your computer or mobile device and the access point match exactly. If you did not change

the SSID, the access point's default SSID is "NETGEARXXXXXX", where XXXXXX represents the last six characters of the access point's MAC address, as printed on the access point label. If you did not change the passphrase (also referred to as network key or WiFi password), the unique default passphrase is also printed on the access point label. The default security is WPA2-Personal [AES].

Note: If you set up an access control list on the access point, you must add each computer or mobile device to the access control list (see [Enable and manage network access control](#) on page 81).

The access point 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 access point's MAC address, and the default password is sharedsecret.
- **Wireless 3.** The default SSID is NETGEARXXXXXX-3, in which XXXXXX represents the last six characters of the access point's MAC address, and the default password is sharedsecret.

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 access point are correct:

- **Router mode.** If the access point is in router mode (the default system mode), make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the access point. 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.
- **Access point mode.** If the access point is in access point mode, the LAN subnet to which your computer or device connects depends on the type of connection to the access point:
 - **Directly connected.** If you are directly connected over WiFi or an Ethernet cable to the access point network, make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the access point. 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 access point, 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 access point 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 it can obtain an IP address automatically using DHCP.

Standard LED behavior when the access point is powered on

After you turn on power to the access point, verify that the following sequence of events occurs:

1. When power is first applied, verify that the Power LED is lit.
2. After about two minutes, verify the following:
 - The Power LED is solid green.
 - The Internet LED is solid or blinking green.
 - The WiFi LED is solid or blinking green.
 - If a powered-up LAN device is connected to one of the LAN ports of the access point, 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 top panel of the access point for troubleshooting (see [Troubleshoot with the LEDs](#) on page 225)

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 access point 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 access point, the Power LED lights solid red for about five seconds and then turns solid amber. After about 90 seconds, the Power LED lights solid green.

When the access point is upgrading firmware, the Power LED blinks amber temporarily and finally lights solid green.

If the LED stays solid red or blinking amber five minutes after startup, or lights solid red or blinking amber at any other time (not including a firmware upgrade), this indicates a problem with the access point. In that situation, do the following:

- Restart the access point to see if it recovers. If the problem occurs again, try one more time.
- If the access point does not recover, press and hold the **Reset** button on the back to return the access point to its factory default settings. For more information, see [Use the dual-function Reset button to return to factory defaults](#) on page 138. 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/.

Internet LED is solid amber or off [router mode]

If the access point is in its default router mode and the Internet LEDs is solid amber, the access point attempted to get an Internet connection but failed. Check the following:

- If the type of WAN connection of the modem is PPPoE, L2TP, or PPTP, or the connection 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 39, [Specify a PPTP or L2TP Internet connection that uses a login \[router mode\]](#) on page 41, or [Specify a dynamic or fixed WAN IP address Internet connection without a login \[router mode\]](#) on page 37.
- Make sure that you completed the initial log-in process. For more information, see [Connect the access point to a router and log in for the first time](#) on page 22 or, if you are connected to the local browser UI, see [Use the Setup Wizard](#) on page 36.
- Make sure that your Internet service provider (ISP) is not experiencing an Internet outage.

If the access point is in its default router mode and the Internet LEDs is off, check the following:

- Make sure that the Ethernet cable connection is secure at the yellow Internet port (*not* a LAN port) of the access point and at an Ethernet port on the modem.
- Make sure that power is turned on to the connected modem.
When you connect the access point's Internet port to an modem, use the cable that was supplied with the modem. This cable can be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Internet LED is solid amber or off [access point mode]

If the access point is in access point mode and the Internet LED is solid amber, the access point attempted to get an Internet connection but failed. Check the following:

- If the network router to which the access point 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 access point 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.

If the access point is in access point mode and the Internet LEDs is off, check the following:

- Make sure that the Ethernet cable connection is secure at the yellow Internet port (*not* a LAN port) of the access point and at an Ethernet port on the existing network router (or switch or hub that is connected to the router), and that you completed the initial log-in process. For more information, see [Connect the access point to a router and log in for the first time](#) on page 22. In access point mode, do not connect the cable directly to a modem.
- Make sure that power is turned on to the connected network router and that the network router is connected to the Internet.
When you connect the access point's Internet port to the network router, use a standard straight-through Ethernet cable or an Ethernet crossover cable.

WiFi LED is Off

If the WiFi LED remains off, check to see if both radios on the access point are disabled (see [Enable or disable a WiFi radio](#) on page 70). By default, both radios are enabled and the WiFi LED lights solid green or blinks green.

Also, check to see if a WiFi schedule turned off both radios (see [Add a WiFi schedule for a radio](#) on page 197).

The LAN LED is off while a device is connected

If the 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 access point 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 access point

If you are unable to log in to the access point's local browser UI from a computer or mobile device, troubleshooting depends on whether the access point is in the default router mode or access point mode.

You cannot log in to the access point [router mode]

If the access point is in router mode and you are unable to log in to its local browser UI from a computer or mobile device on the access point network, check the following:

- Make sure that the yellow Internet port on the access point is connected to the Internet through your modem. The 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 access point.
- Check the Ethernet or WiFi connection between your computer or mobile device and the access point:
 - **Connect over Ethernet directly to the access point.** If you connect the LAN port on your computer directly to the access point, check the Ethernet cable between the computer and the LAN port on the access point. (Do not connect your computer to the yellow Internet port on the access point.)
 - **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 access point. If you did not change the SSID, the access point's default SSID is "NETGEARXXXXXX", where XXXXXX represents the last six characters of the access point's MAC address, as printed on the access point label. If you did not change the passphrase (also referred to as network key or WiFi password), the unique default passphrase is also printed on the access point label.

- 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 access point, you customized the local device password. (By default, the local device password is **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 **http://www.routerlogin.net** (which, in router mode, is the same as 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 access point. 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 it 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 access point 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 access point [access point mode]

If the access point is in access point mode and you are unable to log in to its local browser UI from a computer or mobile device, check the following:

- Make sure that the yellow Internet port on the access point is connected to the Internet through an existing router in your network (or through a switch or hub that is connected to the router). The 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 access point or the same network as the access point.
- Check the Ethernet or WiFi connection between your computer or mobile device and the access point:
 - **Connect over Ethernet directly to the access point.** If you connect the LAN port on your computer directly to the access point, check the Ethernet cable

between the computer and the LAN port on the access point. (Do not connect your computer to the yellow Internet port on the access point.)

- **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 access point. If you did not change the SSID, the access point's default SSID is "NETGEARXXXXXX", where XXXXXX represents the last six characters of the access point's MAC address, as printed on the access point label. If you did not change the passphrase (also referred to as network key or WiFi password), the unique default passphrase is also printed on the access point label.

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 access point, 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 access point, you customized the local device password. (By default, the local device password is **password**.) The user name and password are case-sensitive. Make sure that Caps Lock is off when you enter this information.
- If the access point's IP address was changed and you cannot log in using **<http://www.routerlogin.net>** but you do not know the current IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.
- 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 it 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 access point:
 - **Directly connected.** If you are directly connected over WiFi or an Ethernet cable to the access point network, make sure that the IP address of your computer or mobile device is on the same subnet as the LAN subnet of the access point. 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 access point, 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 access point 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 access point 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 access point is in router mode and you can log in to the access point's local browser UI but cannot get an Internet connection, check if the access point can obtain an IP address from your Internet service provider (ISP).

Check the Internet WAN IP address [router mode]

If the access point is in router mode, unless your ISP provides a fixed IP address, the access point 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 the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.

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 access point did not obtain an IP address from your ISP.

If the access point cannot obtain an IP address from the ISP, you might need to force your modem to recognize the access point by restarting your network. For more information, see [Restart your access point network if in router mode](#) on page 223.

If the access point 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 access point Internet connection \[router mode\]](#) on page 37).
- 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 access point's MAC address.
 - Configure the access point to clone your registered computer's MAC address.

If the access point 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 access point'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 access point might not be configured as the TCP/IP gateway on your computer or mobile device.
If your computer or mobile device obtains its information from the access point 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 access point.

Check or manually start the PPPoE connection [router mode]

If the access point is in router mode and your ISP uses a PPPoE connection, you can check or manually start the PPPoE connection.

To check or manually start the PPPoE connection:

1. Launch a web browser from a computer or mobile device that is connected to the access point network.
2. Enter **http://www.routerlogin.net** in the address field.

If you are not connected to the access point network but to the same network as the access point, enter the IP address that is assigned to the access point. If you do not know the IP address, see [Find the IP address of the access point when you cannot use routerlogin.net](#) on page 27.

A login window displays.

If your browser does not display the login window but displays a security message and does not let you proceed, see [Log in to the access point after initial setup](#) on page 30.

3. Enter the access point 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.
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 PPPoE connection is up and working.

If the access point is not connected, click the **Connect** button.

The access point continues to attempt to connect indefinitely.

7. If you cannot connect after several minutes, the access point might be set up with an incorrect PPPoE login name, password, or service name, or your ISP might be experiencing a provisioning problem.

Note: Unless you connect manually, the access point does not authenticate using PPPoE until data is transmitted to the network.

Troubleshoot Internet browsing

If the access point can obtain an IP address but your computer or mobile device is unable to load any web pages from the Internet, check the following:

- If the access point is in router mode and you can log in to the access point's local browser UI but you cannot get an Internet connection, check if the access point can obtain an IP address from your ISP (see [You cannot access the Internet \[router mode\]](#) on page 231).
- 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 163). 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 access point'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.
- If the access point is in router mode, the access point might not be configured as the default gateway on your computer or mobile device.
Reboot the computer or mobile device and verify that the access point 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 access point.

Troubleshoot the WiFi connectivity

If you are experiencing trouble connecting over WiFi to the access point, try to isolate the problem:

- Make sure that the WiFi settings in your WiFi device and access point match exactly. For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the access point and WiFi device must match exactly. If you did not change the SSID, the access point's default SSID is "NETGEARXXXXXX", where XXXXXX represents the last six characters of the access point's MAC address, as printed on the access point label. If you did not change the passphrase (also referred to as network key or WiFi password), the unique default passphrase is also printed on the access point label.

Note: If you set up an access control list on the access point, you must add each computer or mobile device to the access control list (see [Enable and manage network access control](#) on page 81).

The access point 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 access point's MAC address, and the default password is sharedsecret.
- **Wireless 3.** The default SSID is NETGEARXXXXXX-3, in which XXXXXX represents the last six characters of the access point's MAC address, and the default password is sharedsecret.
- Does the WiFi device that you are using find your WiFi network?
If not, check the WiFi LED on the access point. If the WiFi LED is off, both WiFi radios are probably off too. For more information about the WiFi radios, see [Enable or disable a WiFi radio](#) on page 70.
- If you disabled the access point'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 [Hide or broadcast the SSID for a WiFi network](#) on page 66.
- 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 59.

Tip: If you want to change the WiFi settings of the access point's network, 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 access point too far from your WiFi device or too close? Place your WiFi device near the access point but at least 6 feet (1.8 meters) away and see whether the signal strength improves.
- Are objects between the access point and your WiFi device blocking the WiFi signal? For more information, see [Position the access point](#) on page 245.

Changes are not saved

If the access point does not save the changes that you make through the local browser 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 local browser 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 sends an echo request packet to the designated device. 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 access point

You can ping the access point from a Windows-based computer to verify that the path to your access point is set up correctly. You can do with a WiFi or wired connection to the access point, which can be in router mode or access point mode.

To ping the access point 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 access point, 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 access point and your computer are correct. For more information, see [Check the DHCP network settings of your computer or mobile device](#) on page 224.
- Correct physical connections?
If you are using a wired connection to the access point, make sure that the Ethernet port on your computer is connected to a LAN port on the access point.
If the access point 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 access point and computer.
- Correct software?
If you are using a wired connection to the access point, 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]

If the access point is in router mode, to test the path from a Windows-based computer that is connected to the access point 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 access point on page 237](#).

3. If you do not receive replies, check the following:
 - Check to see that IP address of the access point 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 access point is listed as the default gateway.
 - Check to see that 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.
 - Check to see that 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 access point Internet connection \[router mode\]](#) on page 37).
 - 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:

- [Factory default settings](#)
- [Technical specifications](#)

Factory default settings

You can reset the access point to the factory default settings, which are shown in the following table.

For more information about resetting the access point to its factory settings, see [Factory default settings](#) on page 138.

Table 4. WAX204 access point factory default settings

Feature	Default Setting
Login to the local browser UI	
Login URL	www.routerlogin.net (which is the same as 192.168.1.1) If the access point functions in access point 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.
System modes	
Router mode	Enabled by default.
Access point mode	Disabled by default.
DHCP settings	
DHCP client	Enabled as a WAN client in router mode. (LAN client in access point mode.)
DHCP server	Enabled in router mode. (Disabled in access point mode.)
WiFi network	
WiFi communication	Enabled for Wireless 1 network Disabled for Wireless 2 and Wireless 3 networks
SSID names	In the following factory default SSIDs, XXXXXX represents the last six digits of the MAC address of the access point: Wireless 1 default network: NETGEARXXXXXX Wireless 2 optional network: NETGEARXXXXXX-2 Wireless 3 optional network: NETGEARXXXXXX-3
Security for the default Wireless 1 network	WPA2 Personal [AES] The default WiFi passphrase is a unique passphrase that is printed on the access point label.
Security for the optional Wireless 2 and Wireless 3 networks	WPA2 Personal [AES] The default WiFi passphrase is sharedsecret.

WiFi 6 AX1800 Dual Band Wireless Access Point WAX204

Table 4. WAX204 access point 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	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.
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
ODMFA	Disabled
Smart connect	Enabled
20/40 MHz coexistence	Enabled (applies to the 2.4 GHz radio only)
MU-MIMO	Enabled
Tx beamforming	Enabled
PMF	Enabled (applies to the 5 GHz radio only)
WPS	
WPS capability	Enabled
QoS	
QoS for Internet bandwidth	Disabled
802.11e WMM	Enabled
UPnP	Enabled

Table 4. WAX204 access point factory default settings (Continued)

Feature	Default Setting
Port forwarding and port triggering	Disabled in router mode (does not apply to access point mode)
Security	
Access control	Disabled
Block sites	None in router mode (does not apply to access point mode)
Block services	None in router mode (does not apply to access point mode)
Port Scan and DoS Protection	Enabled in router mode (does not apply to access point mode)
Respond to Ping on Internet Port	Disabled in router mode (does not apply to access point mode)
DMZ server	None (does not apply to access point mode)
IGMP proxying	Disabled (does not apply to access point mode)
NAT filtering	Secured (does not apply to access point mode)
SIP ALG	Enabled in router mode (does not apply to access point mode)

Technical specifications

The following table shows the technical specifications of the access point. For more information, see the product data sheet, which you can download by visiting netgear.com/support/download/.

Table 5. WAX204 access point specifications

Feature	Description
Power adapter	12V, 1.5A (18W) The plug is localized to the country of sale. Power consumption 16.2W maximum
Dimensions (L x W x H)	9.27 x 7.26 x 2.25 in. (236 x 184 x 57 mm)
Weight	1.08 lb (490 g)
Operating temperature	32°F to 104°F (0°C to 40°C)
Operating humidity	10 to 90% maximum relative humidity, noncondensing

WiFi 6 AX1800 Dual Band Wireless Access Point WAX204

Table 5. WAX204 access point specifications (Continued)

Feature	Description
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	Four 10/100/1000BASE-T Ethernet (RJ-45) ports with Auto Uplink (Auto MDI-X)
WiFi standards	IEEE 802.11ax IEEE 802.11ac specification IEEE 802.11n 2.0 specification 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 access point can support a maximum of 256 WiFi clients: Maximum number of 2.4 GHz WiFi clients: 128 Maximum number of 5 GHz WiFi clients: 128 In a WiFi network, the actual number of clients might be limited by the amount of WiFi traffic that is generated by each client.
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	CE (EN60950)

B

Positioning and Wall-Mounting

This appendix includes the following sections:

- [Position the access point](#)
- [Wall-mount the access point](#)

Position the access point

Before you install the access point, consider how you will position the access point.

The access point lets you access your network anywhere within the operating range of your WiFi network. However, the operating distance or range of your WiFi connection can vary significantly depending on the physical placement of your access point. For example, the thickness and number of walls the WiFi signal passes through can limit the range.

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

Position your access point according to the following guidelines:

- Place your access point near the center of the area where your computers and other devices operate and within line of sight to your WiFi devices.
- If you use a power adapter, make sure that the access point is within reach of an AC power outlet.
- Place the access point in an elevated location, minimizing the number walls and ceilings between the access point and your other devices.
- Place the access point away from electrical devices such as these:
 - Ceiling fans
 - Home security systems
 - Microwaves
 - Computers
 - Base of a cordless phone
 - 2.4 GHz and 5.8 GHz cordless phones
- Place the access point 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 you are using adjacent access points, consider to use different radio frequency channels to reduce interference (see [Change the channel for a radio](#) on page 193).

Wall-mount the access point

Wall-mounting holes are on the bottom of the access point. The distance between the holes is 4.125 in. (105 mm), center-to-center.

We recommend that you use M3 type screws, with a length of 0.75 inch (U.S.) or 20 mm (European).

To wall-mount the access point:

1. As an option, create a template:
 - a. Place a piece of white paper on the bottom of the access point, covering the wall-mounting holes.
 - b. Use a pencil to gently scratch around the mounting hole areas.
 - c. Tape the paper onto the wall where you want to mount the access point.
2. Drill holes in the wall where you want to mount the access point.

If you created a template, drill the mounting holes at the center of the template circles.

The distance between the holes in the wall must be 4.125 in. (105 mm).
3. Insert wall anchors in the holes.
4. Insert screws into the wall anchors, leaving 3/16 in (0.5 cm) of each screw exposed.
5. Align the access point's wall-mounting holes with the screws and mount the access point so that the antennas are at the top.
6. Slide down the access point into lock position.